Release Notes for the Catalyst 2900 Series XL and Catalyst 3500 Series XL Switches, Cisco IOS Release 12.0(5)WC3b

March 2002

Cisco IOS Release 12.0(5)WC3b runs on the Catalyst 2900 series XL and Catalyst 3500 series XL switches with 8-MB CPU DRAM.

Note This release is *not* for the Catalyst 2900 LRE XL switches. Do not install this release on the Long-Reach Ethernet (LRE) switches. For information about these switches, refer to Cisco IOS Release 12.0(5)WC2 and Cisco IOS Release 12.0(5)WC2b.

Note This release is *not* for the Catalyst 2900 XL switches with 4-MB CPU DRAM. For information about these switches, refer to Cisco IOS Release 11.2(8.9)SA6 or earlier.

These release notes include important information about this release and any limitations, restrictions, and caveats that apply to it. To verify that these are the correct release notes for your switch:

- If you are installing a new switch, refer to the IOS release label on the rear panel of your switch.
- If your switch is on and running, use the **show version** user EXEC command. See the "Determining the Switch Software Version" section on page 28.
- If you are upgrading to a new release, refer to the software upgrade filename for the IOS version. Before upgrading your switch to this release, read the "Upgrading the Switch Software" section on page 25.

You can download the switch software from these sites:

- http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml
(for registered Cisco.com users with a login password)
- http://www.cisco.com/public/sw-center/sw-lan.shtml
(for nonregistered Cisco.com users)

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

This 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 releases become available, they will be posted to Cisco.com in the Cisco IOS software area.

Contents

This document has the following sections:

Hardware Requirements

Note Catalyst 2900 XL 4-MB switches do not support this release. The 4-MB models are WS-C2908-XL, WS-C2916M-XL, WS-C2924C-XL, and WS-C2924-XL. These switches can only be upgraded up to Release 11.2(8.6)SA6. To be cluster members, these switches must run Release 11.2(8.x)SA6 original edition software. To determine the switch DRAM size, enter the **show version** user EXEC command.

This release supports the 8-MB Catalyst 2900 XL switches (see Table 1) and Catalyst 3500 XL switches (see Table 2).

Table 1 Catalyst 2900 XL Switches with 8-MB CPU DRAM

Switch	Description
Catalyst 2912MF XL	12 100BASE-FX ports and 2 high-speed expansion slots
Catalyst 2912 XL	12 autosensing 10/100 ports
Catalyst 2924M XL	24 autosensing 10/100 ports and 2 high-speed expansion slots
Catalyst 2924M DC XL	24 autosensing 10/100 ports and 2 high-speed expansion slots (DC power)

Table 1 Catalyst 2900 XL Switches with 8-MB CPU DRAM (continued)

Switch	Description
Catalyst 2924 XL	24 autosensing 10/100 ports
Catalyst 2924C XL	22 autosensing 10/100 ports and 2 100BASE-FX ports

Table 2 Catalyst 3500 XL Switches

Switch	Description
Catalyst 3508G XL	8 Gigabit module slots
Catalyst 3512 XL	12 autosensing 10/100 ports and 2 Gigabit module slots
Catalyst 3524 XL	24 autosensing 10/100 ports and 2 Gigabit module slots
Catalyst 3524-PWR XL	24 autosensing 10/100 inline-power ports and 2 Gigabit module slots
Catalyst 3548 XL	48 autosensing 10/100 ports and 2 Gigabit module slots

Software Requirements

This section describes the requirements for the system and for the Cluster Management Suite (CMS) software.

System Requirements

These operating systems are supported for CMS management:

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

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 3 lists the recommended platforms for using CMS.

Table 3 Recommended Minimum 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	65,536	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 and Java Plug-In Requirements

When starting a CMS session, the switch verifies the browser version to ensure that the browser is supported. If the browser is not supported, an error message appears, and the session does not start. Table 4 lists the browsers supported by CMS.

CMS requires the Java plug-ins described in the "Installing the Required Plug-In" section on page 23.

Table 4 Browser Requirements

Operating System	Netscape Communicator[1]	Microsoft Internet Explorer[2]
Windows 95	4.61, 4.7	4.01a or 5.0
Windows 98	4.61, 4.7	4.01a or 5.0
Windows NT 4.0	4.61, 4.7	4.01a or 5.0
Windows 2000	4.61, 4.7	4.01a or 5.0
Solaris 2.5.1 or higher	4.61, 4.7	–

1. Netscape Communicator version 4.60 and 6.0 are *not* supported.
2. Microsoft Internet Explorer is *not* supported on Solaris 2.5.1 or higher.

Note In CMS, Internet Explorer versions 4.01 and 5.0 do not display edge devices that are not connected to the command switch. Other functionality is similar to that of Netscape Communicator.

Note If you receive an Internet Explorer error message that the page might not display correctly because your security settings prohibit the ActiveX controls, your security settings are set too high. To lower security settings, go to **Tools** > **Internet Options**, and select the **Security** tab. Select the indicated **Zone,** and move the **Security Level for this Zone** slider from **High** to **Medium** (the default).

To access CMS, follow the procedures in the "Initial Switch Configuration" section on page 20.

Cluster Requirements and Guidelines

This section describes the hardware and software requirements for clustering Catalyst desktop switches.

Catalyst 2900 XL and Catalyst 3500 XL Switches

Some versions of IOS software do not support clustering, and other versions do not support some of the features in this release. To ensure that all cluster switches are using the same software level, we recommend that you upgrade all cluster switches to the software release that supports the features that you want.

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 Release 11.2(8)SA6, the windows and functionality can be different from a switch running Release 12.0(5)XU or later.

Table 5 describes the Catalyst 2900 XL and Catalyst 3500 XL switches supported by this release and shows which switches can be command switches. All switches can function as standalone devices.

All Catalyst 2900 XL and Catalyst 3500 XL switches running Release 12.0(5.3)WC(1) and later are cluster-capable. All Catalyst 2900 XL modules are supported in cluster configurations.

We recommend that either the command switch has the latest software version installed if there switches in the cluster with older software versions or that all switches in the same platform be upgraded to the latest software version.

Note Release 12.0(5)WC3b is *not* for the Catalyst 2900 LRE XL switches. For information about upgrading the Catalyst 2900 LRE XL switches, refer to Release 12.0(5)WC2 and Release 12.0(5)WC2..

Table 5 Catalyst 2900 XL and Catalyst 3500 XL Switches as Cluster Members

Switch	Release 12.0(5.3)WC(1) or higher?	Command Capable?	Member Capable?
Catalyst 2900 XL (4 MB of DRAM)[1]	No	No	Yes
Catalyst 2900 XL (8 MB of DRAM)	Yes	Yes	Yes
Catalyst 3500 XL	Yes	Yes	Yes

[1] These switches can act as cluster members if they are running Release 11.2(8.x)SA6 original edition software. They can interoperate with this software release, but they cannot be upgraded to it.

Catalyst 3550 Switches

Catalyst 3550 switches running Release 12.0(4)EA1 or higher can be command and member switches. For more information, refer to the documentation for the Catalyst 3550 switches.

Catalyst 2950 Switches

Catalyst 2950 switches running Release 12.0(5)WC(1) or higher can be command and member switches. For more information, refer to the documentation for the Catalyst 2950 switches.

Catalyst 1900 and Catalyst 2820 Switches

Table 6 lists the Catalyst 1900 and Catalyst 2820 switches and the minimum software release that they require to be cluster members. All Catalyst 2820 modules are supported in cluster configurations. For more information, refer to the documentation for the Catalyst 1900 and Catalyst 2820 switches.

Table 6 Catalyst 1900 and Catalyst 2820 Switches as Cluster Members

Switch	Release 9.00 (-EN)	Member Capable?	Command Capable?
Catalyst 1900	Yes	Yes	No
Catalyst 2820	Yes	Yes	No

Minimum Cisco IOS Release for Major Features

Table 7 lists the minimum software release required to support the major features of the Catalyst 2900 XL and Catalyst 3500 XL switches.

Table 7 Catalyst 2900 XL and Catalyst 3500 XL Features and the Minimum Cisco IOS Release Required

Feature	Minimum Release Required
Enhanced web-based switch management (CMS)	12.0(5)WC3
MAC Address Notification	Release 12.0(5)WC3
Internet Group Management Protocol (IGMP) Filtering	Release 12.0(5)WC3
Extended cluster member compatibility with the Catalyst 2950 and Catalyst 3550 switches	Release 12.0(5)WC(1)
Multicast VLAN Registration (MVR)	Release 12.0(5)WC(1)
Cross-stack UplinkFast	Release 12.0(5)XW
Dynamic Host Configuration Protocol (DHCP)-based autoconfiguration	Release 12.0(5)XW
Support for the single-port 1000BASE-T Gigabit Interface Converter (GBIC) (WS-G5482)	Release 12.0(5)XW
WS-C3524-PWR XL switch with 10/100 inline-power ports	Release 12.0(5)XU
WS-C2924M-XL-EN-DC switch with DC power connector	Release 12.0(5)XU
WS-X2932-XL Catalyst 2900 XL 1-port 1000BASE-T module	Release 12.0(5)XU
Hot Standby Router Protocol (HSRP) for clustering	Release 12.0(5)XU
Extended discovery of cluster candidates up to 7 hops from the command switch	Release 12.0(5)XU
Support for up to 16 switches in a cluster	Release 12.0(5)XU
VLAN Trunking Protocol (VTP) pruning	Release 12.0(5)XU
Change management Virtual LAN (VLAN) for a cluster	Release 12.0(5)XU
Private VLAN edge support	Release 12.0(5)XU
UniDirectional Link Detection (UDLD) for detecting unidirectional links	Release 12.0(5)XU
Extended cluster member functionality for Catalyst 1900 and 2820 switches	Release 12.0(5)XP
Remote monitoring (RMON) support through the command-line interface (CLI) or Simple Network Management Protocol (SNMP)	Release 12.0(5)XP
Change management VLAN	Release 12.0(5)XP
Quality of service (QoS) based on IEEE 802.1P class of service (CoS) values	Release 12.0(5)XP
WS-C3548-XL switch with 48 10/100 ports	Release 12.0(5)XP
WS-X2931-XL Catalyst GigaStack GBIC	Release 12.0(5)XP
Catalyst 3500 series XL switches (except WS-C3548-XL)	Release 11.2(8)SA6
Cluster management	Release 11.2(8)SA6
Terminal Access Control Access System Plus (TACACS+)	Release 11.2(8)SA6 (Enterprise Edition Software)
Network Time Protocol (NTP)	Release 11.2(8)SA6

Table 7 Catalyst 2900 XL and Catalyst 3500 XL Features and the Minimum Cisco IOS Release Required

Feature	Minimum Release Required
Spanning Tree Protocol (STP) UplinkFast	Release 11.2(8)SA6 (Enterprise Edition Software)
250 VLANs (some models: see the "Limitations and Restrictions" section on page 9)	Release 11.2(8)SA6
Catalyst 2900 series XL 1000BASE-X modules	Release 11.2(8)SA5
Catalyst 2900 series XL asynchronous transmission mode (ATM) modules	Release 11.2(8)SA5
IEEE 802.1Q trunking	Release 11.2(8)SA5 (Enterprise Edition Software)
Inter-Switch Link (ISL) trunking	Release 11.2(8)SA4 (Enterprise Edition Software)
VLAN Membership Policy Server (VMPS)	Release 11.2(8)SA4 (Enterprise Edition Software)
8192 media access control (MAC) addresses on modular switches	Release 11.2(8)SA4
Switch Network View stack management	Release 11.2(8)SA3
Web-based switch management	Release 11.2(8)SA
Fast EtherChannel port groups	Release 11.2(8)SA

New Software Features in this Release

This section describes the new software features in this release.

IGMP Filtering

IGMP filtering works with the MVR feature so that you can configure profiles of IP multicast groups. IGMP filters are associated with each physical switch port. These filters are applied to all VLANs associated with the physical port.

MAC Address Notification

You can use MAC address notification to track users coming to and going from your network. Whenever a new MAC address is learned or an old MAC address is removed from the switch, an SNMP notification (trap) is generated. If you have many users coming into and going from the network, you can set a trap interval time so that traps can be bundled and sent at regular intervals.

The MAC notification history table stores the MAC address activity for each hardware port for which the trap is enabled. MAC address notifications are generated for dynamic and secure MAC addresses. Events are not generated for self addresses, multicast addresses, or other static addresses.

CMS Enhancements

The CMS software has several enhancements:

- **Access modes**

  CMS now provides two levels of access to the configuration options: read-write and read-only. Read-write access requires privilege level 15. Read-only access requires privilege level from 1 to 14. Privilege level 0 denies access to CMS.

- **Guide and expert modes**

  CMS now provides two modes that control how the VLAN and voice VLAN configuration options are presented. Guide mode takes you step-by-step through these options. Expert mode displays the entire configuration window and lets you decide how to complete a task.

- **Voice VLAN wizard**

  CMS provides a wizard to help you configure a port to forward voice traffic with an 802.1P priority and configure the port as an 802.1Q trunk and as a member of the voice VLAN.

- **Consistent menu bar**, **toolbar, and popup menus**

  There are several changes to the CMS menus:

  - CMS now has a single menu bar and a toolbar for configuring and monitoring a single switch or a switch cluster. The menu bar and toolbar does not change if you have the Front Panel view, the Topology view, or neither view displayed.
  - The menu-bar options are now in these groups: CMS, Administration, Cluster, Device, Port, VLAN, Reports, View, Window, and Help.
  - The menu bar of a Catalyst 2900 XL or Catalyst 3500 XL command switch displays all Layer 2 options available from the cluster, including options from member switches from other cluster-capable switch platforms, such as the Catalyst 2950 and Catalyst 3550 switches. It does not display the Catalyst 2950 Layer 2+ options or the Catalyst 3550 Layer 3 options.
  - Popup menu options appear only if they are supported by all of the selected objects.

- **Views of your switch cluster**

  As before, CMS provides a Front Panel view of a switch cluster and a Topology view of a switch cluster and the devices attached to it. You can now display both views at the same time, display either view, or display neither view. You do not need to display a view to use the menu bar. For configuring and monitoring a standalone switch, CMS continues to provide *Device Manager*, previously referred to as *Switch Manager.*

- **Front Panel view enhancements**

  You can press the left mouse button and drag your mouse across the ports that you want to select. You can highlight the ports and find out their VLAN membership modes. The cluster tree can display icons for Layer 2, Layer 3, and LRE standby-command switches.

- **Topology view enhancements**

  You can press the left mouse button and drag your mouse across the devices and links that you want to select. You have more options for controlling the type of information displayed in the Topology view. When you drag your mouse over a yellow or red device icon, a tool tip displays a status message. This view displays device icons for connected Cisco LRE customer premises equipment (CPE) devices, Cisco access points, Cisco IP phones, Cisco Discovery Protocol (CDP)-capable hubs, and routers. This view displays link icons for routed and LRE links.

- **Dialog enhancements**

  CMS provides change notification by adding a green border around a field or table cell that has an unsaved change. CMS also provides error checking by adding a red border around a field where you entered invalid data. An error message also displays in the window status bar.

  When you drag your mouse over a table heading, a tool tip displays the complete heading. On some table columns, you can sort information in ascending or descending order. Editable table cells are shown with a pencil icon. Links to the Internet are shown with a globe icon.

- **Online help links**

  Links in the online help can display configuration windows, related help topics, and related information from Cisco.com.

- **Printing**

  You can print reports, graphs, and online help topics.

For more information about CMS enhancements, refer to the "What's New" section in the online help on your switch.

Limitations and Restrictions

You should 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.

- All Catalyst 3500 series XL and most Catalyst 2900 series XL switches support a total of 250 VLANs and 64 spanning-tree instances. The Catalyst 2912 XL, 2924 XL, and 2924C XL switches support a total of 64 VLANs and 64 spanning-tree instances. Regardless of the switch model, only 64 spanning-tree instances are supported.
- When connecting to the Catalyst 3524-PWR XL 10/100 inline-power ports, observe this caution:

⚠ **Caution** A Catalyst 3524-PWR XL 10/100 port needs up to 10 seconds to initially detect, power, and link to a Cisco IP Phone. If you disconnect the Cisco IP Phone before link has been established, you must wait 10 seconds before connecting another network device (other than another Cisco IP phone) to that switch port. Failing to do so can damage that network device.

- The Cisco RPS 300 Redundant Power System (RPS) supports the Catalyst 3524-PWR XL switch. When the RPS LED on the switch is amber, the RPS is connected but down. However, this might merely mean that the RPS is in standby mode. Press **Standby/Active** on the RPS to put it into active mode. Refer to the *RPS 300 Hardware Installation Guide* for more information. You can view the RPS status by using the **show rps** privileged EXEC command.
- You can connect the switch to a PC by using the switch console port and the supplied rollover cable and the DB-9 adapter. 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=) with this RJ-45-to-DB-25 female DTE adapter from Cisco.
- Certain combinations of port features create configuration conflicts. Refer to the "Avoiding Configuration Conflicts" section in the "Troubleshooting" chapter of the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide* for a table that defines these conflicts.

- When you add a VTP client, follow this caution and procedure:

Caution Before adding a VTP client to a VTP domain, always verify that its VTP configuration revision number is *lower* than the configuration revision number of the other switches in the VTP domain. If necessary, reset the switch configuration revision number to 0. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. If you add a switch that has a revision number higher than the revision number in the VTP domain, it can erase all VLAN information from the VTP server and VTP domain.

Beginning in user EXEC mode, follow these steps to verify and reset the VTP configuration revision number on a switch *before* adding it to a VTP domain.

	Command	Purpose
Step 1	**show vtp status**	Check the VTP configuration revision number. If the number is 0, add the switch to the VTP domain. If the number is greater than 0, follow these steps: **a.** Write down the domain name. **b.** Write down the configuration revision number. **c.** Continue with the next steps to reset the configuration revision number on the switch.
Step 2	**enable**	Enter privileged EXEC mode.
Step 3	**vlan database**	Enter VLAN database mode.
Step 4	**vtp domain** *domain-name*	Change the domain name from the original one displayed in Step 1 to a new name.
Step 5	**exit**	The VLAN information on the switch is updated and the configuration revision number is reset to 0. You return to privileged EXEC mode.
Step 6	**show vtp status**	Verify that the configuration revision number has been reset to 0.
Step 7	**vlan database**	Enter VLAN database mode.
Step 8	**vtp domain** *domain-name*	Enter the original domain name on the switch.
Step 9	**exit**	The VLAN information on the switch is updated, and you return to privileged EXEC mode.
Step 10	**show vtp status**	(Optional) Verify that the domain name is the same as in Step 1 and that the configuration revision number is 0.

After resetting the configuration revision number, add the switch to the VTP domain.

Note You can use the **vtp transparent** vlan database command to disable VTP on the switch and then change its VLAN information without affecting the other switches in the VTP domain. For more information about using vtp transparent mode, refer to the switch software configuration guide.

- 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. Do not enter commas when also entering multiple DNS names in the Device Configuration tab (**Administration** > **IP Addresses**) in CMS.

- The range of seconds for the **span-tree max-age** global configuration command is now 6 to 200 seconds. If you had used this command in Release 11.2(8)SA6 or earlier to set a value greater than this range and now upgrade your software to Release 11.2(8.1)SA6 or later, the switch sets this value to the default: 20 seconds for IEEE STP and 10 seconds for IBM STP.
- When using the SPAN feature, the monitoring port receives copies of sent 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.
- 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 2900 series XL switches require Release 11.2(8)SA4 or later and RME version 2.1 or 2.2.
  - Catalyst 3500 series XL switches require Release 11.2(8.1)SA6 or later and RME version 2.2.

Caveats

This section describes open caveats and possible unexpected activity in Release 12.0(5)WC3b:

- "Open IOS Caveats" section on page 11
- "Open Cluster Configuration Caveats" section on page 13
- "Open CMS Caveats" section on page 14

Note Release 12.0(5)WC3b is for non-LRE switches only. For information about open and resolved caveats on LRE switches, refer to the *Release Notes for the Catalyst 2900 Series XL and Catalyst 3500 Series XL Switches, Cisco IOS Release 12.0(5)WC2* and the *Release Notes for the Catalyst 2900 Series XL and Catalyst 3500 Series XL Switches, Cisco IOS Release 12.0(5)WC2b*, on Cisco.com.

Open IOS Caveats

This section describes the severity 3 IOS configuration caveats in Release 12.0(5)WC3b:

- CSCdw54637

  Do not use a Category 3 cable to connect a wireless access point to a Catalyst 3500-PWR XL switch.

  The workaround is to use a Category 5 cable.

- CSCdu41214

  When a source port is set at a higher speed than an egress (outgoing) port in a multicast, the transmit buffers are held in use and become full before the packets can be sent out of the egress ports. This causes the source port to run out of buffer space for the remaining traffic it needs to send, and packets are eventually dropped from the source port, causing an `Input ignored multicast` error.

  The problem is caused by oversubscription on the egress ports. If multicast traffic is being sent out on multiple ports, the lowest-speed egress port limits the rate at which frames are dropped at the ingress port.

  The workaround is to upgrade to Release 12.0(5)WC3b. Software modifications in this release alleviate the problem in these ways:

  - The shared memory allocation can be modified so that uplink ports have a larger share of the available switch buffers, and the downlink ports have fewer buffers. This can be done by using the following hidden CLI:
  - Use the **switchport uplink** interface configuration command to specify that the interface is an uplink port. All ports not configured as uplink will be treated as downlink ports.
  - Use the **switchbuffers uplink** global command to enable the buffer redistribution.

  You have to reset the switch before these commands take effect.

- CSCdt53253

  If a port on a switch is configured as a dot1q trunk, and the switch is receiving dot1q frames that have the cfi bit set in the dot1q header, the switch drops these frames. Depending on the number of frames that are received with this bit set, connectivity to the switch can be lost.

  The workaround is to prevent dot1q frames with the cfi bit set from being sent to the switch.

- CSCdt83042

  High rates of traffic sent to a MAC address that is used by an MVR multicast group and received on an MVR receiver port can cause excessive CPU utilization rates and consume enough resources on the switch CPU so that normal spanning-tree processing is interrupted. This can prevent spanning-tree loops from being broken.

  The workaround is to enable multicast storm control on all MVR receiver ports.

- CSCdt84558

  In MVR, when changing the configuration of a port from receiver to source, the port does not start receiving multicast traffic.

  The workaround is to save the configuration and reboot the switch to restore proper traffic flooding.

- CSCdt83212

  MVR does not initialize on a switch if that switch is a cluster member and does not have an IP address.

  The workaround is to set an IP address on the switch.

- CSCdt48569

  If you configure VLAN1 as the management VLAN and configure it as administratively down, VLAN1 correctly appears as *administratively down* in the output of the **show ip interface brief** privileged EXEC command. If you configure any VLAN other than VLAN1 as the management VLAN and configure VLAN1 as administratively down, VLAN1 incorrectly appears as *up* in the output of the **show ip interface brief** command.

  There is no workaround.

- CSCdt18106

  If you perform an **snmpwalk** SNMP operation on the CISCO-IP-STAT-MIB, continuous loops occur through the first element in the MIB tree when IP accounting precedence is configured for a VLAN interface other than VLAN1. The CISCO-IP-STAT-MIB is not supported.

  The workaround is to perform individual **snmpget** SNMP requests to retrieve data.

- CSCds84479

  When you connect two switches by using a GigaStack Gigabit Interface Converter (GBIC) module and you manually set the duplex mode to full duplex or to autonegotiate on both ends, the link sometimes does not stabilize.

  The workaround is to remove and reinsert one of the GBICs.

- CSCds58369

  If the switch is 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.

- CSCdm24487

  The serial port shares the same status bit for hardware flow control and for *ready.*

  The workaround is to not use flow control on the console port.

- CSCdp85954

  Root guard is inconsistent when configured on a port that is in the spanning-tree blocked state when configured.

  There is no workaround.

Open Cluster Configuration Caveats

This section describes the severity 3 cluster configuration caveat in Release 12.0(5)WC3b:

- 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.

Open CMS Caveats

This section describes the severity 3 CMS configuration caveats in Release 12.0(5)WC3b:

- CSCdt42854

  Running a CMS link graph for more than 24 hours can cause an OutOfMemoryException error.

  There is no workaround.

- CSCdt47877

  When running CMS with Windows 98 and JRE plug-in 1.3, the tool tip that shows the exact coordinates of a point on a graph is so small that it is unreadable.

  There is no workaround.

- CSCdt58668

  Checking the Logarithmic Scaling check box in the Link Graph window has no effect if the Total Bytes, Total Packets, or Total Errors options are plotted.

  There is no workaround.

- CSCdp67822

  CMS 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.

- CSCdp82224

  The CMS Time Management 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 Current Time and Set Daylight Saving Time tabs.

  The workaround is to 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.

- 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.

Resolved Caveats

This section describes caveats that have been resolved:

- "Resolved IOS Caveats in Release 12.0(5)WC3b" section on page 15
- "Resolved CMS Caveat in Release 12.0(5)WC3b" section on page 15
- "Resolved IOS Caveats in Release 12.0(5)WC3" section on page 15
- "Resolved CMS Caveats in Release 12.0(5)WC3" section on page 17
- "Resolved IOS Caveats in Release 12.0(5)WC2" section on page 17

Resolved IOS Caveats in Release 12.0(5)WC3b

These configuration caveats were resolved in Release 12.0(5)WC3b:

- CSCdv00304

  When a spanning tree reconverges and VTP is pruning enabled, a Catalyst 2900 XL or 3500 XL switch no longer stops forwarding traffic for a single VLAN.

- CSCdw44304

  When a corrupted STP packet has a maximum age between 0 and 1 second, the switch no longer ages out the Bridge Protocol Data Units (BDPU). This causes a new spanning-tree root to be elected.

- CSCdw65903

  An error no longer occurs with management protocol processing. Use this URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

Resolved CMS Caveat in Release 12.0(5)WC3b

This CMS caveat was resolved in Release 12.0(5)WC3b:

- CSCdw72081

  A command switch no longer fails when it receives SNMP packets that have invalid variable bindings.

Resolved IOS Caveats in Release 12.0(5)WC3

These configuration caveats were resolved in Release 12.0(5)WC3:

- CSCdt83966

  When a receiver VLAN is shut down locally, suspended throughout the VTP domain, or deleted from the VTP database, the **show mvr**, **show mvr int**, and **show mvr member** privileged EXEC commands now show that MVR and its members are disabled. The receiver ports remain as MVR ports, and forwarding of MVR traffic resumes after the VLAN is restored and spanning tree has transitioned to a forwarding state.

- CSCdu10578

  If an IGMP general query is received on a port that is assigned to a VLAN, but that port is not the receiver port VLAN, the query no longer interrupts the multicast streams controlled by MVR in the multicast VLAN and receiver port.

- CSCdw00322

  A switch no longer continues allocating memory for a process that has already been terminated.

  Note Memory that is retained for a process that has already been terminated is often referred to as *dead* memory.

- CSCdu10578

  An IGMP general query received on a port that is assigned to a VLAN no longer interrupts the multicast streams controlled by MVR in the multicast VLAN and receiver port VLAN.

Note The VLAN to which the port is assigned must not be a multicast VLAN or receiver port VLAN for this situation to have occurred.

- CSCdv02485

  Topology changes no longer cause a software forced-reload on a Catalyst 3524 XL switch.

  Note This condition had occurred with heavy, high-priority traffic on a switch.

- CSCdv62652

  It is no longer necessary to clear the MAC address table on a Catalyst 3548 XL switch to be able to ping through the Fast EthernetChannel (FEC) ports on that switch after shutting down a port belonging to the FEC. (See also CSCdv58536.)

- CSCdv58536

  Executing a **shutdown** interface command on a FEC port does not shut down other FEC ports on the same switch.

- CSCds45300

  A Catalyst 2900 XL or Catalyst 3500 XL switch now responds to V2 MIB objects for 64-bit counters.

- CSCdv57676

  Extra characters are no longer added to the login prompt when you log in by using Telnet.

- CSCdu73533

  After you replicate the AAA configuration to a cluster member switch, the `tacacs server host` line is no longer lost after the member switches are rebooted.

- CSCdv53949

  It is no longer necessary to reload the switch for the **snmp-server queue-length** global configuration command to take effect.

- CSCdv56078

  Sending a large amount of CDP neighbor announcements no longer consumes all of a router's available memory.

- CSCdv56187

  The output of the **debug ethernet-controller addresses** privileged EXEC command now shows the physical port numbers of the switch instead of the internal STP port numbers.

- CSCdv63206

  A Cisco router no longer overwrites a MAC address for one of its interfaces stored in the ARP table with an external MAC address received from an ARP packet.

- CSCdw02848

  1000BASE-X GBICs are no longer reported as `unknown type` in the output of the **show interface status** privileged EXEC command.

- CSCdv60082

  When an access port receives misconfigured ISL frames that have the Type and Priority bits set, the frames are now dropped instead of being broadcast to other ports.

Resolved CMS Caveats in Release 12.0(5)WC3

These CMS caveats were resolved in Release 12.0(5)WC3:

- CSCdt82729

  If you launch the **VMPS Configuration** window from the device pop-up menu in VSM, it no longer displays incorrect information.

- CSCdv21358

  The CMS software now accepts device passwords that contain these characters: ‘, “, ., /, \, <, >, [,], {, }, #, %, |, ^, and ~.

- CSCds86420

  Two identical items for the same switch are no longer listed if you select a switch in the tree by selecting **Administration** > **Console Baud Rate**, clicking **cancel,** and selecting **Administration** > **Console Baud Rate** again.

- CSCdt49955

  When viewing CMS dialogue windows, an exception error no longer occurs when you press the Shift key on the keyboard at the same time as you select the **Add** or **Remove** CMS buttons.

Resolved IOS Caveats in Release 12.0(5)WC2

These configuration caveats were resolved in Release 12.0(5)WC2:

- CSCdv66959

  It is no longer necessary to set the maximum number of addresses on a port to a value greater than 1 to prevent a switch from shutting down a secure port if a permitted source address is detected on the port.

- 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.

- CSCdt04001

  When you change the privilege level for an interface on a Catalyst 2900 XL or Catalyst 3500 XL switch, 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.

- CSCdt57171

  When an IP phone is connected to a Fast Ethernet port that is set to 10 Mbps, half duplex on a Catalyst 3524 XL-PWR switch running Cisco IOS 12.0(5.2)XU and the switch is powered cycled, the IP phone now powers up correctly.

- CSCdt57346

  When you use the **show rmon history** EXEC command, the value for the collision is now unique for each sample.

- CSCdt68204

  Least Recently Used (LRU) port election now works properly on a Catalyst 3500 XL switch. When forward error correction (FEC) is broken, FEC now receives ping messages and sends back responses from the correct LRU port.

- 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.

- CSCdu24150

  When FastEtherChannel is configured, a Catalyst 2924 XL switch can now transmit broadcasts after changing the default port from FE0/1 to any other port.

- CSCdu36469

  If you loop a fiber cable to itself on a Catalyst 2924 XL switch, the interface counters now match the **show controller ethernet** <*interface*> privileged EXEC command.

- 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.

- CSCdu56591

  A Catalyst 2924 XL switch port configured for Port Fast can now send out the cold-start trap at reload when the trap is captured from that port.

- CSCdu58304

  When the root bridge is restarted on a Catalyst 3500 XL switch and the topology is stable, removing the link between hubs no longer generates STP topology change traps from both the root bridge and the designated bridge.

- 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.

- CSCdu68001

  When chassisSlots of the old-cisco-chassis-mib is queried on a Catalyst 3524-PWR XL switch by using either the MIB browser or the CLI interface, it returns a “1.”

- 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.

- CSCdv48912

  When using cross-stack UplinkFast, temporary spanning-tree loops no longer occur.

Important Notes

This section describes important information related to this release.

The MVR threshold feature was removed in Release 12.0(5.3)WC(1). Use the port multicast storm control feature instead of the MVR threshold feature to limit rates.

When you are configuring a cascaded stack of Catalyst 3500 XL switches by using a GigaStack GBIC and want to include more than one VLAN in the stack, be sure to configure all the GigaStack GBIC interfaces as trunk ports by using the **switchport mode trunk** interface configuration command and to use the same encapsulation method by using the **switchport encapsulation** {**isl** | **dot1q**} interface configuration command. For more information about these commands, refer to the command reference publication for your switch.

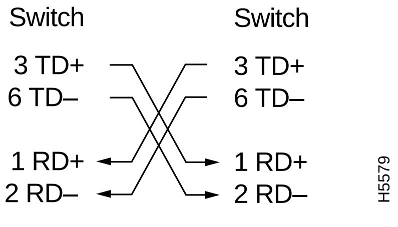
Documentation Notes

This section lists corrections to the hardware and software documentation.

Note Release 12.0(5)WC3 is for non-LRE switches only. For documentation notes about the Catalyst 2900 LRE XL switches, refer to 12.0(5)WC2.

- The following information is now only in the release notes and is no longer in the manuals:
  - Hardware, software, and cluster requirements.
  - Procedures for initial switch configuration.
  - Using the setup program. See the "Using the Setup Program" section on page 20.
  - Installing browser plug-ins. See the "Installing the Required Plug-In" section on page 23.
  - Accessing CMS. See the "Displaying the CMS Access Page" section on page 24.
  - Procedures for upgrading the switch software are now only in the release notes. See the "Guidelines for Upgrading Switch Software" section on page 26.
- The pinouts of a crossover cable shown in the *Catalyst 2900 Series XL Hardware Installation Guide* are incorrect. Figure 1 shows the correct pinouts.

Figure 1 Crossover Cable Pinouts



- The Catalyst 3508 XL switch (WS-C3508G-XL) now ships with a power rating of 1.5A/0.75A. The back-panel illustration of the Catalyst 3508 XL switch in the *Catalyst 3500 Series XL Hardware Installation Guide* shows an outdated power rating of 1A/0.5A.

Initial Switch Configuration

This section provides these procedures:

- "Using the Setup Program" section on page 20
- "Installing the Required Plug-In" section on page 23
- "Displaying the CMS Access Page" section on page 24

This section assumes that you have already installed the switch and connected devices to it, as described in the switch hardware installation 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.

Note If the switch will be a cluster member, you do not always need to assign IP information or a password, as the switch will be managed through the IP address of the command switch. If you are configuring a command switch or standalone switch, you need to assign IP information. Refer to the switch software configuration guide for more information.

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.

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 that 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 "Cable and Connector Specifications" appendix in the *Catalyst 2900 Series XL Hardware Installation Guide* and the *Catalyst 3500 Series XL Hardware Installation Guide*.

At any point you can enter a question mark for help. Use Ctrl-C to stop the configuration dialog at any prompt. The 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 172.20.153.01
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 use 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 23 and the "Displaying the CMS Access Page" section on page 24.)

- Command-line interface (CLI) (Refer to the switch 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.

Installing the Required Plug-In

A Java plug-in is required for the browser to access CMS. Download and install the plug-in before you start CMS. Each platform, Windows and Solaris, supports three plug-in versions. For information on the supported plug-ins, see the "Windows 95, Windows 98, and Windows NT 4.0, and Windows 2000 Users" section on page 23 and the "Solaris Platforms" section on page 24.

You can download the recommended plug-ins from this URL:

http://www.cisco.com/pcgi-bin/tablebuild.pl/java

Note Uninstall older versions of Java plug-ins before installing the Java plug-in.

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 these settings:

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

Note 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 taskbar, right-click the Virus Shield icon, and in the Quick Enable menu, disable the options by deselecting **Internet Filter** or **Download Scan**.

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

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

- Java plug-in 1.3.1
- Java plug-in 1.3.0
- Java plug-in 1.2.2_05

You can download these plug-ins from this URL:

http://www.cisco.com/pcgi-bin/tablebuild.pl/java

Note If you start CMS without having installed the required Java plug-in, the browser automatically detects this. If you are using a supported Internet Explorer browser, it automatically downloads and installs the Java plug-in 1.3.1 (default). If you are using a supported Netscape browser, the browser displays a Cisco.com 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.

Solaris Platforms

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 1.3.1.

- Java plug-in 1.3.1
- Java plug-in 1.3.0
- Java plug-in 1.2.2_07

If you have a SmartNet contract, you can download these plug-ins and instructions from this URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/java

To install the Java plug-in, follow the instructions in the README_FIRST.txt file.

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 Java plug-in JRE 1.3.1.

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

Displaying the CMS Access Page

After the browser is configured, display the CMS 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 switch software configuration guide.

Note If no username is configured on the switch, leave the username field blank.

Step 3 Click **Cluster Management Suite** to display the appropriate CMS application.

Upgrading the Switch Software

Note Release 12.0(5)WC3 is *not* for the Catalyst 2900 LRE XL switches. For information about upgrading the Catalyst 2900 LRE XL switches, refer to Release 12.0(5)WC2.

This section provides topics about upgrading the switch software:

- "Guidelines for Upgrading Switch Software" section on page 26
- "Overview of the Switch Upgrade Process" section on page 27
- "Determining the Switch Software Version" section on page 28
- "Which Software Files to Download from Cisco.com" section on page 28
- "Downloading the New Software and TFTP Server Application to Your Management Station" section on page 29
- "Copying the Current Startup Configuration from the Switch to a PC or Server" section on page 30
- "Using CMS to Upgrade a Specific Switch" section on page 30
- "Using CMS to Upgrade One or More Switches" section on page 32
- "Using the CLI to Upgrade an 8-MB Catalyst 2900 XL Switch" section on page 33
- "Using the CLI to Upgrade a Catalyst 3500 XL Switch" section on page 37
- "Using the CLI to Upgrade Member Switches" section on page 39

Note Before upgrading your switch to Release 12.0(5)WC3, read the "Guidelines for Upgrading Switch Software" section on page 26 for important information.

Guidelines for Upgrading Switch Software

When upgrading the switch software, follow these rules:

- You cannot install Release 11.2(8.x)SA6 or earlier on Catalyst 2900 XL switches with 4 MB of DRAM and Catalyst 3500 XL switches with 8 MB of DRAM.

  Similarly, you cannot upgrade Catalyst 2900 XL switches with 4 MB of DRAM to an 8-MB image. The 4-MB models are WS-C2908-XL, WS-C2916M-XL, WS-C2924C-XL, and WS-C2924-XL. In addition, these switches must run Release 11.2(8.x)SA6 to be cluster members. To determine the switch DRAM size, enter the **show version** user EXEC command.
- You cannot use CMS to upgrade a switch running Release 11.2(8)SA2 or earlier releases. Use the CLI to perform the upgrade.
- If your switch is running Release 11.2(8)SA3, SA4, or SA5 (Catalyst 2900 XL only), we recommend that you upgrade the switch software by using VSM. If you are upgrading a switch running Release 11.2(8)SA6 or later to this release, we recommend that you use Cluster Manager. For CMS instructions for upgrading switch software, refer to the switch software configuration guide or the online help for that release.
- When using CMS, you cannot upgrade Catalyst 2900 XL, Catalyst 2900 LRE XL, or 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.
  - For 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.
- 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.

- When using CMS to upgrade multiple switches from the Cisco TFTP server, the Cisco TFTP server application can process multiple requests and sessions. When using CMS 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.
- If you are using VSM to upgrade a specific switch, follow the steps in the "Using CMS to Upgrade a Specific Switch" section on page 30.
- If you are using Cluster Manager to upgrade a switch or switch cluster running Release 11.2(8)SA6 or later, follow the steps in the "Using CMS to Upgrade One or More Switches" section on page 32.
- If you are using the CLI to upgrade a switch, follow the steps in one of these sections:
  - "Using the CLI to Upgrade an 8-MB Catalyst 2900 XL Switch" section on page 33
  - "Using the CLI to Upgrade a Catalyst 3500 XL Switch" section on page 37
  - "Using the CLI to Upgrade Member Switches" section on page 39

When you upgrade a switch, the switch continues to operate while the new software is copied to Flash memory. Features provided by the new software are not available until you reboot the switch.

- When using XMODEM, if there is enough space on the switch Flash memory, the new image is copied to the switch but does not replace the existing image until you reboot the switch. If a failure occurs while you are copying the new image to the switch, you can use the existing image to reboot the switch.
- If there is *not* enough space for two images on the switch Flash memory, the new image is copied over the existing one. If a failure occurs while you are copying the new image to the switch, or if the new startup configuration fails, you must use the XMODEM Protocol to reinstall a previous or new image to the switch Flash memory. For more information, refer to the "Recovering from Corrupted Software" section in the "Troubleshooting" chapter of the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide*.

Overview of the Switch Upgrade Process

The software upgrade procedure has 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 28.
- Downloading the .tar file from Cisco.com, as described in the "Downloading the New Software and TFTP Server Application to Your Management Station" section on page 29. 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 .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 30. 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 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide*.

- Using CMS or the CLI to upgrade the software on your switch or switch cluster:
  - If you are using CMS to upgrade a switch, follow the steps in the "Using CMS to Upgrade One or More Switches" section on page 32.
  - If you are using the CLI to upgrade a switch, follow the steps in the "Using the CLI to Upgrade an 8-MB Catalyst 2900 XL Switch" section on page 33, the "Using the CLI to Upgrade a Catalyst 3500 XL Switch" section on page 37, or the "Using the CLI to Upgrade Member Switches" section on page 39.

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.

Determining the Switch Software Version

The IOS image is stored as a *.bin* file in a directory that is named with the IOS release. A subdirectory contains the HTML files needed for web management. The image is stored on the system board Flash device (flash:).

You can use the **show version** user EXEC command to see the software version that is running on your switch. For example:

```
switch> show version
Cisco Internetwork Operating System Software IOS (tm)
C2900XL Software (C2900XL-HS-M), Version 11.2(8.2)SA6, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Mon 23-Nov-98 20:59 by paulines
Image text-base: 0x00003000, data-base: 0x00202144
```

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that might be stored in Flash memory.

Which Software Files to Download from Cisco.com

New software releases are posted on Cisco.com and are also available through authorized resellers. From Cisco.com, you can also download a TFTP server application to copy the switch software from your PC to the switch.

Table 8 describes the file extensions and what they mean for the upgrade procedure. Table 9 and Table 10 list the software files that you need from Cisco.com.

Note We recommend that you download the combined .tar file that contains the image file and the HTML files. The procedures in this document are for upgrading a switch by using the combined .tar file.

Table 8 Possible Extensions for IOS Software Files

Extension	Description

Table 8 Possible Extensions for IOS Software Files

.bin	The IOS image file that you can copy to the switch through TFTP.
.tar	A compacted file from which you can extract files by using the **tar** privileged EXEC command. The .tar file that you download from Cisco.com contains both the .bin and CMS files.

Table 9 Catalyst 2900 XL Switch IOS Software Files

Filename	Description
c2900XL-c3h2s-mz.120-5.WC3.bin	IOS image-only file
c2900XL-c3h2s-mz.120-5.WC3.tar	IOS image and HTML files

Table 10 Catalyst 3500 XL Cisco IOS Software Files

Filename	Description
c3500XL-c3h2s-mz.120-5.WC3.bin	IOS image file
c3500XL-c3h2s-mz.120-5.WC3.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 9 and Table 10 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 one of these URLs, and download the appropriate files:

http://www.cisco.com/cgi-bin/tablebuild.pl/cat2900XL
http://www.cisco.com/cgi-bin/tablebuild.pl/cat3500XL

If you do not have a SmartNet contract, go to one of these URLs, and download the appropriate files:

http://www.cisco.com/pcgi-bin/tablebuild.pl/cat2900XL
http://www.cisco.com/pcgi-bin/tablebuild.pl/cat3500XL

Step 3 Use the CLI or CMS to perform a TFTP transfer of the file or files to the switch after you have downloaded the correct files 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 CMS to Upgrade a Specific Switch

Note If you use VSM to upgrade your Catalyst 2900 XL switch from a release before Release 11.2(8)SA6 to this release, you must first perform Steps 1 through 4 to rename the image file to ensure that you can reload the software. You do not need to perform Steps 1 through 4 if you are using VSM to upgrade a Catalyst 2900 XL or Catalyst 3500 XL switch from Release 11.2(8)SA6 or later. You can rename the image file by accessing the CLI through Telnet or by connecting to the switch console port.

Note If the software upgrade from VSM is incomplete, see the "Recovering from an Incomplete CMS Software Upgrade" section on page 32.

Tips If your switch is not configured for Telnet, follow the procedure described in the "Telnet Access to the CLI" section in the "General Switch Administration" chapter of the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide*.

Follow these steps to rename the image file by using the CLI, and then use VSM to upgrade the software:

Step 1 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 this command:

```
server% telnet switch_ip_address
```

Step 2 Enter the Telnet password if you are prompted to do so.

Step 3 Enter privileged EXEC mode:

```
switch> enable
switch#
```

Step 4 Enter the switch password if you are prompted to do so.

Step 5 Display the files in Flash memory:

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

  2  -rwx        4484   Mar 05 1993 00:31:09  vlan.dat
  3 -rwx         110   Mar 01 1993 19:50:50  info
 92  -rwx         877   Mar 06 1993 18:39:38  placement.txt
➔5  -rwx     1644050   Mar 01 1993 19:36:14  c2900XL-c3h2s-mz-112.8.SA5.bin
  6  drwx        6720   Mar 01 1993 00:18:36  html
 86  -rwx         110   Mar 01 1993 19:37:00  info.ver
116  -rwx        3686   Mar 01 1993 19:55:33  config.text
 89  -rwx          25   Mar 01 1993 00:26:30  snmpengineid
  7  -rwx         313   Mar 01 1993 19:34:57  env_vars
```

Step 6 Rename the image file to *boot.bin*:

```
switch# rename flash:c2900XL-c3h2s-mz-112.8.SA5.bin flash:boot.bin
```

Ensure that there are no other image files in Flash memory.

Step 7 Start VSM and display the System Configuration window by selecting **System > System Configuration**.

Step 8 In the **Cisco IOS Image File** field, enter **boot.bin.**

Step 9 Check the **Retain Current IOS Image File Name** check box.

Step 10 Complete the other fields on the window as described in the online help.

Step 11 Click **Upgrade IOS Software and Visual Switch Manager**.

Step 12 Display the contents of Flash memory, and verify that the boot.bin file was downloaded:

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

  2  -rwx        4484   Mar 05 1993 00:31:09  vlan.dat
  4  -rwx         110   Mar 01 1993 19:50:50  info
 92  -rwx         877   Mar 06 1993 18:39:38  placement.txt
➔ 5  -rwx     1644050   Mar 01 1993 19:36:14  boot.bin
  6  drwx        6720   Mar 01 1993 00:18:36  html
 86  -rwx         110   Mar 01 1993 19:37:00  info.ver
116  -rwx        3686   Mar 01 1993 19:55:33  config.text
 89  -rwx          25   Mar 01 1993 00:26:30  snmpengineid
  7  -rwx         313   Mar 01 1993 19:34:57  env_vars

3612672 bytes total (840704 bytes free)
```

Step 13 Verify that the switch reloads correctly by displaying the boot variable (BOOT path-list), boot.bin.

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

Recovering from an Incomplete CMS Software Upgrade

If you do not follow the preceeding procedure, an upgrade can fail due to insufficient space because of multiple software images or other files in Flash memory. When the upgrade fails, the image file is copied to Flash memory, but there is insufficient space for the HTML files, and you lose access to CMS.

If a failure occurs, ensure that the image file in Flash memory has the same name as the contents of the boot variable. You can compare these two names by following Steps 12 and 13 in the procedure.

If the contents of the boot variable and the image file name are the same, the switch can reset successfully. If they are different, rename the image file, or reset the boot variable by entering the **system boot** *name* global configuration command. The boot variable and the image file name should be the same.

To recover from the incomplete download of the HTML files, log in to the switch, and upgrade the software as described in the "Using the CLI to Upgrade Member Switches" section on page 39.

Using CMS to Upgrade One or More Switches

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

- When using CMS, you cannot upgrade Catalyst 2900 XL, Catalyst 2900 LRE XL, or 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.
  - For 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.
- 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.

Follow these steps to use CMS to upgrade switch 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 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 Names** 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 Cluster Manager to upgrade a single switch by following the same software upgrade procedure.

Note Close your browser after the upgrade process is complete.

On the 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.

On the Catalyst 1900 and Catalyst 2820 switches, the new image overwrites the current image during the upgrade.

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 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide*.

Using the CLI to Upgrade an 8-MB Catalyst 2900 XL Switch

Caution The 4-MB Catalyst 2900 XL switches do not have sufficient memory to be upgraded to this release. The 4-MB models are WS-C2908-XL, WS-C2916M-XL, WS-C2924C-XL, and WS-C2924-XL. These switches must run Release 11.2(8.x)SA6 to be cluster members.

This procedure is for upgrading Catalyst 2900 XL switches with 8 MB of DRAM. You upgrade a switch by extracting the IOS image file and the HTML files from a combined .tar file. You copy the files to the switch from a TFTP server and extract the files by entering the **tar** privileged EXEC command with these results:

- Changes the name of the current image file to the name of the new file that you are copying and replacing the old image file with the new one by using the **tar** privileged EXEC command.
- Disables access to the HTML pages and deletes the existing HTML files before you upgrade the software to avoid a conflict with users accessing the web pages during the software upgrade.
- Reenables access to the HTML pages after the upgrade is complete.

Note If you want to separately copy the IOS image or HTML files to the switch, refer to the *Catalyst 2900 Series XL Release Notes for Release 11.2(8)SA4* on Cisco.com.

If you are unsure whether your switch has 4 MB or 8 MB of memory, you can verify memory capacity at Step 4.

Follow these steps to upgrade the switch software by using the **tar** privileged EXEC command to start 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 this 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 a password if you are prompted to do so.

Step 4 Confirm that you have an 8-MB switch:

```
switch# show version
Cisco Internetwork Operating System Software IOS (tm)
C2900XL Software (C2900XL-HS-M), Version 11.2(8.2)SA6, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Mon 23-Nov-98 20:59 by paulines
Image text-base: 0x00003000, data-base: 0x00202144

ROM: Bootstrap program is C2900XL boot loader

2900XL-EN-84.3 uptime is 1 day, 22 hours, 23 minutes
System restarted by power-on
Running default software


cisco WS-C2924-XL (PowerPC403GA) processor (revision 0x11)
with 8192K/1024K bytes of memory.
Processor board ID 0x0E, with hardware revision 0x01
Last reset from power-on

Processor is running Enterprise Edition Software
24 Ethernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:50:80:39:EC:40
Motherboard assembly number: 73-3382-04
Power supply part number: 34-0834-01
Motherboard serial number: FAA02499G7X
Model number: WS-C2924-XL-EN
System serial number: FAA0250U03P
Configuration register is 0xF
```

Step 5 Display the name of the running (default) image file (BOOT path-list). This 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
```

If there is no file defined in the BOOT path-list, enter the **dir flash:** privileged EXEC command to display the contents of Flash memory. For example, the file named *c2900XL-c3h2-mz-120-5.3.WC.1.bin* is the image file.

```
c2900XL-c3h2-mz-120-5.3.WC.1.bin
switch# dir flash:
Directory of flash:/

 2  ---x     1644046   Apr 04 1993 15:22:13  c2900XL-c3h2s-mz-120-5.3.WC.1.bin
  4  d--x        6848   Apr 04 1993 15:23:11  html
  6  -rwx          79   Apr 04 1993 15:20:34  env_vars
  5  ---x         106   Apr 04 1993 15:20:36  info
 68  -rwx        1399   May 16 2000 14:43:42  config.text
259  ---x         106   Apr 04 1993 15:23:12  info.ver

3612672 bytes total (940032 bytes free)
```

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 a .bin extension. The image file name is then the same as the downloaded file name 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:c2900XL-h2-mz-112.8.2-SA6.bin
flash:c2900XL--C3h2s-mz-120-5.3.WC.1.bin
Source filename [c2900XL-h2-mz-112.8.2-SA6.bin]?
Destination filename [c2900XL-c3h2s-mz-120-5.3.WC.1.bin]?
```

Step 7 Enter global configuration mode:

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

Step 8 Disable access to the switch HTML pages:

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

Step 9 If you entered the **boot** global configuration command with the name of the image file, enter this command to change the image filename to the new name.

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

For example:

```
switch(config)# boot system flash:c2900XL-c3h2s-mz-120-5.3.WC.1.bin
```

Note If the **show boot** privileged EXEC command that you entered in Step 5 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 10 Return to privileged EXEC mode:

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

Step 11 Remove the HTML files:

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

Step 12 Press **Enter** to confirm the deletion of each file. Do not press any other keys during this process.

Step 13 If upgrading from Release 11.2(8)SA5 or earlier, remove the files in the Snmp directory:

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

Make sure the *S* in *Snmp* is uppercase.

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** privileged EXEC 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 14 Enter this command to copy the new image and HTML files to the switch 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 (111 bytes)
extracting c2900XL-c3h2s-mz-120-5.3.WC.1.bin (1557286 bytes)!!!!!!!!!!!!!!!!!!!!
html/ (directory)
extracting html/Detective.html.gz (1139 bytes)!
extracting html/ieGraph.html.gz (553 bytes)
extracting html/DrawGraph.html.gz (787 bytes)!
. . .
```

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

Step 15 Enter global configuration mode:

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

Step 16 Re-enable access to the switch HTTP pages:

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

Step 17 Return to privileged EXEC mode:

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

Step 18 Reload the new software with this command:

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

Step 19 Press **Return** to confirm the reload.

Your Telnet session ends when the switch resets.

Step 20 After the switch reboots, use Telnet to return to the switch, and enter the **show version** privileged EXEC command to verify the upgrade procedure. If you have a previously opened browser session to the upgraded switch, close the browser, and restart it to ensure that you are using the latest HTML files.

Using the CLI to Upgrade a Catalyst 3500 XL Switch

This procedure is for upgrading Catalyst 3500 XL 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** privileged EXEC command, with these 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.
- Re-enables 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 this 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). This 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 the **dir flash:** privileged EXEC command 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:c3500XL-c3h2-mz-112.8.2-SA6.bin
flash:c3500XL-C3h2s-mz-120-5.3.WC.1.bin
```

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

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

  2  ---x     1644045   Apr 04 1993 15:17:15  c3500XL-c3h2s-mz-120-5.3.WC.1.bin
   3  -rwx         415   Jun 13 1993 05:15:37  placement.txt
   4  d--x        6848   May 03 2000 10:47:58  html
  70  -rwx          20   Mar 21 1993 09:17:03  prefs.text
   6  ---x         106   Mar 01 1993 21:56:52  info
 228  ---x         106   Apr 04 1993 15:17:54  info.ver
  69  -rwx        2188   Mar 13 1993 03:38:28  config.text
 230  -rwx         744   Mar 25 1993 19:16:46  vlan.dat
 115  -rwx         354   Mar 13 1993 04:17:15  env_vars

3612672 bytes total (936960 bytes free)
```

Step 8 Enter global configuration mode:

```
switch# config 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** global configuration command with the name of the new image filename:

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

For example:

```
switch(config)# boot system flash:c3500XL-C3h2S-mz-120-5.3.WC.1.bin
```

Note If the **show boot** privileged EXEC command 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** privileged EXEC 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 this 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 c3500XL-c3h2s-mz-120-5.3.WC.1.bin (1271095 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** privileged EXEC 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 this 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.

Step 19 After the switch reboots, use Telnet to return to the switch, and enter the **show version** privileged EXEC command to verify the upgrade procedure. If you have a previously opened browser session to the upgraded switch, close the browser, and restart it 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 2900 XL or Catalyst 3500 XL Member Switches" section on page 39
- "Upgrading Catalyst 1900 or Catalyst 2820 Member Switches" section on page 40

Upgrading Catalyst 2900 XL or Catalyst 3500 XL Member Switches

Follow these steps to upgrade the software on a Catalyst 2900 XL or Catalyst 3500 XL 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** privileged EXEC command, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL 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*.

When the download is complete, the `TFTP successfully downloaded operational code` message appears, and the switch resets and begins using the new software.

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.

These publications provide more information about the switches and the switch software:

- *Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide* (order number DOC-786511=)
- *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference* (order number DOC-7812155=)
- Cluster Management Suite (CMS) online help (available only from the switch CMS software)
- *Catalyst 2900 Series XL Hardware Installation Guide* (order number DOC-786461=)
- *Catalyst 3500 Series XL Hardware Installation Guide* (order number DOC-786456=)
- *Catalyst 2900 Series XL Modules Installation Guide* (order number DOC-CAT2900-IG=)
- *Catalyst 2900 Series XL ATM Modules Installation and Configuration Guide* (order number DOC-785472=)
- *1000BASE-T Gigabit Interface Converter Installation Note* (not orderable but is available on Cisco.com)
- *Catalyst GigaStack Gigabit Interface Converter Hardware Installation Guide* (order number DOC-786460=)

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

Cisco Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Cisco 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 submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

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.