



Release Notes for the Catalyst 2900 Series XL and Catalyst 3500 Series XL Switches, Cisco IOS Release 12.0(5.1)WC(1)

May 2001

Cisco IOS Release 12.0(5.1)WC(1) runs on Catalyst 2900 series XL and Catalyst 3500 series XL switches with 8-MB CPU DRAM. This release does not run on Catalyst 2900 series XL switches with 4-MB CPU DRAM.



Note

The documentation shipped with the Catalyst 2900 XL and 3500 XL switches and the Cisco 575 LRE customer premises equipment (CPE) device refers to Release 12.0(5)WC(1). The correct IOS release is Cisco IOS Release 12.0(5.1)WC(1). For a complete list of these documents, see the [“Documentation Notes” section on page 14](#).

These release notes include important information about this IOS release and any limitations, restrictions, and caveats that apply to it. See the [“Related Documentation” section on page 37](#) for the complete list of Catalyst 2900 XL and Catalyst 3500 XL documentation.



Note

Before upgrading your switch to this release, read the [“Upgrading the Switch Software” section on page 22](#).

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

Contents

This document has the following sections:

- [“Hardware Requirements” section on page 2](#)
- [“Software Requirements” section on page 3](#)
- [“Cluster Requirements and Guidelines” section on page 4](#)
- [“Minimum Cisco IOS Release for Major Features” section on page 5](#)
- [“New Features in this Release” section on page 7](#)
- [“Limitations and Restrictions” section on page 8](#)
- [“Caveats” section on page 9](#)
- [“Important Notes” section on page 14](#)
- [“Documentation Notes” section on page 14](#)
- [“Initial Switch Configuration” section on page 16](#)
- [“Upgrading the Switch Software” section on page 22](#)
- [“Related Documentation” section on page 37](#)
- [“Obtaining Documentation” section on page 38](#)
- [“Obtaining Technical Assistance” section on page 39](#)

Hardware Requirements



Note

Catalyst 2900 XL 4-MB switches run original edition software and 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 user EXEC **show version** command.

This release supports the 8-MB Catalyst 2900 XL switches (see [Table 1](#)) and Catalyst 3500 XL switches (see [Table 2](#)). This software also supports the Cisco 575 LRE CPE (customer premises equipment) device.

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

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

Switch	Description
Catalyst 2912 LRE XL	4 autosensing 10/100 ports and 12 Long-Reach Ethernet (LRE) ports
Catalyst 2924 LRE XL	4 autosensing 10/100 ports and 24 LRE 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 system and Cluster Management Suite (CMS) software.

System Requirements

The following 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	65536	1024 x 768	Small
Solaris 2.5.1	SPARC 333 MHz	128 MB	Most colors for applications	—	Small (3)

1. Service Pack 3 or higher required

Browser 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, the switch displays an error message, 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 19.

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
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 16.

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 and Modules

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 Cisco IOS Release 12.0(5.1)WC(1) are cluster-capable. All Catalyst 2900 XL modules are supported in cluster configurations.

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

Switch	Cisco IOS Release 12.0(5.1)WC(1)?	Command Capable?	Member Capable?
Catalyst 3500 XL	Yes	Yes	Yes
Catalyst 2900 XL (8 MB of DRAM)	Yes	Yes	Yes
Catalyst 2900 XL (4 MB of DRAM) ¹	No	No	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 2950 Switches

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

Catalyst 1900 and Catalyst 2820 Switches and Modules

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 or the Catalyst 2820 switches.

Table 6 Catalyst 1900 and Catalyst 2820 Switches as Cluster Members

Switch	Software Release 9.00 (-A)	Software Release 9.00 (-EN)	Member Capable?	Command Capable?
Catalyst 1900	Yes	Yes	Yes	No
Catalyst 2820	Yes	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
WS-C2912-LRE XL and WS-C2912-LRE XL switches with LRE ports	Release 12.0(5.1)WC(1)
Extended cluster member functionality for Catalyst 2950 switches	Release 12.0(5)WC(1)
Multicast VLAN Registration (MVR)	Release 12.0(5)WC(1)

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

Feature	Minimum Release Required
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 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
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 8)	Release 11.2(8)SA6
Catalyst 2900 series XL 1000BASE-X modules	Release 11.2(8)SA5
Catalyst 2900 series XL ATM modules	Release 11.2(8)SA5
IEEE 802.1Q trunking	Release 11.2(8)SA4 (Enterprise Edition Software)
Inter-Switch Link (ISL) trunking	Release 11.2(8)SA5 (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

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

Feature	Minimum Release Required
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 Features in this Release

This section describes the new features in this release.

- [“New Hardware Support” section on page 7](#)
- [“New Software Support” section on page 7](#)

New Hardware Support

This release supports the following new devices:

- Catalyst 2900 LRE XL switches
- Catalyst 2950 switches
- Cisco 575 LRE CPE devices

New Software Support

This release supports the following new software features:

- LRE technology—LRE is the technology that the Catalyst 2900 LRE XL switches use to transfer data and voice traffic through existing telephone lines (categorized and noncategorized unshielded twisted-pair cable) in multidwelling or tenant buildings. The LRE ports on these switches connect the Cisco 575 LRE CPE and the Cisco LRE 48 POTS Splitter (PS-1M-LRE-48). The link between a switch LRE port and CPE can provide up to 15 Mbps of bandwidth to remote Ethernet devices at distances of up to 4921 ft (1500 m).
- Multicast VLAN Registration (MVR)—MVR is designed for applications using wide-scale deployment of multicast traffic (for example, broadcast of multiple television channels) across an Ethernet ring-based service provider network. MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN. It allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. It can continuously send multicast streams in the multicast VLAN, but, for bandwidth and security reasons, can isolate the streams from the subscriber VLANs.

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.

- Regardless of the switch model, only 64 instances of STP are supported.
- When connecting to the Catalyst 3524-PWR XL 10/100 inline-power ports, observe the following 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 supports the Catalyst 2900 LRE XL switches and 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 indicate 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.
- 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 IP Configuration tab of the IP Management window in CMS.
- A configuration conflict occurs if a switch cluster has Catalyst 2900 LRE XL switches using both private and public profiles. If one LRE switch in a cluster is assigned a public profile, all LRE switches in that cluster must have that same public profile. Before you add an LRE switch to a cluster, make sure that you assign it the same public profile used by other LRE switches in the cluster.
- 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.
- All Catalyst 3500 series XL and most Catalyst 2900 series XL switches support a total of 250 VLANs and STP instances. The Catalyst 2912 XL, 2924 XL, and 2924C XL switches support a total of 64 VLANs and STP instances.
- 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 and resolved caveats in Cisco IOS Release 12.0(5.1)WC(1):

Open Caveats

This section describes possible unexpected activity by Cisco IOS Release 12.0(5.1)WC(1):

- CSCdt67450

Alignment and collision Ethernet counters on the Cisco 575 LRE CPE device are not reliable. These counters can increment without an Ethernet link, and they can also be higher than expected when encountering alignment and collision conditions. This is especially noticeable if an LRE port is configured with the LRE-15, the Public-ANSI, or the Public-ETSI profiles.

There is no workaround.

- CSCdt22573

If a port group is set up between the LRE port of a Catalyst 2900 LRE XL switch and the FEC ports of another switch through the LRE CPE devices, and the LRE link on an LRE port drops, the LRE switch no longer uses the LRE port for data transmission. However, the other switch might continue sending data through the FEC port. The packets being sent to the LRE port of the LRE switch are lost.

If the LRE link is restored, data transmission continues as normal.

There is no workaround.

- CSCdt01392


Ethernet statistics that appear in the output of the **show interface** command for LRE ports show the counters of the MAC on the switch instead of the MAC on the CPE device.

The workaround is to use the **show controllers ethernet-controller** command to see the Ethernet statistics on the CPE device. To clear the Ethernet statistics counters on the CPE device, use the **clear controllers ethernet-controller** command.

- 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, there can be a loss of connectivity to the switch.

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

- CSCdt83279
A Multicast VLAN Registration (MVR) receiver port that receives multicast data traffic that exceeds the configured threshold does not shut down.
The workaround is to set the MVR threshold to 1000 (the maximum setting) and then to use the port multicast storm control feature instead of the MVR threshold feature to limit rates.
 - CSCdt84379
The connection between a switch and a console is lost whenever VLAN membership changes on an MVR port.
The workaround is to either Telnet to the switch to access the CLI or to reboot the switch to restore the console session.
 - CSCdt83966
The **show mvr**, **show mvr int**, and **show mvr member** commands do not show that the MVR and its members are disabled when a multicast VLAN or receiver VLAN is deleted from the database. When the VLAN is restored, traffic forwarding does not resume.
The workaround is to save the configuration, reboot the switch, and restore the VLAN.
-
-  **Note** When you restore the VLAN, you *must* stop traffic for at least 1 second before forwarding resumes.
-
- 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.
 - 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 tooltip box 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 Byts, Total Packets, or Total Errors boxes are plotted.
There is no workaround.

- CSCds86420

If you select a switch in the tree by using Cluster Management and choose Console Baud Rate, the baud rate dialog appears with the selected switch in the Selected Device list. If you then click **cancel** and select Console Baud Rate again, two identical items for the same switch are listed.

There is no workaround.

- 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** 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.

- CSCdt57346

When you use the **show rmon history** command, the value for the collision is cumulative, not unique for each sample. The value for a collision in a given sample can be calculated by subtracting from the previous sample.

There is no workaround.

- CSCds72421

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

The workaround is to reboot the switch.

- CSCdt48011

Two problems occur when the Catalyst 2950 switch is in transparent mode:

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

There is no workaround.

- CSCdt04001

On Catalyst 2900 XL and 3500 XL switches, when you change the privilege level for the interface, you can execute commands with the newly configured privilege level. However, the switch does not save the arguments associated with the command, and after a reload, the configured commands are not executable.

There is no workaround.

- CSCdt49955

CMS dialogue windows can display two list selection boxes with **Add** and **Remove** buttons between them. If you press the Shift key on the keyboard at the same time as either **Add** or **Remove**, sometimes an exception error occurs. The exception error is displayed only inside the Java console window and is not displayed by CMS. As a result, the **Add** or **Remove** buttons might not function correctly. If you continue to click these buttons, multiple entries are added to the available or selected lists.

The workaround is to not hold down the Shift key when clicking **Add** or **Remove**.
- CSCdt78498

The switch ports in a VLAN can fail if the MTU of that VLAN is changed in the VLAN database. The workaround is to keep the MTU default value in the VLAN database.
- CSCdt82729

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

The workaround is to not launch the VMPS Configuration window from the device popup menu, as VLAN Membership Policy Server (VMPS) is not supported on the Catalyst 2950 switches.
- CSCdt68204

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

The workaround is to enter the **clear cam** command.
- CSCdt18106

If you enter the **snmpwalk** command 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 workaround is to use individual **snmpget** requests to retrieve data.
- CSCdt48351

The usage of the `c2950BandwidthUsage` MIB always shows zero, instead of displaying the current bandwidth usage statistics.

There is no workaround.
- CSCdt57171

On a Catalyst 3524 XL-PWR switch running Cisco IOS 12.0(5.2)XU, if an IP phone is connected to a Fast Ethernet port that is set to 10 Mbps half duplex and the switch is powered on and off, the IP phone does not power up.

The workaround is to disconnect the Ethernet cable and then reconnect it.
- CSCds84479

When you connect two switches by GigaStack GBICs and you manually set 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 gets configured from the dynamic IP pool, a duplicate or different IP address might be assigned.
The workaround is to make sure that the DHCP server contains reserved addresses that are bound to each switch by the switch hardware address so that the switch does not obtain its IP address from the dynamic pool.
- CSCdp67822
Cluster Management Suite requires a Java plug-in from Sun Microsystems. If you are using Internet Explorer and you disable Java plug-ins by using the Java Plug-In Control Panel, the initial Splash screen shows that the plug-in and Java are enabled, but Internet Explorer fails.
The workaround is to not disable Java plug-ins on the Java Plug-In Control Panel.
- CSCdp82224
The Cluster Manager System Time Management window supports the configuration of the Network Time Protocol (NTP) and system time. When you make changes on this window from a command switch, Java propagates the changes to all cluster members. A conflict can arise if you configure NTP and also use the Set Daylight Saving Time and Set Current Time tabs.
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.
- 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.
- CSCdp70389
When you change the management VLAN on a cluster with command-switch redundancy enabled, the cluster can break if HSRP is configured on any of the cluster members in the new management VLAN.
The workaround is to not change the management VLAN to a VLAN where a member is configured as part of a standby group.
- CSCdp85954
Root guard is inconsistent when configured on a port that is in the STP blocked state at the time of configuration.
- 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

The following problems were resolved in Cisco IOS Release 12.0(5.1)WC(1):

- CSCdt26961
The **power inline never** command now correctly changes the link pulse from a power link pulse to a standard link pulse.

- CSCds78577
If a client is moved from one secure port to another, and the maximum secure address count on the second port is exceeded, the switch now sends security violation traps.
- CSCdt39268
Cisco IOS software now prevents the successful prediction of TCP Initial Sequence Numbers.
- CSCdt13828
When a **loopback** command is followed by a **no loopback** command on a port connected to a device, such as an Ethernet time clock, that port now correctly comes out of loopback.

Important Notes

This section describes important information related to this release.

In this release, 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

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 16.
 - Installing browser plug-ins. See the [“Installing the Required Plug-In”](#) section on page 19.
 - Configuring your browser. See the [“Configuring Your Browser”](#) section on page 20.
 - Accessing CMS. See the [“Displaying the CMS Access Page”](#) section on page 22.
- Procedures for upgrading the switch software. See the [“Guidelines for Upgrading Switch Software”](#) section on page 23.
- All documentation for this release, except for these release notes, is provided on the *Catalyst 2900 XL and Catalyst 3500 XL Documentation CD*.

To view the contents of the documentation CD, double-click the index.htm file. Your browser launches, and you can select and view the documents on the CD.

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

- These documents refer to Cisco IOS Release 12.0(5)WC(1). The correct IOS release is Cisco IOS Release 12.0(5.1)WC(1):
 - *Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide*
 - *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*
 - *Catalyst 2900 Series XL Hardware Installation Guide*
 - *Cisco 575 LRE CPE Hardware Installation Guide*
- Three Long-Reach Ethernet (LRE) profiles were added to this release and are not documented in the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide* and CMS online help:
 - LRE-5LL
 - LRE-10LL
 - LRE-15LL

The PUBLIC-ANSI, PUBLIC-ETSI, LRE-5, LRE-10, and LRE-15 profiles described in the manuals and online help have the interleaver feature enabled for maximum protection against small interruptions on the LRE link.

The interleaver feature delays the data, while increasing protection for the data against very small interruptions in the LRE link. By disabling the low latency feature, data is a slightly more susceptible to interruptions on the LRE link, but the delay is removed. The *LL* in these profiles stands for *low latency*. In these profiles, the interleaver feature is turned off.

[Table 8](#) lists all of the LRE profiles available on the Catalyst 2900 LRE XL switches.

**Note**

Use the rates and distances in [Table 8](#) as guidelines only. Factors such as the type of cable you use, how it is bundled, and the interference and noise on the LRE link can affect the actual LRE link performance. Contact Cisco Systems for information about limitations and optimization of LRE link performance.

**Note**

The net data rates in [Table 8](#) are slightly less than the gross data rates displayed by the **show controllers lre profile names** privileged EXEC command.

Table 8 LRE Profiles

Profile Name	Profile Type	LRE Link Downstream Rate (Mbps)	LRE Link Upstream Rate (Mbps)	Maximum Distance between the LRE Port and the CPE
PUBLIC-ANSI	Public	15.17	4.27	4101 ft (1250 m)
PUBLIC-ETSI	Public	11.38	4.27	4101 ft (1250 m)
LRE-5	Private	5.69	5.69	4921 ft (1500 m)
LRE-10 (default)	Private	11.38	11.38	4101 ft (1250 m)
LRE-15	Private	15.17	17.06	3445 ft (1050 m)
LRE-5LL	Private	5.69	5.69	4921 ft (1500 m)
LRE-10LL	Private	11.38	11.38	4101 ft (1250 m)
LRE-15LL	Private	15.17	17.06	3445 ft (1050 m)

- Use only a 19-inch rack to rack-mount a Catalyst 2900 LRE XL switch. Do not install an LRE switch in a 23- or 24-inch rack as described in the *Catalyst 2900 Series XL Hardware Installation Guide*.

**Caution**

The mounting brackets shipped with a Catalyst 2900 LRE XL switch cannot support the switch in a 23- or 24-inch rack. If you install the switch in a 23- or 24-inch rack, the switch sags towards the rear of the rack.

- The Cisco part number provided for the Category 5 cable with 120-degree, male-to-male RJ-21 connectors in the “Installation” chapter of the *Catalyst 2900 Series XL Hardware Installation Guide* is listed as CAB-5-M180120-5. The correct Cisco part number is CAB-5-M180120M-5.
- 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 16](#)
- [“Installing the Required Plug-In” section on page 19](#)
- [“Configuring Your Browser” section on page 20](#)
- [“Displaying the CMS Access Page” section on page 22](#)

This section assumes 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 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 abort 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 1M3pS$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 19, “Configuring Your Browser” section on page 20, and “Configuring Your Browser” section on page 20)
- 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 browser Java plug-in is required to access the HTML-based CMS. Download and install the plug-in before you start CMS.

If the Java applet does not initialize after you have installed the plug-in, open the Java Plug-in Control Panel (**Start > Programs > Java Plug-in Control Panel**), and verify that in the Proxies tab the **Use browser settings** is checked and that no proxies are enabled.

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

These platforms support three Java plug-ins:

- Java plug-in JRE 1.2.2\_05 and JRE 1.2.2\_07

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

- If you have a SmartNet support contract, download the plug-in from this URL:

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

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

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

- JRE 1.3.0

You do not need to download a separate Java plug-in, as it is included with the JRE 1.3.0. Download and install the JRE 1.3.0 for Solaris from one of these Cisco.com URLs:

- If you have a SmartNet support contract, download the plug-in from this URL:

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

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

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



#### Note

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

## Solaris Users

The Solaris platform supports two Java plug-ins:

- JRE 1.2.2\_05
  - Install the JRE 1.2.2\_05 from this URL:  
<http://www.sun.com/software/solaris/java/download.html>  
Follow the links in the section titled J2SE: Java 2 Standard Edition (1.2.2\_05 Localized) for the JRE 1.2.2\_05 plug-in.
  - Install the Solaris Java plug-in from this URL:  
<http://www.sun.com/software/solaris/netscape/jpis/>
- JRE 1.3.0

You do not need to download a separate java plug-in, as it is included with the JRE 1.3.0. You can download the JRE and the related readme file from one of these URLs:

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

## Configuring Your Browser

To access CMS, your Netscape Communicator or Microsoft Internet Explorer browser must be properly configured.

### Configuring Netscape Communicator (All Versions)

Follow these steps to configure Netscape Communicator:

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

## Configuring Microsoft Internet Explorer (4.01)

Follow these steps to configure Microsoft Internet Explorer 4.01:

- 
- Step 1** Start Internet Explorer.
  - Step 2** From the menu bar, select **View > Internet Options**.
  - Step 3** In the Internet Options window, click the **Advanced** tab.
    - a. Scroll through the list of options until you see Java VM. Check the **Java logging enabled** and **Java JIT compiler enabled** check boxes.
    - b. Click **Apply**.
  - Step 4** In the Internet Options window, click the **General** tab. In the Temporary Internet Files section, click **Settings**.
  - Step 5** In the Settings window, select **Every visit to the page**, and click **OK**.
- 

## Configuring Microsoft Internet Explorer (5.0)



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

Follow these steps to configure Microsoft Internet Explorer 5.0:

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



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

---

## Displaying the CMS Access Page

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

- 
- Step 1** Enter the switch IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer), and press **Return**.
  - Step 2** Enter your username and password when prompted. The password provides level 15 access. The Cisco Systems Access page appears. For more information on setting passwords and privilege levels, refer to the switch software configuration guide.
  - Step 3** Click **Cluster Management Suite** or **Visual Switch Manager** to display the appropriate CMS application.
- 

## Upgrading the Switch Software

This section provides topics about upgrading the switch software:

- [“Guidelines for Upgrading Switch Software” section on page 23](#)
- [“Overview of the Switch Upgrade Process” section on page 23](#)
- [“Which Software Files to Download from Cisco.com” section on page 24](#)
- [“Downloading the New Software and TFTP Server Application to Your Management Station” section on page 25](#)
- [“Copying the Current Startup Configuration from the Switch to a PC or Server” section on page 25](#)
- [“Using VSM to Upgrade a Switch” section on page 26](#)
- [“Using Cluster Manager to Upgrade One or More Switches” section on page 28](#)
- [“Using the CLI to Upgrade Member Switches” section on page 35](#)
- [“Using the CLI to Upgrade a Catalyst 3500 XL Switch” section on page 33](#)
- [“Using the CLI to Upgrade Member Switches” section on page 35](#)



**Note**

Before upgrading your switch to Cisco IOS Release 12.0(5.1)WC(1), read the [“Guidelines for Upgrading Switch Software” section on page 23](#) for important information.



**Note**

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

## Guidelines for Upgrading Switch Software

When upgrading switch software, follow these rules:

- You cannot install the original edition software for switches with 4 MB of DRAM on Catalyst 2900 XL 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 IOS Release 11.2(8.x)SA6 original edition software to be cluster members. No original edition software package is available for this release of IOS. To determine the switch DRAM size, enter the **show version** user EXEC command.
- 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.
- You cannot use the web-based interface to upgrade a switch running Release 11.2(8)SA2 or previous releases. Use the CLI to perform the upgrade in such cases.
- When using Cluster Manager, you cannot upgrade Catalyst 2900 XL and Catalyst 3500 XL switches at the same time. However, you can group together and upgrade Catalyst 1900 and Catalyst 2820 switches at the same time.
  - 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 Cluster Manager to upgrade multiple switches from the Cisco TFTP server, the Cisco TFTP server application can handle multiple requests and sessions. When using Cluster Manager to upgrade multiple switches from the Cisco TFTP server, you must first disable the **TFTP Show File Transfer Progress** and the **Enable Logging** options to avoid TFTP server failures. If you are performing multiple-switch upgrades with a different TFTP server, it must be capable of managing multiple requests and sessions at the same time.

## Overview of the Switch Upgrade Process

The software upgrade procedure consists of these major steps:

- Deciding which software files to download from Cisco.com, as described in the [“Which Software Files to Download from Cisco.com”](#) section on page 24.
- Downloading the combined .tar file from Cisco.com, as described in the [“Downloading the New Software and TFTP Server Application to Your Management Station”](#) section on page 25. This file contains the IOS image and the HTML files. From Cisco.com, you can also download a TFTP server application to copy the switch software from your PC to the switch, if necessary.

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

- Copying the current startup configuration file, as described in the [“Copying the Current Startup Configuration from the Switch to a PC or Server”](#) section on page 25. 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 up 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 VSM to upgrade a switch, follow the steps in the [“Using VSM to Upgrade a Switch”](#) section on page 26.
  - 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 Cluster Manager to Upgrade One or More Switches”](#) section on page 28.
- If you are using the CLI to upgrade a switch, follow the steps in the [“Using the CLI to Upgrade a Catalyst 3500 XL Switch”](#) section on page 33, [“Using the CLI to Upgrade Member Switches”](#) section on page 35, and [“Using the CLI to Upgrade Member Switches”](#) section on page 35.

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

## Which Software Files to Download from Cisco.com

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

[Table 9](#) describes the file extensions and what they mean for the upgrade procedure. It is easier to upgrade the switch software by using a combined .tar file that contains the HTML files and the IOS image. The upgrade procedures in these release notes describe how to perform the upgrade by using a combined .tar file, and you must use a combined .tar file to upgrade a switch through the CMS.

[Table 10](#) and [Table 11](#) list the software files for this IOS release.



**Note**

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

**Table 9** Possible Extensions for IOS Software Files

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

**Table 10** Catalyst 2900 XL Cisco IOS Software Files

| Filename                         | Description              |
|----------------------------------|--------------------------|
| c2900XL-c3h2s-mz-120.5-WC.1.bin  | IOS image-only file      |
| c2900XL-c3h2s-mz-120.5-WC.1.tar  | IOS image and HTML files |
| c2900XL-html-plus.120.5-WC.1.tar | HTML files               |

**Table 11** Catalyst 3500 XL Cisco IOS Software Files

| Filename                         | Description                   |
|----------------------------------|-------------------------------|
| c3500XL-c3h2s-mz-120.5-WC.1.bin  | IOS image file                |
| c3500XL-c3h2s-mz-120.5-WC.1.tar  | IOS image file and HTML files |
| c3500XL-html-plus.120.5-WC.1.tar | 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](#), [Table 10](#), and [Table 11](#) to identify the files that you want to download.
- Step 2** Download the files from one of the following 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 web-based interface 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 VSM to Upgrade a 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 VSM Software Upgrade”](#) section on page 28.



**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 VSM Software Upgrade

If you do not follow the preceding 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 VSM.

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 35.

## Using Cluster Manager to Upgrade One or More Switches

You can upgrade all or some of the switches in a cluster at once, but the software first performs a series of checks. For a faster upgrade process, follow these rules:

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

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

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

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

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

On 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 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. You cannot upgrade the switches to an 8-MB image. 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 original edition software 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** command. The procedure returns 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** command.
- Disables access to the HTML pages and deleting 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** 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 the following command:

```
server% telnet switch_ip_address
```

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

**Step 3** Enter privileged EXEC mode:

```
switch> enable
switch#
```

Enter 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). The following example shows the name in *italic*:

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

If there is no file defined in the BOOT path-list, enter **dir flash:** to display the contents of Flash memory. The file named *c2900XL-c3h2-mz-120.5-WC.1.bin* is your image file.

```
c2900XL-c3h2-mz-120.5-WC.1.bin
switch# dir flash:
Directory of flash:/

→ 2 ---x 1644046 Apr 04 1993 15:22:13 c2900XL-c3h2s-mz-120.5-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-WC.1.bin
Source filename [c2900XL-h2-mz-112.8.2-SA6.bin]?
Destination filename [c2900XL-c3h2s-mz-120.5-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** command with the name of the image file, enter this command to change it to the new name.

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

For example:

```
switch(config)# boot system flash:c2900XL-c3h2s-mz-120.5-WC.1.bin
```



**Note**

If the **show boot** command 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** 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 the following 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-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** 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 the following 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 privileged EXEC **show version** command to verify the upgrade procedure. If you have a previously opened browser session to the upgraded switch, close the browser, and start it again to ensure that you are using the latest HTML files.

## Using the CLI to Upgrade 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** command, with the following results:

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

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

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

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

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

```
server% telnet switch_ip_address
```

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

- Step 3** Enter privileged EXEC mode:

```
switch> enable
switch#
```

Enter the password if you are prompted to do so.

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

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

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

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

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

For example:

```
switch# rename flash:c3500XL-c3h2-mz-112.8.2-SA6.bin
flash:c3500XL-C3h2s-mz-120.5-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-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** 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-WC.1.bin
```



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

- Step 11** Return to privileged EXEC mode:

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

- Step 12** Remove the HTML files:

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

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



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

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

```
switch# tar /x tftp://server_ip_address//path/filename.tar flash:
Loading /path/filename.tar from server_ip_address (via VLAN1):!
extracting info (110 bytes)
extracting c3500XL-c3h2s-mz-120.5-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** command.

**Step 14** Enter global configuration mode:

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

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

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

**Step 16** Return to privileged EXEC mode:

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

**Step 17** Reload the new software with the following command:

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

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

Your Telnet session ends when the switch resets.

**Step 19** After the switch reboots, use Telnet to return to the switch, and enter the privileged EXEC mode **show version** command to verify the upgrade procedure. If you have a previously-opened browser session to the upgraded switch, close the browser, and start it again to ensure that you are using the latest HTML files.

## Using the CLI to Upgrade Member Switches

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

This section provides these procedures:

- [“Upgrading Catalyst 2900 XL or Catalyst 3500 XL Member Switches” section on page 36](#)
- [“Upgrading Catalyst 1900 or Catalyst 2820 Member Switches” section on page 36](#)

## 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** 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`.

You should see the `TFTP successfully downloaded operational code` message. When the download is complete, 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

The following publications provide more information about the switches and the switch software:

- *Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide*
- *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*
- *Catalyst 2900 Series XL Hardware Installation Guide*
- *Catalyst 3500 Series XL Hardware Installation Guide*
- *Using the Catalyst 2924M XL DC Ethernet Switch*
- *Catalyst 2900 Series XL Modules Installation Guide*
- *Catalyst 2900 Series XL ATM Modules Installation and Configuration Guide*
- *1000BASE-T Gigabit Interface Converter Installation Notes*
- *Catalyst GigaStack Gigabit Interface Converter Hardware Installation Guide*
- *Cisco 575 LRE CPE Hardware Installation Guide*



### Note

The *Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide*, the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*, the *Catalyst 2900 Series XL Hardware Installation Guide*, and the *Cisco 575 LRE CPE Hardware Installation Guide* refer to Cisco IOS Release 12.0(5)WC(1). The correct IOS release is Cisco IOS Release 12.0(5.1)WC(1).

# 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](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](mailto:bug-doc@cisco.com).

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

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

We appreciate your comments.

# Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

## Cisco.com

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

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

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

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

<http://www.cisco.com>

## Technical Assistance Center

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

## Contacting TAC by Using the Cisco TAC Website

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

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

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

## Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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

---

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

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

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0103R)

Release Notes for the Catalyst 2900 Series XL and Catalyst 3500 Series XL Switches, Cisco IOS Release 12.0(5.1)WC(1)

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