



Release Notes for the Catalyst 2900 Series XL and 3500 Series XL Cisco IOS Release 12.0(5.2)XU

July 20, 2000

Cisco IOS software Release 12.0(5.2)XU runs on Catalyst 3500 series XL switches and Catalyst 2900 series XL 8-MB switches. Catalyst 2900 series XL 4-MB switches are not supported in this release.

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 32 for the complete list of Catalyst 2900 and 3500 XL switch documentation.



Note

Before upgrading your switch to Release 12.0(5.2)XU, read the “Upgrading to a New Software Release” section on page 15 for important information.

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 CCO in the Cisco IOS software area.

Contents

This document has the following sections:

- “Changes Since Release 12.0(5)XU” section on page 2
- “Important Notes” section on page 3
- “Hardware and Supporting Software” section on page 9
- “New Supported Hardware” section on page 10
- “Changes Since Release 12.0(5.1)XP” section on page 10
- “Minimum IOS Release for Major Features” section on page 11
- “Limitations and Restrictions” section on page 12



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

Copyright © 2000. Cisco Systems, Inc. All rights reserved.

78-10615-03

- “Upgrading to a New Software Release” section on page 15
- “Current Caveats” section on page 27
- “Syslog Error Messages” section on page 29
- “Related Documentation” section on page 32
- “Obtaining Documentation” section on page 32
- “Obtaining Technical Assistance” section on page 33

Changes Since Release 12.0(5)XU



Note

Release 12.0(5.1)XU was functionally identical to Release 12.0(5)XU but contained support for the Catalyst 2900 series XL 1000BaseT module.

The following caveats have been resolved in Release 12.0(5.2)XU:

- The software now supports frames larger than 1518 bytes. (CSCdr70758)
- Dynamic VLAN ports now correctly shut down when they reach the MAC address limit of 20. (CSCdr48085)
- After a reset, the switch no longer waits 15 minutes to attempt to download configuration files. (CSCdr48370)
- The switch now accepts a host name provided in a BOOTP reply packet. (CSCdr11225)
- When the switch is configured as a VTP client, connected to a Catalyst 5000 VTP server, and powered down, the default on powering up is for the switch to be updated by the VTP server. (CSCdr36223)
- On a Catalyst 2900 series XL switch with an ATM module (WS-X2971-XL), SNMP status reporting is now working correctly. (CSCdp96124)
- After a topology change on the switch, the switch no longer sends a newRoot trap message if it was already the spanning-tree root. (CSCdr30003)
- Issuing a **config memory** command in a Telnet session no longer causes the switch to reboot. (CSCdr45415)
- The correct switch chassis serial number is now displayed as the chassisId variable in the OLD-CISCO-CHASSIS MIB. (CSCdr52007)
- In Cluster Manager, the Port Fast field now correctly displays and operates when multiple ports are selected. (CSCdr52689)
- When you enter a **no service timestamps debug uptime** command, this configuration is now saved in the startup configuration and does not have to be reentered after the switch is reloaded. (CSCdp82704)
- When the management VLAN is not VLAN 1 and the switch is powered down and then up, the switch no longer sends out ARP requests before Spanning Tree Protocol (STP) has put the ports into a listening state. (CSCdr32845)
- Issuing the **power inline auto** default command no longer resets the Cisco IP Phone 7960. (CSCdr45216)
- Downloading the IOS Release 12.1 image to the Catalyst 2900 series XL ATM module no longer causes the switch to keep rebooting. (CSCdr66828)

- Issuing an SNMP v2 GetNext request on a Catalyst 2900 Series XL switch with an ATM module no longer causes the switch to reset. Note that the software does not support SNMP version 2. (CSCdr67303)
- The Catalyst 3500 Series XL switches now correctly receive and transmit frames over type-I cabling. (CSCdr76868)

Important Notes

This section describes important information related to Release 12.0(5)XU through 12.0(5.2)XU.

Integration of Enterprise and Standard Edition Software

Catalyst 2900 and 3500 XL switches were previously supported by standard and enterprise editions of IOS software. With Release 12.0(5)XU, the standard and enterprise edition features were included in one release. The differences between the Catalyst 2900 and 3500 XL switches are described in the “Hardware and Supporting Software” section on page 9.

Configuring GigaStack GBIC Interfaces

When you are configuring a cascaded stack of Catalyst 3500 XL switches using the GigaStack GBIC and want to include more than one VLAN in the stack, be sure to configure all of the GigaStack GBIC interfaces as trunk ports.

Upgrading Switch Software by Using VSM

If you are using Visual Switch Manager (VSM) to upgrade your switch to the current release, review the steps in the “Using VSM to Upgrade a Switch” section to ensure a successful upgrade.



Note

Before upgrading your switch, read the “Upgrading to a New Software Release” section on page 15 for important information.

Installing the Required Plug-In

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

Windows 95, Windows 98, and Windows NT 4.0 Users

If you have a SmartNet support contract, log in to one of the following URLs and download the plug-in:

<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, download the plug-in from one of the following URLs:

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

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

If you start CMS without having installed the required Java plug-in, the switch automatically detects the lack of the plug-in. If you are using a supported Netscape browser, the browser displays a Cisco Connection Online (CCO) page that contains the Java plug-in and instructions to install it. If you are using a supported Internet Explorer browser, it automatically downloads and installs the browser.

Solaris Users

Solaris users need to download the Java plug-in and JRE 1.2.2_05.

Download the Java plug-in for Solaris from the following URL:

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

Install the plug-in by following the instructions that are posted on the URL.

Install the JRE 1.2.2_05 from the following URL:

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

Follow the links in the section titled J2SE: Java[tm] 2 SDK, Standard Edition (1.2.2_05) to download and install the JRE.

Documentation Notes

- 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 Figure 1-17 on page 1-23 in the *Catalyst 3500 Series XL Hardware Installation Guide* shows an outdated power rating of 1.0A/0.5A.
- Enterprise edition features that were described in the *Cisco IOS Desktop Switching Enterprise Edition Software Configuration Guide* are now included in the *Cisco IOS Desktop Switching Software Configuration Guide*.
- In the *Catalyst 3500 Series XL Hardware Installation Guide*, there are references to the Cisco RPS 300. The Cisco RPS 300, which supports the Catalyst 3524-PWR XL switch, will be available in late 2000.
- In the *Catalyst 3500 Series XL Hardware Installation Guide*, there are references to the Cisco IP Phone 7940 and Cisco IP Phone 7910. These phones were not available at the time of this publishing. Check with your Cisco sales representative or go to the Cisco Architecture for Voice, Video and Integrated Data (AVVID) web site.
- The RJ-45-to-DB-9 female DTE (labeled PC) adapter is now the only adapter that ships with the switches. Disregard the text in the documentation that refer to the DB-45-to-DB-25 female DTE adapter. You can order a kit (part number ACS-DSBUASYN=) containing the terminal adapter from Cisco.

Setting Up the Catalyst 2900 XL Initial Configuration

The procedure for setting up the initial configuration on the Catalyst 2900 XL switches, as described in the *Catalyst 2900 Series XL Installation Guide*, has been updated. Follow these steps to create an initial configuration for the switch:

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, and allows spaces but ignores leading spaces.

Enter enable secret: *secret_password*

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

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



Note

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

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

Enter Telnet password: *telnet_password*

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



Note

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

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

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

Enter cluster name: *cls_name*



Note

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

Step 12 The initial configuration is displayed:

The following configuration command script was created:

```
ip subnet-zero
interface VLAN1
ip address 172.20.153.36 255.255.255.0
ip default-gateway 172.20.153.01
hostname host_name
enable secret 5 $1$M3pS$cXtAlkyR3/6Cn8/
line vty 0 15
password telnet_password
snmp community private rw
snmp community public ro
cluster enable cls_name

end
```

Step 13 Verify that the information is correct.

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

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

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

- Command-line interface (CLI)
- Cluster Management Suite from your browser

Browser Support

You can access the web-based interfaces through the browsers listed in Table 1. The switch checks the browser version when starting a session to ensure that the browser is supported. If the browser is not supported, the switch displays an error message, and the session does not start.

Table 1 *Browser Support*

Operating System	Minimum Operating System Requirements	Netscape Communicator	Microsoft Internet Explorer
Windows 95	Service Pack 1	4.61, 4.7	4.01a or 5.0
Windows 98	Second Edition	4.61, 4.7	4.01a or 5.0
Windows NT 4.0	Service Pack 3	4.61, 4.7	4.01a or 5.0
Solaris 2.5.1 or higher	SUN-recommended patch cluster for the OS and Motif library patch 103461-24	4.61, 4.7	Not supported

Netscape Communicator version 4.60 is *not* supported.

To use the CMS, complete the browser-configuration instructions described in the *Cisco IOS Desktop Switching Software Configuration Guide*.

Creating Clusters with Different Releases of IOS Software

Some versions of the 2900 and 3500 XL 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 operating with the same level of software, we recommend that you upgrade all cluster switches to Release 12.0(5)X or later. Table 2 lists the available versions of clustering software and their capabilities.

If you have a cluster with switches that are running two different versions of IOS software, changes that have been made to the latest release might not be reflected on switches running the older version. For example, if you start 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 2 *Cluster Software Caveats*

IOS Release	Cluster Status	Caveats
Release 12.0(5)XP and earlier	Member switch	Features introduced with Release 12.0(5)XU, such as VLAN Trunk Protocol (VTP) pruning, appear as read-only.
Release 12.0(5)XP and earlier	Command switch	A 1000BaseT module installed in a switch running Release 12.0(5)XU does not display in Cluster Manager or VSM.
Release 11.2(8)SA6	Member switch	Features introduced with Release 12.0(5)XU, such as VTP pruning, appear as read-only.
Release 11.2(8)SA5 and earlier	Edge device	No clustering capabilities.

Creating Clusters with Catalyst 1900 and 2820 Switches

Catalyst 1900 and 2820 switches are always member switches. However, a cluster with a command switch running Release 11.2(8)SA6 cannot respond to a Catalyst 1900 or 2820. This means that, if the command switch is running Release 11.2(8)SA6, the Cluster Management Suite (CMS) does not support a Catalyst 1900 or 2820 switch in the following CMS features:

- Visual Switch Manager
- Device report
- Link graph
- Bandwidth graph

Configuring Voice Ports to Carry Voice and Data Traffic on Different VLANs

The Cisco 7960 IP Phone contains an integrated 3-port 10/100 switch that can connect to a PC or other device. You can configure a switch port to instruct the phone to forward voice and data traffic on different virtual LANs (VLANs).

In the following configuration, data traffic is carried by VLAN 1, and voice traffic is carried by VLAN 2. In this configuration, all IP phones and other voice-related devices must be connected to switch ports that belong to VLAN 2.

Beginning in privileged EXEC mode, follow these steps to configure a port to receive voice and data from an IP phone in different VLANs:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface</i>	Enter interface configuration mode, and enter the port to be configured.
Step 3	switchport priority default (0)	Assign an IEEE 802.1p priority to untagged traffic that is received on the switch port. The phone forwards this traffic through the native VLAN, VLAN 1.
Step 4	switchport voice vlan (2)	Instruct the IP phone to forward all voice traffic through VLAN 2. The IP phone forwards the traffic with an 802.1p priority of 5.
Step 5	end	Return to privileged EXEC mode.
Step 6	show interface <i>interface</i> switchport	Verify the configuration of the port.

Hardware and Supporting Software

Table 3 lists the Catalyst 3500 XL switches supported by this IOS release, and Table 4 lists the 8-MB Catalyst 2900 XL switches supported by this IOS release. Table 5 lists the Catalyst 2900 and 3500 XL modules and Gigabit Interface converters and the minimum release of IOS required to support them.


Note

Some Catalyst 2900 and 3500 XL modules require a combination of hardware and software to support Inter-Switch Link (ISL) and IEEE 802.1Q trunking. These combinations are shown in Table 5.

Catalyst 2900 series XL 4-MB switches run original edition software and are not supported in this release. These switches cannot be updated to Release 12.0(5.0)XU.

Table 3 Catalyst 3500 Series XL Switches

Switch	Description	Number of VLANs
Catalyst 3508G XL	8 gigabit module slots	250
Catalyst 3512 XL	12 autosensing 10/100 ports and 2 gigabit module slots	250
Catalyst 3524 XL	24 autosensing 10/100 ports and 2 gigabit module slots	250
Catalyst 3524-PWR XL	24 autosensing 10/100 inline-power ports and 2 gigabit module slots	250
Catalyst 3548 XL	48 autosensing 10/100 ports and 2 gigabit module slots	250

Table 4 8-MB Catalyst 2900 Series XL Switches

Switch	Description	Number of VLANs
Catalyst 2912MF XL	12 100BaseFX ports and 2 high-speed expansion slots	250
Catalyst 2912 XL	12 autosensing 10/100 ports	64
Catalyst 2924M XL	24 autosensing 10/100 ports and 2 high-speed expansion slots	250
Catalyst 2924M DC XL	24 autosensing 10/100 ports and 2 high-speed expansion slots (DC power)	250
Catalyst 2924 XL	24 autosensing 10/100 ports	64
Catalyst 2924C XL	22 autosensing 10/100 ports and 2 100BaseFX ports	64

New Supported Hardware

- The Catalyst 2924M XL DC switch, equipped with an on-board direct-current (DC) power converter on its back panel, is designed for DC-powered network environments.
- The Catalyst 3524-PWR XL switch provides inline power to the Cisco IP Phone 7960. No phone adapters are required when connecting this phone to the 10/100 ports on this switch. This switch is designed for IP networks that support both data and voice traffic.

Changes Since Release 12.0(5.1)XP

This section describes new hardware and software features and other changes that were implemented in Release 12.0(5)XU.

New Features

The following new features were added in Release 12.0(5)XU:

- Cluster Management Suite (CMS) has been enhanced and supports most device-management tasks from within Cluster Manager. You can select and configure ports from more than one switch, and you can configure most features without displaying Visual Switch Manager (VSM).
- The Hot Standby Router Protocol (HSRP) can supply command-switch redundancy when you create a standby group and bind it to the command switch. One switch in the group is designated as the standby command switch. It can automatically become the command switch if the active command switch fails. Other switches in the group are ranked in order of their suitability and can become the standby command switch if necessary.
- VLAN Trunk Protocol (VTP) pruning can eliminate the unnecessary flooding of traffic over trunks within a VTP domain. This default activity is disabled by VTP pruning, and you can define the VLANs to be pruned by entering them in the pruning-eligible list.
- A 2900 or 3500 XL switch running Release 12.0(5)XU can connect to a Cisco 7960 IP Phone and carry IP voice traffic. If necessary, the Catalyst 3524-PWR XL can supply inline power to the circuit connecting it to the Cisco 7960 IP Phone.
- You can change the management VLAN for the entire cluster by using CMS or the command switch command-line interface (CLI).
- By default, a cluster can discover candidate switches up to three hops from the command switch. You can configure the command switch to discover candidates up to seven hops from the cluster.
- The private VLAN edge feature can prevent the forwarding of traffic between ports on the same switch. When private VLAN edge is enabled, there is no forwarding of unicast, broadcast, or multicast traffic between ports on a switch, and all traffic between ports on the switch must be forwarded through a router or other Layer 3 device.
- Spanning Tree Protocol (STP) root guard prevents switches on customer premises from becoming an STP root switch in a service provider network. You configure root guard by enabling it on an interface connecting to another switch. If it appears that the connected switch is going to become a root switch, the port is blocked, and STP reconfigures and selects a new root switch.
- Unidirectional link detection (UDLD) support on all Ethernet ports can prevent unidirectional links.

Minimum IOS Release for Major Features

Table 5 lists the minimum IOS release required to support the major features of the Catalyst 2900 and 3500 XL switches.

Table 5 *Catalyst 2900 and 3500 Series XL Features and the Minimum IOS Release Required*

Feature	Minimum Release Required
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
Hot Standby Router Protocol (HSRP)	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 Trunk 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
RMON support through the 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
Catalyst 3500 series XL switches (except 3548 XL)	Release 11.2(8)SA6
Catalyst 3548 XL switch	Release 12.0(5)XP
Cluster management	Release 11.2(8)SA6
Terminal Access Control Access Server+ (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 “Hardware and Supporting Software” section on page 9)	Release 11.2(8)SA6
Catalyst 2900 series XL 1000BaseX modules	Release 11.2(8)SA5
Catalyst 2900 series XL ATM modules	Release 11.2(8)SA5
VLAN Management Policy Server (VMPS)	Release 11.2(8)SA4 (Enterprise Edition Software)
8192 MAC addresses on modular switches	Release 11.2(8)SA4
Inter-Switch Link (ISL) trunking	Release 11.2(8)SA4 (Enterprise Edition Software)
IEEE 802.1Q trunking	Release 11.2(8)SA5 (Enterprise Edition Software)
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

Limitations and Restrictions

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

Connecting to the Catalyst 3524-PWR XL 10/100 Inline-Power Ports

**Caution**

It takes a Catalyst 3524-PWR XL 10/100 port 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. Failure to do so can result in damage to that network device.

Connecting to the 600W Cisco Redundant Power System

The Cisco 600W Redundant Power System (RPS), which supports all Catalyst 2900 and 3500 XL switches other than the Catalyst 3524-PWR XL switch, can provide a quasi-redundant power source for four external devices that use up to 150W DC each. You can use a one-to-one cable (one connector at each cable end) to connect four external devices to the four DC output power modules. The power source is quasi-redundant because there are two AC input power modules for the Cisco RPS and one DC output power module for each external device. The AC input to the Cisco RPS is fully redundant, but the DC output to the external devices is not.

The following restrictions apply to using the 600W Cisco Redundant Power System (RPS) with a Catalyst 2900 or 3500 XL switch:

- The Catalyst 3524-PWR XL switch is not supported by the 600W RPS. It is supported by the Cisco RPS 300.
- The switches *do not* support the fully-redundant configuration with the Cisco 600W RPS, as described in the *Cisco Redundant Power System Hardware Installation Guide*.
- We recommend that you do not use the redundant-with-reboot configuration with the switch connected to the RPS and to the AC power plug, due to the reboot and downtime—approximately 30 seconds. If you do use the redundant with reboot configuration, always power up the switch before you power up the RPS to ensure correct operation. When the RPS powers up first, the LEDs might not indicate the actual state.
- If you are using an RPS with a revision level lower than Z3 with a Catalyst 3508G or a Catalyst 3548 XL switch, the RPS output connector DC status LED and the switch RPS LED might display amber (normally indicating an RPS malfunction) even when the RPS is functioning properly. The LEDs display correctly for RPS revision level Z3 or later. The label on the bottom of the RPS shows the revision level.

Connecting to the Cisco RPS 300

The Cisco RPS 300 Redundant Power System supports the Catalyst 3524-PWR XL switch. This RPS is not available at this time but will be available in late 2000.

Connecting to PCs, Terminals, and Modems

You can connect the switch to a PC by means of the switch console port and the supplied rollover cable and 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=) containing this RJ-45-to-DB-25 female DTE adapter from Cisco.

Port Configuration Conflicts

Certain combinations of port features create configuration conflicts (see Table 6). For example, the network port floods all unknown unicast and multicast packets to a port; therefore, port security, which limits traffic on a port, cannot be enabled on the network port. If you try to enable incompatible features, VSM issues a warning message and prevents you from making the change. Reload the page to refresh VSM.

In Table 6, *No* means that the two referenced features are not compatible.

Table 6 Port Configuration Conflicts

	ATM Port ¹	Port Group	Port Security	Monitor Port	Multi-VLAN Port	Network Port	Connect to Cluster?	Private VLAN edge
ATM port	–	No	No	No	No	No	Yes	No
Port group	No	–	No	No	Yes	Yes ²	Yes	Yes
Port security	No	No	–	No	No	No	Yes	Yes
Monitor port	No ³	No	No	–	No	No	Yes	Yes
Multi-VLAN port	No	Yes	No	No	–	Yes	Yes	Yes
Network port	No	Yes (only source-based group)	No	No	Yes	–	No ⁴	Yes
Connect to Cluster	Yes	Yes	Yes	Yes	Yes	No	–	Yes
Private VLAN edge	No	Yes	Yes	Yes ⁵	Yes	No	Yes	–

1. Catalyst 2900 series XL switches only.
2. A network port cannot connect cluster members to the command switch.
3. An ATM port cannot be a monitor port, but it can be monitored.
4. A network port cannot connect cluster members to the command switch.
5. Switch Port Analyzer (SPAN) can operate only if the monitor port or the port being monitored is not a protected port.

Using Commas in CMS

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

Spanning-Tree Maximum Age Command

The range of seconds for the **span-tree max-age** command is now 6 to 200 seconds. If you used this command in a release before 11.2(8)SA6 to set a value greater than this new range and then 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.

SPAN Limitations

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

Compatibility with the CiscoWorks2000 RME Suite

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

- Catalyst 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.

Upgrading to a New Software Release

This section describes the procedure for upgrading your switch software.



The 4-MB Catalyst 2900 series XL switches do not have sufficient memory to be upgraded to this release.



Before upgrading your switch to Release 12.0(5.2)XU, read this section for important information.

Upgrading a Switch by Using VSM or Cluster Manager

If your switch is running Release 11.2(8)SA3, SA4, or SA5, we recommend that you upgrade the switch software by using the web-based VSM. If you are upgrading a switch running Release 11.2(8)SA6 or Release 12.0(5)XP to the current release, we recommend that you use Cluster Manager.

If you are using VSM to upgrade a switch running Release 11.2(8)SA6 or Release 12.0(5)XP, follow the procedure in the “Using VSM to Upgrade a Switch” section on page 16.

General instructions for upgrading switch software are included in the *Cisco IOS Desktop Switching Software Configuration Guide*; detailed instructions are provided in the online help files.



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.

Using VSM to Upgrade a Switch



Note

If you use VSM to upgrade your switch from Release 11.2(8)SA6 or Release 12.0(5)XP to the current release, you must rename the image file to ensure that you can reload the software. You can rename the image file by accessing the CLI through Telnet or by connecting to the switch console port.



Tips

If your switch is not configured for Telnet, follow the procedure described in the “Configuring the Switch for Telnet” section in the *Cisco IOS Desktop Switching Software Configuration Guide*.

You do not need to perform this procedure if you are using Cluster Manager to upgrade from Release 11.2(8)SA6 or Release 12.0(5)XP. Also, this issue does not apply to the current release of IOS. Follow these steps to rename the image file by using the CLI, and then upgrade the software by using VSM:

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 the following command:

```
server% telnet switch_ip_address
```

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

Step 2 Enter privileged EXEC mode:

```
switch> enable
switch#
```

Enter the password if you are prompted to do so.

Step 3 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     90815  Dec 10 1999 19:27:54  c3500XL-diag-mz-120.5.1-XP
 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  c3500XL-c3h2s-mz-120.0.0.4-XU.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 4 Rename the image file to **boot.bin**:

```
switch# rename flash:c3500XL-c3h2s-mz-120.0.0.4-XU.bin flash:boot.bin
```

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

Step 5 Start VSM as usual and display the System Configuration page by selecting **System>System Configuration** from the menu bar.

- Step 6** In the **Cisco IOS Image File** field, enter **boot.bin**.
- Step 7** Select the **Retain Current IOS Image File Name** check box.
- Step 8** Complete the other fields on the page as described in the “Reloading and Upgrading the Switch Software” section of the *Cisco IOS Desktop Switching Software Configuration Guide*.
- Step 9** Click **Upgrade IOS Software and Visual Switch Manager**.
- Step 10** Verify the upgrade by displaying the contents of Flash memory. The file **boot.bin** should be present:

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

   2  -rwx          4484   Mar 05 1993 00:31:09  vlan.dat
   3  -rwx         90815   Dec 10 1999 19:27:54  c3500XL-diag-mz-120.5.1-XP
   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 11** Verify that the switch reloads correctly by displaying the boot variable. It should also be **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 the procedure described in “Using VSM to Upgrade a Switch” is not followed, 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.

In the event of a failure, 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 the last two steps in the procedure described in the “Using VSM to Upgrade a Switch” section.

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** command in global configuration mode. 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 “Upgrading a Switch by Using the CLI” section.

Upgrading a Switch by Using the CLI

The CLI upgrade procedure consists of the following major steps:

1. Downloading the combined .tar file from CCO, as described in “Downloading the New Software” section on page 19. This file contains the IOS image and the HTML files. The **tar** command extracts the IOS image and the HTML files from the combined .tar file during the TFTP copy to the switch.
2. Downloading the TFTP server application to copy the switch software from your PC to the switch, if necessary.
3. Using the CLI to upgrade your switch or cluster to the new software.

Which Files to Use

Table 7 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.

The software files for this IOS release are listed by switch in Table 8 and Table 9.

Table 7 Possible Extensions for IOS Software Files

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

Table 8 Catalyst 2900 Series XL Cisco IOS Software Files

Filename	Description
c2900XL-c3h2s-mz-120.5.2-XU.bin	IOS image-only file
c2900XL-c3h2s-mz-120.5.2-XU.tar	IOS image and HTML files
c2900XL-html-plus.120.5.2-XU.tar	HTML files

Table 9 Catalyst 3500 Series XL Cisco IOS Software Files

Filename	Description
c3500XL-c3h2s-mz-120.5.2-XU.bin	IOS image file
c3500XL-c3h2s-mz-120.5.2-XU.tar	IOS image file and HTML files
c3500XL-html-plus.120.5.2-XU.tar	HTML files

Downloading the New Software

Follow these steps to download a new version of Release 12.0(5.2)XU software and, if necessary, the TFTP server application.

Step 1 Use Table 7 to Table 9 to identify the files that you want to download.



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.

Step 2 Download the files from the following location:

If you have a SmartNet support contract, log in to one of the following 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, download the appropriate files from one of the following URLs:

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

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

Step 3 Download the TFTP server from this URL, if necessary. The readme.txt file describes how to download the TFTP server.

After you have downloaded the correct files to your PC or workstation, you can use the CLI to perform a TFTP transfer of the file or files to the switch.

Upgrading Catalyst 3500 Series XL Switches

This procedure is only 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.

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. 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 file 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-c3h2s-mz-112.8.2-SA6.bin flash:c3500XL-120.5.2-XU.bin
```

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

```
switch# dir flash:
Directory of flash:
-rwx1557283Aug 17 1999 23:47:28c3500XL-120.5.2-XU.bin
-rwx82475Aug 17 1999 03:10:38c3500XL-diag-mz-120.5.2-XU
-drwx14144Aug 17 1999 00:04:14html
-rwx2047Mar 01 1993 18:46:01config.text
-rwx43Jan 01 1970 00:00:34env_vars

3612672 bytes total (1224704 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** 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# boot system flash:c3500XL-120.5.2-XU.bin
```



**Note**

If you have not entered the **boot** command with the name of the image, 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 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 (110 bytes)
extracting c3500XL-120.5.2-XU.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.

---

## Upgrading 8-MB Catalyst 2900 Series XL Switches

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.

**Note**

---

If you want to copy the IOS image file or HTML files separately to the switch, refer to the Catalyst 2900 series XL release notes for Release 11.2(8)SA4 on CCO.

---

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. 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 6** 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-h2-mz-112.8.2.11-SA6.bin* is your image file.

```
switch# dir flash:
Directory of flash:
 3 ---x80971Sept 14 1998 03:10:38 c2900XL-h2-mz-112.8.2.11-SA6.bin
 4 d--x14144Mar 26 1993 23:17:47 html
 7 -rwx84Mar 26 1993 23:12:21 env_vars
 5 ---x111Mar 26 1993 23:12:23 info
258 ---x111Mar 26 1993 23:17:47 info.ver
230 -rwx1470Mar 26 1993 23:18:53 config.text

3612672 bytes total (1229312 bytes free)
```

- Step 7** 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-120.5.2-XU.bin
Source filename [c2900XL-h2-mz-112.8.2-SA6.bin]?
Destination filename [c2900XL-120.5-XU.bin]?
```

- 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** 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# boot system flash:c2900XL-120.5.2-XU.bin
```



**Note**

---

If you did not previously enter the **boot** command with the name of the image, 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.

- 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-120.5.2-XU.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 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.

# Current Caveats

This section describes possible unexpected activity by Release 12.0(5.2)XU.

- 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 indicates that the plug-in and Java are enabled, but Internet Explorer crashes.

The workaround for this caveat is to not disable Java plug-ins on the Java Plug-In Control Panel. (CSCdp67822)

- You can be prompted twice for the enable password if you use the Domain Name Server (DNS) name instead of the IP address to access a cluster. This can happen if you access a cluster by using the DNS name and then start Visual Switch Manager from Cluster Builder. When you return to Cluster Builder, you are prompted a second time for the password.

The workaround for this caveat is to always use the IP address when starting the Cluster Management Suite. (CSCdp69639)

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

The workaround is to right-click again on the device until the pop-up menu displays correctly. (CSCdp61365)

- A cluster command switch running Release 11.2(8)SA6 might show a link indication for a blocked port.

The workaround for this caveat is to upgrade the command switch to Release 12.0(5)XU or later. (CSCdp70754)

- 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 use the Set Daylight Saving Time and Set Current Time tabs.

To avoid a possible conflict, either set the system time for the entire cluster on the command switch, or configure NTP on the command switch to use an NTP server to provide time to the cluster. Do not use both methods at the same time. (CSCdp82224)

- You can use Cluster Manager to configure an Hot Standby Redundancy Protocol (HSRP) standby group and bind it to a cluster. However, you cannot use Cluster Manager to configure more than one standby group. If you want to configure more than one standby group, use the CLI. (CSCdp82354)

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

The workaround for this caveat is to not use flow control on the console port (CSCdm24487).

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

The workaround for this caveat is to not change the management VLAN to a VLAN where a member is configured as part of a standby group. (CSCdp70389)

- Root guard is inconsistent when configured on a port that is in the STP blocked state at the time of configuration. (CSCdp85954)
- Do not assign a member number of 0 to a switch that is running software other than Release 12.0(5)XU or later. (CSCdp79992)

- HSRP does not support entering a virtual MAC address or a built-in address (BIA) for a cluster. (CSCdp49419).
- All members of an HSRP standby group must be cluster members. (CSCdp97517)
- If a non-private VLAN edge port is configured to monitor (SPAN) a private VLAN edge port, the SPAN port will capture monitored traffic from the private VLAN edge port to other private VLAN edge ports. This happens even though the monitored private VLAN edge port is not forwarding traffic to other private VLAN edge ports. In effect, the SPAN port captures incorrect traffic.  
The workaround is to not monitor private VLAN edge ports. (CSCdp84267)
- If storm control filter is enabled for unicast, multicast, or broadcast traffic and the rising threshold is reached, all traffic on the port is filtered. No unicast, multicast, or broadcast traffic is forwarded from the port. (CSCdp30543)
- Cisco IOS does perform some checks on entered IP addresses. For example, it does not allow the broadcast address to be entered. However, it does not check for the broadcast address on the same subnet as the HSRP VIP or the management VLAN IP address. This means that you could configure HSRP with a virtual IP address that is the same as the broadcast address of the network. (CSCdp87748)
- If you use the command switch DNS name to start CMS for a member that is running an earlier software release, CMS might not display an image of the switch, or it might display an image of the command switch. This can also occur when a standby group is configured for a cluster and you access CMS by entering the command switch IP address and not the virtual IP address.  
The workaround is to always use the IP address of the command switch to access CMS. If a standby group is configured for a cluster, always use the virtual IP address to access CMS. (CSCdp75220)
- CMS can behave unexpectedly if host names or DNS names that it processes contain commas. This means that host names or DNS 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 names in CMS. (CSCdp85928)
- If you click on the list of switches in CMS and press Page Down, the entire list moves to the bottom of the window. This only happens with Windows NT.  
The workaround is to collapse the list into a single icon. This returns the list to the top of the window. (CSCdp62807)
- In VSM, you cannot see the individual menu items when you right-click on the chassis image to display the device pop-up menu.  
The workaround is to right-click on another part of the chassis image to display the device pop-up menu. (CSCdp89945)
- When STP Port Fast or STP root guard are configured on a module port, the configuration is not saved after the module is removed and reinserted. These features need to be reconfigured on the module ports after the module is reinserted. (CSCdr04281)

# Syslog Error Messages

The following messages can appear in the command-line interface (CLI).

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Message     | LINK_FLAP, RTD, LOG_ALERT, 0, "%s link down/up %d times per min                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Explanation | An excessive number of link down-up events has been noticed on this interface. This might be the result of reconfiguring the port, or it might indicate a faulty device at the other end of the connection.                                                                                                                                                                                                                                                                                     |
| Action      | If someone is reconfiguring the interface or device at the other side of the interface, ignore this message. However, if no one is manipulating the interface or device at the other end of the interface, then it is likely that the Ethernet transceiver at one end of the link is faulty and should be replaced.                                                                                                                                                                             |
| Message     | ADDR_FLAP, RTD, LOG_ALERT, 0, "%s relearning %d addrs per min                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Explanation | Normally, MAC addresses are learned once on a port. Occasionally, when a switched network reconfigures, due to either manual or STP reconfiguration, addresses learned on one port are relearned on a different port. However, if there is a port anywhere in the switched domain that is looped back to itself, addresses will jump back and forth between the real port and the port that is in the path to the looped back port.                                                             |
| Action      | Determine the real path (port) to the MAC address. Use <b>debug ethernet-controller addr</b> to see the alternate path-port on which the address is being learned. Go to the switch attached to that port. Note that <b>show cdp neighbors</b> is useful in determining the next switch. Repeat this procedure until the port is found that is receiving what it is transmitting, and remove that port from the network.                                                                        |
| Message     | DEAD_PHY, RTD, LOG_ALERT, 0, "The PHY on %s is dead                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Explanation | The runtime diagnostic code is no longer able to communicate with the PHY for this interface. This is most likely due to an electrostatic discharge (ESD) event.                                                                                                                                                                                                                                                                                                                                |
| Action      | Return Material Authorization (RMA) the switch or module containing the malfunctioning ports.                                                                                                                                                                                                                                                                                                                                                                                                   |
| Notes       | The real danger is not dead ports, but the live ports associated with dead ports. Fast Ethernet ports are deployed eight per controller. This controller provides the MII bus for the PHYs for those ports: eight singles, two quads, or one octal, and DE believes that the dead PHYs can degrade the signals on this bus, thus providing erratic behavior on the remaining live ports. DE has seen one-way link and packets reflected back to itself, but cannot yet definitively prove this. |
| Message     | MAC_TBL_SIZE, MODULES, LOG_ERR, 0,                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Explanation | Dynamic module insertion has smaller MAC addresses supported.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Action      | Reboot system to use the module.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Message     | SECURITYREJECT, PORT_SECURITY, LOG_CRIT, 0,                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Explanation | A packet with unexpected source address is received on a secure port.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Action      | Remove the station with the unexpected MAC address from the secure port, or add the MAC address to the secure address table of the secure port.                                                                                                                                                                                                                                                                                                                                                 |

|             |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Message     | SHUTDOWN, STORM_CONTROL, LOG_CRIT, 0,                                                                                                                                                                                                                                                                                                                                                                           |
| Explanation | Excessive traffic has been detected on a port that has been configured to be shut down if a storm event is detected.                                                                                                                                                                                                                                                                                            |
| Action      | Once the source of the packet storm has been fixed, re-enable the port by using port-configuration commands.                                                                                                                                                                                                                                                                                                    |
| Message     | BLADE_EXTRACT, CHASSIS, LOG_NOTICE, 0,                                                                                                                                                                                                                                                                                                                                                                          |
| Explanation | The hot-swap switch has been depressed.                                                                                                                                                                                                                                                                                                                                                                         |
| Action      | Extract the module.                                                                                                                                                                                                                                                                                                                                                                                             |
| Message     | LOOP_DETECTED, GIGASTACK, LOG_INFO, 0, Gigastack GBIC in %s is selected as Master Loop Breaker.                                                                                                                                                                                                                                                                                                                 |
| Explanation | Loop is detected in the Gigastack and this Gigastack (Gigabit Interface Converter) GBIC is selected as the Master Loop Breaker. Link 2 of this Gigastack GBIC is disabled to break the loop.                                                                                                                                                                                                                    |
| Action      | –                                                                                                                                                                                                                                                                                                                                                                                                               |
| Message     | LOOP_BROKEN, GIGASTACK, LOG_INFO, 0, Link loss is detected in the Gigastack loop                                                                                                                                                                                                                                                                                                                                |
| Explanation | Loop formed by Gigastack modules is broken because of link loss. Link 2 of the Master Loop Breaker is re-enabled to replace the broken line.                                                                                                                                                                                                                                                                    |
| Action      | –                                                                                                                                                                                                                                                                                                                                                                                                               |
| Message     | NO_LOOP_DETECT, GIGASTACK, LOG_ALERT, 0, The link neighbor of link %d of Gigastack                                                                                                                                                                                                                                                                                                                              |
| Explanation | No acknowledgement for Gigastack loop detection request is received from one of the links on a Gigastack GBIC. Either the neighboring switch does not support the Gigastack Loop breaking algorithm, or the link between the two Gigastack GBICs is broken. Under this condition, a Gigastack loop topology is not be automatically detected, and the connectivity between switches in the stack could be lost. |
| Action      | If loop topology is used in the Gigastack, make sure the latest software is running on all switches in the stack. Check the Gigastack GBICs involved to make sure they are functioning.                                                                                                                                                                                                                         |
| Message     | ADD, CMP, LOG_NOTICE, 0, The Device is added to the cluster (Cluster Name:%s, CMDR IP Address %i)                                                                                                                                                                                                                                                                                                               |
| Explanation | The device is added to the cluster.                                                                                                                                                                                                                                                                                                                                                                             |
| Action      | No action is required.                                                                                                                                                                                                                                                                                                                                                                                          |
| Message     | REMOVE, CMP, LOG_NOTICE, 0, The Device is removed from the cluster (Cluster Name:%s)                                                                                                                                                                                                                                                                                                                            |
| Explanation | The device is removed from the cluster.                                                                                                                                                                                                                                                                                                                                                                         |
| Action      | No action is required.                                                                                                                                                                                                                                                                                                                                                                                          |

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Message     | MEMBER_CONFIG_UPDATE, CMP, LOG_NOTICE, 0, Received member configuration from member %d                                                                                                                                                                                                                                                                                                                                            |
| Explanation | Received member configuration.                                                                                                                                                                                                                                                                                                                                                                                                    |
| Action      | No action is required.                                                                                                                                                                                                                                                                                                                                                                                                            |
| Message     | FAN_FAULT, ENVIRONMENT, LOG_CRIT, 0,                                                                                                                                                                                                                                                                                                                                                                                              |
| Explanation | An internal fan fault is detected. This message is available only on the Catalyst 3524-PWR XL switch.                                                                                                                                                                                                                                                                                                                             |
| Action      | Either check the switch itself or use the <b>show env</b> command to check if a fan on the switch has failed. The Catalyst 3524-PWR XL switch can operate normally with one failed fan. Replace the switch at your convenience.                                                                                                                                                                                                   |
| Message     | OVER_TEMP, ENVIRONMENT, LOG_CRIT, 0,                                                                                                                                                                                                                                                                                                                                                                                              |
| Explanation | An overtemperature condition is detected. This message is available only on the Catalyst 3524-PWR XL switch.                                                                                                                                                                                                                                                                                                                      |
| Action      | <ul style="list-style-type: none"><li>• Use the <b>show env</b> command to check if an overtemperature condition exists. If it does:<ul style="list-style-type: none"><li>– Place the switch in an environment that is within 32 to 113°F (0 to 45°C).</li><li>– Make sure fan intake and exhaust areas are clear.</li></ul></li><li>• If a multiple-fan failure is causing the switch to overheat, replace the switch.</li></ul> |

## Related Documentation

The product documentation for the 3500 and 2900 XL switches and modules is as follows:

*Quick Start Guide: Catalyst 2900 Series XL Switches*

*Quick Start Guide: Catalyst 3500 Series XL Switches*

*Catalyst 2900 Series XL Installation Guide*

*Catalyst 3500 Series XL Hardware Installation Guide*

*Cisco IOS Desktop Switching Software Configuration Guide for Cisco IOS Software Release 12.0(5)XU*

*Cisco IOS Desktop Command Reference (online only)*

*Using the Catalyst 2924M XL DC Ethernet Switch*

*Catalyst 2900 Series XL Modules Installation Guide*

*Catalyst 2900 Series XL Gigabit Ethernet Module Installation Guide*

*Catalyst 2900 Series XL ATM Modules Installation and Configuration Guide*

*Release Notes for the Catalyst 2900 Series XL ATM Modules*

*Catalyst GigaStack Gigabit Interface Converter Hardware Installation Guide*

*Release Notes for Catalyst GigaStack Gigabit Interface Converter*

## Obtaining Documentation

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

### Documentation CD-ROM

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

### Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at <http://www.cisco.com/cgi-bin/subcat/kaojump.cgi>.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

# Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

## Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online 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.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, 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 CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: [www.cisco.com](http://www.cisco.com)
- Telnet: [cco.cisco.com](http://cco.cisco.com)
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to [cco-team@cisco.com](mailto:cco-team@cisco.com).

## Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use [www.cisco.com/techsupport](http://www.cisco.com/techsupport).

To contact by e-mail, use one of the following:

| Language         | E-mail Address        |
|------------------|-----------------------|
| English          | tac@cisco.com         |
| Hanzi (Chinese)  | chinese-tac@cisco.com |
| Kanji (Japanese) | japan-tac@cisco.com   |
| Hangul (Korean)  | korea-tac@cisco.com   |
| Spanish          | tac@cisco.com         |
| Thai             | thai-tac@cisco.com    |

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site:  
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

## 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 and value your comments.

---

This document is to be used in conjunction with the document listed in the “Related Documentation” section.

Access Registrar, AccessPath, Any to Any, Are You Ready, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, IQ Breakthrough, IQ Expertise, IQ FastTrack, IQ Readiness Scorecard, The IQ Logo, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, *The Cell*, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and Aironet, ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, CollisionFree, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document 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. (0005R)

Copyright © 2000, Cisco Systems, Inc.  
 All rights reserved.