



# Release Notes for the Catalyst 2918 Switch, Cisco IOS Release 12.2(55)SE and Later

---

Revised May 20, 2011

These release notes include important information about Cisco IOS Release 12.2(55)SE and any limitations, restrictions, and caveats that apply to this release. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the “[Finding the Software Version and Feature Set](#)” section on page 3.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the “[Deciding Which Files to Use](#)” section on page 4.

You can download the switch software from this site (registered Cisco.com users with a login password): [http://www.cisco.com/web/CN/products/products\\_netsol/switches/products/ca2918/download.html](http://www.cisco.com/web/CN/products/products_netsol/switches/products/ca2918/download.html)

## Contents

- [System Requirements](#), page 2
- [Upgrading the Switch Software](#), page 3
- [Installation Notes](#), page 6
- [New Software Features](#), page 6
- [Limitations and Restrictions](#), page 7
- [Important Notes](#), page 11
- [Open Caveats](#), page 13
- [Resolved Caveats](#), page 16
- [Documentation Updates](#), page 17
- [Related Documentation](#), page 23
- [Obtaining Documentation and Submitting a Service Request](#), page 24



---

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

© 2010 Cisco Systems, Inc. All rights reserved.

# System Requirements

- [Supported Hardware, page 2](#)
- [Device Manager System Requirements, page 2](#)
- [Cluster Compatibility, page 3](#)
- [Upgrading the Switch Software, page 3](#)

## Supported Hardware

**Table 1** Catalyst 2918 Switch Supported Hardware

Switch	Description
Catalyst 2918-24TT	24 10/100 BASE-TX Ethernet ports and 2 10/100/1000BASE-T copper ports
Catalyst 2918-24TC	24 10/100BASE-TX Ethernet ports and 2 dual-purpose uplinks <sup>1</sup> (two 10/100/1000BASE-T copper ports and two SFP <sup>2</sup> module slots)
Catalyst 2918-48TT	48 10/100 BASE-TX Ethernet ports and 2 10/100/1000BASE-T copper uplink ports
Catalyst 2918-48TC	48 10/100BASE-TX Ethernet ports and 2 dual-purpose ports
SFP modules	1000Base-LX/LH, -SX, 100Base-FX

1. Each uplink port is considered a single interface with dual front ends (RJ-45 connector and SFP module slot). The dual front ends are not redundant interfaces, and only one port of the pair is active.
2. SFP = small form-factor pluggable.

## Device Manager System Requirements

These sections describes the hardware and software requirements for using the device manager:

- [Hardware Requirements, page 2](#)
- [Software Requirements, page 3](#)

## Hardware Requirements

**Table 2** Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Intel Pentium II <sup>1</sup>	64 MB <sup>2</sup>	256	1024 x 768	Small

1. We recommend Intel Pentium 4.
2. We recommend 256-MB DRAM.

## Software Requirements

- Windows 2000, XP, Vista, and Windows Server 2003.
- Internet Explorer 5.5, 6.0, 7.0, Firefox 1.5, 2.0 or later.

The device manager verifies the browser version when starting a session, and it does not require a plug-in.

## Cluster Compatibility

You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the command-line interface (CLI).

When creating a switch cluster or adding a switch to a cluster, follow these guidelines:

- When you create a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a Catalyst 2918 switch, all standby command switches must be Catalyst 2918 switches.

For additional information about clustering, see the software configuration guide and the command reference.

## Upgrading the Switch Software

- [Finding the Software Version and Feature Set, page 3](#)
- [Deciding Which Files to Use, page 4](#)
- [Upgrading a Switch by Using the Device Manager, page 4](#)
- [Upgrading a Switch by Using the CLI, page 5](#)
- [Recovering from a Software Failure, page 6](#)

## Finding the Software Version and Feature Set

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

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.

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

## Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file and the files needed for the embedded device manager. You must use the combined tar file to upgrade the switch through the device manager. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

These are the Cisco IOS Software image files for the Catalyst 2918 switch:

c2918-lanlitek9-tar.122-55.SE.tar	Catalyst 2918 cryptographic image file and device manager files. This image has the Kerberos and SSH features.
-----------------------------------	--

## Archiving Software Images

Before upgrading your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:

[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod\\_bulletin0900aec80281c0e.html](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aec80281c0e.html)

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.



**Note**

Although you can copy any file on the flash memory to the TFTP server, it is time consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from Cisco.com and archive it on an internal host in your network.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the “Basic File Transfer Services Commands” section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*:

[http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf\\_t1.html](http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html)

## Upgrading a Switch by Using the Device Manager

You can upgrade switch software by using the device manager. For detailed instructions, click **Help**.



**Note**

When using the device manager to upgrade your switch, do not use or close your browser session after the upgrade process begins. Wait until after the upgrade process completes.

## Upgrading a Switch by Using the CLI

This procedure is for copying the combined tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, follow these steps:

- 
- Step 1** Identify the file that you want to download.
- Step 2** Download the software image file. If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:

[http://www.cisco.com/web/CN/products/products\\_netsol/switches/products/ca2918/download.html](http://www.cisco.com/web/CN/products/products_netsol/switches/products/ca2918/download.html)

To download the image for a Catalyst 2918 switch, click **Catalyst 2918 software**.

- Step 3** Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

For more information, see Appendix B in the software configuration guide for this release.

- Step 4** Log into the switch through the console port or a Telnet session.

- Step 5** (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
Switch# ping tftp-server-address
```

For more information about assigning an IP address and default gateway to the switch, see the software configuration guide for this release.

- Step 6** Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

```
Switch# archive download-sw /overwrite /reload
tftp: [ [//location]/directory]/image-name.tar
```

The **/overwrite** option overwrites the software image in flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

For *//location*, specify the IP address of the TFTP server.

For */directory/image-name.tar*, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://198.30.20.19/c2918-lanlite-tar.122-46.SE.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

---

## Recovering from a Software Failure

For recovery procedures, see the “Troubleshooting” chapter in the software configuration guide for this release.

## Installation Notes

You can assign IP information to your switch by using these methods:

- The Express Setup program, as described in the switch getting started guide.
- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the switch software configuration guide.

## New Software Features

- AutoSmartport enhancements, which add support for global macros, last-resort macros, event trigger control, access points, EtherChannels, auto-QoS with Cisco Medianet, and IP phones.
- Support for CDP and LLDP enhancements for exchanging location information with video end points for dynamic location-based content distribution from servers.
- Smart Install enhancements t supporting client backup files, zero-touch replacement for clients with the same product-ID, automatic generation of the image list file, configurable file repository, hostname changes, transparent connection of the director to client, USB storage for image and seed configuration, and changes in **show** command outputs.
- Memory consistency check routines to detect and correct invalid ternary content addressable memory (TCAM) table entries.
- An option to suppress verbose 802.1x, authentication manager, and MAC authentication bypass syslog messages.
- Support for QoS class-default policy placement.
- Support for LLPD-MED and DHCP snooping with Option 82.
- Support for increasing the NVRAM buffer size for saving large configuration files.
- ARP tracking probe enhancement to specify a source IP address for a VLAN.
- Network Edge Access Topology (NEAT) controls the supplicant port during the supplicant authentication period. When you connect a supplicant switch to the authenticator switch, the authenticator port could be error-disabled when receiving Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) packets and the supplicant switch is not authenticated. The NEAT feature is now enhanced to block the supplicant port during authentication, to ensure authentication completes.

Use the **dot1x supplicant controlled transient** global configuration command to *control* access to the supplicant port during authentication. Use the **no** form of this command to *provide* access to the supplicant port during the authentication period.

# Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

## Cisco IOS Limitations

- [“Configuration” section on page 7](#)
- [“Ethernet” section on page 8](#)
- [“IP Telephony” section on page 9](#)
- [“Smart Install” section on page 9](#)
- [“SPAN” section on page 10](#)
- [“Trunking” section on page 10](#)
- [“VLAN” section on page 10](#)

## Configuration

- A static IP address might be removed when the previously acquired DHCP IP address lease expires. This problem occurs under these conditions:
  - When the switch is booted up without a configuration (no config.text file in flash memory).
  - When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
  - When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

The workaround is to reconfigure the static IP address. (CSCe71176 and CSCdz11708)

- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mb/s full duplex or 100 Mb/s half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames.

The workaround is to configure the port for 10 Mb/s and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)

- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked

The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)

- A traceback error occurs if a crypto key is generated after an SSL client session.

There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. (CSCef59331)

- When the **logging event-spanning-tree** interface configuration command is configured and logging to the console is enabled, a topology change might generate a large number of logging messages, causing high CPU utilization. CPU utilization can increase with the number of spanning-tree instances and the number of interfaces configured with the **logging event-spanning-tree** interface configuration command. This condition adversely affects how the switch operates and could cause problems such as STP convergence delay.

High CPU utilization can also occur with other conditions, such as when debug messages are logged at a high rate to the console.

Use one of these workarounds:

- Disable logging to the console.
- Rate-limit logging messages to the console.

Remove the **logging event spanning-tree** interface configuration command from the interfaces. (CSCsg91027)

- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module. The workaround is to configure aggressive UDLD. (CSCsh70244).
- When you enter the **boot host retry timeout** global configuration command to specify the amount of time that the client should keep trying to download the configuration and you do not enter a timeout value, the default value is zero, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.

The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout** *timeout-value* command. (CSCsk65142)

- If you configure a large number of input interface VLANs in a class map, a traceback message similar to this might appear:

```
01:01:32: %BIT-4-OUTOFRANGE: bit 1321 is not in the expected range of 0 to 1024
```

There is no impact to switch functionality.

There is no workaround. (CSCtg32101)

## Ethernet

- Traffic on EtherChannel ports is not perfectly load-balanced. Egress traffic on EtherChannel ports are distributed to member ports on load balance configuration and traffic characteristics like MAC or IP address. More than one traffic stream may map to same member ports based on hashing results calculated by the ASIC.

If this happens, uneven traffic distribution will happen on EtherChannel ports.

Changing the load balance distribution method or changing the number of ports in the EtherChannel can resolve this problem. Use any of these workarounds to improve EtherChannel load balancing:

- for random source-ip and dest-ip traffic, configure load balance method as **src-dst-ip**
- for incrementing source-ip traffic, configure load balance method as **src-ip**
- for incrementing dest-ip traffic, configure load balance method as **dst-ip**
- Configure the number of ports in the EtherChannel so that the number is equal to a power of 2 (i.e. 2, 4, or 8)

For example, with load balance configured as **dst-ip** with 150 distinct incrementing destination IP addresses, and the number of ports in the EtherChannel set to either 2, 4, or 8, load distribution is optimal.(CSCeh81991)

## IP Telephony

- Some access point devices are incorrectly discovered as IEEE 802.3af Class 1 devices. These access points should be discovered as Cisco pre-standard devices. The show power inline user EXEC command shows the access point as an IEEE Class 1 device. The workaround is to power the access point by using an AC wall adaptor. (CSCin69533)
- After you change the access VLAN on a port that has IEEE 802.1x enabled, the IP phone address is removed. Because learning is restricted on IEEE 802.1x-capable ports, it takes approximately 30 seconds before the address is relearned. No workaround is necessary. (CSCea85312)
- The Cisco 7905 IP Phone is error-disabled when the phone is connected to wall power. The workaround is to enable PoE and to configure the switch to recover from the PoE error-disabled state. (CSCsf32300)

## Smart Install

- When upgrading switches in a stack, the director cannot send the correct image and configuration to the stack if all switches in the stack do not start at the same time. A switch in the stack could then receive an incorrect image or configuration.

The workaround is to use an on-demand upgrade to upgrade switches in a stack by entering the **vstack download config** and **vstack download image** commands. (CSCta64962)

- When you upgrade a Smart Install director to Cisco IOS Release 12.2(55)SE but do not upgrade the director configuration, the director cannot upgrade client switches.

When you upgrade the director to Cisco IOS Release 12.2(55)SE, the workaround is to also modify the configuration to include all built-in, custom, and default groups. You should also configure the tar image name instead of the image-list file name in the stored images. (CSCte07949)

- Backing up a Smart Install configuration could fail if the backup repository is a Windows server and the backup file already exists in the server.

The workaround is to use the TFTP utility of another server instead of a Windows server or to manually delete the existing backup file before backing up again. (CSCte53737)

- In a Smart Install network with the backup feature enabled (the default), the director sends the backup configuration file to the client during zero-touch replacement. However, when the client is a switch in a stack, the client receives the seed file from the director instead of receiving the backup configuration file.

The workaround, if you need to configure a switch in a stack with the backup configuration, is to use the **vstack download config** privileged EXEC command so that the director performs an on-demand upgrade on the client.

- When the backup configuration is stored in a remote repository, enter the location of the repository.
- When the backup file is stored in the director flash memory, you must manually set the permissions for the file before you enter the **vstack download config** command. (CSCtf18775)

## SPAN

- Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session *session\_number* destination {interface *interface-id* encapsulation replicate}** global configuration command for local SPAN. (CSCed24036)

## Trunking

- The switch treats frames received with mixed encapsulation (IEEE 802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and the port LED blinks amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an IEEE 802.1Q trunk interface. There is no workaround. (CSCdz33708)
- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y. There is no workaround. (CSCdz42909).
- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics. There is no workaround. (CSCec35100).

## VLAN

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.  
The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)
- When line rate traffic is passing through a dynamic port, and you enter the **switchport access vlan dynamic** interface configuration command for a range of ports, the VLANs might not be assigned correctly. One or more VLANs with a null ID appears in the MAC address table instead.  
The workaround is to enter the **switchport access vlan dynamic** interface configuration command separately on each port. (CSCsi26392)

## Device Manager Limitations

- When you are prompted to accept the security certificate and you click *No*, you only see a blank screen, and the device manager does not launch.  
The workaround is to click *Yes* when you are prompted to accept the certificate. (CSCef45718)

## Important Notes

- [Cisco IOS Notes, page 11](#)
- [Device Manager Notes, page 11](#)

### Cisco IOS Notes

- If the switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

```
00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not responding.
```

If this message appears, check that there is network connectivity between the switch and the ACS. You should also check that the switch has been properly configured as an AAA client on the ACS.

### Device Manager Notes

- When you launch Express Setup, you are prompted for the switch password. Enter the default password, *cisco*. The switch ignores text in the username field. Before you complete and exit Express Setup, you must change the password from the default password, *cisco*.
- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI.
- When the switch is running a localized version of the device manager, the switch displays settings and status only in English letters. Input entries on the switch can only be in English letters.
- For device manager sessions on Internet Explorer, popup messages in simplified Chinese can appear as garbled text. These messages appear properly if your operating system is Chinese.
- We recommend this browser setting to speed up the time needed to display the device manager from Microsoft Internet Explorer.

From Microsoft Internet Explorer:

1. Choose **Tools > Internet Options**.
  2. Click **Settings** in the “Temporary Internet files” area.
  3. From the Settings window, choose **Automatically**.
  4. Click **OK**.
  5. Click **OK** to exit the Internet Options window.
- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

If you are *not* using the default method of authentication (the enable password), you need to configure the HTTP server interface with the method of authentication used on the switch

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip http authentication {aaa   enable   local}</code>	Configure the HTTP server interface for the type of authentication that you want to use. <ul style="list-style-type: none"> <li>• <b>aaa</b>—Enable the authentication, authorization, and accounting feature. You must enter the <b>aaa new-model</b> interface configuration command for the <b>aaa</b> keyword to appear.</li> <li>• <b>enable</b>—Enable password, which is the default method of HTTP server user authentication, is used.</li> <li>• <b>local</b>—Local user database, as defined on the Cisco router or access server, is used.</li> </ul>
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show running-config</code>	Verify your entries.

- The device manager uses the HTTP protocol (the default is port 80) and the default method of authentication (the enable password) to communicate with the switch through any of its Ethernet ports and to allow switch management from a standard web browser.

If you change the HTTP port, you must include the new port number when you enter the IP address in the browser **Location** or **Address** field (for example, `http://10.1.126.45:184` where 184 is the new HTTP port number). You should write down the port number through which you are connected. Use care when changing the switch IP information.

If you are *not* using the default method of authentication (the enable password), you need to configure the HTTP server interface with the method of authentication used on the switch.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip http authentication {enable   local   tacacs}</code>	Configure the HTTP server interface for the type of authentication that you want to use. <ul style="list-style-type: none"> <li>• <b>enable</b>—Enable password, which is the default method of HTTP server user authentication, is used.</li> <li>• <b>local</b>—Local user database, as defined on the Cisco router or access server, is used.</li> <li>• <b>tacacs</b>—TACACS server is used.</li> </ul>
Step 3	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show running-config</code>	Verify your entries.

- If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, `www.cisco.com:84`), you must enter `http://` as the URL prefix. Otherwise, you cannot launch the device manager.

# Open Caveats

- CSCte99366

In a Smart Install network, when the director is connected between the client and the DHCP server and the server has options configured for image and configuration, then the client does not receive the image and configuration files sent by the DHCP server during an automatic upgrade. Instead the files are overwritten by the director and the client receives the image and configuration that the director sends.

Use one of these workarounds:

- If client needs to upgrade using an image and configuration file configured in the DHCP server options, you should remove the client from the Smart Install network during the upgrade.
- In a network using Smart Install, you should not configure options for image and configuration in the DHCP server. For clients to upgrade using Smart Install, you should configure product-id specific image and configuration files in the director.

- CSCtg71149

When ports in an EtherChannel are linking up, the message `EC-5-CANNOT_BUNDLE2` might appear. This condition is often self-correcting, indicated by the appearance of `EC-5-COMPATIBLE` message following the first message. On occasion, the issue does not self-correct, and the ports may remain unbundled.

The workaround is to reload the switch or to restore the EtherChannel bundle by shutting down and then enabling the member ports and the EtherChannel in this order:

- Enter the **shutdown** interface configuration command on each member port.
- Enter the **shutdown** command on the port-channel interface.
- Enter the **no shutdown** command on each member port.
- Enter the **no shutdown** command on the port-channel interface.

- CSCtg98656

If the director in the Smart Install network is located between an access point and the DHCP server, the access point tries to use the Smart Install feature to upgrade even though access points are not supported devices. The upgrade fails because the director does not have an image and configuration file for the access point.

There is no workaround.

- CSCth35152

When a Smart Install director is upgrading a client switch that is not Smart Install-capable (that is, not running Cisco IOS Release 12.2(52)SE or later), the director must enter the password configured on the client switch. If the client switch does not have a configured password, there are unexpected results depending on the software release running on the client:

- When you select the NONE option in the director CLI, the upgrade should be allowed and is successful on client switches running Cisco IOS Release 12.2(25)SE through 12.2(46)SE, but fails on clients running Cisco IOS Release 12.2(50)SE through 12.2(50)SEx.
- When you enter any password in the director CLI, the upgrade should not be allowed, but it is successful on client switches running Cisco IOS Release 12.2(25)SE through 12.2(46)SE, but fails on clients running Cisco IOS Release 12.2(50)SE through 12.2(50)SEx.

There is no workaround.

- CSCtj03875  
When you disconnect the spanning tree protocol (STP) peer link, the STP port path cost configuration changes.  
There is no workaround.
- CSCtj86299  
If a static MAC address entry is configured for an IP address in the global routing table, ping requests are sent through the global context, and replies are sent through Virtual Routing and Forwarding (VRF). This is a VRF leak.  
The workaround is to remove the static MAC address entry.
- CSCtj88307  
When you enter the **default interface, switchport, or no switchport** interface configuration command on the switch, this message appears: *EMAC phy access error, port 0, retrying.....*  
There is no workaround.
- CSCtk00846  
If Auto Smartports macros are configured, access points with the AIR-CAP prefix are not detected.  
The workaround is to manually configure the access point port.
- CSCtl51859  
Neighbor discovery fails for IPv6 hosts connected to the switch when the IPv6 MLD snooping feature is enabled globally on the switch.  
The workaround is to disable IPv6 MLD snooping on the switch.
- CSCto00947  
If more than one host is authenticated in the multiple authentication mode, the source IP addresses of the dynamic authorization policies are not translated and the policies that are applied to one host affect all the hosts. For example:  

```
Cat3560X-auth# show ip access-lists int g0/1
permit ip any any
permit ip host 192.168.0.11 any
```

  
The source IP address `permit ip any any` is not translated. The source IP address `permit ip host 192.168.0.11 any` is translated.  
There is no workaround.
- CSCto06796  
When you disable an interface and configure voice and data on the same VLAN and enable the interface:
  - It causes a security violation but voice and data is authorized.
  - The configuration for the data VLAN policy changes after authentication. Use the `show run interface interface configuration` command to see this.
When you configure voice and data on the same VLAN on an enabled interface, it causes a security violation and an error message is displayed.  
In both cases the workaround is to configure voice and data on separate VLANs.

- CSCto55124

When a member switch port security is used with port-based dot1x authentication and the switch MAC address is sticky, a connected device authenticates itself. Its MAC address is added as sticky in the switch configuration and in the port security tables of the stack switches. When the switch is shut down, the device MAC address is removed from the master switch, but it is retained in the member switch security tables. When the interface is re-enabled, the device MAC address is restored to the master switch configuration.

The workaround is to use port security without dot1x authentication.

- CSCto67688

If a member switch does not have an access control list (ACL) and is running an Enforcement Policy Module (EPM) session, the client on that interface is re-authorized each time that the switch reloads.

The workaround is to configure an ACL on the interface.

- CSCto99322

If the switch is in multidomain authorization (MDA) mode and it receives three or more MAC addresses simultaneously or if the switch is in single-host mode and it receives two or more MAC addresses simultaneously, a security violation trap occurs in the **shutdown** and **protect** violation modes.

The workaround is to connect one device at a time.

- CSCtq01883

If you have configured web authentication on a switch stack as the fallback method and the stack elects a new stack master, the default access control entry (ACE) in the access control list (ACL) changes from implicit deny (auth-default-ACL) to implicit permit (auth-default-ACL-open) even if the port is in closed authentication mode.

The workaround is to enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command to re-enable the interface.

- CSCtq06316

If you configure multidomain authentication (MDA) with Open1x authentication and the **restrict** violation mode, a security violation occurs if the MAC address on the voice LAN is the last MAC address that the switch receives. However, the MAC address is added to the table as a dynamic MAC address and the connected data VLANs continue to access the interface.

The workaround is to connect the voice device first.

- CSCtq06842

In the multidomain authentication (MDA) mode, if you configure the **network-policy profile** global configuration command and you remove a voice VLAN at the interface level after authentication, tracebacks and error messages are generated.

There is no workaround.

- CSCtq07102

If the switch sends untagged and non-CDP traffic in the single-host or multiple-hosts mode after the phone configuration is removed and the Cisco Discovery Protocol (CDP) cache on the switch is cleared, the CDP bypass feature does not work.

The work around is to enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command to restart the interface.

## Resolved Caveats

- [Caveats Resolved in Cisco IOS Release 12.2\(55\)SE3, page 16](#)
- [Caveats Resolved in Cisco IOS Release 12.2\(55\)SE, page 16](#)

### Caveats Resolved in Cisco IOS Release 12.2(55)SE3

- CSCto46868

If you configure multidomain authentication (MDA) with Open1x authentication and the **restrict** violation mode, only two MAC addresses are allowed to access the interface. A security violation occurs when a third MAC address on a voice VLAN tries to access the interface. The voice VLAN is not authenticated, and a syslog message is generated. However, the MAC address is not removed from the voice VLAN because Open1x authentication is configured. If you have authorized the voice VLAN with a policy, such as a dynamic VLAN, the policy is not applied.

The workaround is to not configure a voice VLAN on the phone.

### Caveats Resolved in Cisco IOS Release 12.2(55)SE

- CSCsu31853

The buffer space of a switch running TCP applications is full while the TCP sessions are in the TIME\_WAIT state. Buffer space becomes available after the TCP session the closed.

There is no workaround.

- CSCsz18634

On a switch running Cisco IOS release 12.2(46)SE, the output of the **show interfaces** privileged EXEC command shows 0 packets for port channel input and output rates.

The workaround is to reload the switch by entering the **reload** privileged EXEC command.

- CSCtc02635

On switches running Cisco IOS release 12.2(50)SE3 running MAC authentication bypass with multidomain authentication (MDA, IP phones connected to a port might not be able to regain network connectivity in the VOICE domain if the session times out and all RADIUS servers are unreachable.

There is no workaround.

- CSCtg47738

This error message is displayed after copying a configuration file to the running configuration file fails:

```
%Error opening system:/running-config (No such file or directory)
```

The output of the **dir system:/** EXEC command also does not show a running configuration file.

The workaround is to reload the switch.

# Documentation Updates

- [Updates to the Software Configuration Guide, page 17](#)
- [Updates to the System Message Guide, page 18](#)

## Updates to the Software Configuration Guide

In the “Configuring RIP for IPv6” section in the “Configuring IPv6 Unicast Routing” chapter, the task table is incorrect. This is the correct table:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ipv6 router rip <i>name</i></code>	Configure an IPv6 RIP routing process, and enter router configuration mode for the process.
Step 3	<code>maximum-paths <i>number-paths</i></code>	(Optional) Define the maximum number of equal-cost routes that IPv6 RIP can support. The range is from 1 to 32, and the default is 16 routes.
Step 4	<code>exit</code>	Return to global configuration mode.
Step 5	<code>interface <i>interface-id</i></code>	Enter interface configuration mode, and specify the Layer 3 interface to configure.
Step 6	<code>ipv6 rip <i>name</i> enable</code>	Enable the specified IPv6 RIP routing process on the interface.
Step 7	<code>ipv6 rip <i>name</i> default-information { only   originate }</code>	<p>(Optional) Originate the IPv6 default route (::/0) into the RIP routing process updates sent from the specified interface.</p> <p><b>Note</b> To avoid routing loops after the IPv6 default route (::/0) is originated from any interface, the routing process ignores all default routes received on any interface.</p> <ul style="list-style-type: none"> <li>• <b>only</b>—Select to originate the default route, but suppress all other routes in the updates sent on this interface.</li> <li>• <b>originate</b>—Select to originate the default route in addition to all other routes in the updates sent on this interface.</li> </ul>
Step 8	<code>end</code>	Return to privileged EXEC mode.
Step 9	<code>show ipv6 rip [<i>name</i>] [<i>database</i>] [<i>next-hops</i>]</code> or <code>show ipv6 route rip [<i>updated</i>]</code>	<p>Display information about IPv6 RIP processes.</p> <p>Display the contents of the IPv6 routing table.</p>
Step 10	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

# Updates to the System Message Guide

## New System Messages

**Error Message** AUTHMGR-5-SECURITY\_VIOLATION: Security violation on the interface [chars], new MAC address ([enet]) is seen. AuditSessionID [chars]

**Explanation** A host on the interface attempted to gain access to the network or attempted an authentication. The interface mode does not support the number of hosts that are attached to the interface. This is a security violation, and the interface has been error-disabled. The first [chars] is the interface, [enet] is the Ethernet address of the host, and the second [chars] is the session ID.

**Recommended Action** Make sure that the interface is configured to support the number of hosts that are attached to it. Enter the **shutdown** interface configuration command followed by **no shutdown** interface configuration command to restart the interface.

**Error Message** AUTHMGR-5-VLANASSIGN: VLAN [dec] assigned to Interface [chars] AuditSessionID [chars]

**Explanation** A VLAN was assigned. [dec] is the VLAN ID, the first [chars] is the interface, and the second [chars] is the session ID.

**Recommended Action** No action is required.

**Error Message** AUTHMGR-7-FAILOVER: Failing over from [chars] for client ([chars]) on Interface [chars] AuditSessionID [chars]

**Explanation** The authorization manager is failing over from the current authentication method to another method. The first [chars] is the current authentication method, the second [chars] is the client ID, the third [chars] is the interface, and the fourth [chars] is the session ID.

**Recommended Action** No action is required.

**Error Message** AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client ([chars]) on Interface [chars] AuditSessionID [chars]

**Explanation** All available authentication methods have been tried for the client, but authentication has failed. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

**Recommended Action** No action is required. If local authorization has been configured, the port will be authorized based on the local authorization method. Otherwise, authentication will restart according to the configured reauthentication period.

**Error Message** AUTHMGR-7-RESULT: Authentication result [chars] from [chars] for client [chars] on Interface [chars] AuditSessionID [chars]

**Explanation** The results of the authentication. The first [chars] is the status of the authentication, the second [chars] is the authentication method, the third [chars] is the client ID, the fourth [chars] is the interface, and the fifth [chars] is the session ID.

**Recommended Action** No action is required.

**Error Message** DOT1X-5-FAIL: Authentication failed for client ([chars]) on Interface [chars] AuditSessionID [chars]

**Explanation** The authentication was unsuccessful. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

**Recommended Action** No action is required.

**Error Message** DOT1X-4-MEM\_UNAVAIL: Memory was not available to perform the 802.1X action. AuditSessionID [chars]

**Explanation** The system memory is not sufficient to perform the IEEE 802.1x authentication. [chars] is the session ID.

**Recommended Action** Reduce other system activity to reduce memory demands.

**Error Message** DOT1X-5-SUCCESS: Authentication successful for client ([chars]) on Interface [chars] AuditSessionID [chars]

**Explanation** Authentication was successful. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

**Recommended Action** No action is required.

**Error Message** DOT1X\_SWITCH-5-ERR\_ADDING\_ADDRESS: Unable to add address [enet] on [chars] AuditSessionID [chars]

**Explanation** The client MAC address could not be added to the MAC address table because the hardware memory is full or the address is a secure address on another port. This message might appear if IEEE 802.1x is enabled. [enet] is the client MAC address, the first [chars] is the interface, and the second [chars] is the session ID.

**Recommended Action** If the hardware memory is full, remove some of the dynamic MAC addresses. If the client address is on another port, remove it from that port.

**Error Message** EPM-6-AUTH\_ACL: POLICY [chars]| EVENT [chars]

**Explanation** The switch has sent or received a download request for a downloadable ACL (dACL). The first [chars] is the dACL policy? The second [chars] is the event.

**Recommended Action** No action is required.

**Error Message** HARDWARE-1-TCAM\_ERROR: [traceback] Found error in [chars] TCAM Space and not able to recover the error

**Explanation** The switch cannot fix a ternary content addressable memory (TCAM) integrity error. [chars] is memory location with the error: Unassigned TCAM Space, HFTM TCAM Space (the ASIC forwarding TCAM manager space), or HQATM TCAM Space (the TCAM ASIC quality of service [QoS] and access control list [ACL] TCAM manager space).

**Recommended Action** Restart the switch.

**Error Message** HARDWARE-3-ASICNUM\_ERROR: [traceback] Port-ASIC number [dec] is invalid

**Explanation** The port ASIC number is invalid. [dec] is the port ASIC number.

**Recommended Action** Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

**Error Message** HARDWARE-3-PORTNUM\_ERROR: [traceback] port number [dec] is invalid

**Explanation** The port number is out of range. [dec] is the port number.

**Recommended Action** Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

## Modified System Messages

**Error Message** DOT1X-5-RESULT\_OVERRIDE: Authentication result overridden for client ([chars]) on Interface [chars] AuditSessionID [chars]

**Explanation** The authentication result was overridden. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

**Recommended Action** No action is required.

**Error Message** DOT1X\_SWITCH-5-ERR\_SPAN\_DST\_PORT: Attempt to assign VLAN [dec] to 802.1x port [chars], which is configured as a SPAN destination AuditSessionID [chars]

**Explanation** An attempt was made to assign a VLAN to an 802.1x port that is configured as a Switched Port Analyzer (SPAN) destination port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

**Recommended Action** Change the SPAN configuration so that the port is no longer a SPAN destination port, or change the configuration so that no VLAN is assigned.

**Error Message** DOT1X\_SWITCH-5-ERR\_VLAN\_EQ\_MDA\_INACTIVE: Multi-Domain Authentication cannot activate because Data and Voice VLANs are the same on port AuditSessionID [chars]

**Explanation** Multi-Domain Authentication (MDA) host mode cannot start when the configured data VLAN on a port is the same as the voice VLAN. [chars] is the port session ID.

**Recommended Action** Change either the voice VLAN or the access VLAN on the interface so that they are not the same. MDA then starts.

**Error Message** DOT1X\_SWITCH-5-ERR\_VLAN\_EQ\_VVLAN: Data VLAN [dec] on port [chars] cannot be equivalent to the Voice VLAN AuditSessionID [chars]

**Explanation** An attempt was made to assign a data VLAN to an 802.1x port that is the same as the voice VLAN. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

**Recommended Action** Change either the voice VLAN or the 802.1x-assigned VLAN on the interface so that they are not the same.

**Error Message** DOT1X\_SWITCH-5-ERR\_VLAN\_INTERNAL: Attempt to assign internal VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]

**Explanation** An attempt was made to assign an invalid VLAN to an 802.1x port. The VLAN specified is used internally and cannot be assigned to this port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

**Recommended Action** Assign a different VLAN.

**Error Message** DOT1X\_SWITCH-5-ERR\_VLAN\_INVALID: Attempt to assign invalid VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]

**Explanation** An attempt was made to assign an invalid VLAN to an 802.1x port. The VLAN specified is out of range. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

**Recommended Action** Update the configuration to use a valid VLAN.

**Error Message** DOT1X\_SWITCH-5-ERR\_VLAN\_NOT\_FOUND: Attempt to assign non-existent or shutdown VLAN [chars] to 802.1x port [chars] AuditSessionID [chars]

**Explanation** An attempt was made to assign a VLAN to an 802.1x port, but the VLAN was not found in the VLAN Trunking Protocol (VTP) database. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

**Recommended Action** Make sure the VLAN exists and is not shut down, or use another VLAN.

**Error Message** DOT1X\_SWITCH-5-ERR\_VLAN\_ON\_ROUTED\_PORT: Attempt to assign VLAN [dec] to routed 802.1x port [chars] AuditSessionID [chars]

**Explanation** An attempt was made to assign a VLAN to a supplicant on a routed port, which is not allowed. [dec] is the VLAN ID, the first [chars] is the port, and the second [chars] is the session ID.

**Recommended Action** Either disable the VLAN assignment, or change the port type to a nonrouted port.

**Error Message** DOT1X\_SWITCH-5-ERR\_VLAN\_PROMISC\_PORT: Attempt to assign VLAN [dec] to promiscuous 802.1x port [chars] AuditSessionID [chars]

**Explanation** An attempt was made to assign a VLAN to a promiscuous IEEE 802.1x port, which is not allowed. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

**Recommended Action** Change the port mode so that it is no longer a promiscuous port, or change the configuration so that no VLAN is assigned.

**Error Message** DOT1X\_SWITCH-5-ERR\_VLAN\_RESERVED: Attempt to assign reserved VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]

**Explanation** An attempt was made to assign an invalid VLAN to an IEEE 802.1x port. The VLAN specified is a reserved VLAN and cannot be assigned to this port. [dec] is the VLAN, the first [chars] is the port, and the seconds [chars] is the session ID.

**Recommended Action** Assign a different VLAN.

**Error Message** DOT1X\_SWITCH-5-ERR\_VLAN\_RSPAN: Attempt to assign RSPAN VLAN [dec] to 802.1x port [chars]. 802.1x is incompatible with RSPAN AuditSessionID [chars]

**Explanation** Remote SPAN should not be enabled on a VLAN with IEEE 802.1x-enabled. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

**Recommended Action** Either disable remote SPAN configuration on the VLAN, or disable IEEE 802.1x on all the ports in this VLAN.

**Error Message** SPANTREE-2-BLOCK\_BPDUGUARD\_VP: Received BPDU on port [chars], vlan [dec] with BPDU Guard enabled. Disabling vlan.

**Explanation** A BPDU was received on the interface and the VLAN specified in the error message. The spanning tree BPDU guard feature was enabled and configured to shut down the VLAN. As a result, the VLAN was placed in the error-disabled state. [chars] is the interface, and [dec] is the VLAN.

**Recommended Action** Either remove the device sending BPDUs, or disable the BPDU guard feature. The BPDU guard feature can be locally configured on the interface or globally configured on all ports that have Port Fast enabled. Re-enable the interface and vlan by entering the **clear errdisable** privileged EXEC command.

## Deleted System Messages

**Error Message** DOT1X-4-MEM\_UNAVAIL: Memory was not available to perform the 802.1X action.

**Error Message** DOT1X-5-SUCCESS: Authentication successful for client ([chars]) on Interface [chars]

**Error Message** DOT1X\_SWITCH-5-ERR\_ADDING\_ADDRESS: Unable to add address [enet] on [chars]

## Related Documentation

These documents provide complete information about the switch and are available from this Cisco.com site:

[http://www.cisco.com/web/CN/products/products\\_netsol/switches/products/ca2918/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/web/CN/products/products_netsol/switches/products/ca2918/tsd_products_support_series_home.html)

- *Release Notes for the Catalyst 2918 Switch*
- *Catalyst 2918 Switch Software Configuration Guide*
- *Catalyst 2918 Switch Command Reference*
- *Catalyst 2918 Switch System Message Guide*
- *Auto Smartports Configuration Guide*
- *Catalyst 2918 Switch Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 2918 Switch*
- *Cisco Small Form-Factor Pluggable Modules Installation Notes:*  
[http://www.cisco.com/en/US/docs/interfaces\\_modules/transceiver\\_modules/installation/note/78\\_15160.html](http://www.cisco.com/en/US/docs/interfaces_modules/transceiver_modules/installation/note/78_15160.html)

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

---

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned 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. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2010 Cisco Systems, Inc. All rights reserved.