Release Notes for Catalyst 2350 Switch, Cisco IOS Release 12.2(55)SE and Later

Revised June 28, 2013

Cisco IOS Release 12.2(55)SE runs on all Catalyst 2350 switches.

These release notes include important information about Cisco IOS Release 12.2(55)SE and any limitations, restrictions, and caveats that apply to it. 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 4.
- 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/cisco/web/download/index.html

Contents

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

System Requirements

Supported Hardware

Table 1 Supported Hardware

Device	Description	Supported by Minimum Cisco IOS Release
Catalyst 2350-48TD-S	48 10/100/1000 Ethernet ports, 2 10-Gigabit Ethernet X2 module slots, AC power	Cisco IOS Release 12.2(46)EY
Catalyst 2350-48TD-SD	48 10/100/1000 Ethernet ports, 2 10-Gigabit Ethernet X2 module slots, DC power	Cisco IOS Release 12.2(46)EY
Cisco X2 transceiver modules	X2-10GB-SR V02 or later X2-10GB-CX4 V03 or later X2-10GB-LRM	Cisco IOS Release 12.2(46)EY
Cisco TwinGig Converter Module	Dual SFP X2 converter module to allow the switch to support SFP[1] Gigabit Ethernet modules	Cisco IOS Release 12.2(46)EY
SFP modules	1000BASE-SX 1000BASE-T	Cisco IOS Release 12.2(46)EY
DOM[2] support for these SFP modules	X2-10GB-SR X2-10GB-LRM	Cisco IOS Release 12.2(46)EY
SFP module patch cable[3]	CAB-SFP-50CM	Cisco IOS Release 12.2(46)EY
C3K-PWR-265WAC	265-W AC-power-supply module	Cisco IOS Release 12.2(46)EY
C3K-PWR-265WDC	265-W DC-power-supply module	Cisco IOS Release 12.2(46)EY
C3K-BLWR-60CFM	Fan module	Cisco IOS Release 12.2(46)EY

[1] SFP = small form-factor pluggable.

[2] DOM = digital optical monitoring.

[3] The SFP module patch cable is a 0.5-meter, copper, passive cable with SFP module connectors at each end. The patch cable can connect two Catalyst 2350 switches in a cascaded configuration.

Device Manager System Requirements

Hardware

Table 2 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

[1] We recommend 1 GHz.

[2] We recommend 1 GB DRAM.

Software

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

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

Cluster Compatibility

You cannot create and manage switch clusters through the device manager. Use the command-line interface (CLI) or the Network Assistant application.

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

- When you create a switch cluster, we recommend that you configure the highest-end switch in your cluster as the command switch.
- If you are managing the cluster through Network Assistant, configure the switch with the latest software should be 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 2350 switch, all standby command switches must be Catalyst 2350 switches.

For additional information about clustering, see *Getting Started with Cisco Network Assistant* and *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com), the software configuration guide, and the command reference.

CNA Support

Cisco Network Assistant 5.4 and earlier does not provide specific device support for the Catalyst 2350 switch. For more information about Network Assistant, see the *Release Notes for Cisco Network Assistant* on Cisco.com.

Upgrading the Switch Software

- "Finding the Software Version and Feature Set" section on page 4
- "Deciding Which Files to Use" section on page 4

- "Upgrading a Switch by Using the Device Manager or Network Assistant" section on page 5
- "Upgrading a Switch by Using the CLI" section on page 5
- "Recovering from a Software Failure" section on 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.

Table 3 Cisco IOS Software Image Files

Filename	Description
c2350-lanlitek9-tar.122-55.SE.tar	Catalyst 2350 cryptographic image file and device manager files. This image has 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 from 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_bulletin0900aecd80281c0e.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*:
lhttp://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html

Upgrading a Switch by Using the Device Manager or Network Assistant

You can upgrade switch software by using the device manager or Network Assistant. 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 new image file and replace or keep the current image.

Step 1 Use Table 3 on page 4 to identify the file that you want to download.

Step 2 Download the software image file:

a. If you are a registered customer, go to this URL and log in.

http://www.cisco.com/cisco/web/download/index.html

b. Navigate to **Switches** > **LAN Switches - Access**.

c. Navigate to your switch model.

d. Click **IOS Software**, then select the latest IOS release.

e. Download the image you identified in Step 1.

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 a 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/c2350-lanlite-tar.122-46.EY.tar
```

This example shows how to download an image from a TFTP server and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option:

```
Switch# archive download-sw /leave-old-sw
tftp://198.30.20.19/c2350-lanlite-tar.122-46.EY.tar
```

Recovering from a Software Failure

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

New Software Features

- Support for VLAN Trunking Protocol (VTP) version 3.

Configuration Notes

Use these methods to assign IP information to your switch:

- 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.

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

- "Address Resolution Protocol" section on page 7
- "Cisco X2 Transceiver Modules and SFP Modules" section on page 7
- "Configuration" section on page 7
- "Multicasting" section on page 8
- "QoS" section on page 8
- "SPAN and RSPAN" section on page 9

Address Resolution Protocol

- The switch might place a port in an error-disabled state due to an Address Resolution Protocol (ARP) rate limit exception even when the ARP traffic on the port is not exceeding the configured limit. This could happen when the burst interval setting is 1 second, the default.

  The workaround is to set the burst interval to more than 1 second. We recommend setting the burst interval to 3 seconds even if you are not experiencing this problem.(CSCse06827)

Cisco X2 Transceiver Modules and SFP Modules

- When switches are installed closely together and the uplink ports of adjacent switches are in use, you might have problems accessing the SFP module bale-clasp latch to remove the SFP module or the SFP cable (Ethernet or fiber). Use one of these workarounds:
  - Allow space between the switches when installing them.
  - Use long, small screwdriver to access the latch then remove the SFP module and cable. (CSCsd57938)
- When a Cisco X2-10GB-CX4 transceiver module is in the X2 transceiver module port and you enter the **show controllers ethernet-controller tengigabitethernet** privileged EXEC command, the command displays some fields as unspecified. This is the expected behavior based IEEE 802.3ae. (CSCsd47344)

Configuration

- When a switch port configuration is set at 10 Mb/s half duplex, sometimes the port does not send in one direction until the port traffic is stopped and then restarted. You can detect the condition by using the **show controller ethernet-controller** or the **show interfaces** privileged EXEC commands.

  The workaround is to stop the traffic in the direction in which it is not being forwarded, and then restart it after 2 seconds. You can also use the **shutdown** interface configuration command followed by the **no shutdown** command on the interface. (CSCsh04301)
- 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)

- When the configuration file is removed from the switch and the switch is rebooted, port status for VLAN 1 and the management port (Fast Ethernet 0) is sometimes reported as `up` and sometimes as `down`, resulting in conflicts. This status depends on when you respond to the reboot query:

  ```
  Would you like to enter the initial configuration dialog?
  ```

  - After a reboot if you wait until the Line Protocol status of VLAN 1 appears on the console before responding, VLAN 1 line status is always shown as `down`. This is the correct state.
  - The problem (VLAN 1 reporting `up`) occurs if you respond to the query before VLAN 1 line status appears on the console.

  The workaround is to wait for approximately 1 minute after rebooting and until the VLAN 1 interface line status appears on the console before you respond to the query. (CSCsl02680)

Multicasting

- When you configure the **ip igmp max-groups** *number* and **ip igmp max-groups action replace** interface configuration commands and the number of reports exceed the configured max-groups value, the number of groups might temporarily exceed the configured max-groups value. No workaround is necessary because the problem corrects itself when the rate or number of IGMP reports are reduced. (CSCse27757)
- When you configure the IGMP snooping throttle limit by using the **ip igmp max-groups** *number* interface configuration on a port-channel interface, the groups learned on the port-channel might exceed the configured throttle limit number, when all of these conditions are true:
  - The port-channel is configured with member ports across different switches in the stack.
  - When one of the member switches reloads.
  - The member switch that is reloading has a high rate of IP IGMP joins arriving on the port-channel member port.

  The workaround is to disable the IGMP snooping throttle limit by using the **no ip igmp max-groups** *number* interface configuration command and then to reconfigure the same limit again. (CSCse39909)

QoS

- When QoS is enabled and the egress port receives pause frames at the line rate, the port cannot send packets.

  There is no workaround. (CSCeh18677)
- Egress shaped round robin (SRR) sharing weights do not work properly with system jumbo MTU frames.

  There is no workaround. (CSCsc63334)
- In a hierarchical policy map, if the VLAN-level policy map is attached to a VLAN interface and the name of the interface-level policy map is the same as that for another VLAN-level policy map, the switch rejects the configuration, and the VLAN-level policy map is removed from the interface.

  The workaround is to use a different name for the interface-level policy map. (CSCsd84001)
- If the ingress queue has low buffer settings and the switch sends multiple data streams of system jumbo MTU frames at the same time at the line rate, the frames are dropped at the ingress.

  There is no workaround. (CSCsd72001)

- When you use the **srr-queue bandwidth limit** interface configuration command to limit port bandwidth, packets that are less than 256 bytes can cause inaccurate port bandwidth readings. The accuracy is improved when the packet size is greater than 512 bytes. There is no workaround. (CSCsg79627)
- 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)

SPAN and RSPAN

- When egress SPAN is running on a 10-Gigabit Ethernet port, only about 12 percent of the egress traffic is monitored.

  There is no workaround. This is a hardware limitation. (CSCei10129)

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" section on page 9
- "Device Manager Notes" section on page 10

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, make sure that there is network connectivity between the switch and the ACS. You should also make sure that the switch has been properly configured as an AAA client on the ACS.

Device Manager Notes

- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.
- 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	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**aaa** | **enable** | **local**}	Configure the HTTP server interface for the type of authentication that you want to use. • **aaa**—Enable the authentication, authorization, and accounting feature. You must enter the **aaa new-model** interface configuration command for the **aaa** keyword to appear. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	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 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

- 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.

  The workaround is to use port security without dot1x authentication.

- 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 Protcol (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.

- CSCtx73953

A port that is programatically configured with auth-default ACL does not allow any traffic on the switch except DHCP traffic. If the configurations on the interface are cleared and the interface is restarted, the auth-default ACL configuration remains and the problem persists.

There is no workaround.

Resolved Caveats

Caveats Resolved in Cisco IOS Release 12.2(55)SE8

- CSCtf23298

  When a Terminal Access Controller Access Control System (TACACS) server is configured with a single connection, the CPU usage is high.

  The workaround is to remove the single connection option.

- CSCtt19737

  Cisco IOS IP SLAs probes fail because the control message is blocked. The firewalls block the control message when a response packet is not returned to the originating port.

  The workaround is to disable IP SLAs control messages for this probe instance.

- CSCty66157

  The **snmp-server group** command does not associate both IPv6 and IPv4 ACLs simultaneously with an SNMP group.

  The workaround is to use the **snmp-server user** command, which associates both IPv4 and IPv6 ACLs with an SNMP user.

- CSCud79753

  When a switch is configured with Cisco IOS IP SLAs FTP GET operation and if the target file is unavailable, the switch experiences a memory leak and may become unresponsive if it runs out of memory.

  The workaround is to configure the Cisco IOS IP SLAs FTP GET operation only after verifying the availability of the remote target file and setting the permissions for the file, as appropriate. This allows the switch to retrieve the file and not experience a memory leak.

- CSCue07405

When manually running on-demand diagnostic tests on a stack member using the **diagnostic start switch number test all** interface configuration command, the test TestPortAsicRingLoopback fails arbitrarily.

The workaround is to run only the TestPortAsicRingLoopback test (**diagnostic start switch number test 4** interface configuration command) on the stack member. Isolate the stack member and then run the **diagnostic start switch number test all** interface configuration command on the rest of the stack.

Caveats Resolved in Cisco IOS Release 12.2(55)SE7

- CSCtg52885

  The Hot Standby Router Protocol (HSRP) on dot1q sub-interfaces remains in INIT state after a physical link flap on the trunk port.

  The workaround is to enter the **shutdown** and **no shutdown** command on the interface.

- CSCtz96168

  IPv6 packets travel randomly between two isolated ports that are in the same VLAN.

  There is no workaround.

- CSCub92642

  If the switch is configured with Multicast Distributed Switching (MDS), memory leaks if the **multicast-routing distributed** command is toggled repeatedly.

  There is no workaround.

- CSCud17778

  Memory leaks (due to SNMP traps) cause the switch to respond slowly to commands; eventually the switch fails. This is observed when more than one SNMP server host is configured, one of the host broadcasts SNMP traps, or the **snmp-server enable traps snmp authentication coldstart warmstart** command is configured.

  The workaround is to disable the **snmp-server enable traps snmp authentication coldstart warmstart** command and reload the switch.

Caveats Resolved in Cisco IOS Release 12.2(55)SE6

- CSCef01541

  The switch processes data packets that are sent to the network address of an interface if the layer-2 frame encapsulating that packet is specifically crafted to target layer-2 address of the interface or a broadcast layer-2 address.

  The workaround is to use Cisco Express Forwarding (CEF).

- CSCtk18810

  High memory usage is seen with the 'Virtual Exec" process.

  There is no workaround.

- CSCto57723

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a crafted request to an affected device that has the DHCP version 6 (DHCPv6) server feature enabled, causing a reload.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcpv6
- CSCtt31901

  The **sh udld neighbor** command does not work.

  The workaround is to enable the **udld port aggressive** command on the interface level once.
- CSCtw58495

  The switch stops working when you enter the **show epm session summary** privileged EXEC command.

  There is no workaround.
- CSCtx20903

  In a single connection-enabled Terminal Access Controller Access Control System (TACACS) server, when the primary TACACS server goes down , the authentication fallback to the secondary server fails.

  The workaround is to disable the single connection.
- CSCtx61557

  The switch stops working even after a successful 802.1x authentication of the client.

  There is no workaround.
- CSCtx96491

  A port configured and authenticated with 802.1x security may not correctly detect a loop even if the Bridge Protocol Data Unit (BPDU) guard is configured on the interface. This may result in 100 percent CPU utilization because of the Spanning Tree Protocol (STP) process of the switch.

  The workaround is to configure the switch with the **authentication open** or **authentication mac-move permit** command.
- CSCtx99483

  The switch reloads unexpectedly due to segV exception while making PBR configuration changes.

  There is no workaround.
- CSCty93544

  Traffic that should be dropped or denied by an Access Control List (ACL) is permitted by the switch.

  The workaround is to remove and reapply the ACL.
- CSCtz27507

  When a switch is configured for SNMP and receives SNMP packets from an authenticated user, a successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended Denial of Service (DoS) condition.

  There is no workaround.
- CSCtz92782

Advanced Access Control List (dACL) does not get applied to a switch interface configured for Multi-Domain Authentication (MDA).

The workaround is to modify the dACL name and configuration.

- CSCua09639

  ARP is blocked with open authentication-enabled switchports.

  The workaround is to run the command **clear authentication session**.

Caveats Resolved in Cisco IOS Release 12.2(55)SE5

- CSCsy43147

  During a Telnet session, the router crashes when the TACACS+ server is configured or unconfigured (**tacacs-server host** command) using the **single-connection** keyword.

  The workaround is to not use the **single-connection** keyword.

- CSCtb35715

  When you enter the **show running-config** interface configuration command, IP Service Level Agreement notifications are shown as enabled even when you have not enabled this configuration using the **ip sla enable reaction-alerts** interface configuration command.

  There is no workaround.

- CSCtc18841

  If local proxy Address Resolution Protocol (ARP) is configured on the VLAN interface, the ARP entry for the Hot Standby Router Protocol (HSRP) enters into an incomplete state.

  The workaround is to remove the proxy ARP feature on the VLAN interface (by using the **no ip local-proxy-arp** interface configuration command) and restart the interface.

- CSCtg38468

  When AAA authorization is used with TACACS+, an error is displayed if the banner message (**banner exec** global configuration command) starts with a blank character.

  The workaround is to not start the banner message with a blank character.

- CSCth00398

  If the **no vtp** VLAN configuration command is used on a port that receives VTP updates, the switch does not process Layer 2 control traffic (STP and CDP) after some time.

  The workaround is to configure VTP on the port or to not use the **no vtp** command.

- CSCtj89743

  CPU usage is high when a device connected to the switch is accessed using the *https://IP_address* command on the router.

  The workaround is to reload the device.

- CSCtn10697

  The switch crashes when DCHP snooping is enabled with value 125 and an offer packet is received.

  There is no workaround.

- CSCto72927

  If a Tcl policy is copied to the router, the router fails when an event manager policy is configured.

There is no workaround.

- CSCtq09233

  If a CLI configuration text file is copied from a Windows system to the switch, a space is appended to the end of the macro description command when the file is read from the flash of the switch. This leads to errors resulting in high CPU utilization on the switch. Another possible issue is that the macro is not removed when the link goes down or the connected device is removed from the switch.

  The workaround is to copy the configuration file from a non-Windows system (like UNIX or Linux) or convert the file to an appropriate UNIX format before copying.

- CSCtr28857

  A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

- CSCtr91106

  A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS Software are not vulnerable.

  Cisco has released free software updates that address these vulnerabilities.

  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

- CSCts34688

  The switch crashes due to the "HACL Acl Manager" memory fragmentation when a large access control list (ACL) is modified.

  The workaround is add or remove ACE entries in sequential order when the ACL is modified.

- CSCts75641

  Routing Information Protocol (RIP) Version 2 packets egressing an 801.1Q tunnel interface are triplicated.

  There is no workaround.

- CSCtt16051

  Cisco IOS Software contains a vulnerability in the Smart Install feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if the Smart Install feature is enabled. The vulnerability is triggered when an affected device processes a malformed Smart Install message on TCP port 4786.

  Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate this vulnerability.

This advisory is available at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall

- CSCtt37202

  If a client switch is authorized using MAC Authentication Bypass (MAB), and then by using the 802.1x standard and dynamic VLAN assignment, the MAC address of the switch is not updated in the MAC address table of slave switches.

  The workaround is to not use both the 802.1x and dynamic VLAN assignment configurations for the client switch.

- CSCtu17483

  The switch crashes when an IP phone that uses LLDP and authenticates itself using MAC Authentication Bypass (MAB) or 802.1x is physically disconnected and reconnected to the switch port.

  The workaround is to remove the **aaa authorization network default group SG-PBA** global configuration command.

Caveats Resolved in Cisco IOS Release 12.2(55)SE4

- CSCta85026

  The Dynamic Host Configuration Protocol (DHCP) CLI does not accept white spaces in raw ASCII option in the DHCP pool configuration submode. This issue is seen in Cisco IOS Release 12.4(24)T1 and later.

  There is no workaround.

- CSCtg11547

  In a VPN Routing and Forwarding (VRF) aware setup, messages are not sent to the syslog server. This issue applies to Cisco IOS Release 12.2(53)SE and 12.2(53)SE1. This situation does not occur if system logging is configured in the global table.

- CSCth87458

  A memory leak occurs in the SSH process, and user authentication is required.

  The workaround is to allow SSH connections only from trusted hosts.

- CSCti37197

  If a tunnel interface is configured with Cisco Discovery Protocol (CDP), the switch fails when it receives a CDP packet.

  The workaround is to disable CDP on the interface by using the **no cdp enable** interface configuration command.

- CSCtj56719

  The switch fails when the Differentiated Services Code Point (DSCP) mutation name is longer than 25 characters.

  The workaround is to configure DSCP mutation names with fewer than 25 characters.

- 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.
- CSCtl60151

  The switch sometimes reloads after a CPU overload, regardless of the process that is overloading the CPU.

  This problem has been corrected.
- 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.
- CSCtr79386

  The switch fails when DHCP snooping is configured and packet data traffic is excessive. The traffic exhausts the I/O memory and triggers the switch to crash.

  There is no workaround.

Caveats Resolved in Cisco IOS Release 12.2(55)SE3

- CSCto10165

  A vulnerability exists in the Smart Install feature of Cisco Catalyst Switches running Cisco IOS Software that could allow an unauthenticated, remote attacker to perform remote code execution on the affected device.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available to mitigate this vulnerability other than disabling the Smart Install feature.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20110928-smart-install.shtml.
- 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.
- 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.

Caveats Resolved in Cisco IOS Release 12.2(55)SE1

- 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.

Caveats Resolved in Cisco IOS Release 12.2(55)SE

- CSCsg28558

  Cisco X2-10GB-CX4 transceiver modules with a version identification number lower than V03 might be difficult to insert because of a dimensional tolerance discrepancy.

  The workaround is to use modules with a version identification number of V03 or later.

- 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.

- CSCte14603

  A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-igmp.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtf19991

  If the RADIUS authentication server is unavailable and inaccessible authentication bypass is enabled, the switch grants the client access to the network by putting the connected port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN. After the server is available, the client is not reinitalized and moved out of the critical VLAN.

  There is no workaround.

- CSCtf33948

  A PC in 802.1x or multidomain authentication (MDA) mode is connected to an IP phone and connected to a MDA-enabled switch port. After the PC and phone are authenticated on the port, the PC is down. The port does not automatically reauthenticate the PC.

  There is no workaround.

- CSCtf78276

  A switch running Cisco IOS Release 12.2(53)SE1 stops when IEEE 802.1x authentication is enabled.

  The workaround is to apply a VLAN that the RADIUS server assigned to the switch.

- CSCtg26941

  Multidomain authentication (MDA) with guest VLAN or MAC authentication bypass (MAB) as a fallback method is enabled on a switch running Cisco IOS Release 12.2(53)SE. When a non-802.1x client is connected to a IP phone and the phone connected to a switch port shuts down and then restarts, the client MAC address status is *drop* in the MAC address table. It takes 5 minutes for the client to access the network.

  The workaround is to use another software release, such as Cisco IOS Release 12.2(44)SE2.

- 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 VTP Chapter, page 21
- Other Updates to the Software Configuration Guide, page 26
- Updates to the Command Reference, page 27

- Updates for the System Message Guide, page 34
- Update for the Getting Started Guide, page 41

Updates to the Software Configuration Guide VTP Chapter

Cisco IOS Release 12.2(55)SE adds support for VTP version 3, which introduces these changes:

- In VTP versions 1 and 2, the switch must be in VTP transparent mode when you create extended-range VLANs (VLANs 1006 to 4094). VTP version 3 supports extended-range VLANs in client and server modes.
- Support for database propagation of extended range VLANs. VTP versions 1 and 2 propagate only VLANs 1 to 1005. If you configure extended VLANs, you cannot convert from VTP version 3 to version 1 or 2.

Note VTP pruning still applies only to VLANs 1 to 1005, and VLANs 1002 to 1005 are still reserved and cannot be modified.

- In VTP versions 1 and 2, in VTP client mode, VLAN configurations *are not* saved in NVRAM. In VTP version 3, VLAN configurations *are* saved in NVRAM in client mode.
- VTP advertisements: In VTP version 3, VTP advertisements also include the primary server ID, an instance number, and a start index.

  VTP version 3 supports these features that are not supported in versions 1 or 2:

- A switch in VTP **off** mode functions like a VTP transparent switch, except that it does not forward VTP advertisements on trunks.
- Enhanced authentication—You can configure the authentication as **hidden** or **secret**. When **hidden**, the secret key from the password string is saved in the VLAN database file, but it does not appear in plain text in the configuration. Instead, the key associated with the password is saved in hexadecimal format in the running configuration. You must reenter the password if you enter a takeover command in the domain. When you enter the **secret** keyword, you can configure the password secret key.
- Support for any database in a domain. In addition to propagating VTP information, version 3 can propagate Multiple Spanning Tree (MST) Protocol database information. A separate instance of VTP runs for each application that uses VTP.
- VTP primary and secondary servers. A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can back up in NVRAM only the updated VTP configurations received from the primary server.

  By default, all devices come up as secondary servers. You can enter the **vtp primary** privileged EXEC command to specify a primary server. Primary server status is only needed for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers. Primary server status is lost if the device reloads or domain parameters change, even when a password is configured on the switch.
- The option to turn VTP on or off on a per-trunk (per-port) basis. You can enable or disable VTP per port by entering the [**no**] **vtp** interface configuration command. When you disable VTP on trunking ports, all VTP instances for that port are disabled. You cannot disable VTP for the MST database and enable it for the VLAN database on the same port.

Globally setting VTP mode to off applies to all the trunking ports in the system. However, you can specify on or off per-VTP instance. For example, you can configure the switch as a VTP server for the VLAN database but with VTP *off* for the MST database.

VTP v3 Defaults

- VTP version 2 and version 3 are disabled by default.
- VTP mode is the same as VTP version 1 or 2 mode before conversion to VTP 3.
- VTP v3 server type is secondary.

Configuring the VTP Version

Follow these guidelines when deciding which VTP version to implement:

- All switches in a VTP domain must have the same domain name, but they do not need to run the same VTP version.
- Do not enable VTP version 2 on a switch unless all of the switches in the same VTP domain are version-2-capable. When you enable version 2 on a switch, all of the version-2-capable switches in the domain enable version 2. A version 1-only switch does not exchange VTP information with switches that have version 2 enabled.

Caution VTP version 1 and VTP version 2 are not interoperable on switches in the same VTP domain. Do not enable VTP version 2 unless every switch in the VTP domain supports version 2.

- A VTP version 2-capable switch can operate in the same VTP domain as a switch running VTP version 1 if version 2 is disabled on the version 2-capable switch. (Version 2 is disabled by default.)
- If a switch running VTP version 1 but capable of running VTP version 2 receives VTP version 3 advertisements, it automatically moves to VTP version 2.
- If a switch running VTP version 3 is connected to a switch running VTP version 1, the VTP version 1 switch moves to VTP version 2, and the VTP version 3 switch sends scaled-down versions of the VTP packets so that the VTP version 2 switch can update its database.
- A switch running VTP version 3 cannot move to version 1 or 2 if it has extended VLANs.
- We recommend placing VTP version 1 and 2 switches at the edge of the network because they do not forward VTP version 3 advertisements.
- If there are TrBRF and TrCRF Token Ring networks in your environment, you must enable VTP version 2 or version 3 for Token Ring VLAN switching to function properly. To run Token Ring and Token Ring-Net, disable VTP version 2.
- VTP version 1 and version 2 do not propagate configuration information for extended range VLANs (VLANs 1006 to 4094). You must manually configure these VLANs on each device. VTP version 3 supports extended-range VLANs. You cannot convert from VTP version 3 to VTP version 2 if extended VLANs are configured.
- When a VTP version 3 device trunk port receives messages from a VTP version 2 device, it sends a scaled-down version of the VLAN database in VTP version 2 format on that particular trunk. A VTP version 3 device does not send VTP version 2-formatted packets on a trunk unless it first receives VTP version 2 packets on that trunk port.

- When a VTP version 3 device detects a version 2 device on a trunk port, it continues to send version 3 packets in addition to VTP version 2 packets, allowing both kinds of neighbors to co-exist on the same trunk.
- A VTP version 3 device does not accept configuration information from a VTP version 2 or version 1 device.
- Two VTP version 3 regions can communicate only in transparent mode over a VTP version 1 or version 2 region.
- Devices that are only VTP version 1 capable cannot interoperate with VTP version 3 devices.
- When you enable VTP version 2 on a switch, every VTP version 2-capable switch in the VTP domain enables version 2. To enable VTP version 3, you must manually configure it on each switch.
- With VTP versions 1 and 2, you can configure the version only on switches in VTP server or transparent mode. If a switch is running VTP version 3, you can change to version 2 when the switch is in client mode if no extended VLANs exist, no private VLANs exist, and no hidden password was configured.
- VTP version 3 is supported on switches running Cisco IOS Release 12.2(55) SE or later.

⚠

Caution In VTP version 3, both the primary and secondary servers can exist on an instance in the domain.

Beginning in privileged EXEC mode, follow these steps to configure the VTP version:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp version** {**1** | **2** | **3**}	Enable the VTP version on the switch. The default is VTP version 1.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vtp status**	Verify that the configured VTP version is enabled.
Step 5	**copy running-config startup-config**	(Optional) Save the configuration in the startup configuration file.

To return to the default VTP version 1, use the **no vtp version** global configuration command**.**

Configuring the VTP Mode

Beginning in privileged EXEC mode, follow these steps to configure the VTP mode:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp domain** *domain-name*	Configure the VTP administrative-domain name. The name can be 1 to 32 characters. All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name. This command is optional for modes other than server mode. VTP server mode requires a domain name. If the switch has a trunk connection to a VTP domain, the switch learns the domain name from the VTP server in the domain. You should configure the VTP domain before configuring other VTP parameters.
Step 3	**vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**}	Configure the switch for VTP mode (client, server, transparent, or off). (Optional) Configure the database: • **vlan**—the VLAN database is the default if none are configured. • **mst**—the multiple spanning tree (MST) database. • **unknown**—an unknown database type.
Step 4	**vtp password** *password*	(Optional) Set the password for the VTP domain. The password can be 8 to 64 characters. If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain. See the "Configuring a VTP Version 3 Password" section on page 25 for options available with VTP version 3.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show vtp status**	Verify your entries in the VTP Operating Mode and the VTP Domain Name fields of the display.
Step 7	**copy running-config startup-config**	(Optional) Save the configuration in the startup configuration file. **Note** Only the VTP mode and the domain name are saved in the switch running configuration and can be copied to the startup configuration file.

To return a switch in another mode to VTP server mode, use the **no vtp mode** global configuration command. To return the switch to a no-password state, use the **no vtp password** global configuration command.

This example shows how to configure the switch as a VTP server with the domain name *eng_group* and the password *mypassword*:

```
Switch(config)# vtp domain eng_group
Setting VTP domain name to eng_group.
Switch(config)# vtp mode server
Setting device to VTP Server mode for VLANS.
Switch(config)# vtp password mypassword
Setting device VLAN database password to mypassword.
```

```
Switch(config)# end
```

Configuring a VTP Version 3 Password

Beginning in privileged EXEC mode, follow these steps to configure the password when using VTP version 3:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp password** *password* [**hidden** | **secret**]	(Optional) Set the password for the VTP domain. The password can be 8 to 64 characters. • (Optional) **hidden**—Enter **hidden** to ensure that the secret key generated from the password string is saved in the nvam:vlan.dat file. If you configure a takeover by configuring a VTP primary server, you are prompted to reenter the password. • (Optional) **secret**—Enter **secret** to directly configure the password. The secret password must contain 32 hexadecimal characters.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vtp password**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save the configuration in the startup configuration file.

To clear the password, enter the **no vtp password** global configuration command.

This example shows how to configure a hidden password and how it appears.

```
Switch(config)# vtp password mypassword hidden
Generating the secret associated to the password.
Switch(config)# end
Switch# show vtp password
VTP password: 89914640C8D90868B6A0D8103847A733
```

Configuring a VTP Version 3 Primary Server

Beginning in privileged EXEC mode, follow these steps on a VTP server to configure it as a VTP primary server (version 3 only), which starts a takeover operation:

	Command	Purpose
Step 1	**vtp primary-server** [**vlan** | **mst**] [**force**]	Change the operational state of a switch from a secondary server (the default) to a primary server, and advertise the configuration to the domain. If the switch password is configured as **hidden**, you are prompted to reenter the password. • (Optional) **vlan**—Select the VLAN database as the takeover feature. This is the default. • (Optional) **mst**—Select the multiple spanning tree (MST) database as the takeover feature. • (Optional) **force**—Entering **force** overwrites the configuration of any conflicting servers. If you do not enter **force**, you are prompted for confirmation before the takeover.

This example shows how to configure a switch as the primary server for the VLAN database (the default) when a hidden or secret password was configured:

```
Switch# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP  domain

VTP Database Conf Switch ID      Primary Server Revision System Name
------------ ---- -------------- -------------- -------- --------------------
VLANDB       Yes  00d0.00b8.1400=00d0.00b8.1400 1        stp7

Do you want to continue (y/n) [n]? y
```

Configuring VTP on a Per-Port Basis

With VTP version 3, you can enable or disable VTP on a per-port basis. You can enable VTP only on ports that are in trunk mode. Incoming and outgoing VTP traffic is blocked, not forwarded.

Beginning in privileged EXEC mode, follow these steps to enable VTP on a port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Identify an interface, and enter interface configuration mode.
Step 3	**vtp**	Enable VTP on the specified port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config interface** *interface-id*	Verify the change to the port.
Step 6	**show vtp status**	Verify the configuration.

To disable VTP on the interface, use the **no vtp** interface configuration command.

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# vtp
Switch(config-if)# end
```

Other 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	**configure terminal**	Enter global configuration mode.
Step 2	**ipv6 router rip** *name*	Configure an IPv6 RIP routing process, and enter router configuration mode for the process.
Step 3	**maximum-paths** *number-paths*	(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	**exit**	Return to global configuration mode.

	Command	Purpose
Step 5	**interface** *interface-id*	Enter interface configuration mode, and specify the Layer 3 interface to configure.
Step 6	**ipv6 rip** *name* **enable**	Enable the specified IPv6 RIP routing process on the interface.
Step 7	**ipv6 rip** *name* **default-information** {**only** | **originate**}	(Optional) Originate the IPv6 default route (::/0) into the RIP routing process updates sent from the specified interface. **Note** 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. • **only**—Select to originate the default route, but suppress all other routes in the updates sent on this interface. • **originate**—Select to originate the default route in addition to all other routes in the updates sent on this interface.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show ipv6 rip** [*name*] [**database**] [**next-hops**]	Display information about IPv6 RIP processes.
	or	
	show ipv6 route rip [*updated*]	Display the contents of the IPv6 routing table.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Updates to the Command Reference

These commands are new or changed:

- vtp (global configuration)
- vtp (interface configuration)
- vtp primary

vtp (global configuration)

To set or modify the VLAN Trunking Protocol (VTP) configuration characteristics, use the **vtp** global configuration command. To remove the settings or to return to the default settings, use the **no** form of this command.

vtp {**domain** *domain-name* | **file** *filename* | **interface** *name* [**only**] | **mode** {**client** | **off** | **server** | **transparent**} [**mst** | **unknown** | **vlan**] | **password** *password* [**hidden** | **secret**] | **pruning** | **version** *number*}

no vtp {**file** | **interface** | **mode** [**client** | **off** | **server** | **transparent**] [**mst** | **unknown** | **vlan**] | **password** | **pruning** | **version**}

Syntax Description

domain *domain-name*	Specifies the VTP domain name, an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.
file *filename*	Specifies the Cisco IOS file system file where the VTP VLAN configuration is stored.
interface *name*	Specifies the name of the interface providing the VTP ID updates for this device.
only	(Optional) Use only the IP address of this interface to provide VTP IP updates.
mode	Specifies the VTP device mode as client, server, or transparent.
client	Puts the switch in VTP client mode. A switch in VTP client mode is enabled for VTP, and can send advertisements, but it does not have enough NVRAM to store VLAN configurations. You cannot configure VLANs on the switch. When a VTP client starts, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
off	Puts the switch in VTP off mode. A switch in VTP off mode functions the same as a VTP transparent device except that it does not forward VTP advertisements on trunk ports.
server	Puts the switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on the switch. The switch can recover all the VLAN information in the current VTP database from NVRAM after reboot.
transparent	Puts the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not send advertisements, or learn from advertisements sent by other devices. It cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received. When VTP mode is transparent, the mode and domain name are saved in the switch running configuration file, and you can save them in the switch startup configuration file by entering the **copy running-config startup config** privileged EXEC command.
mst	(Optional) Sets the mode for the multiple spanning tree (MST) VTP database (only VTP version 3).
unknown	(Optional) Sets the mode for unknown VTP databases (supported only with VTP version 3).
vlan	(Optional) Sets the mode for VLAN VTP database. This is the default (supported only in VTP version 3).
password *password*	Sets the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculations to be sent in VTP advertisements and to validate received VTP advertisements received. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
hidden	(Optional) Specifies that the key generated from the password string is saved in the VLAN database file. When you do not enter the **hidden** keyword, the password string is saved in clear text. When you enter the **hidden** password, you need to reenter the password to issue a command in the domain. This keyword is supported only in VTP version 3.

secret	(Optional) Allows the user to directly configure the password secret key (only VTP version 3).
pruning	Enables VTP pruning on the switch.
version *number*	Sets VTP version to version 1, version 2, or version 3.

Defaults

The default filename is *flash:vlan.dat***.**

The default mode is server mode, and the default database is VLAN.

In VTP version 3, the default mode for the MST database is transparent.

No domain name or password is defined.

No password is configured.

Pruning is disabled.

The default version is Version 1.

Command Modes

Global configuration

Command History

Release	Modification
12.2(46)EY	This command was introduced.
12.2(55)SE	The **mode off** keyword was added, support was added for VTP version 3, and the password **hidden** and **secret** keywords and the mode database keywords **vlan**, **mst**, and **unknown** were added with VTP version 3.

Usage Guidelines

When you save VTP mode, domain name, and VLAN configurations in the switch startup configuration file and reboot the switch, the VTP and VLAN configurations are selected by these conditions:

- If both the VLAN database and the configuration file show the VTP mode as transparent and the VTP domain names match, the VLAN database is ignored. The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the startup VTP mode is server mode, or the startup VTP mode or domain names do not match the VLAN database, VTP mode and VLAN configuration for the first 1005 VLANs are selected by VLAN database information, and VLANs greater than 1005 are configured from the switch configuration file.

The **vtp file***filename* cannot be used to load a new database, It renames only the file in which the existing database is stored.

Follow these guidelines when configuring a VTP domain name:

- The switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not send any VTP advertisements even if changes occur to the local VLAN configuration. The switch leaves the no-management-domain state after it receives the first VTP summary packet on a trunk port or after you configure a domain name by using the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to 0. After the switch leaves the no-management-domain state, you cannot configure it to re-enter that state until you clear the NVRAM and reload the software.

- Domain names are case-sensitive.
- After you configure a domain name, you cannot remove it. You can only reassign it to a different domain.

Follow these guidelines when setting a VTP mode:

- The **no vtp mode** command returns the switch to VTP server mode.
- The **vtp mode server** command is the same as **no vtp mode**, but it does not return an error if the switch is not in client or transparent mode.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, be sure to make all VTP or VLAN configuration changes on a switch that is in server mode. If the receiving switch is in server mode or transparent mode, the switch configuration is not changed.
- Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch that is in transparent mode, the changes are not propagated to other switches in the network.
- If you change the VTP or VLAN configuration on a switch that is in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the switch.
- In VTP versions 1 and 2, the VTP mode must be transparent for you to add extended-range VLANs or for VTP and VLAN information to be saved in the running configuration file. VTP supports extended-range VLANs in client and server mode and saves them in the VLAN database.
- With VTP versions 1 and 2, if extended-range VLANs are configured on the switch and you attempt to set the VTP mode to server or client, you receive an error message that the configuration is not allowed. Changing VTP mode is allowed with extended VLANs in VTP version 3.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.
- The **vtp mode off** command sets the device to off. The **no vtp mode off** command resets the device to the VTP server mode.

Follow these guidelines when setting a VTP password:

- Passwords are case sensitive. Passwords should match on all switches in the same domain.
- When you use the **no vtp password** form of the command, the switch returns to the no-password state.
- The **hidden** and **secret** keywords are supported only in VTP version 3. If you change from VTP version 2 to VTP version 3, you must remove the **hidden** or **secret** keyword before the change.

Follow these guidelines when setting VTP pruning:

- VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no devices belonging to that VLAN.
- If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.
- Only VLANs in the pruning-eligible list can be pruned.
- Pruning is supported with VTP Version 1 and Version 2.

Follow these guidelines when setting the VTP version:

- Toggling the Version 2 (v2) mode state modifies parameters of some default VLANs.
- Each VTP switch automatically detects the capabilities of all the other VTP devices. To use Version 2, all VTP switches in the network must support Version 2. Otherwise, you must configure them to operate in VTP Version 1 mode.
- If all switches in a domain are VTP Version 2-capable, you only need only to configure Version 2 on one switch. The version number is then propagated to the other Version-2 capable switches in the VTP domain.
- If you are using VTP in a Token Ring environment, VTP Version 2 must be enabled.
- If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use Version 2.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use Version 1.
- In VTP version 3, all database VTP information (not just VLAN database information) is propagated across the VTP domain.
- Two VTP version 3 regions can only communicate through a VTP version 1 or VTP version 2 region in transparent mode.

You cannot save password, pruning, and version configurations in the switch configuration file.

Examples

This example shows how to rename the filename for VTP configuration storage to *vtpfilename*:

```
Switch(config)# vtp file vtpfilename
```

This example shows how to clear the device storage filename:

```
Switch(config)# no vtp file vtpconfig
Clearing device storage filename.
```

This example shows how to specify the name of the interface providing the VTP updated ID for this device:

```
Switch(config)# vtp interface gigabitethernet 0/1
```

This example shows how to set the administrative domain for the switch:

```
Switch(config)# vtp domain OurDomainName
```

This example shows how to place the switch in VTP transparent mode:

```
Switch(config)# vtp mode transparent
```

This example shows how to configure the VTP domain password:

```
Switch(config)# vtp password ThisIsOurDomain'sPassword
```

This example shows how to enable pruning in the VLAN database:

```
Switch(config)# vtp pruning
Pruning switched ON
```

This example shows how to enable Version 2 mode in the VLAN database:

```
Switch(config)# vtp version 2
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

Related Commands

Command	Description
show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
vtp (interface configuration)	Enables or disables VTP on an interface.

vtp (interface configuration)

To enable the VLAN Trunking Protocol (VTP) on a per-port basis, use the **vtp** interface configuration command. To disable VTP on the interface, use the **no** form of this command.

vtp

no vtp

Note This command is supported only when the switch is running VTP version 3.

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

Interface configuration.

Command History

Release	Modification
12.2(55)SE	This command was introduced.

Usage Guidelines

Enter this command only on interfaces that are in **switchport trunk** mode.

This command is supported only on switches configured for VTP version 3.

Examples

This example shows how to enable VTP on an interface:

```
Switch(config-if)# vtp
```

This example shows how to disable VTP on an interface:

```
Switch(config-if)# no vtp
```

Related Commands

Command	Description
vtp (global configuration)	Globally configures VTP domain-name, password, pruning, version, and mode.

vtp primary

To configure a switch as the VLAN Trunking Protocol (VTP) primary server, use the **vtp primary** privileged EXEC command.

vtp primary [**mst** | **vlan**] [**force**]

There is no **no** form of the command.

Note This command is supported only when the switch is running VTP version 3.

Note Although visible in the command line help, the **vtp** {**password** *password* | **pruning** | **version** *number*} commands are not supported.

Syntax Description

mst	(Optional) Configure the switch as the primary VTP server for multiple spanning tree (MST).
vlan	(Optional) Configure the switch as the primary VTP server for VLANs.
force	(Optional) Configure the switch to not check for conflicting devices when you configure the primary server.

Defaults

The switch is a VTP secondary server.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(55)SE	This command was introduced.

Usage Guidelines

This command is supported only on switches configured for VTP version 3.

A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can only back up to NVRAM the updated VTP configurations received from the primary server.

By default, all devices come up as secondary servers. Primary server status is needed only for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers.

Primary server status is lost if the device reloads or domain parameters change.

Examples

This example shows how to configure the switch as the primary VTP server for VLANs:

```
Switch# vtp primary vlan
This sytems is becoming primary server for feature vlan.
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

Related Commands

Command	Description
show vtp status	Displays the VTP statistics for the switch and general information about the VTP management domain status.
vtp (global configuration)	Configures the VTP filename, interface, domain name, mode, and version.

Updates for 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-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.

Error Message
```
IFMGR-3-IFINDEX_PERSIST_ENTRY_CORRUPT: [chars] seems to be corrupted.
Trying to read [dec] size
```

Explanation The ifIndex table is corrupted. [chars] is the path to the IfIndex file, and [dec] is the number of bytes that was being read from the ifIndex table when the corruption was detected.

Recommended Action Delete the ifindex table.

Error Message
```
IFMGR-3-INVALID_PERSISTENT_DATA: Invalid persistent data
```

Explanation The interface manager attempts to write invalid persistent data.

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
```
ILET-1-AUTHENTICATION_FAIL: This Switch may not have been manufactured
by Cisco or with Cisco’s authorization.  This product may contain software that
was copied in violation of Cisco’s license terms.  If your use of this product is
the cause of a support issue, Cisco may deny operation of the product, support
under your warranty or under a Cisco technical support program such as Smartnet.
Please contact Cisco’s Technical Assistance Center for more information.
```

Explanation A license authentication failure occurred for the switch.

Recommended Action Contact your Cisco sales representative for assistance.

Error Message
```
ILET-1-DEVICE_AUTHENTICATION_FAIL: The [chars] inserted in this switch
may not have been manufactured by Cisco or with Cisco's authorization. If your use
of this product is the cause of a support issue, Cisco may deny operation of the
product, support under your warranty or under a Cisco technical support program
such as Smartnet.  Please contact Cisco's Technical Assistance Center for more
information.
```

Explanation A license authentication failure occurred for a component that was inserted in the switch. [chars] is the component.

Recommended Action Contact your Cisco sales representative for assistance.

Error Message
```
SCHED-3-UNEXPECTEDEVENT: [traceback] [process information] Process
received unknown event (maj [hex], min [hex])
```

Explanation A process did not handle an event. The first [hex] is the major event number, and the second [hex] is the minor event number, both of which allow you to identify the event that occurred.

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.

Removed System Messages

Error Message `DOT1X-4-MEM_UNAVAIL: Memory was not available to perform the 802.1X action.`

Explanation The system memory is not sufficient to perform the IEEE 802.1x authentication.

Recommended Action Reduce other system activity to reduce memory demands.

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

Explanation Authentication was successful. [chars] is the interface.

Recommended Action No action is required.

Error Message `DOT1X_SWITCH-5-ERR_ADDING_ADDRESS: Unable to add address [enet] on [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, and [chars] is the interface.

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.

Update for the Getting Started Guide

In the "Running Express Setup" section of the *Catalyst 2350 Switch Getting Started Guide*, Step 12 incorrectly states that the VLAN ID range is 1 to 1001. The correct range is 1 to 4094.

Related Documentation

These documents provide complete information about the Catalyst 2350 switch and are available on Cisco.com:
http://www.cisco.com/en/US/products/ps10116/tsd_products_support_series_home.html

- *Catalyst 2350 Switch Getting Started Guide*
- *Catalyst 2350 Switch Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 2350 Switch*
- *Catalyst 2350 Switch Software Configuration Guide*
- *Catalyst 2350 Switch Command Reference*
- *Catalyst 2350 Switch System Message Guide*
- *Installation Notes for the Power Supply Modules for the Catalyst 2350 Switch*
- *Installation Notes for the 60CFM Fan Module for the Catalyst 2350 Switch*
- Device manager online help (available on the switch)

These compatibility matrix documents are available from this Cisco.com site:
http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

- *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*
- *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix*
- *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*
- *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*

For other information about related products, see these documents:

- *Getting Started with Cisco Network Assistant*
- *Release Notes for Cisco Network Assistant*

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.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

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.