Release Notes for Catalyst 2350 Switch, Cisco IOS Release 12.2(52)SE

October 1, 2009

Cisco IOS Release 12.2(52)SE runs on all Catalyst 2350 switches.

These release notes include important information about Cisco IOS Release 12.2(52)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 5.

You can download the switch software from this site (registered Cisco.com users with a login password):

http://www.cisco.com/public/sw-center/index.shtml

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

Contents

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

Table 1   Supported Hardware (continued)

Device	Description	Supported by Minimum Cisco IOS Release
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 5
- "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 6
- "Recovering from a Software Failure" section on page 7

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-lanlite-tar.122-52.SE.tar	Catalyst 2350 image file and device manager files. This image has Layer 2 features.
c2350-lanlitek9-tar.122-52.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/products/sw/iosswrel/ps5187/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,* at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a00800811e0.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 5 to identify the file that you want to download.

Step 2 Download the software image file. If you have a SmartNet support contract, go to this URL, and log in.

http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml

To download the image for a Catalyst 2350 switch, click **Catalyst 2350 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 2350 3DES Cryptographic Software**.

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

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

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

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

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

For more information about assigning an IP address and 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

There are no new software features in this release.

Configuration Notes

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

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

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 8
- "Cisco X2 Transceiver Modules and SFP Modules" section on page 8
- "Configuration" section on page 8
- "Multicasting" section on page 9
- "QoS" section on page 9
- "SPAN and RSPAN" section on page 10

Address Resolution Protocol

This is an Address Resolution Protocol limitation:

- 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

These are the Cisco X2 transceiver module and SFP module limitations:

- 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. (CSCsg28558)

- 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)

SPAN and RSPAN

This is the SPAN and Remote SPAN (RSPAN) limitation.

• 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

These sections describe the important notes related to this software release for the Catalyst 2350 switches:

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 o r 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

- CSCsy85676

  When you configure an ACL and enter the **access-group** interface configuration command to apply it to an interface for web authentication, the output from the **show epm session ip-address** or **show ip access_list interface** *interface-id* privileged EXEC command does not show any web authentication filter ID.

  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.

Resolved Caveats

This release resolves these previously open caveats:

- CSCsx78068

  If you enable 802.1Q native VLAN tagging by entering the **vlan dot1q tag native** global configuration command and then change the native VLAN ID on an ingress trunk port by entering the sw**itchport trunk native vlan** *vlan-id* interface command, untagged traffic is forwarded instead of being dropped.

  The workaround is to use one of these methods:

  - Enter a **shutdown** followed by a **no shutdown** interface configuration command on the trunk port.

  - Disable and then reenable native VLAN tagging by entering the **no vlan dot1q tag native** global configuration command followed by the **vlan dot1q tag native** command.

- CSCsy90265

  If you repeatedly enter the **show tech-support** privileged EXEC command, the switch might leak memory and, in some cases, shut down.

  The workaround is to reload the switch to clear the memory after repeated use of the **show tech-support** command.

- CSCta78502

  When you have configured a login banner by entering the **banner login** *c message c* global configuration command and the switch reloads, the output of banner is missing a carriage return, making the format incorrect.

  There is no workaround.

- CSCtb97439

    When remote neighbors change, the LLDP MIB does not properly update the remote neighbors.

    The workaround is to clear the LLDP table by entering the **clear lldp table** privileged EXEC command.

Documentation Updates

This section provides these updates to the product documentation for the Catalyst 2350 switch:

Update for the System Message Guide

This section contains the system message guide updates.

New System Messages

These messages were added to all of the system message guides:

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 `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 IEEE 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 if 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 IEEE 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 IEEE 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 IEEE 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.

Explanation 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 IEEE 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 IEEE 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 shutdown or use another VLAN.

Deleted

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.

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

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

> **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 [chars]

> **Recommended Action** Multi-Domain Authentication (MDA) host mode cannot start if the configured data VLAN on a port is the same as the voice VLAN. [chars] is the port.

> **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.

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

> **Recommended Action** Change either the voice VLAN or the IEEE 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]

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

> **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]`

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

> **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 [dec] to 802.1x port [chars]`

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

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

Error Message `DOT1X_SWITCH-5-ERR_VLAN_ON_ROUTED_PORT: Dot1x cannot assign a VLAN`
`[dec] to a routed port [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 and [chars] is the port.

> **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]`

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

> **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]`

> **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, and [chars] is the port.

> **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`

> **Explanation** This message means that remote SPAN should not be enabled on a VLAN with IEEE 802.1x-enabled. [dec] is the VLAN, and [chars] is the port.

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

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.

Update for the Device Manager Online Help

The device manager online help 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, at:

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.