



# Release Notes for the Cisco IE 3000 Switch, Cisco IOS Release 12.2(52)SE and Later

---

**February 16, 2010**

Cisco IOS Release 12.2(52)SE1 runs on all Cisco IE 3000 switches.

These release notes include important information about Cisco IOS Release 12.2(52)SE and later, and any limitations, restrictions, and caveats that apply to the releases. 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.

For the complete list of Cisco IE 3000 switch documentation, see the “[Related Documentation](#)” section on page 31.

You can download the switch software from this site (registered Cisco.com users with a login password):  
<http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml>

## Contents

This information is in the release notes:

- [System Requirements](#), page 2
- [Upgrading the Switch Software](#), page 4
- [Installation Notes](#), page 7
- [New Features](#), page 7
- [Limitations and Restrictions](#), page 9
- [Important Notes](#), page 13
- [Open Caveats](#), page 15



---

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

- [Resolved Caveats, page 15](#)
- [Documentation Updates, page 17](#)
- [Related Documentation, page 31](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 32](#)

## System Requirements

The system requirements are described in these sections:

- [Hardware Supported, page 2](#)
- [Device Manager System Requirements, page 3](#)
- [Cluster Compatibility, page 3](#)
- [CNA Compatibility, page 4](#)

## Hardware Supported

This section lists the hardware and SFP modules that the switch supports.

### Switches and Modules

[Table 1](#) lists the hardware supported on this release.

**Table 1** *Cisco IE 3000 Switch Models*

Switch Model	Description
Cisco IE-3000-4TC	4 10/100BASE-T Ethernet ports and 2 dual-purpose ports, each with a 10/100/1000BASE-T copper port and an SFP (small form-factor pluggable) module slot
Cisco IE-3000-8TC	8 10/100BASE-T Ethernet ports and 2 dual-purpose ports
Cisco IE-3000-4TC-E	4 10/100BASE-T Ethernet ports and 2 dual-purpose ports (supports the IP services software feature set)
Cisco IE-3000-8TC-E	8 10/100BASE-T Ethernet ports and 2 dual-purpose ports (supports the IP services software feature set)
Cisco IEM-3000-8TM	Expansion module with 8 10/100BASE-T copper Ethernet ports
Cisco IEM-3000-8FM	Expansion module with 8 100BASE-FX fiber-optic Ethernet ports

## SFP Modules

These are the SFP modules that the switch supports:

**Table 2** *SFP Models*

Type of SFP	SFP Models
Industrial temperature SFP modules	GLC-FE-100FX-RGD GLC-SX-MM-RGD GLC-FE-100LX-RGD GLC-LX-SM-RGD GLC-ZX-SM-RGD
Extended temperature SFP modules	100BASE-BX
Commercial temperature SFP modules	CWDM 1000BASE-BX

## Device Manager System Requirements

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

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

## Hardware Requirements

[Table 3](#) lists the minimum hardware requirements for running the device manager.

**Table 3** *Minimum Hardware Requirements*

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum <sup>1</sup>	512 MB <sup>2</sup>	256	1024 x 768	Small

1. We recommend 1 GHz.
2. We recommend 1 GB DRAM.

## Software Requirements

These are the supported operating systems and browsers for the device manager:

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

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

## Cluster Compatibility

You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the command-line interface (CLI) 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 configuring the highest-end switch in your cluster as the command switch.
- If you are managing the cluster through Network Assistant, 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 Cisco IE 3000 switch, all standby command switches must be Cisco IE 3000 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 Compatibility

Cisco IOS 12.2(46)SE1 and later is only compatible with Cisco Network Assistant (CNA) 5.4 and later.



### Note

CNA 5.4 does not support the `cisco-ie-macros` that were introduced in this release. Using the new Smartport role names will cause CNA errors.

You can download Cisco Network Assistant from this URL:

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

For more information about Cisco Network Assistant, see the *Release Notes for Cisco Network Assistant* on Cisco.com.

## Upgrading the Switch Software

These are the procedures for downloading software. Before downloading software, read this section for important information:

- [Finding the Software Version and Feature Set, page 4](#)
- [Deciding Which Files to Use, page 5](#)
- [Archiving Software Images, page 5](#)
- [Upgrading a Switch by Using the Device Manager or Network Assistant, page 6](#)
- [Upgrading a Switch by Using the CLI, page 6](#)
- [Recovering from a Software Failure, 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 compact flash memory card.

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 4 lists the filenames for this software release.

If you download the IP services image and plan to use Layer 3 functionality, you must use the Switch Database Management (SDM) routing template. To see which template is currently active template, enter the **show sdm prefer** privileged EXEC command. If necessary, change the SDM template to the routing template by entering the **sdm prefer routing** global configuration command. You will be prompted to reload the switch to activate the new template.



### Note

The switch must be running Cisco IOS Release 12.2(52)SE or later to configure the routing template.

**Table 4** Cisco IOS Software Image Files

Filename	Description
ies-lanbase-tar.122-52.SE1.tar	Cisco IE 3000 image file and device manager files. This image has Layer 2+ features.
ies-lanbasek9-tar.122-52.SE1.tar	Cisco IE 3000 cryptographic image file and device manager files with Layer 2+ features. This image has the Kerberos and SSH features.
ies-ipservices-tar.122-52.SE1.tar	Cisco IE 3000 IP services image (noncryptographic image) with device manager files. This image has both Layer 2+ and full Layer 3 routing features.
ies-ipservicesk9-tar.122-52.SE1.tar	Cisco IE 3000 IP services cryptographic image with device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.

## Archiving Software Images

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

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

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod\\_bulletin0900aecd80281c0e.html](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\\_chapter09186a00800ca744.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca744.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 image file and replace or keep the current image.

**Note**

Make sure that the compact flash card is inserted into the switch before downloading the software.

To download software, follow these steps:

- 
- Step 1** Use [Table 4 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 to download the appropriate files:
- <http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml>
- To download the image for a Cisco IE 3000 switch, click **Cisco IE 3000 software**. To obtain authorization and to download the cryptographic software files, click **Cisco IE 3000 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 the *Cisco IE 3000 Switch Software Configuration Guide*.
- Step 4** Log into the switch through the console port or a Telnet session.
- Step 5** (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

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

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

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

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

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

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

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

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

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

```
Switch# archive download-sw /overwrite tftp://198.30.20.19/ies-lanbase-tar.122-52.SE1.tar
```

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

## Recovering from a Software Failure

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

## Installation Notes

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

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

## New Features

These sections describe the new supported hardware and the new and updated software features provided in this release:

- [New Hardware Features, page 8](#)
- [New Software Features, page 8](#)

## New Hardware Features

There are no new hardware features for this release. For a list of all supported hardware, see the [“Hardware Supported” section on page 2](#).

## New Software Features

- Support for IP source guard on static hosts.
- RADIUS Change of Authorization (CoA) to change the attributes of a certain session after it is authenticated. When there is a change in policy for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server, such as Cisco Secure ACS to reinitialize authentication, and apply to the new policies.
- IEEE 802.1x User Distribution to allow deployments with multiple VLANs (for a group of users) to improve scalability of the network by load balancing users across different VLANs. Authorized users are assigned to the least populated VLAN in the group, assigned by RADIUS server.
- Support for critical VLAN with multiple-host authentication so that when a port is configured for multi-auth, and an AAA server becomes unreachable, the port is placed in a critical VLAN in order to still permit access to critical resources.
- Customizable web authentication enhancement to allow the creation of user-defined *login*, *success*, *failure* and *expire* web pages for local web authentication.
- Support for Network Edge Access Topology (NEAT) to change the port host mode and to apply a standard port configuration on the authenticator switch port.
- VLAN-ID based MAC authentication to use the combined VLAN and MAC address information for user authentication to prevent network access from unauthorized VLANs.
- MAC move to allow hosts (including the hosts connected behind an IP phone) to move across ports within the same switch without any restrictions to enable mobility. With MAC move, the switch treats the reappearance of the same MAC address on another port in the same way as a completely new MAC address.
- Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms to SNMPv3.
- Support for including a hostname in the option 12 field of DHCPDISCOVER packets. This provides identical configuration files to be sent by using the DHCP protocol.
- DHCP Snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field.
- Increased support for LLPD-MED by allowing the switch to grant power to the power device (PD), based on the power policy TLV request.
- Support for VTP version 3 that includes support for configuring extended range VLANs (VLANs 1006 to 4094) in any VTP mode, enhanced authentication (hidden or secret passwords), propagation of other databases in addition to VTP, VTP primary and secondary servers, and the option to turn VTP on or off by port.
- Support for PROFINET IO, a modular communication framework for distributed automation applications. The switch provides a PROFINET management connection to the IO controllers.
- Support for the IP services image that includes support for Layer 3 routing protocols and advanced features.

- Enhancement to the Common Industrial Protocol (CIP) that adds the ability to configure DHCP parameters with CIP.
- Support for the LLPD-MED MIB and the CISCO-ADMISSION-POLICY-MIB.

## 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.

This section contains these limitations:

- [Cisco IOS Limitations, page 9](#)
- [Device Manager Limitations, page 13](#)

## Cisco IOS Limitations

These limitations apply to the Cisco IE 3000 switches:

- [Configuration, page 9](#)
- [Ethernet, page 10](#)
- [IP, page 11](#)
- [Multicasting, page 11](#)
- [QoS, page 12](#)
- [SPAN and RSPAN, page 12](#)
- [Trunking, page 12](#)
- [VLAN, page 13](#)

## Configuration

- A static IP address might be removed when the previously acquired DHCP IP address lease expires.

This problem occurs under these conditions:

- When the switch is booted up without a configuration (no config.text file in flash memory).
- When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
- When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)

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

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

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

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

- A traceback error occurs if a crypto key is generated after an SSL client session.  
There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. (CSCef59331)
- When the **logging event-spanning-tree** interface configuration command is configured and logging to the console is enabled, a topology change might generate a large number of logging messages, causing high CPU utilization. CPU utilization can increase with the number of spanning-tree instances and the number of interfaces configured with the **logging event-spanning-tree** interface configuration command. This condition adversely affects how the switch operates and could cause problems such as STP convergence delay.

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

Use one of these workarounds:

- Disable logging to the console.
- Rate-limit logging messages to the console.
- Remove the **logging event spanning-tree** interface configuration command from the interfaces. (CSCsg91027)

- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.  
The workaround is to configure aggressive UDLD. (CSCsh70244)
- When you enter the **boot host retry timeout** global configuration command to specify the amount of time that the client should keep trying to download the configuration and you do not enter a timeout value, the default value is zero, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.  
The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout *timeout-value*** command. (CSCsk65142)
- On a switch running both Resilient Ethernet Protocol (REP) and Bidirectional Forwarding Detection (BFD), when the REP link status layer (LSL) age-out value is less than 1 second, the REP link flaps if the BFD interface is shut down and then brought back up.

The workaround is to use the **rep lsl-age-out timer** interface configuration command to configure the REP LSL age timer for more than 1000 milliseconds (1 second). (CSCsz40613)

## Ethernet

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

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

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

- for random source-ip and dest-ip traffic, configure load balance method as **src-dst-ip**

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

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

## IP

When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console. The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)

## Multicasting

- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise. The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)
- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port. There is no workaround. (CSCdy82818)
- If an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
  - If the **ALLOW\_NEW\_SOURCE** record is before the **BLOCK\_OLD\_SOURCE** record, the switch removes the port from the group.
  - If the **BLOCK\_OLD\_SOURCE** record is before the **ALLOW\_NEW\_SOURCE** record, the switch adds the port to the group.

There is no workaround. (CSCec20128)

- When IGMP snooping is disabled and you enter the **switchport block multicast** interface configuration command, IP multicast traffic is not blocked.

The **switchport block multicast** interface configuration command is only applicable to non-IP multicast traffic.

There is no workaround. (CSCee16865)

- Incomplete multicast traffic can be seen under either of these conditions:
  - You disable IP multicast routing or re-enable it globally on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.

The workaround is to enter the **clear ip mroute** privileged EXEC command on the interface. (CSCef42436)

After you configure a switch to join a multicast group by entering the **ip igmp join-group** *group-address* interface configuration command, the switch does not receive join packets from the client, and the switch port connected to the client is removed from the IGMP snooping forwarding table.

Use one of these workarounds:

- Cancel membership in the multicast group by using the **no ip igmp join-group** *group-address* interface configuration command on an SVI.
- Disable IGMP snooping on the VLAN interface by using the **no ip igmp snooping vlan** *vlan-id* global configuration command. (CSCeh90425)
- Entering the **shutdown** and the **no shutdown** interface configuration commands on the internal link can disrupt the PoE operation. If a new IP phone is added while the internal link is in shutdown state, the IP phone does not get inline power if the internal link is brought up within 5 minutes.

The workaround is to enter the **shutdown** and the **no shutdown** interface configuration commands on the Fast Ethernet interface of a new IP phone that is attached to the service module port after the internal link is brought up. (CSCeh45465)

## QoS

- Some switch queues are disabled if the buffer size or threshold level is set too low with the **mls qos queue-set output** global configuration command. The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue. The workaround is to choose compatible buffer sizes and threshold levels. (CSCea76893)
- When auto-QoS is enabled on the switch, priority queuing is not enabled. Instead, the switch uses shaped round robin (SRR) as the queuing mechanism. The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing mechanism supported on each platform might be different. There is no workaround. (CSCee22591)

## SPAN and RSPAN

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

## Trunking

- The switch treats frames received with mixed encapsulation (IEEE 802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and the port LED blinks amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an IEEE 802.1Q trunk interface. There is no workaround. (CSCdz33708)
- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y. There is no workaround. (CSCdz42909).

- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics. There is no workaround. (CSCec35100).

## VLAN

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)

- When line rate traffic is passing through a dynamic port, and you enter the **switchport access vlan dynamic** interface configuration command for a range of ports, the VLANs might not be assigned correctly. One or more VLANs with a null ID appears in the MAC address table instead.

The workaround is to enter the **switchport access vlan dynamic** interface configuration command separately on each port. (CSCsi26392)

## Device Manager Limitations

- When you are prompted to accept the security certificate and you click *No*, you only see a blank screen, and the device manager does not launch.

The workaround is to click *Yes* when you are prompted to accept the certificate. (CSCef45718)

- When you successfully upgrade an image by using device manager and click *No* when prompted to reload the image, device manager becomes unusable.

The workaround is to manually reload the switch. (CSCsj88169)

## Important Notes

### 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.

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

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

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

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

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

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

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

## Open Caveats

- CSCsy85L676  
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

### Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(52)SE1

- CSCtd16478  
In the STEP 7 network management tool, when you select the IE3000-STC module to see the software version, the Properties window shows the software revision as *V12.2.46*, instead of *V12.2.52*.
- CSCtd88091  
When you establish a Profinet session with the switch, the LLDP *Chassis MAC* field shows the MAC address of the egress port instead of the system MAC address.

### Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(52)SE

- CSCsm95883  
When an unsuccessful forward open request message is returned on the switch, the response does not contain the connection serial number, vendor ID, or vendor serial number information. Only the general and extended error codes are returned.  
This problem only applies to unsuccessful forward open response messages.  
The workaround is to enable the **CIP debug** command to determine the cause of the forward open failure.

- CSCsr13187
 

The **show cip object tcp/ip interface** privileged EXEC command displays an old value for the domain name after it has been unconfigured with the **no ip domain-name** global configuration command.

The workaround is to ignore the domain name output of the **show cip object tcp/ip interface** privileged EXEC command.
- CSCsv63055
 

When you configure PTP in forward mode by entering the **ptp mode forward** global configuration command, the PTP page in device manager breaks due to a parser error.

There is no workaround. No PTP information is displayed when PTP is in forward mode.
- CSCsv69430
 

The device manager Legend incorrectly shows solid green for the Alarm and Setup LEDs in the Off state. The correct color of these LEDs in the Off state is solid black (dark).

There is no workaround.
- CSCsw20148
 

When one power supply in a redundant pair fails, a CIP query continues to show that both supplies are present and okay. Redundant supplies are connected to the switch and one fails.

There is no workaround.
- CSCsw68528
 

On switches running Cisco IOS Release 12.2(44)SE or 12.2(46)SE, when you enter the **show mvr interface interface-id members** privileged EXEC command to see status of an MVR port, an MVR member port that is not connected always shows as *ACTIVE*.

The workaround is to use the **show mvr interface interface-id** or the **show mvr members** privileged EXEC command. These command outputs show the correct status of an MVR port.
- CSCsw69015
 

When you enter the **mvr vlan vlan-id** global configuration command to create an MVR VLAN and enable MVR on the switch by entering the **mvr** global configuration command, if you enter the **show mvr interface interface-id members** privileged EXEC command, the output shows the MVR groups on the interface. However, if you enable MVR first and then create the MVR VLAN, the MVR groups are not displayed correctly.
- CSCsx71632
 

When VLAN-based quality of service (QoS) is enabled and then disabled on an interface by entering the **mls qos vlan-based** interface configuration command followed by the **no** version of the command, the port policy is not applied properly and could result in undefined behavior for packets matching the port policy.

The workaround is to remove the port policy by entering the **no service-policy input policy-map-name** interface configuration command and then reapply it to the interface.
- 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 **switchport 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 reenables 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.

- CSCta57846

The switch unexpectedly reloads when copying a configuration file from a remote server or from flash memory containing logging file flash:

The workaround is to enter the **logging file flash:filename** global configuration command to configure logging to flash instead of copying to flash.

- 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.

- CSCtb33780

The link between a switch with a 100BaseFX-FE small form-factor pluggable (SFP) module and a connected device remains up when one of the fiber cables is removed.

The workaround is the use UniDirectional Link Detection (UDLD) in aggressive mode

- 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

These sections provide updates to the product documentation:

- [Update to the Software Configuration Guide, page 18](#)
- [Updates to the Getting Started Guide, page 18](#)
- [Updates to the Regulatory Compliance and Safety Information for the Cisco IE 3000 Switch, page 22](#)
- [Updates to the Hardware Installation Guide, page 24](#)
- [Updates to the System Message Guide, page 25](#)

## Update to the Software Configuration Guide

The switch running Cisco IOS Release 12.2(50)SE does not support EnergyWise.

This section was added to the "Configuring IEEE 802.1x Port-Based Authentication" chapter:

### Common Session ID

Authentication manager uses a single session ID (referred to as a common session ID) for a client no matter which authentication method is used. This ID is used for all reporting purposes, such as the show commands and MIBs. The session ID appears with all per-session syslog messages.

The session ID includes:

- The IP address of the Network Access Device (NAD)
- A monotonically increasing unique 32 bit integer
- The session start time stamp (a 32 bit integer)

This example shows how the session ID appears in the output of the **show authentication** command. The session ID in this example is 160000050000000B288508E5:

```
Switch# show authentication sessions
```

Interface	MAC Address	Method	Domain	Status	Session ID
Fa4/0/4	0000.0000.0203	mab	DATA	Authz Success	160000050000000B288508E5

This is an example of how the session ID appears in the syslog output. The session ID in this example is also 160000050000000B288508E5:

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

The session ID is used by the NAD, the AAA server, and other report-analyzing applications to identify the client. The ID appears automatically. No configuration is required.

## Updates to the Getting Started Guide

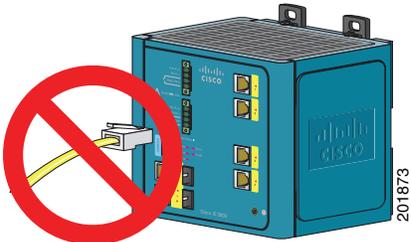
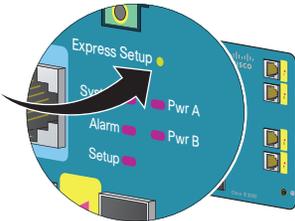
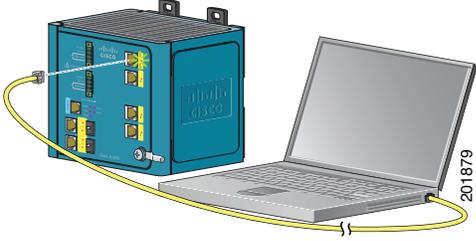
### Express Setup

When you launch Express Setup, you are prompted for the switch password. Enter the default password, *cisco*. The switch ignores text in the username field. Before you complete and exit Express Setup, you must change the password from the default password, *cisco*.

In the "Running Express Setup" section of the *Cisco IE 3000 Switch Getting Started Guide*, Steps 8 to 10 have changed.

## Running Express Setup:

To run Express Setup:

<b>Step 1</b>	<p>Make sure that nothing is connected to the switch.</p> <p>During Express Setup, the switch acts as a DHCP server. If your PC has a static IP address, change your PC settings before you begin to temporarily use DHCP.</p>	
<b>Step 2</b>	<p>Connect power to the switch.</p> <p>See the wiring instructions in the “Grounding the Switch” section and the “Wiring the DC Power Source” section.</p>	
<b>Step 3</b>	<p>When the switch powers on, it begins the power-on self-test (POST). During POST, the System LED blinks while a series of tests verify that the switch functions properly. Wait for the switch to complete POST, which takes approximately 1 minute.</p>	
<b>Step 4</b>	<p>Make sure that POST has completed by verifying that the System LED is solid green. If the switch has not been configured, the Setup LED blinks green. If the Setup LED stops blinking, you can still continue with the next step.</p> <p>If the switch fails POST, the System LED turns red. See the “In Case of Difficulty” section if your switch fails POST.</p>	
<b>Step 5</b>	<p>Press the Express Setup button. This button is recessed behind the front panel, so you can use a simple tool, such as a paper clip.</p> <p>When you press the Express Setup button, a switch port LED begins blinking green.</p>	
<b>Step 6</b>	<p>Connect a Category 5 Ethernet cable (not provided) from the blinking switch port to the Ethernet port on your PC.</p> <p>The port LEDs on your PC and the switch blink green while the switch configures the connection.</p>	
<b>Step 7</b>	<p>When the Setup LED turns solid green, start a browser session on the PC.</p>	

**Step 8**

The Express Setup window automatically appears. If the window does not appear, verify that any proxy settings or pop-up blockers are disabled on your browser and that any wireless client is disabled on your PC. You might also need to enter a URL in your browser, such as *Cisco.com* or another well-known website. If you need help, see the “In Case of Difficulty” section.



**Note** If the switch has been previously configured, the device manager page appears. You can use it to change the switch IP address.

Network Settings	
Management Interface (VLAN):	default - 1
IP Assignment Mode:	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Subnet Mask:	255.255.255.0
Default Gateway:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Password:	<input type="text"/>
Confirm Password:	<input type="text"/>
CIP VLAN Settings	
CIP VLAN:	default - 1
IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Subnet Mask:	255.255.255.0
Optional Settings	
Host Name:	Switch
Telnet Access:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Telnet Password:	<input type="text"/>
Confirm Telnet Password:	<input type="text"/>
System Date (DD/MMM/YYYY):	4 / Mar / 2008
System Time (HH:MM):	10 : 30 AM
Time Zone:	(GMT - 08:00) Pacific Time (US & Canada): Tijuana
Daylight Saving Time:	<input checked="" type="checkbox"/> Enable

**Step 9**

Enter the network settings. All entries must be in English letters and Arabic numbers.

- **Management Interface (VLAN):** We recommend using the default, **VLAN 1**. The management VLAN establishes an IP connection to the switch.
- **IP Assignment Mode:** We recommend using the default, **Static**, which means that the switch always has the IP address that you assign. Use the **DHCP** setting when you want the switch to automatically obtain an IP address from a DHCP server.
- **IP Address:** Enter the IP address for the switch. Later, you can use the IP address to access the switch through the device manager.
- **Subnet Mask:** Select a mask from the drop-down list.
- **Default Gateway:** Enter the IP address of the router.
- **Password:** Enter a password. The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows embedded spaces, but does not allow spaces at the beginning or end. In the **Confirm Password** field, enter the password again.

For more information about the network settings, click **Help** on the toolbar.

- 
- Step 10** Enter the Control Industrial Protocol (CIP) VLAN settings:
- **CIP VLAN:** Enter the VLAN on which CIP will be enabled. The CIP VLAN can be the same as the management VLAN, or you can isolate CIP traffic on another VLAN that is already configured on the switch. The default CIP VLAN ID is **VLAN 1**.
  - **IP Address:** Enter the IP address for the CIP VLAN. If the CIP VLAN is different from the management VLAN, you must specify an IP address for the CIP VLAN. Make sure that the IP address that you assign to the switch is not being used by another device in your network.
  - **Subnet Mask:** Select a mask from the drop-down list.
- For more information about the CIP VLAN settings, click **Help** on the toolbar.
- 
- Step 11** Enter the Optional Settings now, or enter them later by using the device manager interface:
- Enter a **Host Name** for the switch.
  - Select **Enable** or **Disable** for Telnet access. If enabled, enter and confirm the Telnet password in the **Password** fields.
  - The date and time fields are populated from your PC.
  - Click **Enable** to use Daylight Saving Time.
- For more information about the optional settings, click **Help** on the toolbar.
- 
- Step 12** Click **Submit** to save the information that you entered and to finish the basic configuration. You have completed the initial switch setup. If you click **Cancel**, the fields are cleared, and you can start over.
- 
- Step 13** Turn off DC power at the source, disconnect all cables to the switch, and install the switch in your network. See the “Managing the Switch” section for information about configuring and managing the switch.
- 

## Warning Statement 1067

This warning statement has been removed from the *Cisco IE 3000 Switch Getting Started Guide* on Cisco.com.

## Grounding the Switch

Step 6: Use a ratcheting torque screwdriver to tighten the ground screw and ring terminal lug to the switch front panel to 8.5 in-lb, the maximum recommended torque.

## Wiring the DC Power Source

Step 6: Use a ratcheting torque flathead screwdriver to torque the power and relay connector captive screws (above the installed wire leads) to 2 in-lb, the maximum recommended torque.

## Resetting the Switch

Follow these steps to return your switch to the factory default settings. These are reasons why you might want to reset the switch:

- You installed the switch in your network and cannot connect to it because you assigned the wrong IP address.
- You want to clear all configurations from the switch and assign a new IP address.
- You want to reset the password on the switch.

**Caution**

---

Resetting the switch deletes the configuration and reboots the switch.

---

To reset the password on the switch:

1. Power off the switch.
2. Power on the switch, and at the same time, press and hold down the Express Setup button until all the system LEDs turn red.
3. Release the Express Setup button, and the switch continues to boot.

After the switch restarts, continue to run Express Setup.

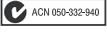
## Updates to the Regulatory Compliance and Safety Information for the Cisco IE 3000 Switch

### Warning Statement 1067

Warning statement 1067 has been removed from the *Regulatory Compliance and Safety Information for the Cisco IE 3000 Switch* on Cisco.com.

# Compliance Labels

Figure 1 Compliance Label for the Cisco IE 3000 Switch

 <p>1. 기기의 명칭 (모델명): 2. 제조년월일: 3. 제조사/제조국가: Cisco Systems, Inc. 4. 인증발급자의 식별부호:</p>	<p>MAC ADDRESS</p> <p>PID / VID</p>
<p>Cisco Systems, Intl., BV 170 West Tasman Dr San Jose, Ca 95134 USA</p> <p> <a href="http://cisco-returns.com">http://cisco-returns.com</a></p>	
<p>  ACN 050-332-940</p> <p> </p>	<p>MODEL NO.</p> <p>IOS VERSION</p> <p>PRODUCT OF</p>
<p>18-60V ~, 2.0 A -40°C to +80°C IND. CONT. EQ. FOR USE IN HAZARDOUS LOCATIONS ALSO LISTED AS: I.T.E. FOR USE IN HAZARDOUS LOCATIONS Class I, Div. 2, Groups A B C D Class I, Zone 2, Group IIC Ex nC nL II C T4 X AEx nC II C T4 X</p> <p>  LISTED 5BA2</p> <p></p> <p>CE  II 3 G, DEMKO 08ATEX0723302X</p>	
<p>This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.</p>	<p><b>CUIDADO</b> PARTES ADENTRO NO REPARABLES PRO EL OPERADOR. REFERIR REPARO A PERSONAL AUTORIZADO.</p> <p><b>ATTENTION</b> ENTRETIEN ET REPARATIONS INTERIEURES NE SONT AUTORISEES QU'AU PERSONNEL TECHNIQUE QUALIFIE.</p> <p><b>CAUTION</b> NO OPERATOR SERVICEABLE PARTS INSIDE. REFER SERVICING TO QUALIFIED PERSONNEL.</p>
<p>This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.</p>	
<p>この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A</p>	
<p>警告使用者： 這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。</p>	
<p>CLEI CODE</p> <p><input type="text"/></p>	
<p>SERIAL NO.</p> <p><input type="text"/></p>	
<p>47-20864-01 REV. B0</p>	<p>204083</p>

**Figure 2 Compliance Label for the Cisco IE 3000 Switch Extension Module**

Cisco Systems, Intl., BV 170 West Tasman Dr San Jose, Ca 95134 USA		 <a href="http://cisco-returns.com">http://cisco-returns.com</a>	
		 ACN 050-332-940	
			
-40°C ≤ T ≤ 60°C			
IND. CONT. EQ. FOR USE IN HAZARDOUS LOCATIONS ALSO LISTED AS: I.T.E. FOR USE IN HAZARDOUS LOCATIONS Class I, Div. 2, Groups A B C D Class I, Zone 2, Group IIC Ex nA II C T4 X AEx nA II C T4 X		 	
C E  DEMKO 08ATEX0723302X			
MODEL NO.		PID / VID	
IOS VERSION			
PRODUCT OF			
CLEI CODE		SERIAL NO.	
<input type="text"/>		<input type="text"/>	
47-21200-01 REV. B0			

204360

## Updates to the Hardware Installation Guide

This update is for the “Overview” chapter. These switches were added:

**Table 5 Cisco IE 3000 Switch Model Descriptions**

Switch Model	Description
Cisco IE-3000-4TC-E	4 10/100BASE-T Ethernet ports and 2 dual-purpose ports (supports the IP services software feature set)
Cisco IE-3000-8TC-E	8 10/100BASE-T Ethernet ports and 2 dual-purpose ports (supports the IP services software feature set)

This update is for the “Technical Specifications” chapter.

The technical specifications listed in Table A-2 for the Cisco IE-3000-8TC and IE-3000-4TC switches also apply to the Cisco IE-3000-4TC-E and IE-3000-4TC-E switches.

## Updates to the System Message Guide

This section contains the system message guide updates.

### New System Messages

These messages were added to the system message guide:

**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.

**Note**


---

This messages applies to switches running the IP base image.

---

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

**Explanation** An attempt was made to assign a primary VLAN to an 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** Use a different VLAN.

**Note**


---

This messages applies to switches running the IP base image.

---

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

**Explanation** An attempt was made to assign a nonsecondary VLAN to a private VLAN host IEEE 802.1x port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

**Recommended Action** Change the mode of the port so that it is no longer a PVLAN host port or use a valid secondary VLAN.

**Note**


---

This messages applies to switches running the IP base image.

---

**Error Message** DOT1X\_SWITCH-5-ERR\_PRIMARY\_VLAN\_NOT\_FOUND: Attempt to assign VLAN [dec], whose primary VLAN does not exist or is shutdown, to 802.1x port [chars] AuditSessionID [chars]

**Explanation** An attempt was made to assign a private VLAN whose primary VLAN does not exist or is shut down. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

**Recommended Action** Make sure the primary VLAN exists and is not shut down. Verify that the private VLAN is associated with a primary VLAN.

**Note**


---

This messages applies to switches running the IP base image.

---

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

**Explanation** An attempt was made to assign a secondary VLAN to a port that is not a private VLAN host 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 mode of the port so that it is configured as a private VLAN host port, or use a different VLAN that is not configured as a secondary VLAN.

**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 System Messages

These messages were deleted from the system message guide:

**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.



### Note

---

This messages applies to switches running the IP base image.

---

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

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

**Recommended Action** Use a different VLAN.

**Note**


---

This messages applies to switches running the IP base image.

---

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

**Explanation** An attempt was made to assign a nonsecondary VLAN to a private VLAN host IEEE 802.1x port. [dec] is the VLAN, and [chars] is the port.

**Recommended Action** Change the mode of the port so that it is no longer a private VLAN host port, or use a valid secondary VLAN.

**Note**


---

This messages applies to switches running the IP base image.

---

**Error Message** DOT1X\_SWITCH-5-ERR\_PRIMARY\_VLAN\_NOT\_FOUND: Attempt to assign VLAN [dec], whose primary VLAN does not exist or is shutdown, to 802.1x port [chars]

**Explanation** An attempt was made to assign a private VLAN whose primary VLAN does not exist or is shut down. [dec] is the VLAN, and [chars] is the port.

**Recommended Action** Make sure the primary VLAN exists and is not shut down. Verify that the private VLAN is associated with a primary VLAN.

**Note**


---

This messages applies to switches running the IP base image.

---

**Error Message** DOT1X\_SWITCH-5-ERR\_SEC\_VLAN\_INVALID: Attempt to assign secondary VLAN [dec] to non-PVLAN host 802.1x port [chars]

**Explanation** An attempt was made to assign a secondary VLAN to a port that is not a private VLAN host port, which is not allowed. [dec] is the VLAN, and [chars] is the port.

**Recommended Action** Change the mode of the port so that it is configured as a private VLAN host port, or use a different VLAN that is not configured as a secondary VLAN.

**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.

## Related Documentation

These documents provide complete information about the Cisco IE 3000 switches and are available at Cisco.com:

[http://www.cisco.com/en/US/products/ps9703/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9703/tsd_products_support_series_home.html)

- *Cisco IE 3000 Switch Software Configuration Guide*
- *Cisco IE 3000 Switch Command Reference*
- *Cisco IE 3000 Switch System Message Guide*
- *Cisco IE 3000 Switch Hardware Installation Guide*
- *Cisco IE 3000 Switch Getting Started Guide*—available in English, simplified Chinese, French, German, Italian, Japanese, Brazilian Portuguese and Spanish

For other information about related products, see these documents:

- Device manager online help (available on the switch)
- *Getting Started with Cisco Network Assistant*
- *Release Notes for Cisco Network Assistant*

These SFP module installation notes are available from this Cisco.com site:

[http://www.cisco.com/en/US/products/hw/modules/ps5455/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html)

- *Cisco Small Form-Factor Pluggable Modules Installation Notes*
- *Cisco CWDM GBIC and CWDM SFP Installation Note*

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](http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html)

- Cisco Small Form-Factor Pluggable Modules Compatibility Matrix
- Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules

## Obtaining Documentation, Obtaining Support, and Security Guidelines

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

© 2009-2010 Cisco Systems, Inc. All rights reserved.