



Release Notes for the Cisco IE 3000 Switch, Cisco IOS Release 12.2(44)EX and Later

Revised July 31, 2008

Cisco IOS Release 12.2(44)EX and later runs on all Cisco IE 3000 switches.

These release notes include important information about Cisco IOS Release 12.2(44)EX 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 5](#).
- 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 20](#).

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>

This software release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com in the Cisco IOS software area.



Americas Headquarters:

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

Contents

This information is in the release notes:

- [System Requirements, page 2](#)
- [Upgrading the Switch Software, page 5](#)
- [Installation Notes, page 8](#)
- [New Features, page 8](#)
- [Limitations and Restrictions, page 8](#)
- [Important Notes, page 13](#)
- [Open Caveats, page 14](#)
- [Resolved Caveats, page 16](#)
- [Documentation Updates, page 17](#)
- [Related Documentation, page 20](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 21](#)

System Requirements

The system requirements are described in these sections:

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

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 ¹	512 MB ²	256	1024 x 768	Small

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

Software Requirements

Table 4 lists the supported operating systems and browsers for using the device manager. The device manager verifies the browser version when starting a session to ensure that the browser is supported.


Note

The device manager does not require a plug-in.

Table 4 **Supported Operating Systems and Browsers**

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer	Mozilla FireFox
Windows 2000	None	6.0 or 7.0	1.5 or 2.0
Windows 2003	None	6.0 or 7.0	1.5 or 2.0
Windows XP	None	6.0 or 7.0	1.5 or 2.0
Vista	None	6.0 or 7.0	1.5 or 2.0

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(44)EX and later is only compatible with Cisco Network Assistant (CNA) 5.4 and later. 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 5](#)
- [Deciding Which Files to Use, page 5](#)
- [Archiving Software Images, page 6](#)
- [Upgrading a Switch by Using the Device Manager or Network Assistant, page 6](#)
- [Upgrading a Switch by Using the CLI, page 7](#)
- [Recovering from a Software Failure, page 8](#)

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 5](#) lists the filenames for this software release.

Table 5 *Cisco IOS Software Image Files*

Filename	Description
ies-lanbase-tar.122-44.EX1.tar	Catalyst IE 3000 image file and device manager files. This image has Layer 2+ features.
ies-lanbasek9-tar.122-44.EX1.tar	Catalyst IE 3000 cryptographic image file and device manager files. This image has the Kerberos and SSH features.

Archiving Software Images

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

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

http://www.cisco.com/en/US/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

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 5 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.122-44.EX.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

For a list of all supported hardware, see the [“Hardware Supported” section on page 2](#).

New Software Features

This release is the first software release for the Cisco IE 3000 switches. For a detailed list of key features for this software release, see the *Cisco IE 3000 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.

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 10](#)
- [Multicasting, page 10](#)
- [QoS, page 11](#)
- [SPAN and RSPAN, page 12](#)
- [Trunking, page 12](#)
- [VLAN, page 12](#)

Configuration

These are the configuration limitations:

- 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).

Ethernet

These is the Ethernet limitation:

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

This is the IP limitation:

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

These are the multicasting limitations:

- 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 IG MP 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

These are the quality of service (QoS) limitations:

- 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

These are the SPAN and Remote SPAN (RSPAN) limitations.

- 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

These are the trunking limitations:

- 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

These are the VLAN limitations:

- 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

This is the device manager limitation:

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

This section describe the important notes related to this software release for the Cisco IE 3000 switches.

Device Manager Notes

These notes apply to the device manager:

- 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:

- Choose **Tools > Internet Options**.
 - Click **Settings** in the “Temporary Internet files” area.
 - From the Settings window, choose **Automatically**.
 - Click **OK**.
 - 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	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. <ul style="list-style-type: none"> 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.

	Command	Purpose
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 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 {enable local tacacs}	Configure the HTTP server interface for the type of authentication that you want to use. <ul style="list-style-type: none"> 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. tacacs—TACACS server is used.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.

Open Caveats

This section describes the open caveats in this software release:

- CSCsc96474

The switch might display tracebacks similar to these examples when a large number of IEEE 802.1x supplicants try to repeatedly log in and log out.

Examples:

```
Jan 3 17:54:32 L3A3 307: Jan 3 18:04:13.459: %SM-4-BADEVENT: Event 'eapReq' is invalid
for the current state 'auth_bend_idle': dot1x_auth_bend Fa9
```

```
Jan 3 17:54:32 L3A3 308: -Traceback= B37A84 18DAB0 2FF6C0 2FF260 8F2B64 8E912C Jan 3
19:06:13 L3A3 309: Jan 3 19:15:54.720: %SM-4-BADEVENT: Event 'eapReq_no_reAuthMax' is
invalid for the current ate 'auth_restart': dot1x_auth Fa4
```

```
Jan 3 19:06:13 L3A3 310: -Traceback= B37A84 18DAB0 3046F4 302C80 303228 8F2B64 8E912C
Jan 3 20:41:44 L3A3 315: .Jan 3 20:51:26.249: %SM-4-BADEVENT: Event 'eapSuccess' is
invalid for the current state 'auth_restart': dot1x_auth Fa9
```

```
Jan 3 20:41:44 L3A3 316: -Traceback= B37A84 18DAB0 304648 302C80 303228 8F2B64 8E912C
```

There is no workaround.

- CSCsd03580

When IEEE 802.1x is globally disabled on the switch by using the **no dot1x system-auth-control** global configuration command, some interface level configuration commands, including the **dot1x timeout** and **dot1x mac-auth-bypass commands**, become unavailable.

The workaround is to enable the **dot1x system-auth-control** global configuration command before attempting to configure interface level IEEE 802.1x parameters.

- CSCsk65142

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.

- CSCsi70454

The configuration file used for the configuration replacement feature requires the character string *endn* at the end of the file. The Windows Notepad text editor does not add the *endn* string, and the configuration rollback does not work.

These are the workarounds. (You only need to do one of these.)

- Do not use a configuration file that is stored by or edited with Windows Notepad.
- Manually add the character string *endn* to the end of the file.

- CSCsj87991

A switch configured for Link Layer Discovery Protocol (LLDP) might not correctly report the enabled switch capabilities in the LLDP type, length, and value (TLV) attributes. System capabilities appear correctly, but the enabled capabilities are not identified if the switch is configured only as a Layer 2 switch.

There is no workaround.

- CSCsj88169

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.

- 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.

- CSCso00078

When a 100FX-FE SFP module is connected to the switch, and you change the media-type from SFP to copper, the copper link does not come up. This problem only occurs when two IE3000 switches are connected with both copper and fiber connections on the same port.

These are the workarounds:

- To bring the fiber link back up, set the media-type to SFP module mode.
- To bring the copper link back up, reload the switch.

- CSCsq19944

When configuring a switch management VLAN to be another VLAN during Express Setup, the PC loses the network connection to the switch if it remains connected to the same port.

These are the workarounds:

- Unplug the PC that was running Express Setup, and plug it into a different port.
- Change the management VLAN by using the device manager.

- CSCsq52244

When a diagnostic or port mirroring role is defined on an interface and you change it to another port role, the port role icon in device manager shows as **Unknown**.

The workaround is to configure the port role on the interface to **none** before you configure the other port roles.

- CSCsq76774

If you remove the secure MAC address from an interface through CIP (Common Industrial Protocol), the **switchport port-security violation restrict** CLI configuration remains on the interface.

The workaround is to use the CLI to remove any settings remaining on the port.

- 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.

Resolved Caveats

These are the caveats resolved in Cisco IOS Release 12.2(44)EX1:

- CSCsq03277

When you disable switch ports over CIP through the output assembly, the switch no longer fails to disable switch ports.

- CSCsq77659

This version of the software contains the latest version of the EDS (Electronic Data Sheet) files.

- CSCsq85207

The redundant power status in the CIP switch parameter is now consistent with the output from the **show facility-alarm status** user EXEC command.

- CSCsq92092

During the ODVA (Open DeviceNet Vendors Association) encapsulation test, the switch no longer fails at the maximum-size NOP packet test. The switch no longer replies to the UnRegister session message.

The ODVA File object test no longer fails when the file size is a multiple of the transfer buffer size. After loading the EDS file, the EDS file now correctly changes to the FileLoaded state.

- CSCsq92227

The switch no longer returns a success response for a request to set an invalid interface configuration attribute value at the CIP TCP/IP interface object.

- CSCsq92438

The autonegotiation status is now set in the CIP InterfaceFlag attribute of the Ethernet link object.

- CSCsr05262

The CIP **get** and **set** services no longer return invalid data or cause the switch to fail for invalid Ethernet link instances. Instead, the invalid destination error is returned.

The CIP response that is returned after you set the file type attribute is now formatted correctly.

When you use the CIP **set** service on read-only attributes, you now receive an error response. When you set read-only attributes of the vlan and config file instances you now receive correct error code.

When a CIP file download transfer is aborted, the file object now returns to the fileEmpty state.

- CSCsr23823

The CIP Ethernet link object no longer returns a blank MAC address for the physical address attribute of instance 27. Instance 27 is the switch virtual interface over which CIP traffic passes.

Documentation Updates

These sections provide updates to the product documentation:

- [“Updates to the Cisco IE 3000 Switch Getting Started Guide” section on page 17](#)
- [“Documentation Updates to the Regulatory Compliance and Safety Information for the Cisco IE 3000 Switch” section on page 18](#)

Updates to the Cisco IE 3000 Switch Getting Started Guide

These corrections were made to the English version of the *Cisco IE 3000 Switch Getting Started Guide* on Cisco.com.

Warning Statment 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.

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

This information in the “Regulatory Standards Compliance” section has been revised in the *Regulatory Compliance and Safety Information for the Cisco IE 3000 Switch* on Cisco.com.







Warning Statment 1067

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

Compliance Label

The compliance labels for the switch are shown in [Figure 1](#) and [Figure 2](#).

Figure 1 Compliance Label for the Cisco IE 3000 Switch

 <p>1. 기기의 명칭 (모델명): 2. 제조년월일: 3. 제조자/제조국가: Cisco Systems, Inc. 4. 인증받은자의 식별부호:</p> <p>Cisco Systems, Intl., BV 170 West Tasman Dr San Jose, Ca 95134 USA http://cisco-returns.com</p> <p>     ACN 050-332-940</p> <p>18-60V ~, 2.0 A -40°C to 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 nC nL II C T4 X AEx nC II C T4 X CE II 3 G, DEMKO 08ATEX0723302X</p>	<p>MAC ADDRESS</p> <p>PID / VID</p> <p>MODEL NO.</p> <p>IOS VERSION</p> <p>PRODUCT OF</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>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> <div style="border: 1px solid black; height: 30px; width: 100%;"></div>	<p>CUIDADO PARTES ADENTRO NO REPARABLES PRO EL OPERADOR. REFERIR REPARO A PERSONAL AUTORIZADO.</p> <p>ATTENTION ENTRETIEN ET RÉPARATIONS INTERNES NE SONT AUTORISÉS QU'AU PERSONNEL TECHNIQUE QUALIFIÉ.</p> <p>CAUTION NO OPERATOR SERVICEABLE PARTS INSIDE. REFER SERVICING TO QUALIFIED PERSONNEL.</p>
<p>SERIAL NO.</p> <div style="border: 1px solid black; height: 30px; width: 100%;"></div>	
<p>47-20864-01 REV. B0</p>	

204083

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
http://cisco-returns.com

GS
CE
ACN 050-332-940
ANATEL

-40°C ≤ T_a ≤ 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

UL US LISTED 5BA2
20

CE II 3 G, DEMKO 08ATEX0723302X

MODEL NO. PID / VID

IOS VERSION

PRODUCT OF

CLEI CODE SERIAL NO.

47-21200-01 REV. B0

204350

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

- *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

- *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

- 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. CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0805R)