Release Notes for the Cisco IE 3000 Switch, Cisco IOS Release 12.2(50)SE and later

Revised October 5, 2010

Cisco IOS Release 12.2(50)SE and later runs on all Cisco IE 3000 switches.

These release notes include important information about Cisco IOS Release 12.2(50)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 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 34.

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

The system requirements are described in these sections:

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 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[1]	512 MB[2]	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/pcgi-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

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.

Table 4 Cisco IOS Software Image Files

Filename	Description
ies-lanbase-tar.122-50.SE5.tar	Catalyst IE 3000 image file and device manager files. This image has Layer 2+ features.
ies-lanbasek9-tar.122-50.SE5.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 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.122-46.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

- DHCP reserved-only option to allow users to allocate only reserved addresses in the Dynamic Host Configuration Protocol (DHCP) address pool.
- Network Edge Access Topology (NEAT) with 802.1X switch supplicant, host authorization with CISP, and auto enablement to authenticate a switch outside a wiring closet as a supplicant to another switch.
- IEEE 802.1x with open access to allow a host to access the network before being authenticated.
- IEEE 802.1x authentication with downloadable ACLs and redirect URLs to allow per-user ACL downloads from a Cisco Secure ACS server to an authenticated switch.
- Flexible-authentication sequencing to configure the order of the authentication methods that a port tries when authenticating a new host.
- Multiple-user authentication to allow more than one host to authenticate on an 802.1x-enabled port.
- IP source guard restricts traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings.
- Dynamic ARP inspection to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN.
- Wired location service sends location and attachment tracking information for connected devices to a Cisco Mobility Services Engine (MSE).
- CPU utilization threshold trap monitors CPU utilization.
- Support for the Cisco IOS Configuration Engine, previously referred to as the Cisco IOS CNS agent.
- Support for Embedded Event Manager Version 2.4.
- LLDP-MED network-policy profile time, length, value (TLV) for creating a profile for voice and voice-signalling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.
- RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group.
- Support for Resilient Ethernet Protocol (REP) for improved convergence times and network loop prevention without the use of spanning tree, including configuration of REP edge ports when the neighbor port is not REP-capable.

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

These limitations apply to the Cisco IE 3000 switches:

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).

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 (that is, 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 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

- 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	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**aaa** | **enable** | **local**}	Configure the HTTP server interface for the type of authentication that you want to use. • **aaa**—Enable the authentication, authorization, and accounting feature. You must enter the **aaa new-model** interface configuration command for the **aaa** keyword to appear. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

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

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

  If you 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. • **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

- 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.

- 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.

- 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.

- CSCti79385

  When a redirect URL is configured for a client on the authentication server and a large number of clients are authenticated, high CPU usage could occur on the switch.

  There is no workaround.

Resolved Caveats

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE5

- CSCte14603

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

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

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

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

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

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

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE4

- CSCsh59019

  Authentication, authorization, and accounting (AAA) fails, preventing authentication and requiring you to recover your password. For example, when you enter the **aaa authentication login default group tacacs line** global configuration command, AAA fails.

  There is no workaround.

- CSCsk85192

  When you use an access control server (ACS) to enable command authorization, the ACS does not process a **copy** command ending with a colon (for example, *scp***:**, *ftp***:**, *tftp***:**, *flash***:**).

  This problem affects authentication, authorization, and accounting (AAA) authorization:

  - If the ACS denies a **copy** command ending with a colon, you *can* use that command on a switch.
  - If the ACS permits a **copy** command ending with a colon, you *cannot* use that command on a switch.

  To workaround is to either deny or permit the **copy** command without entering any arguments on the ACS.

- CSCsv93104

  When a Catalyst IE 3000 master switch is configured for Precision Time Protocol (PTP) and a port operates at 1 GB/s while a member-switch port operates at 100 Mb/s (or the reverse), a 5-microsecond delay occurs between the ports.

  The workaround is to ensure that the master-switch port and the member-switch port operate at the same speed.

- CSCsy83366

  On a switch that is configured for quality of service (QoS), a memory leak occurs when a small portion (about 90 bytes) of the processor memory is not released by the HRPC QoS request handler process.

  There is no workaround.

- 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.

- CSCta09189

  Packet loss and output drops occur on the egress interface for routed multicast traffic.

  This problem occurs when multiple S,G entries time out at the same time and then are re-established at the same time, when multiple Protocol Independent Multicast (PIM) neighbors time out at the same time and then are re-established at the same time, or when multiple high-volume multicast streams are routed through multiple Layer-3 interfaces.

Use one of these workarounds:

- Enter the **clear ip mroute *** EXEC command.
- Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the egress interface.

- 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.

- CSCta87523

  When you use Auto Smartports macros on an interface that is connected to an Cisco IP phone, the the quality of service (QoS) configuration for that interface is not completed.

  The workaround is to enter the **no mls qos vlan-based** interface configuration command, and then enable QoS for voice over IP (VoIP) by entering the **auto qos voip cisco-phone** interface configuration command.

- CSCtb10158

  A switch can fail when an SNMP process attempts to configure dot1x authentication when it is already configured.

  There is no workaround.

- CSCtb91572

  A switch enters a loop in which it continues to fail after it first has failed while starting, and then has failed again while attempting to recover. This failure loop occurs only after you have entered the **archive upload-sw** privileged EXEC command to write the configuration to a remote server using Secure Copy Protocol (SCP) and when the connection to the remote server is configured for spanning-tree PortFast.

  The workaround is to not use SCP to write to the remote server. Use File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP).

- CSCtc39809

  A memory leak occurs when there is a stuck in active (SIA) state condition for an Enhanced Interior Gateway Routing Protocol (EIGRP) route.

  There is no workaround.

- CSCtc43231

  A switch does not receive SNMP trap and inform messages from the correct interface after you have entered the **snmp-server trap-source loopback0** and **snmp-server source-interface informs loopback0** global configuration commands.

  There is no workaround.

- CSCtc57809

  When the **no mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* global configuration command is used to remove a dynamically learned MAC address, the switch fails under these conditions:

  - The physical interface is in a *no shut* state.
  - The MAC address is first dynamically learned and then changed to static.

  There is no workaround.

- CSCtc70571

  When you have configured an output service policy, performing an SNMPWALK on cportQosStatistics causes loops.

  There is no workaround.

- CSCtc90039

  A memory leak occurs on a device that uses Enhanced Interior Gateway Routing Protocol (EIGRP) when the external routes are being exchanged.

  The workaround is to stabilize the network to minimize the impact of external route advertisement.

- CSCtd17296

  When you enter the **dot1x pae** interface configuration command on a switch access port and then enable an access list in the inbound direction on an ingress switched virtual interface (SVI), the access list does not work, allowing all packets to pass.

  The workaround is to enable the access list in the outbound direction on the egress SVI.

- CSCtd30053

  When you enter the **no spanning-tree etherchannel guard misconfig** global configuration command, enter the **write memory** privileged EXEC command, and then restart the switch, the **spanning-tree etherchannel guard misconfig** global configuration command is saved instead of the **no** form of this command.

  There is no workaround.

- CSCtd31242

  An IP phone loses network connectivity under these conditions:

  - The IP phone is authenticated by MAB (in Open1x mode) on a supplicant switch.
  - The supplicant switch is connected to an authenticator switch through the NEAT protocol.

  A call is placed using the IP phone. After approximately 5 minutes, network connectivity to the phone is lost.

  The workaround is to statically configure the MAC address of the IP phone on the authenticator switch.

- CSCtd72456

  After you have entered the **snmp-server host informs** global configuration command to enable SNMP informs on a switch, the switch might fail if you enter the **show snmp pending** user EXEC command.

  There is no workaround. Do not enter the show command when SNMP informs are enabled.

- CSCtd72626

  A Remote Switched Port Analyzer (RSPAN) does not detect IPv6 multicast packets on an RSPAN destination port.

  There is no workaround.

- CSCtd73256

  A switch fails when you enter the **show ip ospf interface** user EXEC command and then stop the command output at the this line:

  ```
  Backup Designated router (ID) xx.x.x.x, Interface address xx.x.x.x
  ```

  The failure occurs when the Backup Designated Router (BDR) neighbor of the switch is shut down while you press Enter or the spacebar to advance the command output.

  When the switch fails, it sends this error message:

  ```
  Unexpected exception to CPUvector 2000, PC = 261FC60
  ```

  There is no workaround.

- CSCte67201

  On a switch that is configured for IP routing and that is running Cisco IOS Release 12.2(50)SE or later, Cisco Express Forwarding (CEF) can use a large amount of memory. The IP RIB Update process uses about 2000 bytes for each prefix that CEF uses.

  There is no workaround. You can reduce the memory use by reducing the number of routes the switch processes.

- CSCte81321

  After you have entered the **logging filter** global configuration command on a switch to specify a syslog filter module to be used by the Embedded Syslog Manager (ESM), processes logging many system messages retain increasing amounts of processor memory.

  The workaround is to enter the **no logging filter** global configuration command.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE3

- CSCso57496

  A switch no longer fails when you enter the **configure replace** privileged EXEC command, and a banner is already present in the switch configuration.

- CSCsq51052

  The output of the **show ip ssh** privileged EXEC command no longer displays *SSH Enabled - version 2.99*. Instead, a correct SSH version (*1.5*, *1.99* or *2.0*) now appears.

- CSCsw45277

  Third-party IP phones now automatically power up when reconnected to enabled PoE ports on the switch.

- CSCsx49718

  Re-authentication now occurs on a port under these conditions:

  - The port is in single-host mode.
  - The port is configured with the **authentication event no-response action authorize vlan** *vlan-number* command.
  - An EAPOL start packet is sent to the port.

- CSCsy48370

  The switch no longer fails when you use the **vacant-message** line configuration command.

- CSCsy66686

  The switch no longer reloads when the default port cost of service (CoS) value is updated on a port that has a policy map configured and CoS override enabled with the **mls qos cos override** privileged EXEC command.

- CSCsy72669

  If a link failure occurs on a secondary edge port, preemption now occurs after the link comes up.

- CSCsz12381

  When open1x authentication and MAC authentication bypass are enabled on a port, an IP phone is connected to the port, and DHCP snooping is enabled on the switch, DHCP traffic is now forwarded on the voice VLAN before open 1x authentication times out and the switch uses MAC authentication bypass to authorize the port.

- CSCsz13490

  The switch no longer reloads when you enter several key strokes while in interface-range configuration mode.

- CSCsz14369

  If MAC authentication bypass is enabled and the RADIUS server is not available, the switch now tries to re-authenticate a port after a server becomes available.

- CSCsz79652

  A memory leak no longer occurs when Cisco Network Assistant is polling the switch and the **ip http server** or **ip http-secure-server** global configuration command is enabled.

- CSCsz81762

  If you enable automatic server testing through the **radius-server host** *ip-address* [**test username** *name*] global configuration command, the switch no longer sends requests to the RADIUS server if the server is not available.

- CSCta32597

  A switch no longer fails when a host moves from a dynamically assigned VLAN to a configured VLAN.

- CSCta36155

  A switch configured with 802.1x and port security on the same ports no longer might inappropriately put the ports into an error-disabled state.

- CSCta56469

  Moving a PC between two IP Phones without disconnecting either phone from the switch no longer triggers a port-security violation.

- CSCta67777

  A port security violation error no longer occurs when MAC address sticky learning is enabled on a port and a CDP is enabled on a connected IP Phone.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE2

- CSCsg00102

  Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

  Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed.

  This vulnerability is documented in CSCso04657 and CSCsg00102, both of which are required for a full fix.

- CSCsz25416

  This release addresses several issues regarding Common Industrial Protocol (CIP) compliance.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE1

- CSCej42445

  Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) authentication no longer fails on an interface that is configured with TACASC+.

- CSCsb46724

  If the connection to a primary AAA server fails, the backup server is now queried for login access.

- CSCsr92741

  When a TCP packet with all flags set to zero (at the TCP level) is sent to a remote router, the remote (destination) router no longer returns an ACK/RST packet back to the source of the TCP segment.

- CSCsy24510

  The switch now accepts an encrypted secret password.

- CSCsy41470

  The switch no longer runs out of memory when an smnpwalk, snmpget, or snmpbulkwalk is run on the CISCO-ENERGYWISE-MIB

- CSCsy45235, CSCsy62256, CSCsy74548, CSCsx59130, CSCsx82691

  This release addresses several issues regarding Common Industrial Protocol (CIP) compliance.

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(50)SE

- CSCsq67398

  Traffic is now forwarded to the interfaces that are configured with static multicast MAC addresses after the switch is reloaded.

Note You cannot configure the static MAC address (unicast or multicast) entries on EtherChannel member interfaces, or add an interface into the EtherChannel if that interface is associated with a static MAC address entry.

- CSCsr50766

  When keepalive is disabled on an interface, the interface is no longer put in an error-disabled state when it receives keepalive packets.

- CSCsr64007

  The Switched Port Analyzer (SPAN) destination port no longer detects IPv6 multicast packets from a VLAN that is not being monitored by SPAN.

- CSCsr65689

  This message no longer appears in the log during the system bootup on a switch that is running Cisco IOS 12.2(50)SE:

  ```
  %COMMON_FIB-3-FIBIDBINCONS2
  ```

- CSCsr79279

  When the switch is connected to a Catalyst 4500 E-Series Supervisor Engine 6-E and the cable is disconnected from the Catalyst 4500 switch, it now detects the link-down condition.

- CSCsu10065

  When SFP ports are configured as status multicast router ports, IPv6 Multicast Listener Discovery (MLD) snooping now works after the switch reloads.

- CSCsu57030

  The *PMD Auto-Negotiation Advertised Capability* is now correct on the GigabitEthernet switch ports.

- CSCsu59214

  The *`Set TxPortFifo SRR Failed`* message no longer appears when you enter both the s**rr-queue bandwidth shape 200 0 2 200** and the **priority-queue out** interface configuration commands on the same interface.

- CSCsu88168

  The switch no longer reloads when the Forwarding Information Base (FIB) adjacency table is added.

- CSCsv30429

  A Cisco IP Phone connected to a Catalyst switch no longer becomes unauthorized when it transitions from the data authorization domain to the voice authorization domain.

- CSCsv64023

  A switch port configured for IGMP snooping no longer lose its group membership when the port receives a query comes from an upstream device that is not configured for IGMP snooping.

- CSCsv89005

  A switch configured with class-based policies that are applied and active on at least one interface no longer might reload or display CPU hog messages during SNMP polling for the ciscoCBQosMIB.

- CSCsv91358

  When you have entered the **vlan dot1q tag native** global configuration command to configure a switch to tag native VLAN frames on 802.1Q trunk ports, and you configure a new voice VLAN on an access port, the MAC address of a connected PC is now correctly relearned.

- CSCsw30249

  When a switch virtual interface (SVI) is configured as unnumbered and is pointing to a loopback interface, the switch no longer fails when the SVI receives a packet.

- CSCsw45337

  When LLDP is enabled and a voice VLAN is configured, the L2 Priority and DSCP Value fields in the LLDP type, length, and value descriptions (TLVs) are now correctly marked to give the voice traffic the correct DSCP and Layer 2 priority.

- CSCsw65548

  Switch ports no longer attempt authentication at the interval configured for the port security timer instead of the configured IEEE 802.1x timer.

Documentation Updates

These sections provide updates to the product documentation:

Updates to the Software Configuration Guide and the Command Reference

The switch does not support Cisco EnergyWise, which manages the energy usage of power over Ethernet (PoE) entities.

Updates to the Cisco IE 3000 Switch 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*.

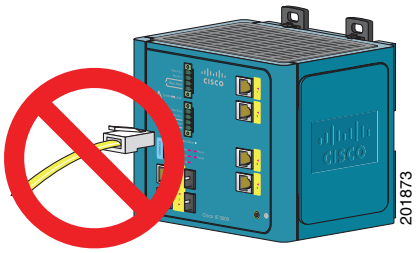
In the “Running Express Setup” section of the *Cisco IE 3000 Switch Getting Started Guide*, Steps 8 to 10 have changed.

Running Express Setup:

To run Express Setup:

Step 1 Make sure that nothing is connected to the switch.

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.



Step 2 Connect power to the switch.

See the wiring instructions in the "Grounding the Switch" section and the "Wiring the DC Power Source" section.

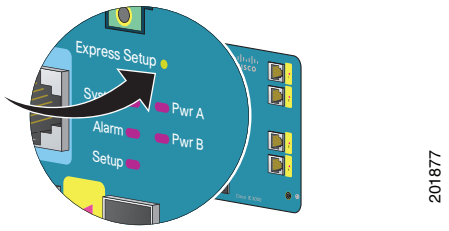
Step 3 When the switch powers on, it begins the power-on self-test (POST). During POST, the System LED blinks while a series of tests verify that the switch functions properly. Wait for the switch to complete POST, which takes approximately 1 minute.

Step 4 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.

If the switch fails POST, the System LED turns red. See the "In Case of Difficulty" section if your switch fails POST.

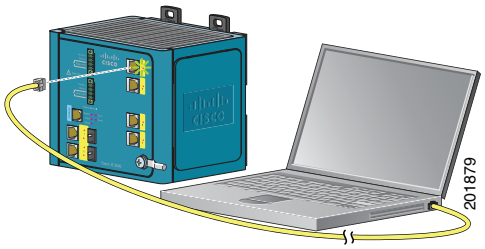
Step 5 Press the Express Setup button. This button is recessed behind the front panel, so you can use a simple tool, such as a paper clip.

When you press the Express Setup button, a switch port LED begins blinking green.



Step 6 Connect a Category 5 Ethernet cable (not provided) from the blinking switch port to the Ethernet port on your PC.

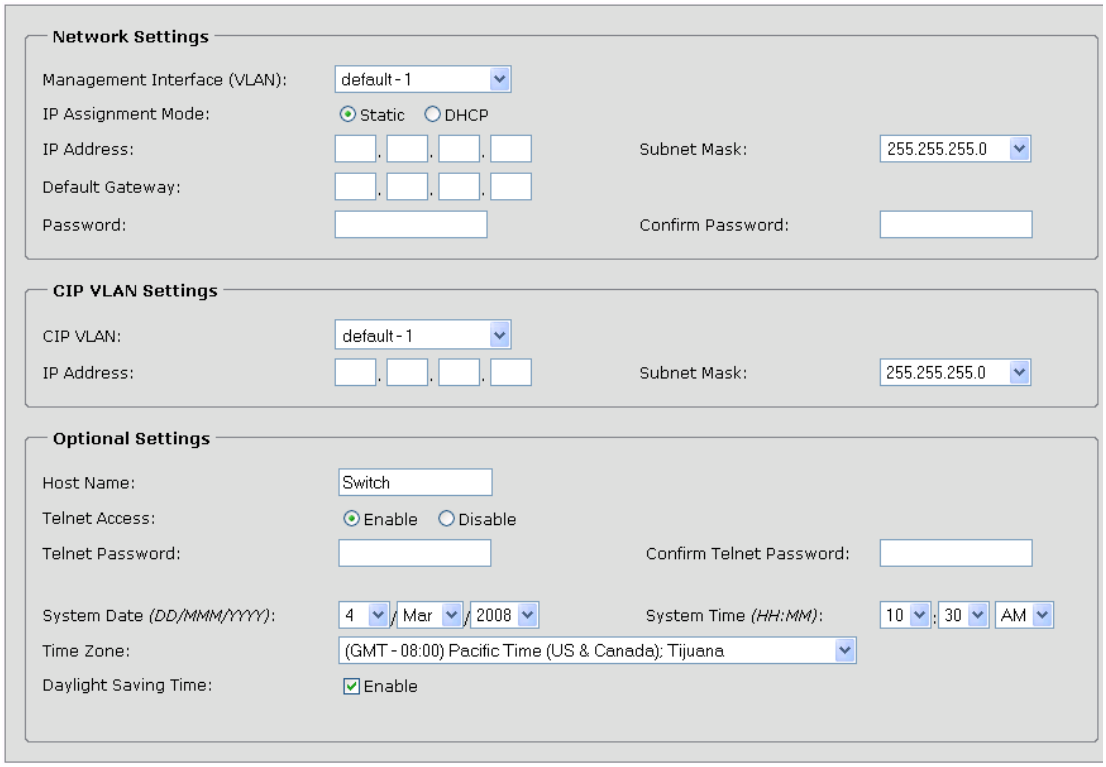
The port LEDs on your PC and the switch blink green while the switch configures the connection.



Step 7 When the Setup LED turns solid green, start a browser session on the PC.

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.



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

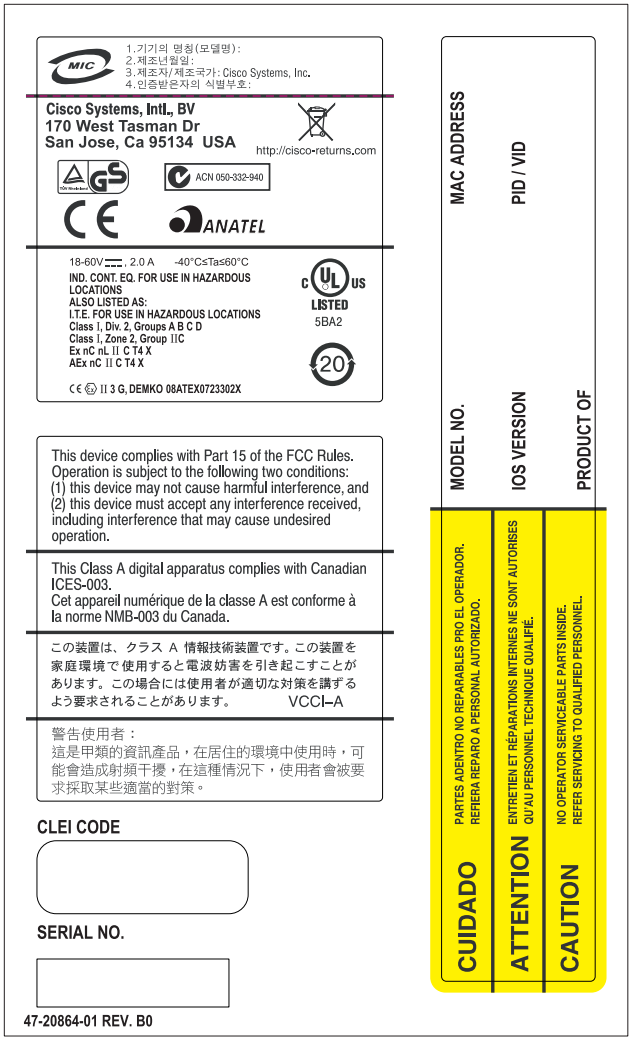
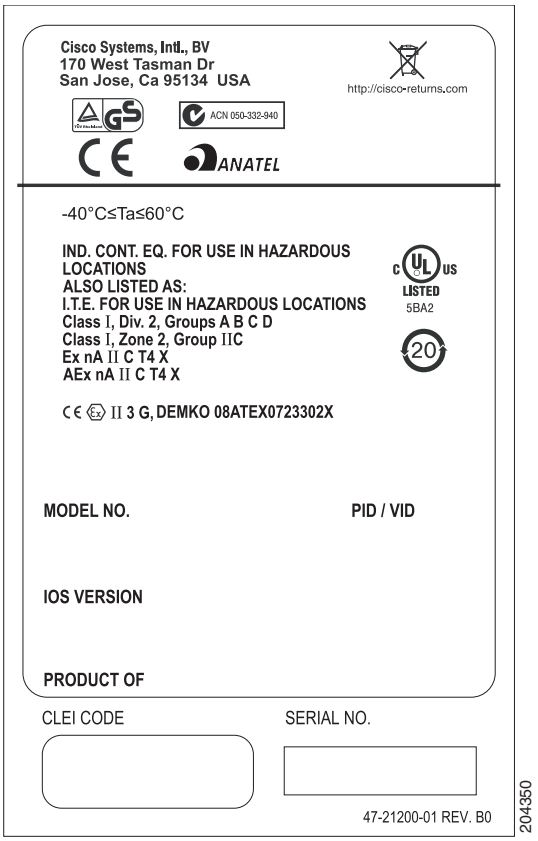


Figure 2 Compliance Label for the Cisco IE 3000 Switch Extension Module



Updates to the System Message Guide

Added System Messages

Error Message `ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]`

Explanation There are insufficient resources available to create a hardware representation of the ACL. A lack of available logical operation units or specialized hardware resources can cause this problem. Logical operation units are needed for a TCP flag match or a test other than **eq** (**ne**, **gt**, **lt**, or **range**) on TCP, UDP, or SCTP port numbers.

Recommended Action Modify the ACL configuration to use fewer resources, or rename the ACL with a name or number that alphanumerically precedes the other ACL names or numbers.

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

Explanation Authentication was unsuccessful. The first [chars] is the hostname, and the second [chars] is the interface.

Recommended Action No action is required.

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

Explanation Authentication was successful. The first [chars] is the host name, and the second [chars] is the interface.

Recommended Action No action is required.

Error Message `%DOT1X_SWITCH-4-PROC_START_ERR: Unable to start dot1x switch process.`

Explanation The software could not start the 802.1x authentication process.

Recommended Action Use the **reload** privileged EXEC command to reload the switch.

Error Message `%EC-5-MINLINKS_MET: Port-channel [chars] is up as its bundled ports ([dec]) meets min-links`

Recommended Action The administrative configuration of minimum links is equal to or less than the number of EtherChannel ports. The port channel is up. [chars] is the EtherChannel, and [dec] is the EtherChannel group number.

Recommended Action No action is required.

Error Message `%EC-5-MINLINKS_NOTMET: Port-channel [chars] is down bundled ports ([dec]) doesn't meet min-links`

Explanation The administrative configuration of minimum links is greater than the number of bundled ports. The port channel is down. [chars] is the EtherChannel, and [dec] is the EtherChannel group number.

Recommended Action Reduce the value of the minimum-links configuration parameter for an EtherChannel, or add more ports to the EtherChannel to create a bundle.

Error Message `%PHY-4-SFP_PLUS_NOT_SUPPORTED: The SFP PLUS in [chars] is not supported`

Explanation The Cisco X2 transceiver module is not supported on the switch. [chars] is the port in which the SFP module is inserted.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Enter the **show tech-support** user EXEC command to gather data that might help identify the nature of the error.

Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section on page 2-7.

Error Message `%SPANTREE_VLAN_SHIM-3-ADD_REGISTRY_FAILED: Subsystem [chars] fails to add callback function [chars]`

Explanation A subsystem has added its callback functions. Use this message only for debugging. The first [chars] is the subsystem name, and the second [chars] is the function name.

Recommended Action No action is required.

Error Message `%SPANTREE_VLAN_SHIM-2-MAX_INSTANCE: Platform limit of [dec] STP instances exceeded. No instance created for [chars] (port [chars]).`

Explanation The number of VLAN spanning-tree instances has reached the allowable maximum. No more VLAN instances are created until instances are less than the maximum. [dec] is the maximum, the first [chars] is the VLAN for which an STP instance is not created, and the second [chars] is the port number.

For example, when you are configuring spanning tree and the allowable maximum is 128 instances

- If the switch has already created 128 instances and you enter the **vlan 200-1000** global interface configuration command, the first [chars] is 200, and an STP instance for VLAN 200 is not created.
- If the switch has already created 100 instances and you enter the **vlan 200-1000** global interface configuration command, the first [chars] is 228. The switch creates STP instances for VLAN 200 to VLAN 227, but not for VLAN 228. 200 is not created.

STP instances are also not created for the remainder of the VLANs in the range

Recommended Action Reduce the number of active spanning-tree instances by either disabling some or deleting the VLANs associated with them. To create STP instances, manually create them. If you do not, the switch automatically creates an STP instances when a VLAN is created.

For example, if the switch has already created 128 instances and you want to create an STP instance for VLAN 200, remove a spanning-tree instance with one of these commands:

- To delete one of the VLANs with an STP instance, enter the **no vlan** *vlan-id* global configuration command.
- To disable spanning tree on a per-VLAN basis. enter the **no spanning-tree** *vlan-id* global configuration command.

Then enter the **spanning-tree 200** global configuration command to create an instance for VLAN 200.

Deleted System Messages

Error Message ACLMGR-2-NOVMR: Cannot create VMR data structures for access list [chars].

Error Message DOT1X-5-INVALID_INPUT: Dot1x Interface parameter is Invalid on interface [chars].

Error Message DOT1X-5-SECURITY_VIOLATION: Security violation on interface [chars], New MAC address [enet] is seen.

Error Message DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or shutdown VLAN [dec] to 802.1x port [chars]

Error Message DOT1X_SWITCH-5-ERR_VLAN_ROUTED_PORT: Attempt to assign VLAN [dec] to routed 802.1x port [chars]

Error Message UDLD-3-UDLD_IDB_ERROR: UDLD error handling [chars] interface [chars].

Error Message UDLD-3-UDLD_INTERNAL_ERROR: UDLD internal error [chars].

Error Message UDLD-3-UDLD_INTERNAL_IF_ERROR: UDLD internal error, interface [chars] [chars].

Error Message UDLD-4-UDLD_PORT_DISABLED: UDLD disabled interface [chars], [chars] detected.

Error Message UDLD-6-UDLD_PORT_RESET: UDLD reset interface [chars].

Error Message UFAST_MCAST_SW-3-PROC_START_ERROR: No process available for transmitting UplinkFast packets.

Error Message UFAST_MCAST_SW-4-MEM_NOT_AVAILABLE: No memory is available for transmitting UplinkFast packets on Vlan [dec].

Error Message VQPCLIENT-2-CHUNKFAIL: Could not allocate memory for VQP.

Error Message `VQPCLIENT-2-DENY: Host [enet] denied on interface [chars].`

Error Message `VQPCLIENT-3-IFNAME: Invalid interface ([chars]) in response.`

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*
- Information about Cisco SFP, SFP+, and GBIC modules is available from this Cisco.com site:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

  SFP 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

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.