Release Notes for the Cisco IE 3000 Switch, Cisco IOS Release 15.0(2)EY and Later

March 11, 2013

Cisco IOS Release 15.0(2)EY runs on all Cisco IE 3000 switches.

These release notes include important information about Cisco IOS Release 15.0(2)EY 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 6.

You can download the switch software from this site (registered Cisco.com users with a login password): http://www.cisco.com/cisco/software/navigator.html?a=ahttp://www.cisco.com/cisco/web/download/index.htmli=rpm

Contents

- System Requirements, page 2
- Upgrading the Switch Software, page 5
- Installation Notes, page 8
- New Software Features, page 8
- Limitations and Restrictions, page 9
- Important Notes, page 13
- Open Caveats, page 15
- Resolved Caveats, page 17
- Documentation Updates, page 17

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

- Related Documentation, page 22
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 23

System Requirements

- Supported Hardware, page 2
- Device Manager System Requirements, page 4
- Cluster Compatibility, page 4
- CNA Compatibility, page 5

Supported Hardware

Switches and Modules

.

Table 1 Cisco IE 3000 Switches and Modules

Switch Model	Description	Supported by Minimum/Suggested Cisco IOS Release
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	Minimum: Cisco IOS Release 12.2(55)SE; Suggested: Cisco IOS Release 15.0(2)EY1 for PoE and SFP expansion modules.
Cisco IE-3000-8TC	8 10/100BASE-T Ethernet ports and 2 dual-purpose ports	Minimum: Cisco IOS Release 12.2(55)SE; Suggested: Cisco IOS Release 15.0(2)EY1 for PoE and SFP expansion modules.
Cisco IE-3000-4TC-E	4 10/100BASE-T Ethernet ports and 2 dual-purpose ports (supports the IP services software feature set)	Minimum: Cisco IOS Release 12.2(55)SE; Suggested: Cisco IOS Release 15.0(2)EY1 for PoE and SFP expansion modules.
Cisco IE-3000-8TC-E	8 10/100BASE-T Ethernet ports and 2 dual-purpose ports (supports the IP services software feature set)	Minimum: Cisco IOS Release 12.2(55)SE; Suggested: Cisco IOS Release 15.0(2)EY1 for PoE and SFP expansion modules.
Cisco IEM-3000-8TM	Expansion module with 8 10/100BASE-T copper Ethernet ports	Minimum: Cisco IOS Release 12.2(55)SE2
Cisco IEM-3000-8FM	Expansion module with 8 100BASE-FX fiber-optic Ethernet ports	Minimum: Cisco IOS Release 12.2(55)SE2

Table 1 Cisco IE 3000 Switches and Modules

Switch Model	Description	Supported by Minimum/Suggested Cisco IOS Release
Cisco IEM-3000-4SM	Expansion module with 4 100BASE-FX fiber-optic Ethernet ports **Note** The base switch supports up to two expansion modules with various combinations including the IEM-3000-8FM, IEM-3000-8TM and the PoE/PoE+ modules IEM-3000-4PC and IEM-3000-4PC-4TC. An exception to the combination is that if you install an 8-port IEM-3000-8FM or IEM-3000-8SM right after the base switch, then you can install only one expansion module.	Cisco IOS Release 15.0(2)EY
Cisco IEM-3000-8SM	Expansion module with 8 100BASE-FX fiber-optic Ethernet ports	Cisco IOS Release 15.0(2)EY
Cisco IEM-3000-4PC	Expansion module with 4 PoE 10/100BASE-T Ethernet ports **Note** Each Power over Ethernet (PoE) or Power over Ethernet Plus (PoE+) module requires an external power supply besides the existing power supply used to power up the base unit. A 44–57 V DC power output is required to support PoE ports (15.4 W) and a 50–57 V DC power output is required to support PoE+ ports (30 W) to meet the IEEE 802.3at standard. Cisco power modules PWR-IE65W-PC-AC (for AC input) and PWR-IE65-PC-DC (for DC input) provide the 54 V DC/1.2 A output to the PoE/PoE+ ports.	Cisco IOS Release 15.0(2)EY1
Cisco IEM-3000-4PC-4TC	Expansion module with 4 PoE and 4 non-PoE 10/100BASE-T copper Ethernet ports	Cisco IOS Release 15.0(2)EY1

SFP Modules

.

Table 2 SFP Transceivers Support for IE 3000 Series Switches

Type of SFP	SFP Models
Industrial Temperature 100-Megabit Transceivers	GLC-FE-100FX-RGD 100BASE-FX, 2km[1]/MMF GLC-FE-100LX-RGD 100BASE-LX,10km/MMF
Industrial Temperature Gigabit Uplink	GLC-SX-MM-RGD 1000BASE-T, 220–550m/MMF GLC-LX-SM-RGD 1000BASE-LX/LH 550m/MMF, 10km/SMF GLC-ZX-SM-RGD 10000BASE-ZX 70–100km/SMF

Table 2 SFP Transceivers Support for IE 3000 Series Switches

Type of SFP	SFP Models
Commercial Temperature 100-Megabit Transceivers	GLC-FE-100FX 100BASE-FX, 2km/MMF GLC-FE-100LX 100BASE-LX, 10km/SMF GLC-FE-100EX 100BASE, 40km/SMF GLC-FE-100ZX 100BASE, 80km/SMF GLC-FE-100BX-D 10km/SMF GLC-FE-100BX-U 10km/SMF
Commercial Temperature Gigabit Uplink	GLC-SX-MM 1000BASE-SX, 220–500m/MMF GLC-LH-SM 1000BASE-LH, 550m/MMF, 10km/SMF GLC-SX-MMD 1000BASE-SX, 220–500m/MMF, DOM GLC-LH-SMD 1000BASE-LH, 550m/MMF, 10km/SMF, DOM GLC-EX-SMD 1000BASE-EX, 40km, DOM GLC-ZX-SMD 1000BASE-ZX, 70–100km/SMF, DOM GLC-BX-D 1000BASE-BX10 10km/SMF GLC-BX-U 1000BASE-BX10 10km/SMF CWDM SFP 100km/SMF

[1] Cable distance.

Device Manager System Requirements

- Hardware, page 4
- Software, page 4

Hardware

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

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

Device Manager verifies the browser version when starting a session and does not require a plug-in.

Cluster Compatibility

You cannot create and manage switch clusters through 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 Cisco 12.2(55)SE and later. Using the new Smartport role names will cause CNA errors.

You can download Cisco Network Assistant from this URL:
http://www.cisco.com/cisco/software/navigator.html?mdfid=279230132http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistanti=rp

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

Upgrading the Switch Software

- Finding the Software Version and Feature Set, page 5
- Deciding Which Files to Use, page 6
- Archiving Software Images, page 6
- Upgrading a Switch by Using Device Manager or Network Assistant, page 7
- 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 Device Manager. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Table 4 lists the filenames for this software release.

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

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

Table 4 Cisco IOS Software Image Files

Filename	Description
ies-lanbasek9-tar.150-2.SE.tar	Cisco IE 3000 cryptographic image file and Device Manager files with Layer 2+, Kerberos, and SSH features.
ies-ipservicesk9-tar.150-2.SE.tar	Cisco IE 3000 IP services cryptographic image and Device Manager files with Kerberos, SSH, Layer 2+, and full Layer 3 features.

Archiving Software Images

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

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.

Note Although you can copy any file on the flash memory to the TFTP server, it is time consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from Cisco.com and archive it on an internal host in your network.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the "Basic File Transfer Services Commands" section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*:
http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html

Upgrading a Switch by Using Device Manager or Network Assistant

You can upgrade switch software by using Device Manager or Network Assistant. For detailed instructions, click **Help**.

Note When using 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 6 to identify the file that you want to download.

Step 2 Download the software image file:

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

http://software.cisco.com/download/navigator.html?mdfid=282082952&catid=268438038

b. Navigate to **Switches** > **Industrial Ethernet Switches**.

c. Navigate to your switch model.

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

e. Download the image you identified in Step 1.

Step 3 Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.
For more information, see 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/image-name.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 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 Software Features

Power over Ethernet (PoE) and Power Over Ethernet Plus (PoE+)

Support for IEEE 802.3af (Power over Ethernet) and IEEE802.3at (Power over Ethernet+) features. For more information, see the *Power Over Ethernet Ports* section in the software configuration guide on Cisco.com.

Note Power over Ethernet (PoE) and Power over Ethernet Plus (PoE+) features are supported only on the switch with expansion modules IEM-3000-4PC-4TC and IEM-3000-4PC for Cisco IOS Release 15.0(2)EY1.

For the Cisco IE 3000 Switch Software Configuration Guide, Release 15.0(2)EY and Later, go to http://www.cisco.com/en/US/docs/switches/lan/cisco_ie3000/software/release/15.0_2_ey/configuration/guide/IE3000Config.html.

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

- Configuration, page 9
- Ethernet, page 10
- IP, page 10
- Multicasting, page 11
- QoS, page 11
- SPAN and RSPAN, page 12
- Trunking, page 12
- VLAN, page 12

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)
- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

  The workaround is to configure aggressive UDLD. (CSCsh70244)
- When you enter the **boot host retry timeout** global configuration command to specify the amount of time that the client should keep trying to download the configuration and you do not enter a timeout value, the default value is zero, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.

  The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout** *timeout-value* command. (CSCsk65142)
- On a switch running both Resilient Ethernet Protocol (REP) and Bidirectional Forwarding Detection (BFD), when the REP link status layer (LSL) age-out value is less than 1 second, the REP link flaps if the BFD interface is shut down and then brought back up.

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

Ethernet

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

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

  Changing the load balance distribution method or changing the number of ports in the EtherChannel can resolve this problem.

  Use any of these workarounds to improve EtherChannel load balancing:

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

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

IP

- When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console.

  The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)

Multicasting

- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise.

  The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)
- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port.

  There is no workaround. (CSCdy82818)
- If an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
  - If the ALLOW_NEW_SOURCE record is before the BLOCK_OLD_SOURCE record, the switch removes the port from the group.
  - If the BLOCK_OLD_SOURCE record is before the ALLOW_NEW_SOURCE record, the switch adds the port to the group.

  There is no workaround. (CSCec20128)
- When IGMP snooping is disabled and you enter the **switchport block multicast** interface configuration command, IP multicast traffic is not blocked.

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

  There is no workaround. (CSCee16865)
- Incomplete multicast traffic can be seen under either of these conditions:
  - You disable IP multicast routing or re-enable it globally on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.

  The workaround is to enter the **clear ip mroute** privileged EXEC command on the interface. (CSCef42436)
- After you configure a switch to join a multicast group by entering the **ip igmp join-group** *group-address* interface configuration command, the switch does not receive join packets from the client, and the switch port connected to the client is removed from the IGMP snooping forwarding table.

  Use one of these workarounds:
  - Cancel membership in the multicast group by using the **no ip igmp join-group** *group-address* interface configuration command on an SVI.
  - Disable IGMP snooping on the VLAN interface by using the **no ip igmp snooping vlan** *vlan-id* global configuration command. (CSCeh90425)

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)

- If you configure a large number of input interface VLANs in a class map, a traceback message similar to this might appear:

  ```
  01:01:32: %BIT-4-OUTOFRANGE: bit 1321 is not in the expected range of 0 to 1024
  ```

  There is no impact to switch functionality.

  There is no workaround. (CSCtg32101)

SPAN and RSPAN

- 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)
- When many VLANs are configured on the switch, high CPU utilization occurs when many links are flapping at the same time.

  The workaround is to remove unnecessary VLANs to reduce CPU utilization when many links are flapping. (CSCtl04815)

Device Manager Limitations

- When you are prompted to accept the security certificate and you click *No*, you only see a blank screen, and 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, page 13
- SDM Template Notes, page 15

Device Manager Notes

- You cannot create and manage switch clusters through 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 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 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.

- 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.

SDM Template Notes

Due to changes in the default image settings, IP routing is no longer enabled in the default SDM template. Systems that upgrade from an earlier Cisco IOS release to Release 15.0(2)EY must run a non-default SDM template to preserve the earlier IP routing configurations.

Open Caveats

- CSCee32792

  When using SNMP v3, the switch unexpectedly reloads when it encounters the snmp_free_variable_element.

  There is no workaround.
- CSCth59458

  If a redundant power supply (RSP) switchover occurs during a bulk configuration synchronization, some of the line configurations might disappear.

  The workaround is to reapply the line configurations.
- CSCtl12389

  The **show ip dhcp pool** command displays a large number of leased addresses.

  The workaround is to turn off **ip dhcp remember** and reload the switch.
- CSCtq64716

  The following warning messages might be displayed during the boot process even when a RADIUS or a TACACS server have been defined:

  ```
  %RADIUS-4-NOSERVNAME:
  ```

  or

  ```
  %AAAA-4-NOSERVER: Warning: Server TACACS2 is not defined
  ```

  There is no workaround.
- CSCtt00966

  The maximum number of VPN routing and forwarding (VRF) instances that can be configured is 25 instead of 26.

  There is no workaround.
- CSCtx35080

  When an attempt is made to view the web pages of a switch, the initial request for a password by Device Manager is an unsecure connection. After the password is accepted, the next dialog box asks if a secure connection is desired.

  There is no workaround.
- CSCtx35101

  The password must be entered twice before it is accepted in Express Setup.

  There is no workaround.

- CSCtx37061

  The vendor specific attribute PortLogSyncIntervalCfg is a struct with a UINT type member variable called PortLogSyncInterval. The specified range of valid values for PortLogSyncInterval is from -1 to 6. A value of -1 cannot be assigned to the PortLogSyncInterval variable.

  There is no workaround.

- CSCtx69656

  After the switch boots up, a connected device does not receive Gratuitous ARP (GARP) packets from the switch.

  The workaround is to perform one of the following actions:

  - clear the ARP cache on the connected device
  - use the **switchport nonegotiate** command on the port to which the device is connected
  - ping from the switch to the connected device

- CSCty66669

  When a master switch in a switch stack reloads or loses power and rejoins the stack as a member switch (Switch A), traffic from Switch A to the destination is lost.

  The workaround is to ping the destination from Switch A.

- CSCua38239

  When you attempt to reconfigure a flow monitor on an interface, errors occur.

  The workaround is to use the **no flow monitor** command in interface configuration mode and then configure flow monitor on the interface again.

- CSCua54137

  When the switch reverts from a floating static route to a static route, packets are lost.

  The workaround is to set static ARP.

- CSCua58659

  The global **power inline consumption default 15400** command fails to restrict the power consumption of a PoE+ port 15.4 W.

  The workaround is to use the **power inline consumption default 15400** command in interface configuration mode.

- CSCua74302 (Switches running the LAN base image)

  ACLs applied to outbound traffic on the switch virtual interface (SVI) do not work.

  There is no workaround.

- CSCud21309

  The Address Resolution Protocol (ARP) packets leak in the isolated ports of a private VLAN when dot1x is enabled.

  There is no known workaround.

Resolved Caveats

- CSCtg47129

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

  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_mar13.html

Documentation Updates

Note The “Supported MIBs” appendix is no longer in the software configuration guide. To locate and download MIBs for a specific Cisco product and release, use the Cisco MIB Locator: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

- Updates to the Hardware Installation Guide, page 17
- Updates to the Software Configuration Guide, page 18
- Updates to the System Message Guide, page 19

Updates to the Hardware Installation Guide

Updates to the “Overview” Chapter

These extension modules were added:

Table 5 Cisco IE 3000 Switch Model Descriptions

Switch Model	Description
Cisco IE-3000-4SM	Expansion module with 4 100BASE-X SFP Ethernet ports
Cisco IE-3000-8SM	Expansion module with 8 100BASE-X SFP Ethernet ports

Table 5 Cisco IE 3000 Switch Model Descriptions

Switch Model	Description
Cisco IEM-3000-4PC	Expansion module with 4 PoE 10/100BASE-T Ethernet ports
Cisco IEM-3000-4PC-4TC	Expansion module with 4 PoE and 4 non-PoE 10/100BASE-T copper Ethernet ports

The new power supply (PWR-IE50W-AC= and PWR-IE50W-AC-IEC=) were added to power up the base unit switches. The –AC version of the power supply uses a terminal block as the connection point for source AC; the –AC-IEC version of the power supply replaces the terminal block with an IEC C14 connector for the source AC power cord.

Updates to the "Switch Installation" Chapter

For 100BASE-X SFP ports in the IEM-3000-4SM and the IEM-3000-8SM expansion modules, the cable length is dependent on the type of SFP installed in the port.

Updates to the Software Configuration Guide

Updates to the "Configuring Interface Characteristics" Chapter

The "Power over Ethernet Ports" section was added to the chapter.

Cisco IOS Release 15.0(2)EY1 adds the Power over Ethernet (PoE) and Power over Ethernet Plus (PoE+) feature to the switch through the extension modules Cisco IEM-3000-4PC and Cisco IEM-3000-4PC-TC.

Updates to the "Troubleshooting" Chapter

In the "Troubleshooting Power over Ethernet (PoE)" section in the table "Power Over Ethernet Troubleshooting Scenarios" the following problem was added:

Symptom or problem	Possible cause and solution
No PoE on one expansion module.	Verify that PoE power supply is connected and working on the expansion module. Check **#show post** to verify that power-on-self-test (POST) is passed for power controllers. Ensure that the PoE power supply is on and reload the switch if POST has failed for the expansion module.

Updates to the System Message Guide

New System Messages

Error Message `ILPOWER-3-CONTROLLER_ERR: Controller error, Controller number [dec]: [chars].`

Explanation An error reported or caused by the PoE controller is detected. [dec] is the controller instance, which is 0 to 1 depending upon number of PoE expansion modules present in the switch. [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section in the *Cisco IE 3000 Switch System Message Guide*.

Error Message `ILPOWER-3-CONTROLLER_IF_ERR: Controller interface error, [chars]: [chars].`

Explanation An interface error is detected between the PoE controller and the system. The first [chars] is the interface. The second [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section in the *Cisco IE 3000 Switch System Message Guide*.

Error Message `ILPOWER-3-CONTROLLER_PORT_ERR:Controller port error, Interface Fa0/7:Power given, but link is not up.`

Explanation The inline-power-controller reported an error on an interface.

Recommended Action Enter the **shutdown** and **no shutdown** interface configuration commands on the affected interfaces. Upgrade to Cisco IOS Release12.1(14)EA1 or later, which provides an electrostatic discharge (ESD) recovery mechanism.

Error Message `ILPOWER-3-CONTROLLER_POST_ERR: Inline Power Feature is disabled on this switch because Power On Self Test (POST) failed on this switch. Please consult TECH support for further assistance`

Explanation An error reported or caused by the Power over Ethernet (PoE) controller is detected during power-on self-test (POST).

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section in the *Cisco IE 3000 Switch System Message Guide*.

Error Message `ILPOWER-3-ILPOWER_INTERNAL_IF_ERROR: Inline Power internal error, interface [chars]: [chars].`

Explanation A software check failed during PoE processing. The first [chars] is the interface. The second [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the "Error Message Traceback Reports" section in the *Cisco IE 3000 Switch System Message Guide*.

Error Message `ILPOWER-3-SHUT_OVERDRAWN: Interface [chars] is shutdown as it is consuming more than the maximum configured power ([dec]) milliwatts.`

Explanation The interface is shut down because it is consuming more than the maximum power allocation. [chars] is the port, and [dec] is the maximum configured power.

Recommended Action Ensure that the cutoff-power value is configured for the device and is based on the powered-device specifications or ratings. We recommend configuring the cutoff power to a value higher than the required power for the device.

Error Message `ILPOWER-4-ILPOWER_POWER_SUPPLY: PoE Power Supply for [dec]:[chars]`

Explanation This message means that the power supply is inserted or removed from the expansion module. [dec] is the slot number and [chars] is the status of power supply on the module during Online Insertion Removal (OIR).

Recommended Action Ensure that the power supply to the expansion module is re-inserted after removal.

Error Message `ILPOWER-4-ILPOWER_PS_ABSENCE: PoE module Power Supply not present Inline Power Feature is disabled on [chars] because Power On Self Test(POST) failed:[chars]`

Explanation This message means that the power supply for the PoE expansion module is not present or not inserted properly or it is faulty. The first [chars] is the switch or expansion module and the second [chars] is the slot number on which POST has failed.

Recommended Action Ensure that the power supply to the expansion module is inserted properly and reload the switch when PoE power supply is present.

Error Message `ILPOWER-4-LOG_OVERDRAWN: Interface [chars] is overdrawing power. it is consuming [dec] milliwatts where as maximum configured power is ([dec]) milliwatts.`

Explanation The powered device is drawing more power than the maximum power configured on the interface. The power budgeting calculations determined by the switch are no longer valid, and you might risk overloading the switch. [chars] is the interface, and [dec] is the maximum configured power.

Recommended Action Ensure that the correct power is budgeted for this interface based on the powered-device electrical specifications or ratings. We recommend that you change the cutoff power value.

Error Message `ILPOWER-5-CLR_OVERDRAWN: Interface [chars] is NOT overdrawing power. it is consuming [dec] milliwatts where as maximum configured value is ([dec]) milliwatts.`

Explanation The device connected to the PoE interface is consuming less power than the maximum power allocation. [chars] is the interface. The first [dec] is the power being consumed, and the second [dec] is the maximum allocated power value.

Recommended Action No action is required.

Error Message `ILPOWER-5-IEEE-DISCONNECT: Interface [chars]: PD removed.`

Explanation The powered device is not connected to the switch, or the connected powered device is being powered by an external AC power source. The switch is no longer providing power to the port. [chars] is the interface.

Recommended Action No action is required.

Error Message `ILPOWER-5-ILPOWER_POWER_CDP_SHUT: Interface [chars]: inline power shut`

Explanation Inline power is shut down because CDP consumption power on this PoE port is greater than the allocation power, the hardware interface limit, the user-configured maximum power, or the available power on this switch. [chars] is the interface.

Recommended Action No action is required.

Error Message `ILPOWER-5-ILPOWER_POWER_DENY: Interface [chars]: inline power denied`

Explanation The switch does not have enough power to supply the Power over Ethernet (PoE) port. [chars] is the PoE port identifier.

Recommended Action No action is required.

Error Message `ILPOWER-5-INVALID_IEEE_CLASS: Interface [chars]: has detected invalid IEEE class: [dec] device. Power denied`

Explanation The powered device has an invalid IEEE class so that the switch is not providing power to the device. [chars] is the interface. [dec] is the IEEE class number.

Recommended Action No action is required.

Error Message `ILPOWER-5-LINKDOWN_DISCONNECT: Interface [chars]: Link down disconnect.`

Explanation The powered device is no longer connected to the switch, or the connected powered device is being powered by an external AC power source. The switch is no longer providing power on the interface. [chars] is the interface.

Recommended Action No action is required.

Error Message `ILPOWER-5-POWER_GRANTED: Interface [chars]: Power granted.`

Explanation The switch can provide power to the interface. [chars] is the interface.

Recommended Action No action is required.

Error Message `ILPOWER-7-DETECT: Interface [chars]: Power Device detected:[chars].`

Explanation The switch has detected a connected powered device. The first [chars] is the interface. The second [chars] is the Cisco pre-standard powered device or the IEEE-compliant powered device.

Recommended Action No action is required.

Related Documentation

User documentation in HTML format includes the latest documentation updates and might be more current than the complete book PDF available on Cisco.com.

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:
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.