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

September15, 2017

Cisco IOS Release 15.0(2)SE and higher runs on all Cisco IE 3000 switches.

These release notes include important information about Cisco IOS releases 15.0(2)SE and higher, and any limitations, restrictions, and caveats that apply to the releases. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 4.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 4.

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

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

System Requirements

Supported Hardware

Switches and Modules

Table 1 Cisco IE 3000 Switch Models

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

SFP Modules

Table 2 SFP Models

Type of SFP	SFP Models
Industrial temperature modules	GLC-FE-100FX-RGD GLC-SX-MM-RGD GLC-FE-100LX-RGD GLC-LX-SM-RGD GLC-ZX-SM-RGD
Extended temperature modules	100BASE-BX
Commercial temperature modules	CWDM 1000BASE-BX GLC-FE-100EX (Cisco IOS Release 12.2(55)SE and later.) **Note** 100EX SFP support is Version -02 (10-2262-02) or later

Device Manager System Requirements

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

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 5 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://www.cisco.com/cisco/software/navigator.html?a=ahttp://www.cisco.com/cisco/web/download/index.htmli=rpm

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

- Support for IPv6 multicast. For more information, see the *Implementing IPv6 Multicast* chapter of the Software Configuration Guide on Cisco.com.
- Option to minimize boot up time with the **boot fast** command. For more information, see the *Assigning the Switch IP Address and Default Gateway* chapter in the Software Configuration Guide on Cisco.com
- Support for static routes on switch virtual interfaces (SVIs). For more information, see the *Configuring SDM Templates* and *Configuring Static IP Unicast Routing* chapters in the Software Configuration Guide.
- Support for port security on Etherchannels. For more information, see the *Configuring Port-Based Traffic Control* chapter in the Software Configuration Guide.

For the Cisco IE 3000 Software Configuration Guide, Release 15.0(2)SE and Later, go to http://www.cisco.com/en/US/partner/docs/switches/lan/cisco_ie3000/software/release/15.0_2_se/configuration/guide/scg_ie3000.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 7
- Device Manager Limitations, page 12

Cisco IOS Limitations

- Configuration, page 8

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

- 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)SE must run a non-default SDM template to preserve the earlier IP routing configurations.

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat listed in this document:

1. Access the BST (use your Cisco user ID and password) at https://tools.cisco.com/bugsearch/.
2. Enter the bug ID in the **Search For:** field.

Open Caveats

- CSCtt00966

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

  There is no workaround.

- 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.

Resolved Caveats

Caveats Resolved in Cisco IOS Release 15.0(2)SE11

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to *https://tools.cisco.com/bugsearch/*.

Bug ID	Headline
CSCsy56638	Switch crashes after getnext on the last cafServerAliveAction index
CSCvd48893	Cisco IOS and IOS XE Software Cluster Management Protocol Remote Code Execution Vulnerability
CSCve60507	Crash in "mac auth bypass" SNMP code
CSCsm45390	DHCP relay security vulnerability
CSCva37748	When enable ip source guard, a part of the clients cannot communicate
CSCuw77959	1801M - %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCuz81292	IPv6 neighbor discovery packet processing behavior
CSCva74756	OSPF Rogue LSA with maximum sequence number vulnerability

Caveats Resolved in Cisco IOS Release 15.0(2)SE10a

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to *https://tools.cisco.com/bugsearch/*.

Bug ID	Headline
CSCuu13476	Cisco IOS & IOS XE Software OpenSSH TCP Denial of Service Vulnerability
CSCuu43892	Switch crashes on qpair_full after executing dhcpd_* functions
CSCvb16274	PPTP Start-Control-Connection-Reply packet leaks router memory
CSCvb29204	BenignCertain on IOS and IOS-XE

Caveats Resolved in Cisco IOS Release 15.0(2)SE10

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to *https://tools.cisco.com/bugsearch/*.

Bug ID	Headline
CSCum45713	UUT crashed for scale session
CSCuo95194	Switch fails while copying a configuration file to running-config using RCP
CSCus21950	Crash seen after getting LINEPROCDEAD errors and tracebacks
CSCuw71809	No warning message when switch configures "ip tcp adjust-mss"
CSCux38041	Broadcast packet does not send when port channel changes to normal port
CSCux81884	RADIUS server failover leaves port in inconsistent state
CSCuy33215	Cannot apply REP config under portchannel after initial boot up

Caveats Resolved in Cisco IOS Release 15.0(2)SE9

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to *https://tools.cisco.com/bugsearch/*.

Bug ID	Headline
CSCul01067	Memory leak in NTP client with IPv6 configuration
CSCus13476	CSR handled only one MACSec interface's authentication
CSCus40723	No simulated EAP success message to the client for credential failure
CSCut20271	C3560X responds to ARP request from management port
CSCuu28768	C2960 ARP Table adding MACs on Incorrect Interface
CSCuu41771	Members in a 2960 cluster unable to save configuration in IOS 15.x
CSCuv05123	c3560e/v151_sy_throttle platform doesn't store NTP drift values properly
CSCuv94875	SmartPort Macro with SCP not working

Caveats Resolved in Cisco IOS Release 15.0(2)SE8

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to *https://tools.cisco.com/bugsearch/*.

Bug ID	Headline
CSCtq21722	SNMP crash forced due to an invalid memory block
CSCuo66933	Switch sent Failure packet after reboot and caused PC to fail authenticate
CSCue80816	Crash while routine config push through SNMP
CSCud65150	Crash after Kron runs a TCL script

Bug ID	Headline
CSCtx23014	HSRP hellos cannot be sourced from certain IPs for specific vlan
CSCuo31164	match prefix is removed from SNMP V3 configuration after host command
CSCum75962	abnormal dot1x authentication failure msg from some specific mac address
CSCuq85748	dot1x authorization fails, when we recovering from Guest VLAN
CSCum65703	Inconsistency on config "privilege" commands as seen in running-config
CSCsq42459	No log message of falling the cpu threshold
CSCuh46221	EEM Tcl policies fail due to false out of memory error
CSCtj17637	MF: HTTPS generates a new self-signed cert on reboot even if one exists
CSCud66899	IOS supplicant: ACS5 authc fail for PEAPv1/MSCHAPv2
CSCur58372	"snmp-server enable traps syslog" still in "show run all" after removal
CSCui43116	dot1x State Radius AV pair not send while failing over between AAA grps
CSCur76305	Memory leak in ASP proces Catalyst 2960s
CSCuq10827	C3560X cHsrpGrpStandbyState is incorrect
CSCur50403	LOGIN_FAILED log message should not display the bad username
CSCur74187	Device sending Client IP address as "Calling-Station-Id" with WebAuth
CSCut05808	UDP(1975) causes Error msg %IPC-2-INVALIDZONE
CSCuq79479	Reloading 3750x causes link to err-disabled on IE3000.

Caveats Resolved in Cisco IOS Release 15.0(2)SE6

- CSCuj77426

  After performing a **shut** or **no shut** on the ports of a Catalyst Switch, the status of some of the ports are displayed as **Not Connected**, even if they are connected to a remote device.

  The workaround is to perform a **shut or no shut** on the affected ports.

- CSCul58877

  When the hostname is limited to 16-characters, it gets truncated when displayed in the show REP topology.

  There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)SE5

- CSCug26848

CPU usage goes above 90% when Internet Group Management Protocol (IGMP) version 3 report packets are sent to the switch which has IGMP version 2 configured on the switch virtual interface.

The workaround is to either disable multicast fast convergence or configure IGMP version 3 on switch virtual interface.

- CSCug52714

  TACACS+ single connect authentication request from a switch stack takes around 10 to 12 minutes to failover to secondary server after the primary TACACS server is unreachable.

  The workaround is to disable TACACS+ single connect configuration on the switch.

- CSCui41032

  Switch runs out of memory within few seconds of configuring the **level <n> show spanning-tree active/detail** privilege EXEC command.

  There is no workaround.

- CSCui87793

  Web authentication does not work.

  There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)SE4

- CSCuf77683

  Internal VLANs are displayed when the **show snmp mib ifmib ifindex** command is entered or the SNMP is queried for the ipMIB object.

  The workaround is to check if the displayed VLANs are internal and then to hide them.

- CSCug62154

  When the switch is started using TACACS+ configurations, the CPU utilization increases to 100% and the VTY device does not work.

  The workaround is to remove the TACACS+ configurations and restart the switch.

- CSCuh41077

  The ipAddrEntry value in the IP Address Table shows an interface index that is not exposed by the ifEntry Object ID.

  There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)SE3

- CSCta43825

  CPU usage is high when an SNMP Walk of the Address Resolution Protocol (ARP) table is performed.

  The workaround is to implement SNMP view using the following commands:

  snmp-server view cutdown iso included

  snmp-server view cutdown at excluded

  snmp-server view cutdown ip.22 excluded

snmp-server community public view cutdown ro

snmp-server community private view cutdown rw

- CSCts95370

  If an ACL is configured on a router VTY line for ingress traffic, the ACL is applied for egress traffic also. As a result, egress traffic to another router on an SSH connection is blocked.

  The workaround is to permit egress traffic to the specific destination router using the **permit tcp host** <*destination router IP address*> **eq 0 any** interface configuration command.

- CSCua97084

  Prior to Cisco IOS Release 15.0(2)SE3, IP routing commands were disabled from the default SDM template. With Release 15.0(2)SE3, all IP routing information and configuration is erased from the switch.

  There is no workaround. However, IP routing commands will work in templates other than the default SDM template.

- CSCub14238

  The DHCP client is not assigned an IP address from the DHCP server if port-based allocation is enabled on the server.

  There is no workaround.

- CSCub85948

  Memory leak is seen in the switch when it sends CDP, LLDP or DHCP traffic and when the link flaps.

  The workaround is to apply protocol filters to the device sensor output by entering the following global configuration commands:

  no macro auto monitor

  device-sensor filter-spec dhcp exclude all

  device-sensor filter-spec lldp exclude all

  device-sensor filter-spec cdp exclude all

  If the memory leak continues in the "DHCPD Receive" process, disable the built-in DHCP server by entering the **no service dhcp** global configuration command.

- CSCuc40634

  STP loop occurs on Flexstack connected by parallel links when a link state is changed on Flexlink port.

  The workaround is to change the switch to root bridge.

- CSCud14419

  CLI messages are not displayed when the cisco-phone smartport macro is applied to the switch through CIP.

  The workaround is to apply the smartport macro to the switch through CLI.

- CSCud44884

  If a policy map attached to the switch interface is modified then the corresponding QoS policy works incorrectly.

  The workaround is to delete the policy map, create a new policy map and then attach it to the interface.

- CSCud83248

  When native VLAN is configured on the trunk or when switchport trunk native vlan 99 is configured on the interface, spanning-tree instance is not created for native VLAN.

  The workaround is to keep VLAN1 as a native on the trunk. In Cisco IOS Release15.0(2) SE, **dot1.x** is enabled by default and causes authentication fail in the native VLAN. This results in **pm_vp_statemachine** not triggering any event to spanning tree. To disable **dot1x** internally, run the **no macro auto monitor** command. The stp instance is created for native vlan 99 after running the **show** and **no show** command on the interface.

- CSCue86180

  On the Catalyst 2960S switch stack, when the login block command is configured and the running config is saved using the **wr** command on the master, it makes the master down. When the running config is saved on the new master , the following lines are displayed on entering the show running-config command.

  ip access-list extended sl_def_acl

  deny tcp any any eq telnet

  deny tcp any any eq www

  deny tcp any any eq 22

  permit ip any any

  There is no workaround.

- CSCue87815

  When the secret password is configured, the password is not saved. The default password is used as the secret password.

  The workaround is to use the default password to login and then change the password.

Caveats Resolved in Cisco IOS Release 15.0(2)SE1

- CSCee32792

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

  There is no workaround.

- CSCth03648

  When two traps are generated by two separate processes, the switch fails if one process is suspended while the other process updates variables used by the first process.

  The workaround is to disable all SNMP traps.

- 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.

- CSCtr37757

  The secure copy feature (**copy:** *source-filename* **scp**: *destination-filename* command) does not work.

  There is no workaround.

- CSCtz99447

  Local web authorization and HTTP services on the switch do not respond because of a web authorization resource limitation in the system. The resource limitation is normally caused by incorrectly terminated HTTP or TCP sessions.

  These are possible workarounds and are not guaranteed to solve the problem:

  - Enter the **ip admission max-login-attempts** privileged EXEC command to increase the number of maximum login attempts allowed per user.
  - If the web authorization module is intercepting HTTP sessions from web clients in an attempt to authorize them, try using a different browser.
  - Eliminate background processes that use HTTP transport.

- CSCua54224

  Heavy traffic load conditions may cause the loop guard protection function to be automatically activated and almost immediately deactivated. These conditions can be caused by entering the **shutdown** and **no shutdown** interface configuration commands or by interface link flaps on more than forty ports. These log messages appear:

  ```
  %SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet1/0/1 on MST0.
  %SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet1/0/1 on
  MST0.
  ```

  There is no workaround.

- CSCua87594

  When a peer switch sends inferior Bridge Protocol Data Units (BPDUs) on the blocking port of the Cisco switch (with the proposal bit ON), the Cisco switch waits for three such BPDUs before responding with a better BPDU. This leads to a convergence time of more than 5 seconds. The problem appears under these conditions:

  - The Cisco switch is not configured as the root switch.
  - The Cisco switch uses Multiple Spanning-Tree Protocol (MSTP) and the peer switch uses Rapid Spanning Tree Protocol (RSTP) or rapid per-VLAN spanning-tree plus (rapid PVST+).

  There is no workaround.

- CSCub14238

  With switches running Cisco IOS Release 15.0(2)SE, there was a problem when port-based address allocation was configured. The DHCP client did not receive IP addresses from the server if the client ID was configured as an ASCII string or if the subscriber ID was used as the client ID.

  This problem has been fixed now. No action is required.

- CSCub14641

  When you configure and save the monitor session source interface, the configuration is not saved after reboot.

  There is no workaround.

- CSCub55790

  The Smart Install client feature in Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

  Affected devices that are configured as Smart Install clients are vulnerable.

  Cisco has released free software updates that address this vulnerability. There are no workarounds for devices that have the Smart Install client feature enabled.

  This advisory is available at the following link:

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

- CSCub93357

  If an interface is configured with the **switchport port-security maximum 1 vlan** command, the following error message is displayed:

  ```
  %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address XXXX.XXXX.XXXX on port <interface>
  ```

  There is no workaround.

- CSCuc03555

  The flash memory is corrupted when you format the flash manually.

  The workaround is to reload the switch. (Note that this will erase the flash memory, and you will need to reload the software image using TFTP, a USB drive, or a serial cable.

- CSCuc17720

  If the Performance Monitor cache is displayed (using the **show performance monitor cache** command) and you attempt to stop the command output display by entering the **q** keyword, there is an unusually long delay before the output is stopped.

  The workaround is to enter the **term len 0** privileged EXEC command so that all command outputs are displayed without any breaks.

Caveats Resolved in Cisco IOS Release 15.0(2)SE

- CSCto57723

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a crafted request to an affected device that has the DHCP version 6 (DHCPv6) server feature enabled, causing a reload.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcpv6

- CSCtr07908

The archive download feature does not work if the flash contains an “update” directory. This situation is likely to occur if a previous download failed or was interrupted and the “update”" directory is still left in the flash.

The workaround is to delete the “update” directory in the flash before starting the archive download.

- CSCtr55645

  OSPFv3 neighbors might flap because of the way the switch handles IPv6 traffic destined for well-known IPv6 multicast addresses.

  There is no workaround.

- CSCts36715

  Users connecting to the network through a device configured for web proxy authentication may experience a web authentication failure.

  There is no workaround. Use the **clear tcp tcb** command to release the HTTP Proxy Server process.

- CSCtt11621

  Using the **dot1x default** command on a port disables access control on the port and resets the values of the **authentication host-mode** and **authentication timer reauthenticate** commands to the default values.

  The workaround is to avoid using the **dot1x default** command and set various dot1x parameters individually. You can also reconfigure the parameters that were changed after you entered the **dot1x default** command.

- CSCtx33436

  When using the **switchport port-security maximum** 1 **vlan access** command, if an IP-phone with a personal computer connected to it is connected to an access port with port security, a security violation will occur on the interface. This type of message is displayed on the console:

  ```
  %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address
  XXXX.XXXX.XXXX on port FastEthernet0/1.
  ```

  Here is a sample configuration:

  ```
  interface gigabitethernet 3/0/47
  switchport access vlan 2
  switchport mode access
  switchport voice vlan 3
  switchport port-security maximum 2
  switchport port-security maximum 1 vlan access
  switchport port-security maximum 1 vlan voice
  switchport port-security
  ```

  The workaround is to remove the line **switchport port-security maximum** 1 **vlan access**.

- CSCtx37046

  You can use Express Setup to enter the initial configuration of a Cisco IE 3000 switch. You enter the IP address and VLAN information.

  When you enter a different VLAN for the management and CIP interfaces and you click **submit** no error message is generated. If you then look at the Express Setup page, the CIP management VLAN is changed to the same VLAN ID as the management interface. If you enter the **show vlan** command at the CLI, the CIP VLAN was never created by the switch.

  The workaround is to edit the running configuration by using the CLI, and entering the **vlan** *vlan-id* command, where *vlan-id* is the CIP VLAN.

- CSCtx96491

The switch does not correctly detect a loopback when the switch port on an authenticated IP phone is looped to a port configured and authenticated with dot1x security, even when **bpduguard** is configured on the interface. This situation can result in 100 percent CPU utilization and degraded switch performance.

The workaround is to configure the interface with the **authentication open** command or to configure **authentication mac-move permit** on the switch.

- CSCty88456

  The Catalyst 4500E series switch with Supervisor Engine 7L-E contains a denial of service (DoS) vulnerability when processing specially crafted packets that can cause a reload of the device.

  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-20120926-ecc

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 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*.

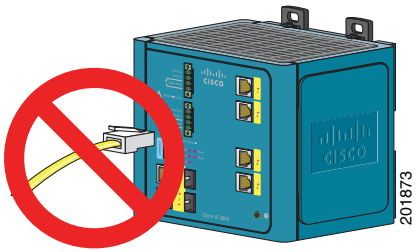
In the "Running Express Setup" section of the *Cisco IE 3000 Switch Getting Started Guide*, Steps 8 to 10 have changed.

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.

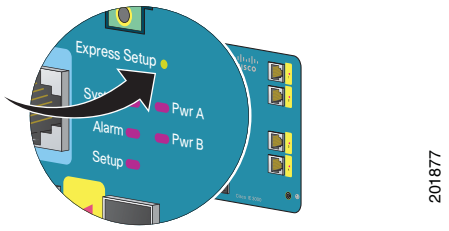
Step 3 When the switch powers on, it begins the power-on self-test (POST). During POST, the System LED blinks while a series of tests verify that the switch functions properly. Wait for the switch to complete POST, which takes approximately 1 minute.

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.

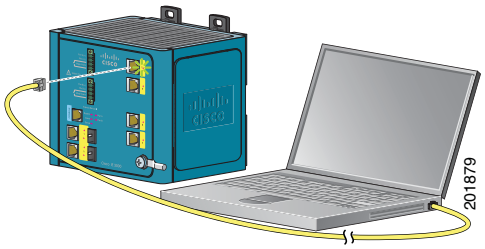
Step 5 Press the Express Setup button. This button is recessed behind the front panel, so you can use a simple tool, such as a paper clip.

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.

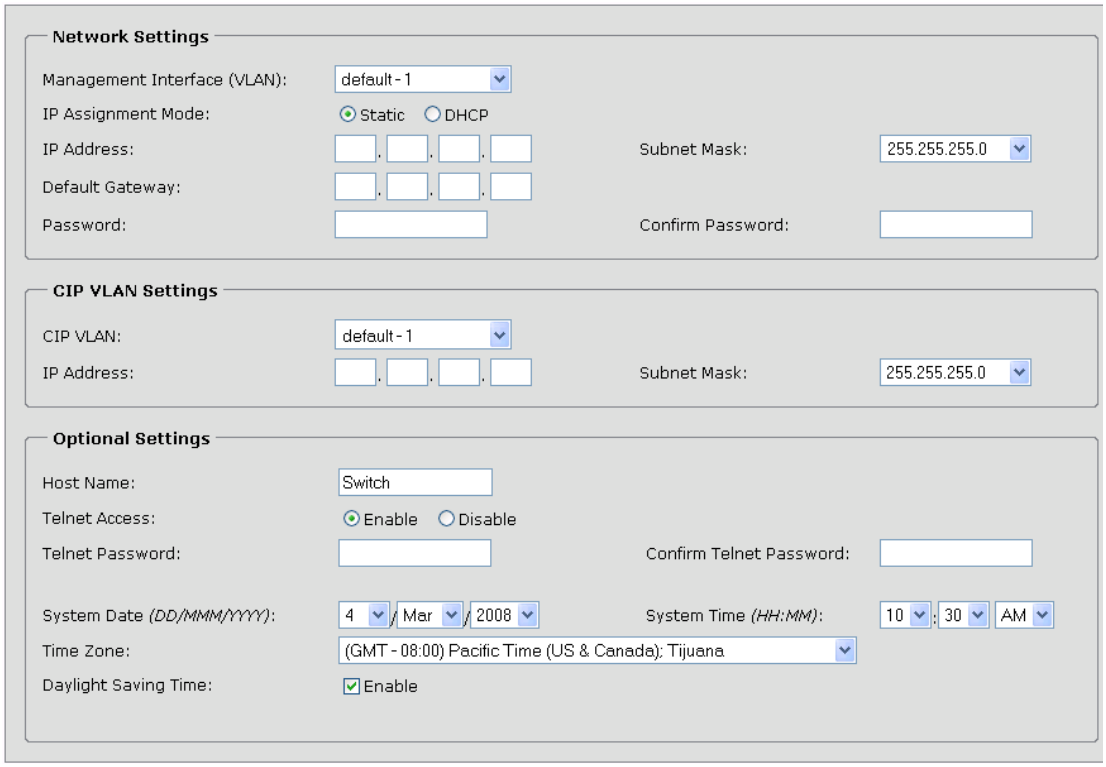
The port LEDs on your PC and the switch blink green while the switch configures the connection.



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.

Hazardous Locations Standards

The hazardous locations standards are updated in the *Regulatory Compliance and Safety Information for the Cisco IE 3000 Switch* on Cisco.com as shown in Table 5.

Table 5 Hazardous Locations Standards Compliance for the Cisco IE 3000 Switches

Specification	Description
Hazardous Locations	ANSI/ISA 12.12.01-2012 UL 60079-0, 5th Ed, 2009-10-21 UL 60079-15, 3rd Ed, 2009-7-17 CSA C22.2 No. 213-M1987 CAN/CSA-C22.2 No. 60079-15: 12 CAN/CSA-C22.2 No. 60079-0: 11 EN 60079-0:2012 EN 60079-15:2010 IEC 60079-0, 6th Edition IEC 60079-15, 4th Edition

Compliance Labels

The Cisco IE 3000 switch compliance label (see Figure 1) is updated with revised ATEX directive titles in the Regulatory Compliance and Safety Information for the Cisco IE 3000 Switch on Cisco.com.

For the expansion modules, separate labels are used for the IEM-3000-8FM and IEM-3000-8TM models (see Figure 2), and the IEM-3000-4SM and IEM-3000-8SM models (see Figure 3). The IEM-3000-4SM and IEM-3000-8SM models have perforated sections for Anatel and KCC requirements, so that they can be removed if they do not apply.

Figure 1 Compliance Label for the Cisco IE 3000 Switch

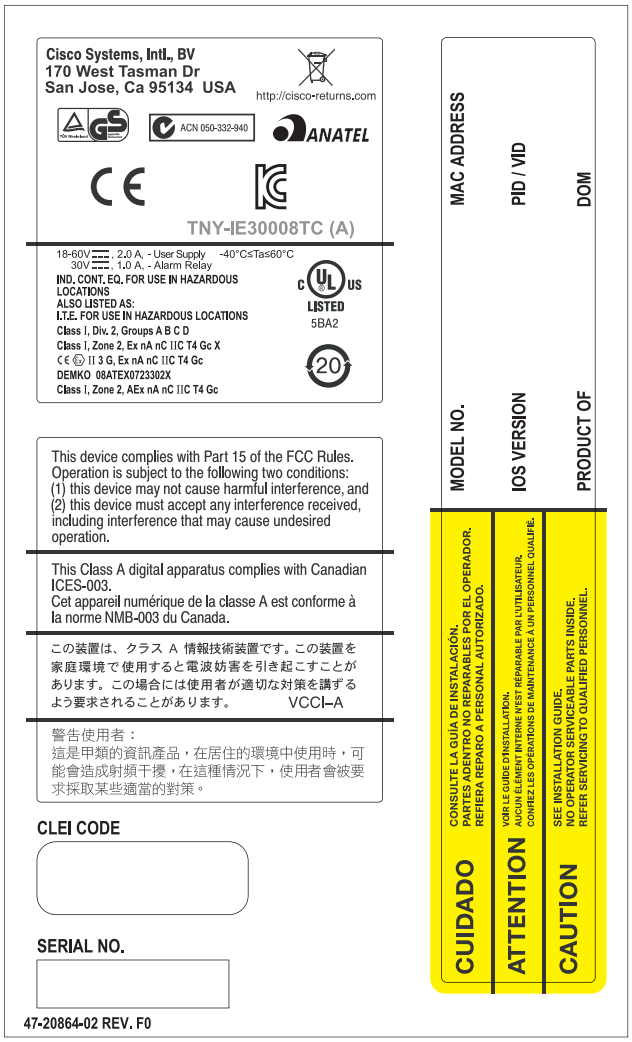


Figure 2 Compliance Label for the IEM-3000-8FM and IEM-3000-8TM Switch Expansion Modules

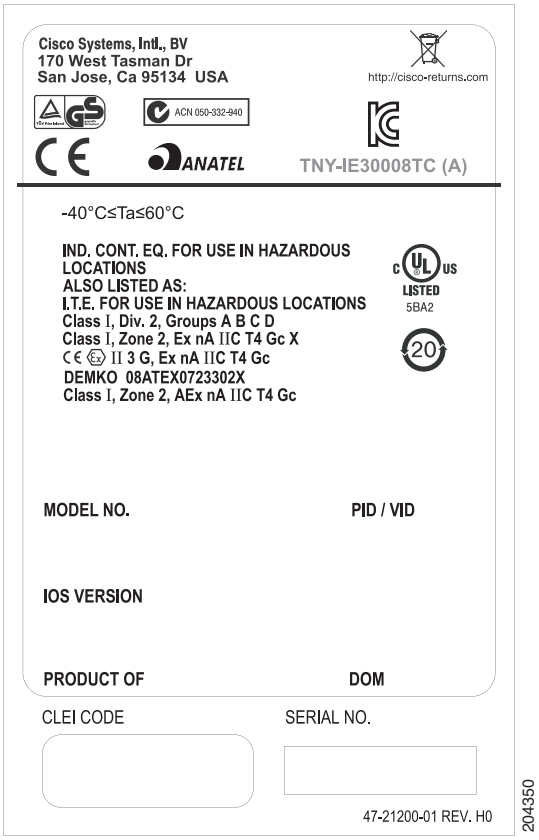


Figure 3 Compliance Label for the IEM-3000-4SM and IEM-3000-8SM Expansion Modules

Note The IEM-3000-4SM and IEM-3000-8SM expansion modules comply with Anatel and KCC requirements only if those marks are present in the compliance label.

Updates to the Hardware Installation Guide

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

Table 6 Cisco IE 3000 Switch Model Descriptions

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

This update is for the "Technical Specifications" chapter.

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

Updates to the Software Configuration Guide

Correction to the "Clustering Switches" Chapter

In the "Candidate Switch and Cluster Member Switch Characteristics" section, the requirements should include:

- The **ip http server** global configuration command must be configured on the switch.

Correction to the "Configuring Network Security with ACLs" Chapter

There is an error in the "Creating a Numbered Extended ACL" section. Contrary to the note in this section, ICMP echo-replies can be filtered.

Correction to the "Unsupported Commands" Chapter

The "Miscellaneous" section of the "Unsupported Commands" chapter should include the **logging discriminator** global configuration command.

Updates to the System Message Guide

New System Messages

Error Message `IP-3-SBINIT: Error initializing [chars] subblock data structure. [chars]`

Explanation The subblock data structure was not initialized. [chars] is the structure identifier.

Recommended Action No action is required.

Error Message `AUTHMGR-7-STOPPING: Stopping '[chars]' for client [enet] on Interface [chars] AuditSessionID [chars]`

Explanation The authentication process has been stopped. The first [chars] is the authentication method, [enet] is the Ethernet address of the host, the second [chars] is the interface for the host, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation All available authentication methods have been tried. The first [chars] is the client identifier, the second [chars]s is the interface for the client, and the third [chars] is the session ID.

Recommended Action No action is required.

Modified System Messages

Error Message `AUTHMGR-5-MACMOVE: MAC address ([enet]) moved from Interface [chars] to Interface [chars]`

Explanation The client moved to a new interface but did not log off from the first interface. [enet] is the MAC address of the client, the first [chars] is the earlier interface, and the second [chars] is the newer interface.

Recommended Action No action is required.

Error Message `AUTHMGR-5-MACREPLACE: MAC address ([enet]) on Interface [chars] is replaced by MAC ([enet])`

Explanation A new client has triggered a violation that caused an existing client to be replaced. The first [enet] is the first client, [chars] is the interface, the second [enet] is the new client.

Recommended Action No action is required.

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

Explanation Authentication was unsuccessful. The first [chars] is the client, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

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

Explanation Authentication was successful. The first [chars] is the client, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Deleted System Messages

Error Message `IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry: [inet], hw: [enet] by hw: [enet]\n", MSGDEF_LIMIT_FAST`

Explanation Multiple stations are configured with the same IP address in a private VLAN. (This could be a case of IP address theft.) [inet] is the IP address that is configured, the first [enet] is the original MAC address associated with the IP address, and the second [enet] is the MAC address that triggered this message.

Recommended Action Change the IP address of one of the two systems.

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.