Release Notes for the Cisco IE 3010 Switch, Cisco IOS Release 15.0(2)SE and Later

August 31, 2018

Cisco IOS Release 15.0(2)SE and higher runs on all Cisco IE 3010 switches.

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

- If you are installing a new switch, see the Cisco IOS release label on your switch rear panel.
- 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/web/download/index.html

Contents

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

System Requirements

Hardware Supported

.

Switch Model	Description	Supported by Minimum Cisco IOS Release
Cisco IE-3010-24TC	24 10/100 FastEthernet ports, 2 dual-purpose ports (2 10/100/1000BASE-T copper ports and 2 SFP[1] module slots), and 2 AC- and DC-power-supply module slots.	Cisco IOS Release 15.0(2)SE
Cisco IE-3010-16S-8PC	16 100BASE-FX SFP-module slots; 8 10/100 FastEthernet PoE[2] ports, 2 dual-purpose ports (2 10/100/1000BASE-T copper ports and 2 SFP module slots), and 2 AC- and DC-power-supply module slots.	Cisco IOS Release 15.0(2)SE
Rugged and industrial SFP modules[3]	GLC-SX-MM-RGD GLC-LX-SM-RGD GLC-FE-100LX-RGD GLC-FE-100FX-RGD GLC-ZX-SM-RGD	Cisco IOS Release 15.0(2)SE
Commercial SFP modules	GLC-BX-D with digital optical monitoring (DOM) support BLC-BX-U with DOM support GLC-FE-100LX GLC-FE-100BX-D GLC-FE-100BX-U GLC-FE-100FX GLC-FE-100EX GLC-FE-100ZX CWDM SFP with DOM support	Cisco IOS Release 15.0(2)SE

Switch Model	Description	Supported by Minimum Cisco IOS Release
Extended temperature SFP modules	SFP-GE-L with DOM support SFP-GE-S with DOM support SFP-GE-Z with DOM support GLC-EX-SMD with DOM support	Cisco IOS Release 15.0(2)SE
SFP module patch cable	CAB-SFP-50CM	Cisco IOS Release 15.0(2)SE
Power supply modules	PWR-RGD-AC-DC/IA PWR-RGD-LOW-DC/IA **Note** For power supply module descriptions and supported configurations on switch models, see the hardware installation guide.	Cisco IOS Release 15.0(2)SE

1. SFP = small form-factor pluggable.
2. PoE = Power over Ethernet.
3. The maximum operating temperature of the switch varies depending on the type of SFP module that you use. See the *Cisco IE 3010 Switch Hardware Installation Guide* for more information.

Express Setup Requirements

Hardware

Table 1 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
- Web browser (Internet Explorer 6.0, 7.0, or Firefox 1.5, 2.0 or later) with JavaScript enabled

Express Setup verifies the browser version when starting a session, and it does not require a plug-in.

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 Express Setup. You must use the combined tar file to upgrade the switch through Express Setup. To upgrade the switch through the CLI, use the tar file and the **archive download-sw** privileged EXEC command.

Table 2 Cisco IOS Software Image File

Filename	Description
ie3010-ipservicesk9-tar.150-2.SE.tar	Cisco IE 3010 IP services cryptographic image and Device Manager files with Kerberos, SSH, Layer 2+, and full Layer 3 features.
ie3010-lanbasek9-tar.150-2.SE.tar	Cisco IE 3010 LAN Base, with all Layer 2 features plus basic 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 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 2 on page 4 to identify the file that you want to download.

Step 2 Download the software image file. If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:
http://www.cisco.com/cisco/web/download/index.html

To download the image for an IE 3010 switch, click **Switches > Industrial Ethernet Switches > Cisco IE 3010 Series Switches**, and then click on the Cisco IOS software for your specific switch model.

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 Appendix B of the software configuration guide for this release.

Step 4 Log into the switch through the console port or a Telnet session.

Step 5 (Optional) Check 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 additional recovery procedures, see the "Troubleshooting" chapter in the software configuration guide for this release.

Installation Notes

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

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

New Software Features

- 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.
- Support for Layer 3 functionality in IP services image. For more information, see the software configuration guide for this feature.

For the *Cisco IE 3010 Switch Software Configuration Guide, Release 15.0(2)SE and Later*, go to http://www.cisco.com/en/US/docs/switches/lan/cisco_ie3010/software/release/15.0_2_se/configuration/guide/scgie3010.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.

- Cisco IOS Limitations, page 6
- Express Setup Notes, page 10

Cisco IOS Limitations

- Configuration, page 7
- Ethernet, page 8
- IP, page 8
- QoS, page 8
- SPAN and RSPAN, page 9

- Trunking, page 9
- VLAN, page 9

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

  The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)
- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mb/s full duplex or 100 Mb/s half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames.

  The workaround is to configure the port for 10 Mb/s and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)
- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked

  The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)
- A traceback error occurs if a crypto key is generated after an SSL client session.

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

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

  Use one of these workarounds:

  - Disable logging to the console.
  - Rate-limit logging messages to the console.
  - Remove the **logging event spanning-tree** interface configuration command from the interfaces. (CSCsg91027)
- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

  The workaround is to configure aggressive UDLD. (CSCsh70244)

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

  The workaround is to always enter a non-zero value for the timeout value when you enter the **boot host retry timeout** *timeout-value* command. (CSCsk65142)

- On a switch running both Resilient Ethernet Protocol (REP) and Bidirectional Forwarding Detection (BFD), when the REP link status layer (LSL) age-out value is less than 1 second, the REP link flaps if the BFD interface is shut down and then brought back up.

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

Ethernet

Traffic on EtherChannel ports is not perfectly load-balanced. Egress traffic on EtherChannel ports is distributed to member ports on a load-balance configuration, and traffic characteristics such as MAC or IP address.

More than one traffic stream might map to same member ports based on hashing results calculated by the ASIC. If this happens, uneven traffic distribution happens 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 the load-balance method as **src-dst-ip.**
- For incrementing source-ip traffic, configure the load-balance method as **src-ip.**
- For incrementing dest-ip traffic, configure the load-balance method as **dst-ip.**
- Configure the number of ports in the EtherChannel so that the number is equal to a power of 2 (that is, 2, 4, or 8)

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

IP

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

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

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 method. The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing method supported on each platform might be different.

  There is no workaround. (CSCee22591)

SPAN and RSPAN

- Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session.

  The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN. (CSCed24036)

Trunking

- 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 the 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 correctly assigned. 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)

Important Notes

Express Setup Notes

- We recommend using this browser setting to speed up the time needed to display Express Setup 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 Express Setup. 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**	Enters global configuration mode.
Step 2	**ip http authentication** {**aaa** | **enable** | **local**}	Configures the HTTP server interface for the type of authentication that you want to use. • **aaa**—Enables the authentication, authorization, and accounting feature. You must enter the **aaa new-model** interface configuration command for the **aaa** keyword to appear. • **enable**—Enables the 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**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entries.

- Express Setup 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). 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**	Enters global configuration mode.
Step 2	**ip http authentication** {**enable** | **local** | **tacacs**}	Configures the HTTP server interface for the type of authentication that you want to use. • **enable**—Enables the 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**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entries.

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

- CSCtj19181

  When a second power supply is inserted into a Cisco IE 3010 switch, the system message log might register in this order:

  ```
  *Mar 1 00:16:10.217: %POWER_SUPPLIES-3-PWR_FAIL: Power supply 1 is not functioning
  *Mar 1 00:16:13.321: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 inserted
  *Mar 1 00:16:13.346: %POWER_SUPPLIES-5-PWR_OK: Power supply 1 is functioning
  ```

  The initial “not functioning” system message is not a problem.

  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.

- 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
CSCsm45390	DHCP relay security vulnerability
CSCsv05154	Cisco IOS HTTP server vulnerable to CSRF attacks
CSCsy56638	Switch crashes after getnext on the last cafServerAliveAction index
CSCuh91645	Cisco IOS and IOS XE Software DHCP Version 4 Relay Denial of Service Vulnerability
CSCuj73916	Cisco IOS and IOS XE Software Internet Key Exchange Version 1 Denial of Service Vulnerability
CSCur29331	Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities
CSCut47751	Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities
CSCut50727	Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities

Bug ID	Headline
CSCuu76493	Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities
CSCuw77959	1801M - %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCuz81292	IPv6 neighbor discovery packet processing behavior
CSCva37748	When enable ip source guard, a part of the clients cannot communicate
CSCva74756	OSPF Rogue LSA with maximum sequence number vulnerability
CSCvd40673	Cisco Smart Install Denial of Service Vulnerability
CSCvd48893	Cisco IOS and IOS XE Software Cluster Management Protocol Remote Code Execution Vulnerability
CSCvd72069	Test CLI Command Removal
CSCvd73487	Link Layer Discovery Protocol Buffer Overflow Vulnerability
CSCve60507	Crash in "mac auth bypass" SNMP code
CSCvg62730	Cisco IOS and IOS XE Software DHCP Version 4 Relay Heap Overflow Denial of Service Vulnerability
CSCvg62754	Cisco IOS and IOS XE Software DHCP Version 4 Relay Reply Denial of Service Vulnerability
CSCvg76186	Cisco Smart Install Remote Code Execution and Denial of Service Vulnerability
CSCvi05126	SAKMP Notification messages carry unnecessary data

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 process 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

- 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.

- CSCuh99647

  Bandwidth limit configuration for ingress and egress queues (**srr-queue bandwidth limit** interface configuration command) does not work on POE ports that are up.

  There is no workaround

- 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

- 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.

- 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.

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.

- CSCub08979

  The Private VLAN feature is not available on the switch.

  The workaround is to configure protected ports on the switch by entering the following interface configuration commands:

  switchport mode access

  switchport protected

  switchport block unicast

  switchport block multicast

  For details on protected ports, go to: *http://www.cisco.com/en/US/tech/tk389/tk814/tk841/tsd_technology_support_sub-protocol_home.html*

- 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.

- 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.

- CSCug57072

  When IE3010 switch is configured as a service provider dot1q tunnel switch, it passes traffic only in the native VLAN and does not pass traffic on any other VLANs, as the VLAN ID for these VLANs gets set to 0.

  The workaround is to change the native VLAN to the VLAN ID of the incoming packet so that it pings between the dot1q tunnel port (in IE3010) and the customer trunk port.

Caveats Resolved in Cisco IOS Release 15.0(2)SE2

- CSCty63718

  The **down-when-looped** interface configuration command is not supported with default speed or with 1000BaseT advertisements on the gigabit medium independent interface (GMII interface). This is because the down-when-looped feature and 1000BaseT advertisements both make use of the “next page” function as defined in IEEE 802.3, clause 28 and may result in the link staying down.

  There is no workaround.

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.

- CSCty10239

  When ipl=5, the Catalyst 2960 switch receives the malloc failure message of 20 bytes, and traceback occurs due to interrupt level.

  There is no known 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.

- 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**.

- 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

Updates to the Getting Started Guide

- In the "Wiring the Power Supply Source" section, power supply PWR-RGD-AC-DC is now PWR-RGD-AC-DC/IA, and PWR-RGD-LOW-DC is now PWR-RGD-LOW-DC/IA.
- In Step 5 of the "Running Express Setup" section press the Express Setup button for 3 to 5 seconds.

Note If you are using the console terminal, this message appears when the switch enters Express Setup mode:

```
Entering consoleless access mode EXPRESS SETUP
```

- Warning statement 403 is added to the "Rack-Mounting the Switch" section of the English version of the *Cisco IE 3010 Switch Getting Started Guide* on Cisco.com.
- Warning statement 1063 is removed from the "Installation Warning Statements" section of the English version of the *Cisco IE 3010 Switch Getting Started Guide* on Cisco.com.

Updates to the Hardware Installation Guide

Power Supply Information

In the hardware installation guide, power supply PWR-RGD-AC-DC is now PWR-RGD-AC-DC/IA, and PWR-RGD-LOW-DC is now PWR-RGD-LOW-DC/IA:

- "Power Supply Features" section in Chapter 1, "Overview"
- Table 3-1, Figure 3-1, and Figure 3-2 in Chapter 3, "Power Supply Installation"
- Table A-2, A-3, A-4, A-5, and A-6 in Appendix A, "Technical Specifications"

IP-30 Compliance

The “Rack Mounting” and “Wall Mounting” sections in the Installation chapter are updated to add the IP-30 compliance information. See these URLs for the updated sections:

- http://www.cisco.com/en/US/docs/switches/lan/cisco_ie3010/hardware/installation/guide/higinstall.html#wp1043215
- http://www.cisco.com/en/US/docs/switches/lan/cisco_ie3010/hardware/installation/guide/higinstall.html#wp1180849

Warning Statements

- Warning statement 403 is added to the “Rack-Mounting” and “Wall-Mounting” sections of the English version of the *Cisco IE 3010 Switch Hardware Installation Guide* on Cisco.com.
- Warning statement 1063 is removed from the “Warning Statements” section of the English version of the *Cisco IE 3010 Switch Hardware Installation Guide* on Cisco.com.
- Warning statement 1001 is replaced by Statement 1088 in the “Warning Statements” section, and in the “Installation Guidelines” section of the “Power Supply Installation” chapter of the English version of the *Cisco IE 3010 Switch Hardware Installation Guide* on Cisco.com.

Updates to the Regulatory Compliance and Safety Information for the Cisco IE 3010 Switch

- Warning statement 403 is added to the English version of the *Regulatory Compliance and Safety Information for the Cisco IE 3010 Switch* on Cisco.com:

Statement 403—Install Switch in a Rack Mid-Mounting Position Only

Warning **For mounting railway-application equipment and for EN50155 standard compliance, the switch must be installed only in a rack mid-mounting position. If you install the switch in a front rack-mounting (cable side or power supply side) position or in a wall-mounting position, a mechanical failure can occur that results in the switch becoming detached from the rack.** Statement 403

Waarschuwing **Bij het monteren van apparatuur voor een spoorwegtoepassing en ter naleving van de norm EN50155, mag de switch uitsluitend met behulp van de middelste montagepositie in een rack worden geïnstalleerd. Als u de switch met de voorste montagepositie in een rack installeert (kabelkant of kant met stroomvoorziening) of aan de muur monteert, kan zich een mechanische storing voordoen, waardoor de switch uit het rack kan losraken.**

Varoitus **Rautatiesovelluslaitteiston kiinnittämistä varten ja EN50155-standardin noudattamiseksi kytkimen saa asentaa telineeseen vain keskikiinnitysasentoon. Jos kytkin asennetaan telineeseen etukiinnitysasentoon (kaapelipuoli tai virtalähdepuoli) tai seinäkiinnitysasentoon, mekaaninen vika voi esiintyä, jonka seurauksena kytkin irtoaa telineestä.**

Attention **Pour l'équipement d'application de rails de montage et pour la comformité à la norme EN50155, le commutateur doit être installé uniquement en position de montage en rack centrale. Si vous installez le commutateur en position de montage sur rack avant (côté câble ou côté alimentation) ou en position de montage murale, une défaillance mécanique risque de se produire qui peut entraîner le détachement du commutateur du rack.**

Warnung **Zur Montage von Geräten im Einsatz auf Rollmaterial und der Einhaltung des EN50155-Standards darf der Switch nur in der mittleren Montageposition befestigt werden. Wenn der Switch in der vorderen Montageposition (Kabel- oder Stromversorgungsseite) oder der Position für die Wandmontage befestigt wird, kann es zu mechanischen Ausfällen kommen, die dazu führen, dass der Switch sich vom Rack löst.**

Avvertenza **Per il montaggio di apparecchiature per il settore ferroviario e per la conformità con lo standard EN50155, lo switch deve essere installato solo in posizione di montaggio mediana sul rack. Se si installa lo switch in posizione di montaggio anteriore sul rack (lato cablaggio o lato alimentatore) o con montaggio a muro, potrebbe verificarsi un guasto meccanico e lo switch potrebbe scollegarsi dal rack.**

Advarsel **For montering av railway-application utstyr og i henhold til EN50155 standarden, må bryteren kun installeres i en posisjon midt på et stativ. Hvis du installerer bryteren på framsiden av stativet (kabel side eller strømforsyning side) eller på en vegg, kan en mekanisk svikt oppstå. Dette kan resultere i at bryteren blir løsrevet fra stativet.**

Aviso **Para montagem de equipamento ferroviário, e em conformidade com as normas EN50155, o interruptor deverá ser instalado unicamente, numa prateleira central. Se instalar o interruptor na parte da frente da prateleira (no lado do cabo ou da alimentação eléctrica) ou numa parede, poderá ocorrer falha mecânica, causando o desprendimento do interruptor.**

¡Advertencia! **Para el montaje en equipos para raíles y para cumplir con la norma EN50155, el switch debe instalarse exclusivamente en una posición intermedia para montaje en rack. Si instala el switch en una posición para montaje en rack delantera (al lado del cable o del suministro de alimentación) o en una posición para montaje en pared, puede producirse un fallo mecánico y el switch puede separarse del rack.**

Varning! **För montering av rälstillämpningsutrustningen och för att kunna uppfylla EN50155-standarden, måste reglaget endast vara installerat i mittenpositionen på stället. Om du installerar reglaget på ställets framsida (kabelsidan eller nätaggregatets sida) eller i en position på väggen, kan ett mekaniskt fel uppstå vilket resulterar i att reglaget lösgörs från stället.**

Figyelem Vasúton alkalmazott berendezések felszerelésekor és az EN50155 szabványnak való megfelelés érdekében a kapcsolót kizárólag középső rögzítésű keretre lehet felszerelni. Amennyiben a kapcsolót elülső keretre szerelt pozícióban (kábel oldalra vagy energiaellátás oldalra), vagy falra szerelt pozlcióban helyezi üzembe, mechanikai probléma fordulhat elő, ami a kapcsolónak a tartóról való leválását eredményezheti.

Предупреждение При монтаже оборудования, поддерживающего работу приложений для железнодорожного транспорта, а также в целях обеспечения соответствия стандартам EN50155, коммутатор должен быть установлен только в среднюю часть стойки. В случае установки коммутатора в переднюю часть стойки (коммутационной панелью или панелью источника питания вперед) или при монтаже на стену может произойти механический отказ, в результате которого крепление коммутатора может ослабиться.

警告 为了便于安装火车应用设备和 符合标准EN50155 ，交换器只应安装在安装位置居中的机架上。如果交换机安装的位置在机架前侧（电缆或电源侧）或为墙壁安装位置，机械故障可能导致交换机从机架脱落。

警告 鉄道用アプリケーション機器の取り付けおよびEN50155 標準規格上、スイッチは、ラックの中間取り付け位置へ設置されなければなりません。前面ラック取り付け位置（ケーブル側または電源側）もしくは壁側取り付け位置へスイッチを設置した場合、機械的な不具合が発生し、スイッチがラックから外れてしまう可能性があります。

Aviso **O switch deve ser instalado somente em uma posição mediana de montagem de rack para que a montagem do equipamento do aplicativo de via-férrea e a conformidade padrão do EN50155 sejam bem-sucedidas. Se instalar o switch em uma posição frontal de montagem de rack (ao lado do cabo ou do fornecedor de energia) ou em uma posição de montagem em parede uma falha mecânica poderá ocorrer e isso resultará na separação do switch e do rack.**

- Warning statement 1001 is replaced by warning statement 1088 in the English version of the *Regulatory Compliance and Safety Information for the Cisco IE 3010 Switch* on Cisco.com.

Statement 1088—Avoid Servicing Outdoor Connections During an Electrical Storm

Warning **Avoid using or servicing any equipment that has outdoor connections during an electrical storm. There may be a risk of electric shock from lightning.** Statement 1088

Waarschuwing **Vermijd het gebruik van en onderhoud aan apparatuur met buitenaansluitingen tijdens een onweersbui.**
Er bestaat een gering risico op elektrische schokken door blikseminslag.

Varoitus **Vältä kaikkien ulkoliitäntöjä sisältävien laitteiden käyttöä ja huoltoa ukonilman aikana.**
Saatat saada sähköiskun salamoinnin johdosta.

Attention **Les équipements pourvus de connexions extérieures ne doivent pas être utilisés ni entretenus pendant un orage.**
La foudre est susceptible de provoquer des décharges électriques.

Warnung **Vermeiden Sie bei Gewitter die Nutzung oder Bedienung von Geräten mit Außenanschlüssen.**
Da bei einem Blitzeinschlag die Gefahr von Stromschlägen besteht.

Avvertenza **Evitare l'utilizzo o la manutenzione di qualsiasi apparecchiatura con collegamenti per esterni durante un temporale.**
In quanto vi è la possibilità di folgorazione da fulmine.

Advarsel **Under tordenvær må det unngås å bruke eller reparere utstyr som har utendørs forbindelser.**
Det finnes en risiko for elektrisk støt fra lyn.

Aviso **Evite utilizar ou realizar manutenção em qualquer equipamento que tenha ligações exteriores durante uma tempestade eléctrica.**
Pode haver um risco remoto de choque eléctrico devido aos relâmpagos.

¡Advertencia! **Evite el uso o mantenimiento de cualquier material con conexiones al aire libre durante una tormenta eléctrica.**
Ya que el riesgo de descarga eléctrica es mayor debido a los rayos.

Varning! **Använd eller reparera inte någon utrustning som har anslutningar utomhus under åskväder.**
Det finns en liten risk för elektriska stötar vid blixtnedslag.

Figyelem Ügyeljen arra, hogy vihar közben ne használjon vagy szereljen kültéri csatlakozókkal rendelkező készüléket.
Villámlás esetén áramütésveszély áll fenn.

Предупреждение Не используйте и не обслуживайте оборудование, имеющее внешние подключения, во время грозы.
Существует опасность удара электрическим током от молнии.

警告 雷雨の際に、屋外の接続部がある装置を使用または修理しないでください。
雷により感電する危険性があります。

警告 避免在雷暴天气使用或维修任何配备室外线路的设备。
雷电可能带来电击风险。

- Warning statement 1063 is removed from the English version of the *Regulatory Compliance and Safety Information for the Cisco IE 3010 Switch* on Cisco.com.

Related Documentation

These documents provide complete information about the Cisco IE 3010 switches and are available at Cisco.com:

http://www.cisco.com/en/US/products/ps11245/tsd_products_support_series_home.html

- *Cisco IE 3010 Switch Software Configuration Guide*
- *Cisco IE 3010 Switch Command Reference*
- *Cisco IE 3010 Switch System Message Guide*
- *Cisco IE 3010 Switch Hardware Installation Guide*
- *Cisco IE 3010 Switch Getting Started Guide*—available in English, simplified Chinese, French, German, Italian, Japanese, Brazilian Portuguese, and Spanish
- *Regulatory Compliance and Safety Information for the Cisco IE 3010 Switch*

For other information about related products, see these documents:

- Express Setup online help (available on the switch)

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

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*

Compatibility matrix documents:

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

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.