Release Notes for the Industrial Ethernet 3010 Switch, Cisco IOS Release 15.2(2)E

January 10, 2017

Cisco IOS Release 15.2(2)E runs on all Cisco IE 3010 switches.

These release notes include important information about Cisco IOS release 15.2(2)E, 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

Table 1

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
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

Table 1

Switch Model	Description	Supported by Minimum Cisco IOS Release
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 2 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, Windows 7, and Windows Server 2003.
- Internet Explorer 6.0, 7.0, Firefox up to version 26.0 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 3 Cisco IOS Software Image File

Filename	Description
ie3010-ipservicesk9-mz.152-2.E.bin ie3010-ipservicesk9-tar.152-2.E.tar[1]	Cisco IE 3010 IP Services cryptographic image with Layer 2 and Layer 3 features.
ie3010-lanbasek9-mz.152-2.E.bin ie3010-lanbasek9-tar.152-2.E.tar	Cisco IE 3010 LAN Base cryptographic image with all Layer 2 features, IPv4 static routing, and inter-VLAN routing.

1. The ie3010-ipservicesk9-tar.152.2.E.tar image is greater than 32MB, and you cannot have more than one image file on the flash.

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 3 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

- Features Introduced in Cisco IOS Release 15.2(2)E1, page 6
- Features Introduced in Cisco IOS Release 15.2(2)E, page 7

Features Introduced in Cisco IOS Release 15.2(2)E1

What’s New	Description
Device Sensor	(LAN Base)

Features Introduced in Cisco IOS Release 15.2(2)E

What's New	Description
Cisco IOS Release 15E Documentation Roadmap	Provides quick and easy access to all relevant documentation for specific platforms. Look for *Quick Links to Platform Documentation* on the respective platform documentation pages.
Integrated Documentation Guides	Provides platform and software documentation for two technologies: • IP Multicast Routing Configuration Guide • Cisco Flexible Netflow Configuration Guide.
Smart Install	Smart Install is a plug-and-play configuration and image-management feature that provides zero-touch deployment for new switches. You can ship a switch to a location, place it in the network and power it on with no configuration required on the device. The IE 3010 switch can be a Smart Install Director. For more information, see Smart Install Configuration Guide here: http://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install.html
Cisco EnergyWise	Support for Cisco EnergyWise Version 2.8. For more information, see the Cisco EnergyWise software release notes and configuration guide. For more information, see the Cisco EnergyWise software release notes and the configuration guide here: http://www.cisco.com/c/en/us/td/docs/switches/lan/energywise/version2_8/ios/release/notes/ol23554.html
IP Device Tracking	Enhancement to IP device tracking for ARP probes; command now supports new keyword **ip device tracking probe auto-source fallback 0.0.0.100 255.255.255.0 override**.
Plug-N-Play	Cisco Open Plug-n-Play agent is a software application that is running on a Cisco IOS or IOS-XE device and provides zero-touch deployment of all new devices. The application facilitates the acquisition and loading of pertinent images, configuration files, and other required files to the device along with notifications for various events. (Cisco IE 3010 only supports Cisco IOS)

For the *Software Configuration Guide, Cisco IOS Release 15.2(2)E (Industrial Ethernet 3010 Switch)*, go to http://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3010/software/release/15-2_2_e/configuration/guide/SwCfg.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

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.

Caveats

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

No Open Caveats.

Caveats Resolved in Cisco IOS Release 15.2(2)E6

No caveats were resolved in this release.

Caveats Resolved in Cisco IOS Release 15.2(2)E5a

Bug ID	Severity	Headline
CSCvb19326	2	NTP leap second addition is not working during leap second event

Caveats Resolved in Cisco IOS Release 15.2(2)E5

Bug ID	Severity	Headline
CSCut86361	3	3010, 2520 Temperature & Power monitor SNMP status report incorrectly

Caveats Resolved in Cisco IOS Release 15.2(2)E4

No caveats were resolved in this release.

Caveats Resolved in Cisco IOS Release 15.2(2)E3

Bug ID	Severity	Headline
CSCul73513	2	Server-client clock not in sync after leap configuration
CSCum17258	2	EPM_SESS_ERR: Error in activating feature (EPM ACL PLUG-IN)
CSCup81878	2	Line by Line Sync fails while deleting dynamic NTP peer
CSCur11439	3	EnergyWise Activitycheck powers off phone during an active call
CSCur58372	3	"snmp-server enable traps syslog" shows in "show run all" output after removal
CSCur59242	2	Crash due to tplus_client_stop_timer
CSCus09761	2	IOS-Phone not placed in critical voice VLAN when AAA server is unreached
CSCus13924	2	Device crashes while configuring 'Identity' commands
CSCus47009	3	Switch does not increment the "Received on untrusted ports" DHCP counter
CSCus79132	2	Dot1x authentication legacy behavior broken
CSCut10251	2	Some commands are not in running-config after AUTOINSTALL finishes
CSCut13064	3	BPDU filter does not work on output port when STP is disabled
CSCut20271	2	C3560X responds to ARP request from management port

Bug ID	Severity	Headline
CSCut27272	2	CPUHOG and crash due to Auth Manager process
CSCut79680	3	ip default-gateway is not seen in running-config after AUTOINSTALL
CSCut87425	2	CPU hog in "EEM TCL Proc" after TCL script termination with long runtime
CSCuu50392	2	Auth Manager memory leak with ISE authentication
CSCuu97116	2	Acct messages should include Class attribute from authentication
CSCuv06451	2	IOSd crash in eap_auth_terminal_state calling free_internal

Caveats Resolved in Cisco IOS Release 15.2(2)E2

No caveats were resolved in this release

Caveats Resolved in Cisco IOS Release 15.2(2)E1

Bug ID	Severity	Headline
CSCun68507	1	IE3K Bad CF card (bzip not handling corrupted image data correctly)
CSCun80959	2	Desg port on the RootBridge experienced block forward for 30 sec
CSCuo25980	2	EA branches must fix: tftp from CNA crash IE switches
CSCup96299	2	IPv6 Multicast RIB entry refer to wrong distance
CSCuq10827	3	C3560X cHsrpGrpStandbyState is incorrect
CSCur00722	1	Hard Reset of the Active Sup cause switch to power cycle

Caveats Resolved in Cisco IOS Release 15.2(2)E

Bug ID	Severity	Headline
CSCum65206	3	VLAN-based QoS support to be enabled for IE3000/IE3010 platforms
CSCum76147	3	No warning for Port Security Settings changes displayed via Device Mgr

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.