Release Notes for the Cisco IE 3010 Switch, Cisco IOS Release 15.2(1)EY

First Published: January 2014

Last Updated: September 2015

Cisco IOS Release 15.2(1)EY runs on Cisco IE 3010 switches.

These release notes include important information about Cisco IOS release 15.2(1)EY and later, 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

Cisco Systems, Inc.
www.cisco.com

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
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.

SFP Modules Supported

The SFP modules are switch Ethernet SFP modules that provide connections to other devices. Depending on the switch model, these field-replaceable transceiver modules provide uplink or downlink interfaces. The modules have LC connectors for fiber-optic connections.

You can use any combination of the supported SFP modules.

Switch Model	Description
Rugged and industrial SFP modules[1]	GLC-FE-100LX-RGD GLC-FE-100FX-RGD GLC-SX-MM-RGD[2] GLC-LX-SM-RGD[2] GLC-ZX-SM-RGD[2]
Commercial SFP modules	GLC-SX-MM GLC-LH-SM GLC-BX-U[2] GLC-BX-D[2] CWDM-SFP[2] DWDM-SFP[2] GLC-T
Extended temperature SFP modules	SFP-GE-S[2] SFP-GE-L[2] SFP-GE-Z[2] GLC-EX-SMD GLC-LX-SMD GLC-FE-100FX GLC-FE-100LX GLC-FE-100EX GLC-FE-100ZX GLC-FE-100BX-U GLC-FE-100BX-D

[1] The maximum operating temperature of the switch varies depending on the type of SFP module that you use. See the *Hardware Installation Guide* for more information.

[2] These SFP modules have digital optical monitoring (DOM) support.

For the most up-to-date list of supported SFP models for Cisco Industrial Ethernet switches, see http://www.cisco.com/en/US/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_6981.html#wp138176

Express Setup Requirements

Hardware

- 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor

- 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
- 16 GB available hard disk space (32-bit) or 20 GB (64-bit)

Software

- PC with Windows 7, or Mac OS 10.6.x
- Web browser (Internet Explorer 9.0, 10.0, and 11.0, or Firefox 25, 26) with JavaScript enabled

  Express Setup verifies the browser version when starting a session, and it does not require a plug-in.
- Straight-through or crossover Category 5 or 6 cable

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 1 Cisco IOS Software Image File

Filename	Description
ie3010-ipservicesk9-tar.152-1.EY.tar	Cisco IE 3010 IP services cryptographic image with Kerberos, SSH, Layer 2+, and full Layer 3 features.
ie3010-lanbasek9-tar.152-1.EY.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 Secure Digital (SD) flash card is inserted into the switch before downloading the software.

To download software, follow these steps:

Step 1 Use Table 1 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

Digital Optical Monitoring

Digital Optical Monitoring (DOM) is supported when using a DOM-capable SFP transceiver module. For information about the switch models that have SFP or dual-purpose ports and about DOM-capable SFP modules, see SFP Modules Supported, page 2.

Note DOM is not supported on downlink SFP ports.

DOM allows monitoring real-time parameters of the switch, such as optical input and output power, temperature, laser bias current, and transceiver supply voltage. These parameters are monitored against the threshold values. The real-time DOM parameters can be monitored using command line interface or SNMP interface.

DOM is possible only with DOM-capable transceiver modules. When using an SFP module in a dual purpose port, DOM is supported if the interface media type is configured to SFP or if global transceiver monitoring is enabled.

Transceiver monitoring is enabled by default.

Security Group Tag Exchange Protocol for Cisco TrustSec

Cisco Industrial Ethernet switches now can participate in the Cisco TrustSec security architecture by using the SGT Exchange Protocol (SXP). Cisco TrustSec establishes domains of trusted network devices. After a device is authenticated, communication is secured by using encryption and other mechanisms. As packets enter the network, they are classified by security group tags (SGTs) for the purpose of applying security policies. SXP is used to propagate the SGTs across network devices, such as the IE switches, that do not have hardware support for Cisco TrustSec.

To use this feature, enable SXP and configure the connections on each device that needs to participate in SXP exchanges.

- Enable SXP by entering the **cts sxp enable** command in global configuration mode.
- Configure each SXP connection by specifying the peer's IP address, the password, and the role. For role, you can specify which device is the "speaker" and the "listener" in the exchange.

For detailed information about the configuration commands and show commands, see "SGT Exchange Protocol over TCP (SXP)" at
http://www.cisco.com/en/US/partner/docs/switches/lan/trustsec/configuration/guide/sxp_config.html#wp1056896

IP Device Tracking

IP Device Tracking (IPDT) is globally enabled in the 15.2(1)EY release on all IE platforms. You can disable IPDT probing at the interface level using the CLI **ip device tracking maximum 0** to avoid timeouts when end devices are in IP probing tentative state. This is especially critical if the switches are used in control automation, such as in an EtherNet/IP and Profinet network environment.

Web Device Manager Enhancements

The 15.2(1)EY release introduces an enhanced Web Device Manager GUI that is easier to use. The upgrade requires IOS tar file extraction and upgrade.

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 8
- Express Setup Notes, page 10

Cisco IOS Limitations

- Ethernet
- IP
- QoS
- RADIUS
- SPAN and RSPAN
- Spanning Tree Protocol
- Trunking
- VLAN

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)

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)

RADIUS

- RADIUS change of authorization (COA) reauthorization is not supported on the critical auth VLAN.

  There is no workaround. (CSCta05071)

SPAN and RSPAN

- When the RSPAN feature is configured on a switch, Cisco Discovery Protocol (CDP) packets received from the RSPAN source ports are tagged with the RSPAN VLAN ID and forwarded to trunk ports carrying the RSPAN VLAN. When this happens a switch that is more than one hop away incorrectly lists the switch that is connected to the RSPAN source port as a CDP neighbor.

  This is a hardware limitation. The workaround is to disable CDP on all interfaces carrying the RSPAN VLAN on the device connected to the switch. (CSCeb32326)
- 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)

Spanning Tree Protocol

- CSCtl60247

  When a switch or switch stack running Multiple Spanning Tree (MST) is connected to a switch running Rapid Spanning Tree Protocol (RSTP), the MST switch acts as the root bridge and runs per-VLAN spanning tree (PVST) simulation mode on boundary ports connected to the RST switch. If the allowed VLAN on all trunk ports connecting these switches is changed to a VLAN other than VLAN 1 and the root port of the RSTP switch is shut down and then enabled, the boundary ports connected to the root port move immediately to the forward state without going through the PVST+ slow transition.

  There is no workaround.

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 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)

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.

Open Caveats

Note You can click the issue number to view more information in the Cisco Bug Search tool (login required).

Issue	Description
CSCum65206	HQOS, Vlan-based qos and QOS mapping to multiple interfaces was disabled in 15.2(1)EY. **Workaround:** There is no workaround.

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.
	Workaround: There is no workaround.

Caveats Resolved in This Release

Note You can click the issue number to view more information in the Cisco Bug Search tool (login required).

Issue	Description
CSCua74302	(Switches running the LAN base image) ACLs applied to outbound traffic on the switch virtual interface (SVI) do not work. **Workaround:** There is no workaround.

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.