Release Notes for the Cisco ESS 2020 Switch, Cisco IOS Release 15.0(2)EC and Later

April, 2013

These release notes include important information about Cisco IOS Release 15.0(2)EC and later releases, 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 Models Supported

15.0(2)EC

Table 1   Cisco ESS 2020 Switches Supported

Switch Model	Description	Supported by Minimum Cisco IOS Release
ESS 2020-NCP	Embedded Service Switch 2020, No Cooling Plate, LAN Lite	Cisco IOS Release 15.0(2)EC
ESS 2020-CON	Embedded Service Switch 2020, Conduction Cooled, LAN Lite	Cisco IOS Release 15.0(2)EC
ESS 2020-24TC-NCP	ESS 2020 Main Switch with 16 Port Expansion bundle, No Cooling Plate, LAN Lite	Cisco IOS Release 15.0(2)EC
ESS 2020-24TC-CON	ESS 2020 Main Switch with 16 Port Expansion bundle, Conduction Cooled, LAN Lite	Cisco IOS Release 15.0(2)EC
ESS 2020-NCP-B	Embedded Service Switch 2020, No Cooling Plate, LAN Base	Cisco IOS Release 15.0(2)EC
ESS 2020-CON-B	Embedded Service Switch 2020, Conduction Cooled, LAN Base	Cisco IOS Release 15.0(2)EC
ESS 2020-24TC-NCPB	ESS 2020 Main Switch with 16 Port Expansion bundle, No Cooling Plate, LAN Base	Cisco IOS Release 15.0(2)EC
ESS 2020-24TC-CONB	ESS 2020 Main Switch with 16 Port Expansion bundle, Conduction Cooled, LAN Lite	Cisco IOS Release 15.0(2)EC

SFP Modules Supported

Table 2   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]
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 *Cisco IE 2000 Switch Hardware Installation Guide* for more information.

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

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 also can 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. 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
c2020-universalk9.tar	Cisco ESS 2020 cryptographic Cisco IOS image file.

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 *Cisco IOS Configuration Fundamentals Command Reference*:

http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/test_cable-diagnostics_through_xmodem.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 ESS 2020 switch, click **Switches > Industrial Ethernet Switches > Cisco ESS 2020 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:

- CLI-based setup program, as described in the switch hardware installation guide.
- DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manual assignment of an IP address, as described in the switch software configuration guide.

New Software Features

This release is the first software release for the ESS 2020 switches. For a detailed list of key features for this software release, see the "Overview" chapter of the *Cisco ESS 2020 Switch Software Configuration Guide*.

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 7

Cisco IOS Limitations

Ethernet

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

If this situation occurs, uneven traffic distribution occurs 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.**

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

- 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 one in VLAN Y is sent on the trunk port in VLAN Y. This is 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 flashes amber, and the frames are not counted on the interface statistics.

  There is no workaround. (CSCec35100).

VLAN

- 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

- IPv4 Static Routing Notes, page 9
- 61000-4-3 Standard Notes, page 9

IPv4 Static Routing Notes

Cisco ESS 2020 supports IPv4 static routing in the lanbase image. To access static routing commands you need to change the SDM template from the default template to lanbase-routing, followed by a switch reload sequence.

61000-4-3 Standard Notes

The following note is an update to the *Regulatory Compliance and Safety Information* (RCSI) guide. This note applies to the 61000-4-3 standard listed in the "EMC Interface Immunity" section of Table 1 of the guide.

Note To meet 10V/m or 20V/m Radiated Immunity levels, shielded cables must be used on the uplink ports, G1/1 and G1/2.

This note applies to these SKUs:
– ESS 2020-CON
– ESS 2020-CON-B
– ESS 2020-NCP
– ESS 2020-NCP-B

Open Caveats

- CSCuf94887

  If fast boot is not enabled when reloading the switch, the power and system LEDs remain off for up to 1 minute.

Documentation Updates

Updates to the Hardware Installation Guide

These corrections are for the English version of the *Cisco ESS 2020 Hardware Installation Guide* on Cisco.com. These corrections also apply to the French version of the hardware guide; however, this version has not yet been updated.

SFP Modules

- GLC-LX-SMD is supported and has been added to Table 1-2 in the "SFP Modules" section.
- References to copper SFPs are removed because the Cisco ESS 2020 switch does not support them. A note is added to the "SFP Modules" section indicating that copper SFPs are not supported.

Note The Cisco ESS 2020 switch does not support copper SFP modules.

Updates to the Regulatory Compliance and Safety Information Guide

61000-4-3 Standard

This note applies to the 61000-4-3 standard listed in the "EMC Interface Immunity" section of Table 1 in the *Regulatory Compliance and Safety Information* guide.

Note To meet 10V/m or 20V/m Radiated Immunity levels, shielded cables must be used on the uplink ports, G1/1 and G1/2.

This is applicable to these SKUs:
– IE-2000-4T-G-L
– IE-2000-4T-G-B
– IE-2000-8TC-G-L
– IE-2000-8TC-G-B

Related Documentation

These documents provide complete information about the Cisco ESS 2020 switches and are available at Cisco.com:

www.cisco.com/go/embedded

- Cisco ESS 2020 Embedded Service Switch Hardware Technical Guide
- Cisco ESS 2020 Switch Software Configuration Guide

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*

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

- Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix
- Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix

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.