

Upgrading the Cisco ONS 15454 SDH MSTP to Release 9.2.3

First Published: 2022-10-11

Last Modified: 2023-10-25

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-31791-01

© 2023 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Upgrading the Cisco ONS 15454 SDH MSTP to Release 1**

Test 1

Errorless Upgrades and Exceptions 1

Document Procedures 2

NTP-U487 Preparing to Upgrade to a New Release 2

NTP-U488 Back Up the Cisco Software Database 3

NTP-U489 Upgrade the Cisco Software 4

DLP-U546 Download the Software 5

DLP-U548 Activate the New Cisco Software 7

DLP-U549 Delete Cached JAR Files 8

DLP-U551 Set the Date and Time 9

NTP-U490 Install Public-Key Security Certificate 10

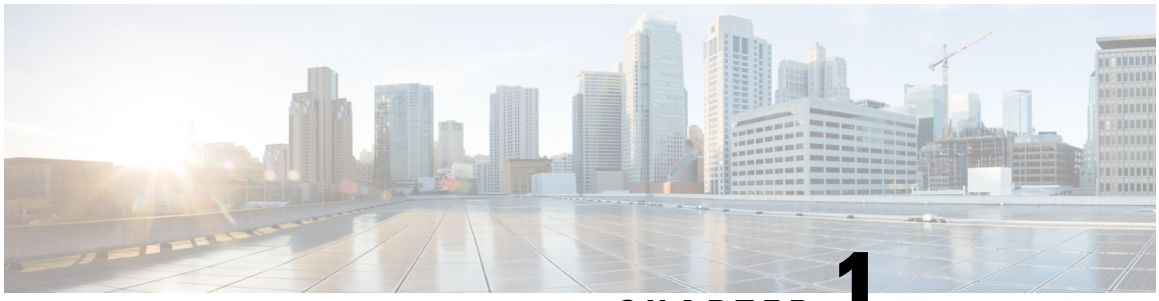
NTP-U491 Restore the Previous Software Load and Database 11

DLP-U552 Revert to Protect Load 12

DLP-U553 Manually Restore the Database 13

Related Documentation 14

Obtaining Documentation and Submitting a Service Request 14



CHAPTER 1

Upgrading the Cisco ONS 15454 SDH MSTP to Release

This document explains how to upgrade Cisco ONS 15454 SDH Cisco Transport Controller (CTC), using the advanced Timing, Communications, and Control (TCC2) or advanced Timing, Communications, and Control Plus (TCC2P), Timing Communications Control Three (TCC3), Transport Node Controller (TNC), or Transport Shelf Controller (TSC) card.

To understand the supported software upgrade paths, refer to the Software Upgrade Matrix .

Note The TSC and TNC cards are the control cards installed on ONS 15454 M2 and ONS 15454 M6 shelves.

- Test , on page 1
- Errorless Upgrades and Exceptions, on page 1
- Document Procedures, on page 2
- NTP-U487 Preparing to Upgrade to a New Release, on page 2
- NTP-U488 Back Up the Cisco Software Database, on page 3
- NTP-U489 Upgrade the Cisco Software , on page 4
- NTP-U490 Install Public-Key Security Certificate, on page 10
- NTP-U491 Restore the Previous Software Load and Database, on page 11
- Related Documentation, on page 14
- Obtaining Documentation and Submitting a Service Request, on page 14

Test

Errorless Upgrades and Exceptions

This section describes important information to be aware of before you begin the upgrade process:

Document Procedures

Procedures in this document must be performed in consecutive order unless noted otherwise. Ensure that the procedure is completed for each node in a given network. If you are new to upgrading the software, make a printed copy of this document and use it as a checklist.

Each non-trouble procedure (NTP) is a list of steps designed to accomplish a specific procedure. Follow the steps until the procedure is complete. If you need more detailed instructions, refer to the detail-level procedure (DLP) specified in the procedure steps. Throughout this guide, NTPs are referred as “procedures” and DLPs as “tasks.” Every reference to a procedure includes its NTP number, and every reference to a task includes its DLP number.

The DLP (task) supplies additional task details to support the NTP. The DLP lists numbered steps that lead you through completion of a task. Some steps require that equipment indications be checked for verification. When a proper response is not obtained, a trouble clearing reference is provided.

This section lists the document procedures (NTPs). Turn to a procedure for applicable tasks (DLPs).

1. NTP-U487 Preparing to Upgrade to a New Release, on page 2—This procedure contains critical information and tasks that you must read and complete before beginning the upgrade process.
2. NTP-U488 Back Up the Cisco Software Database, on page 3—Complete the database backup to ensure that you have preserved your node and network provisioning in the event that you need to restore them.
3. NTP-U489 Upgrade the Cisco Software , on page 4—Complete this procedure to complete the upgrade.
4. NTP-U490 Install Public-Key Security Certificate, on page 10— Complete this procedure to be able to run the software.
5. NTP-U491 Restore the Previous Software Load and Database, on page 11— Complete this procedure if you want to return to the previous software load you were running before activating the new release.
6. — Complete this procedure only if you want to upgrade to a new release using Transaction Language (TL1).

NTP-U487 Preparing to Upgrade to a New Release

Purpose	This procedure provides critical information checks and tasks you must complete before beginning an upgrade to the latest release.
Tools/Equipment	
Prerequisite Procedures	"DLP-G46 Log into CTC" in the "Connect the PC and Log into the GUI" document.
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Procedure

Step 1 Before you begin, make sure that information related to your site, for example, date, street address, site phone number, and dialup number are stored in a safe and accessible location. The data will be useful during and after the upgrade.

Step 2 Read the release notes of the release you are upgrading to. Visit Release Notes to download the release notes.

Step 3 Ensure your workstation meets the minimum hardware and software requirements before starting the upgrade. For more information on the hardware and software requirements, read the release notes.

Step 4 Refer to the to verify if the upgrade path is supported.

Step 5 Make sure that the control cards are installed in the appropriate slots on all the nodes in the network and on both the slots as indicated here. For a complete list of supported control cards, see Supported Control Cards:

Step 6 Repeat the above step for every node in the network.

Step 7 Collect the node diagnostics logs from the node. This action is very useful incase the upgrade fails, as the diagnostics help in understanding if the node had issues before the upgrade.

Step 8 Export the current alarms and conditions to your local storage. After the upgrade, if new alarms or conditions arise, then comparing the time stamp of the alarm to the previously saved time stamp helps in identifying new alarms or conditions.

Step 9 Perform a backup of the node database. This is very useful incase the upgrade fails, then the database can be restored using the backup. The detailed procedure for backing up the database is discussed in the next section.

Stop. You have completed this procedure.

NTP-U488 Back Up the Cisco Software Database

Purpose	This procedure retains all configuration data for your network before performing the upgrade.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	• "DLP-G46 Log into CTC" in the "Connect the PC and Log into the GUI " document. • NTP-U487 Preparing to Upgrade to a New Release, on page 2
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Procedure

Step 1 In the node view, click the **Maintenance**>**Database** tabs.

Step 2 In the database pane, click the **Backup** button.

The Database Backup dialog box is displayed.

Step 3 Click **Browse**. Navigate to the local PC directory or network directory and type a database name using the IP address of the node to upgrade in the File Name field and click **OK**. To overwrite an existing file, click **Yes**.

Step 4 When the backup is complete, click **OK.**

Step 5 Repeat Steps 1 through 5 for each node in the network.

Step 6 (Optional) It is recommended that you manually log critical information by either writing it down, printing screens, or by exporting the data to an appropriate format, as applicable. Use the following table to determine the information that should be logged.

Information	Record Data Here
IP address of the node	
Node name	
Timing settings	
DCC[1] connections—list all optical ports with active DCCs	
User IDs of all users, including at least one Superuser	
Inventory—A print screen of the Inventory window	
Network information—A print screen of the Provisioning tab in the network view	
List all protection groups in the system—A print screen of the Protection group window	
List alarms—A print screen of the Alarm window	
List circuits—A print screen of the Circuit window	

[1] DCC=data communications channel

Stop. You have completed this procedure.

NTP-U489 Upgrade the Cisco Software

Purpose	This procedure upgrades the CTC software to and must be performed on all nodes, or groups of nodes to be upgraded.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U488 Back Up the Cisco Software Database, on page 3
Required/As Needed	Required

Onsite/Remote	Onsite or remote
Security Level	Superuser

Caution Do not perform maintenance or provisioning activities during the activation task.

Procedure

Step 1 Insert the software CD into the workstation CD-ROM drive (or otherwise acquire access to the software) to begin the upgrade process.

Note Inserting the software CD activates the CTC Java Setup Wizard. Use the setup wizard to install the components or click **Cancel** to continue with the upgrade.

Step 2 Complete the DLP-U546 Download the Software, on page 5 task for all nodes to be upgraded.

Step 3 Complete the DLP-U548 Activate the New Cisco Software, on page 7 task for all nodes to be upgraded.

Note Only one node can be activated at a time. During a parallel upgrade, activate another node as soon as the controller cards reboot successfully. To perform parallel upgrade remotely, wait five minutes for the controller cards to reboot completely.

Step 4 Complete the DLP-U549 Delete Cached JAR Files, on page 8 task, as necessary.

Step 5 (Optional) If you want to prevent a software revert to an earlier software release, complete the DLP-U546 Download the Software, on page 5 task on all nodes, or groups of nodes you are upgrading a second time.

Step 6 If you need to return to the software and database you had before activating Software , proceed with the NTP-U491 Restore the Previous Software Load and Database, on page 11 procedure.

Step 7 To back up the Software database for the working software load, see NTP-U488 Back Up the Cisco Software Database, on page 3 procedure in order to preserve the database for the current release.

Stop. You have completed this procedure.

What to do next

After upgrading the software to a different build, if there is a change in the FPGA, the FPGA is upgraded automatically. During the FPGA upgrade process, the card goes for a cold reboot. If Optical Supervisory Channel (OSC) is provisioned, then the transient PPM-IMPROPER-REMOVAL alarm is raised, which gets cleared in a short span of time. This happens because of the power glitches to the PPM while the card is coming up after the cold reboot.

DLP-U546 Download the Software

Purpose	This task downloads software to the nodes before activation.
Tools/Equipment	PC or UNIX workstation

Prerequisite Procedures	NTP-U488 Back Up the Cisco Software Database, on page 3
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Maintenance user or higher

Note The control card contains flash memory with two partitions—Working and protect (backup). The software is downloaded to the protect (backup) partition of the flash memory on both the standby and active cards. This download is not traffic affecting because the active software continues to run in the primary RAM location. The software can therefore be downloaded at any time.

Note To download and upgrade the software using TL1, see the procedure.

Procedure

Step 1 From CTC View menu, choose **Go to Network View**.

Step 2 Make sure that the alarm filter is turned off. To do so, complete the following:

a) Click the **Filter** tool that is located at the lower-left side of the window.

The Alarm Filter dialog box appears.

b) Click to select any check box that is not selected in the Show Severity section of the **General** tab.

Step 3 Resolve any outstanding alarms. To view alarms for all the nodes in the network, click the **Alarms** tab.

Note The SFTWDOWN alarm is raised on the standby and active control cards during software download. The alarms clear when the download is complete.

Step 4 From the CTC View menu, choose **Go to Home View** to go to the node view.

Step 5 Click the **Maintenance**> **Software** tabs.

Step 6 Click the **Download** button. The Download Selection dialog box appears.

Step 7 Locate the software files on the software CD or on your hard drive.

Step 8 To open the folder, choose the file with the PKG extension and click **Open**.

Step 9 From the list of compatible nodes, select the nodes where the software must be downloaded.

Note It is recommended that simultaneous software downloads on the section data communications channel (SDCC) be limited to eight nodes at a time, using the central node to complete the download. If more than eight concurrent software downloads are selected at a time, it is placed in a queue.

Step 10 Click **OK**. The Download Status column monitors the progress of the download.

Step 11 Return to your originating procedure (NTP).

DLP-U548 Activate the New Cisco Software

Purpose	This task activates the software on each node in the network.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U546 Download the Software, on page 5
Required/As Needed	Required
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note It is recommended that the first node that is activated be connected via LAN. This ensures that the new CTC JAR files download to the workstation as quickly as possible.

If a node is provisioned to have no LAN access, the value is overridden in the case of node isolation. Additionally, if the node is not reachable, the LAN access is turned on. It is recommended that you avoid node isolation.

Note During the activation process, when the node is being upgraded to R11.0 (and later releases), the USB-MOUNT-FAIL alarm is raised. In MSM, the USB-MOUNT-FAIL alarm is raised on all subtended shelf controllers and the node controller. When all the subtended shelf controllers and the node controller complete the upgrade successfully, the USB-MOUNT-FAIL alarm is cleared. No manual intervention is required to clear the USB-MOUNT-FAIL alarm. After the USB-MOUNT-FAIL alarm is cleared, USB sync is triggered. After USB sync is successfully completed, the node is migrated to the latest software successfully.

Procedure

Step 1 If CTC is not already started, start CTC.

Step 2 Record the IP address of the node. The IP address can be obtained either on the LCD or on the upper left corner of the CTC window.

Step 3 Make sure that the alarm filter is turned off. To do so, complete the following:

a) Click the **Filter** tool at the lower-left side of the window.

The Alarm Filter dialog box appears.

b) Click to select any check box that is not selected in the Show Severity section of the **General** tab.

Step 4 Make sure that all cards that are part of a 1+1 or Y-cable protection group must be active on the working card of the protection group and no protection switches are occurring. Also, ensure that traffic carrying protect cards are in a standby state. To do so, complete the following:

a) In the node view, click **Maintenance** > **Protection** tabs.
b) Select each protection group listed and view the active or standby status of each card in the Selected Group area.

Step 5 In shelf view, click the **Maintenance** > **Software** tabs.

Step 6 Verify that the version in the Protect Version column is .

Step 7 Click the **Activate** button. The Activate dialog box displays a warning message.

Step 8 Click **Yes** to proceed with the activation.

During node activation, all the common control cards in the node reboot beginning with the standby card. As soon as the standby card recovers from the reboot, it signals the active card to reset as a standby card and the standby card transitions to active. An Activation Successful message indicates that the software is successfully activated.

Step 9 Click **OK**.

The connection between CTC and the node is lost and CTC displays the Network view. The INCOMPATIBLE-SW alarm is raised in CTC for the first node that is activated because CTC is unable to connect to the NE due to differing, incompatible versions of the software between CTC and the NE. A CTC alert is displayed to update the CTC software. To clear the INCOMPATIBLE-SW alarm, perform steps 10 through 12 only for the first node that is activated on the network.

During the activation process:

- The SYSBOOT alarms are raised when the common control cards and cross-connect card reset. These alarms clears when all the cards reset.

  The activation process can take up to 30 minutes, depending on the number of cards installed in the node.

- The GCC-EOC, EOC, and EOC-E alarms are transient. These alarms are raised and cleared during the upgrade process when the control cards and line cards reset.
- Protect cards in the Y-cable protection group boot next, in the order that the protection group was created.
- Other line cards reset one after the other in the order of slot number.

If you are upgrading remotely and cannot see the nodes, wait for 5 minutes for the process to complete, then check to ensure that related alarms have cleared before proceeding.

Step 10 In CTC, choose **File > Update CTC**. The CTC software is updated. A CTC alert is displayed to restart CTC.

Step 11 In CTC, choose **File > Exit.**

Step 12 Start CTC again.

Step 13 Click the **Launch CTC** button in the CTC launcher window.

The new CTC applet loads. The login window is displayed.

Step 14 Type the user name and password and click **Login**.

Step 15 Return to your originating procedure (NTP).

DLP-U549 Delete Cached JAR Files

Purpose	This task deletes cached JAR files.
Tools/Equipment	PC or UNIX workstation

Prerequisite Procedures	None
Required/As Needed	You need to complete this task after you activate the first network node.
Onsite/Remote	Onsite or remote
Security Level	Maintenance user or higher

Note Whenever the CTC software is upgraded or reverted, make sure that the browser and hard drive cache files are cleared.

Procedure

Step 1 Delete cached files from your browser directory.

In Netscape:

a) Select **Edit** > **Preferences**. Click the **Advanced** tab and click the **Cache** button.
b) Click the **Clear Memory Cache** button, and click **OK**.
c) Click the **Clear Disk Cache** button, and click **OK** twice.

In Microsoft Internet Explorer:

a) Select **Tools** > **Internet Options**. The Internet Options dialog box appears.
b) Click the **General** tab, and then click the **Delete Files** button.
c) Select the **Delete all offline content** check box.
d) Click **OK** twice.

Step 2 Close the browser.

Note Cached JAR files cannot be deleted from the hard drive until the browser is closed. Other applications that use JAR files must also be closed.

Step 3 On Windows systems, delete cached files from your workstation in this location:

`C:\Documents and Settings\`*`username`*`\Application Data\Cisco\CTC`

Step 4 Reopen the browser. You should now be able to connect to CTC.

Step 5 Return to your originating procedure (NTP).

DLP-U551 Set the Date and Time

Purpose	This task sets the date and time. If you are not using SNTP, the upgrade procedure can cause the Date/Time setting to change. Perform this task to reset the date and time at each node.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	None

Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note If you are using SNTP, this task is not applicable.

Procedure

Step 1 In CTC node view, click the **Provisioning** > **General** tabs.

Step 2 Set the correct date and time. Click **Apply** .

Step 3 Repeat Steps 1 and 2 on all the remaining nodes.

Step 4 Return to your originating procedure (NTP).

NTP-U490 Install Public-Key Security Certificate

Purpose	This procedure installs the ITU Recommendation X.509 public-key security certificate. The public-key certificate is required to run software R4.1 or later.
Tools/Equipment	None
Prerequisite Procedures	This procedure is performed when logging into CTC. You cannot perform it at any other time.
Required/As Needed	This procedure is required to run software R4.1 or later.
Onsite/Remote	Onsite or remote
Security Level	Provisioning or higher

Procedure

Step 1 Log into CTC.

Step 2 If the Java Plug-in Security Warning dialog box appears, choose one of the following options:

- Grant This Session—Installs the public-key certificate on the PC only for the current session. After the session ends, the certificate is deleted. This dialog box appears at the next login into the node.
- Deny—Denies permission to install the certificate. If this option is chosen, login into the node is denied.

- Grant always—Installs the public-key certificate and does not delete it after the session is over. It is recommended to use this option.
- View Certificate—The public-key security certificate is displayed.

After the completion of the security certificate dialog boxes, the web browser displays information about the Java and system environments. If this is the first login, a CTC downloading message appears while CTC files are downloaded to the computer. The process can take several minutes, if it is the first time. After the download, the CTC Login dialog box appears.

Step 3 Return to the software and database you had before activating the software, proceed with the NTP-U491 Restore the Previous Software Load and Database, on page 11 procedure.

Stop. You have completed this procedure.

NTP-U491 Restore the Previous Software Load and Database

Purpose	This procedure returns to the software and database provisioning that was present before was activated. The software load and database cannot be restored to the previous version if the software on both the working and protect cards were upgraded to .
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	"DLP-G46 Log into CTC" in the "Connect the PC and Log into the GUI" document. NTP-U487 Preparing to Upgrade to a New Release, on page 2 NTP-U488 Back Up the Cisco Software Database, on page 3 NTP-U489 Upgrade the Cisco Software , on page 4
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note Tasks to revert to a previous load are not part of the upgrade, and are provided here as a convenience to those wishing to perform a revert after an upgrade. If you have successfully performed all necessary procedures up to this point, you have finished the software upgrade.

Caution If a node is set to secure, dual-IP mode, the database information is overwritten with this configuration and cannot be reverted to single-IP repeater mode.

Note All line cards of the subtended shelf controller may undergo a reboot during a software revert from Release 11.0 or earlier to a previous software release and is traffic impacting.

Procedure

Step 1 Complete the DLP-U552 Revert to Protect Load, on page 12 task.

Step 2 If the software revert to your previous release failed to restore the database, complete the DLP-U553 Manually Restore the Database, on page 13 task.

Stop. You have completed this procedure.

DLP-U552 Revert to Protect Load

Purpose	This task reverts to the software you were running prior to the last activation.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	NTP-U487 Preparing to Upgrade to a New Release, on page 2 NTP-U488 Back Up the Cisco Software Database, on page 3 NTP-U489 Upgrade the Cisco Software , on page 4
Required/As Needed	Required for revert
Onsite/Remote	Onsite or remote
Security Level	Superuser

Note To perform a supported (non-service-affecting) revert from , the release you want to revert to must have been working at the time you activated to the current software version on that node. Also, a supported revert automatically restores the node configuration at the time of the previous activation. The exception to this is when you have downloaded a second time, ensuring that no revert to a previous load can take place. In this case, the revert occurs, but is not traffic-affecting and does not change the database.

Note Ensure that all cards that are part of a protection group (1+1 or Y-cable) are active on the working card of that protection group and that no protection switches are occurring. To ensure that traffic carrying protect cards are in a standby state, in the node view click the **Maintenance** tab, and view the Protect column for each of the listed protection groups. View the active/standby status of each card in the Maintenance tab.

Procedure

Step 1 From the node view, click the **Maintenance** tab, then click the **Software** button.

Step 2 Verify that the protect software displays the release you upgraded from.

Step 3 Click the **Revert** button. Revert activates the protect software and restores the database from the previous load. A confirmation dialog box appears.

Note Any FPGA downgrades during the revert process may affect traffic. Configuration changes made after activation are lost when you revert.

Step 4 Click **OK**. This begins the revert process and drops the connection to the node.

Step 5 Wait until the software revert completes before continuing.

Note The system reboot may take up to 30 minutes to complete.

Step 6 Wait one minute before reverting another node.

Step 7 After reverting all the nodes in the network, restart the browser and log back into the last node that was reverted. This uploads the appropriate CTC applet to your workstation.

Step 8 Perform the DLP-U549 Delete Cached JAR Files, on page 8 task.

Step 9 Return to your originating procedure (NTP).

DLP-U553 Manually Restore the Database

Purpose	This task manually restores the database. Use this task if you were unable to perform a revert successfully and need to restore the database.
Tools/Equipment	PC or UNIX workstation
Prerequisite Procedures	DLP-U552 Revert to Protect Load, on page 12
Required/As Needed	As needed
Onsite/Remote	Onsite or remote
Security Level	Superuser



Caution Do not perform these steps unless the software revert failed.



Caution This process is service affecting and should be performed during a maintenance window.

Procedure

Step 1 In CTC node view, click the **Maintenance** tab, then click the **Database** button.

Step 2 Click the **Restore** button. The DB Restore dialog box appears.

Step 3 Click **Browse** to locate the database file stored on the workstation hard drive or on network storage.

Step 4 Click the database file to highlight it and click **Open**. The DB Restore dialog box appears.

Step 5 If you need a complete database restore, check the **Complete database (System and Provisioning)** checkbox.

Note The following parameters are restored only when the **Complete Database (System and Provisioning)** checkbox is checked: node name, IP address, subnet mask and gateway, and IIOP port. If you change the node name and then restore a backed up database on this node, the circuits automatically map to the newly renamed node. It is recommended to keep a record of the old and new node names.

Step 6 Click **Ok**.

The database is restored and the control cards reboot.

Step 7 When the control cards have finished rebooting, log into CTC and verify that the database is restored.

Wait one minute before restoring the next node.

Step 8 Repeat Steps 1 to 7 for each node in the network.

You have now completed the manual database restore.

Step 9 Return to your originating procedure (NTP).

Related Documentation

Use this document in conjunction with the following publications:

- Release notes:
- TL1 command guides:
- Troubleshooting guides:

Obtaining Documentation and Submitting a Service Request

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)