



# Release Notes for StarOS™ Software Version 21.20.4

**First Published:** August 31, 2020

**Last Updated:** August 31, 2020

## Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.20.3. These release notes are applicable to the ASR5500, VPC-SI and VPC-DI platforms.

## Release Package Version Information

**Table 1 - Release Package Version Information**

| Software Packages | Version              |
|-------------------|----------------------|
| StarOS packages   | 21.20.4, build 77215 |

Descriptions for the various packages provided with this release are located in [Release Package Descriptions](#).

## Feature and Behavior Changes

The following features and/or behavior changes have been introduced in this emergency release.

Refer to the [Release Change Reference](#) for a complete list of feature and behavior changes associated with this software release.

## Related Documentation

For a complete list of documentation available for this release, go to <http://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html>.

## Installation and Upgrade Notes

This Release Note does not contain installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

## Firmware Updates

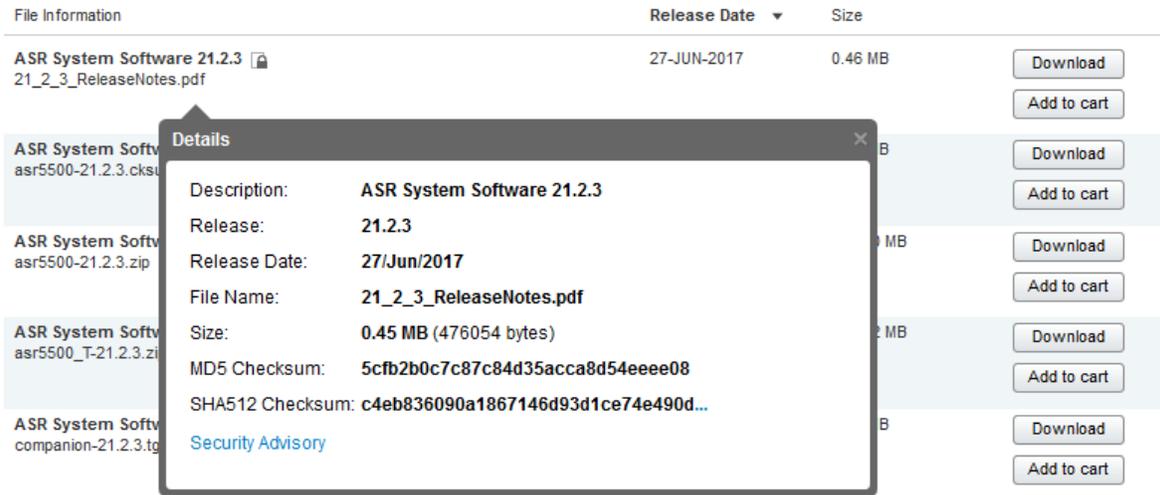
There are no firmware upgrades required for this release.

## Software Integrity Verification

To verify the integrity of the software image you have from Cisco, you can validate the SHA512 checksum information against the checksum identified by Cisco for the software.

Image checksum information is available through the following mechanisms:

- **Cisco.com Software Download Details:** To find the checksum, hover the mouse pointer over the software image you have downloaded.



At the bottom you find the SHA512 checksum, if you do not see the whole checksum you can expand it by pressing the "..." at the end.

- **.cksums file:** A file containing software image checksum information is distributed with the image files. The naming convention for this file is:

`<product>-<version>.cksums`

Example: `asr5500-21.4.0.cksums`

To validate the information, calculate a SHA512 checksum using the information in [Table 2](#) and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop please see the table below.

**Table 2 - Checksum Calculations per Operating System**

| Operating System  | SHA512 checksum calculation command examples  |
|-------------------|---|
| Microsoft Windows | Open a command line window and type the following command<br><br>> certutil.exe -hashfile <filename>.<extension> SHA512 |
| Apple MAC         | Open a terminal window and type the following command<br><br>\$ shasum -a 512 <filename>.<extension>                    |

## Open Bugs in this Release

| Operating System   | SHA512 checksum calculation command examples   |
|--|--|
| Linux  | Open a terminal window and type the following command<br><br><pre>\$ sha512sum &lt;filename&gt;.&lt;extension&gt;</pre> Or<br><br><pre>\$ shasum -a 512 &lt;filename&gt;.&lt;extension&gt;</pre> |
| <b>NOTES:</b><br><br><filename> is the name of the file.<br><br><extension> is the file extension (e.g. .zip or .tgz). |  |

If the SHA512 checksum matches, you can be sure that no one has tampered with the software image or the image has not been corrupted during download.

If the SHA512 checksum does not match, we advise you to not attempt upgrading any systems with the corrupted software image. Download the software again and verify the SHA512 checksum again. If there is a constant mismatch, please open a case with the Cisco Technical Assistance Center.

## Certificate Validation

In 21.12.0 and later releases, software images for StarOS, VPC-DI, and VPC-SI, and the companion software packages for StarOS and VPC are signed via x509 certificates. In pre-21.12.0 releases, image signing is not supported for VPC-DI and VPC-SI images, and for StarOS and VPC companion software packages.

USP ISO images are signed with a GPG key.

For more information and instructions on how to validate the certificates, refer to the README file available with the respective software packages.

## Open Bugs in this Release

The following table lists the known bugs that were found in, and/or that remain open in this software release.

**NOTE:** This software release may contain open bugs first identified in other releases. Additional information for all open bugs for this release are available in the [Cisco Bug Search Tool](#).

**Table 3 - Open Bugs in this Release**

| Bug ID     | Headline  | Product Found* |
|------------|---|----------------|
| CSCvu96189 | [BP-CUPS] Session is not coming out of SU state after CP switchover                                 | cups-cp        |
| CSCvu86949 | [BP-CUPS]: sessmgr restart at acsmgr_allocate_far_id()  | cups-cp        |
| CSCvu81900 | [PLT-CUPS]: huge CRR recovery failures on back-to-back SRP-Switchover leading to call-drop          | cups-cp        |
| CSCvu45618 | [BP-CUPS] huge number of session disconnects with reason sxfail-opr-get-usagereport                 | cups-cp        |
| CSCvu14068 | [BP_CUPS] : Incorrect i/p o/p data in "sh sub user-plan full all" after SR under specific condition | cups-up        |
| CSCvu80679 | MME doesn't handle the Exp Result Code 5511 when received from IWK-SCEF in CIA message              | mme            |

## Resolved Bugs in this Release

| Bug ID  | Headline   | Product Found* |
|---|--|----------------|
| CSCvu82139  | [CP-MME]- Post unplanned card failure diamproxy/diactrl instances went to over state                 | mme            |
| CSCvu65266  | Assertion failure while configuring "Diameter destination realm under mme-service" with context MME  | mme            |
| CSCvu81466  | [MONTE Roaming] On VPC-DI while doing mmemgr restart seen 18K subs drop from total 1.4M              | mme            |
| CSCvv18943  | MME not sending ERABModifyRequest for dedicated bearer when UBR is triggered for default & dedicated | mme            |
| CSCvu37233  | On VPC-DI Multiple Sessmgr restarts seen while doing SF card migration from active to standby        | mme            |
| CSCvu94647  | [N26] - MME not responding for Fwd-Reloc-Req and Reloc-Cancel-Req from LPS AMF                       | mme            |
| CSCvv55758  | [CP-MME]- Multiple Sessmgr task went in to warn state on Longevity more than 72hr                    | mme            |
| CSCvv36310  | IP Bad checksum with "Rewrite TTL on Downlink Packets" feature                                       | pdn-gw         |
| CSCvu36991  | BP-ICUPS : Existing flows/throughput impacted when new flows/calls are made                          | pdn-gw         |
| * Information in the "Product Found" column identifies the product in which the bug was initially identified. |  |                |

## Resolved Bugs in this Release

The following table lists the known bugs that are resolved in this specific software release.

**NOTE:** This software release may contain bug fixes first introduced in other releases. Additional information for all resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

**Table 4 - Resolved Bugs in this Release**

| Bug ID     | Headline  | Product Found* |
|------------|---|----------------|
| CSCvq81083 | [PLT-CUPS-VPN] same USED address are displayed multiple time in show ip pool command. | cups-cp        |
| CSCvu20051 | Fatal Signal 11: 11 PC: [0ce596da/X] sn_memblock_cache_block_flush()                  | cups-cp        |
| CSCvu64755 | Session manager restart at sn_memblock_cache_block_flush()                            | cups-cp        |
| CSCvu98232 | [BP-CUPS-GGSN]:Sessmgr restart at sessmgr_ggsn_sx_deallocate_trans_info_node()        | cups-cp        |
| CSCvu98532 | Assertion failure at sess/smgr/sessmgr_ggsn.c   | cups-cp        |
| CSCvv13404 | [BP-CUPS]: Fatal Signal 11 at sessmgr_is_clp_disconnecting                            | cups-cp        |
| CSCvv24973 | v4_sx_message_limit_reached()   | cups-cp        |
| CSCvv12548 | [TS-CUPS] : Traffic not getting steered on RCM testbed with OWM UDP call              | cups-up        |
| CSCvv13894 | Cleanup the NSH OAM NPU flow on removal of global config                              | cups-up        |
| CSCvv15774 | npumgr memory leak on UP  | cups-up        |
| CSCvv29752 | memory leak in vpp stats client library   | cups-up        |

## Operator Notes

| Bug ID  | Headline   | Product Found* |
|---|--|----------------|
| CSCvu70861  | [MONTE] RIR is not sent in case if eDRX activated not during Attach but in TAU                     | mme            |
| CSCvu70881  | [MONTE] Missing AVP 3142 Monitoring-Event-Config-Status in IDA from MME                            | mme            |
| CSCvu91668  | Assertion Failure for aaamgr_sred occurring frequently   | mme            |
| CSCvu96133  | [CP-MME]- InterMME S1HO failing when src-to-trgt container received in FRR with size 6k+           | mme            |
| CSCv13748   | [MONTE] RIR - Maximum-UE-Availability-Time - wrong encoding and wrong value                        | mme            |
| CSCv28114   | [MME] S1AP encoding of InitialContextSetup Request fails with MDT configuration                    | mme            |
| CSCvu94529  | msisdn-no-cc-length 10 got added under xheader-format on vPC-DI PGW after upgrade to 21.18.4.76010 | pdn-gw         |
| CSCv01123   | [BP-ICUPS] : Traffic issue for Override Rule with Wildcard Charging action name & AVP DONT_WAIT    | pdn-gw         |
| CSCv11380   | PLT-ICUPS : CUTO policy parameters' ranges and documentation changes                               | pdn-gw         |
| CSCv18085   | sessmgr reload in 21.15.45 Build No: 76717   | pdn-gw         |
| CSCvt74168  | UltraM / StarOs configuration was not fully loaded after chassis reloaded                          | staros         |
| CSCvu93040  | "npumgr, hatsystem restart and UP reload with 'show sx peers' cli"                                 | staros         |
| CSCv21979   | [VPC] sw-rss does not handle ipv4 packets correctly that introduces out of order packets           | staros         |
| CSCv24217   | ESC recovery action results in a card migration failure  | staros         |
| * Information in the "Product Found" column identifies the product in which the bug was initially identified. |  |                |

## Operator Notes

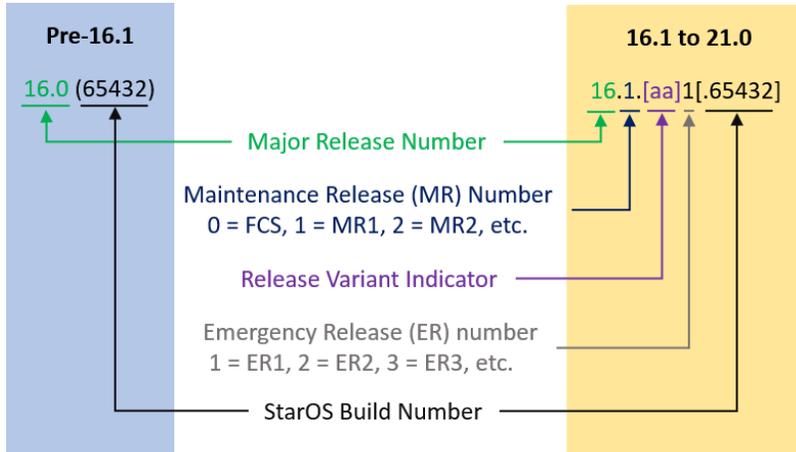
### StarOS Version Numbering System

The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5x00 or Cisco Virtualized Packet Core platform.

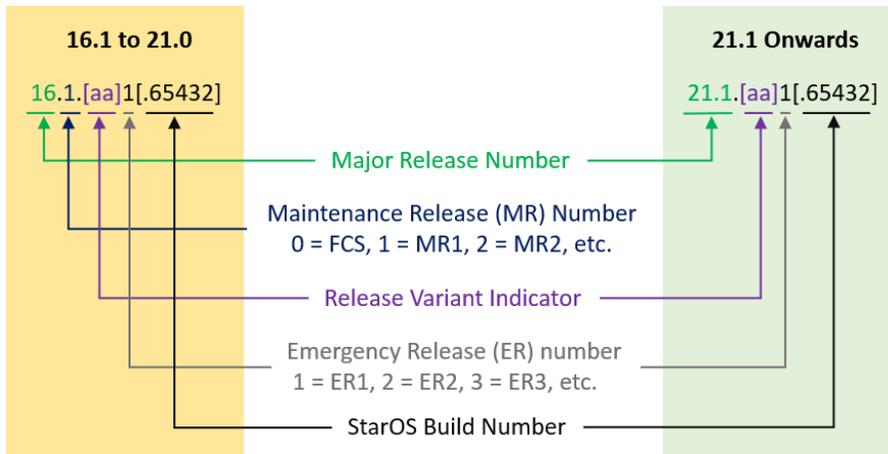
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build number.

From release 16.1 onwards, the output of the **show version** command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, **show version** will display slightly different information depending on whether or not a build is suitable for deployment.

The Version Build Number for releases between 16.1 and 21.0 include a major, maintenance, and emergency release number, for example "16.1.2".



The Version Build Number for releases 21.1 and later include a major and emergency release number, for example, “21.1.1”.



In either scenario, the appropriate version number field increments after a version has been released. The new version numbering format is a contiguous sequential number that represents incremental changes between releases. This format will facilitate identifying the changes between releases when using Bug Search Tool to research software releases.

## Release Package Descriptions

[Table 5](#) provides descriptions for the packages that are available with this release.

**Table 5 - Release Package Information**

| In 21.12.0 and later Releases | In pre-21.12.0 Releases | Description   |
|-------------------------------|-------------------------|---|
| <b>ASR 5500</b>               |                         |   |
| asr5500-<release>.zip         | asr5500-<release>.bin   | Contains the signed ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.          |
| asr5500_T-<release>.zip       | asr5500_T-<release>.bin | Contains the signed, trusted ASR 5500 software image, the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate. |

| In 21.12.0 and later Releases               | In pre-21.12.0 Releases                     | Description   |
|---|---|---|
| <b>StarOS Companion Package</b>             |   |   |
| companion-<br><release>.zip                 | companion-<br><release>.tgz                 | <p>Contains numerous files pertaining to this version of the StarOS including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both trusted and non-trusted build variants.</p> <p>In 21.12.0 and later releases, the StarOS companion package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p> |
| <b>VPC-DI</b>                               |   |   |
| qvpc-di-<br><release>.bin.zip               | qvpc-di-<release>.bin                       | <p>Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>  |
| qvpc-di_T-<br><release>.bin.zip             | qvpc-di_T-<release>.bin                     | <p>Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>  |
| qvpc-di-<release>.iso.zip                   | qvpc-di-<release>.iso                       | <p>Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>   |
| qvpc-di_T-<br><release>.iso.zip             | qvpc-di_T-<release>.iso                     | <p>Contains the trusted VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>   |
| qvpc-di-template-<br>vmware-<release>.zip   | qvpc-di-template-<br>vmware-<release>.tgz   | <p>Contains the VPC-DI binary software image that is used to on-board the software directly into VMware.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>   |
| qvpc-di-template-<br>vmware_T-<release>.zip | qvpc-di-template-<br>vmware_T-<release>.tgz | <p>Contains the trusted VPC-DI binary software image that is used to on-board the software directly into VMware.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>   |

| In 21.12.0 and later Releases                | In pre-21.12.0 Releases                      | Description   |
|--|--|---|
| qvmc-di-template-libvirt-kvm-<release>.zip   | qvmc-di-template-libvirt-kvm-<release>.tgz   | <p>Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>  |
| qvmc-di-template-libvirt-kvm_T-<release>.zip | qvmc-di-template-libvirt-kvm_T-<release>.tgz | <p>Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>  |
| qvmc-di-<release>.qcow2.zip                  | qvmc-di-<release>.qcow2.tgz                  | <p>Contains the VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>         |
| qvmc-di_T-<release>.qcow2.zip                | qvmc-di_T-<release>.qcow2.tgz                | <p>Contains the trusted VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p> |
| <b>VPC-SI</b>                                |  |   |
| qvmc-si-<release>.bin.zip                    | qvmc-si-<release>.bin                        | <p>Contains the VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>          |
| qvmc-si_T-<release>.bin.zip                  | qvmc-si_T-<release>.bin                      | <p>Contains the trusted VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>  |
| qvmc-si-<release>.iso.zip                    | qvmc-si-<release>.iso                        | <p>Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>                 |

## Operator Notes

| In 21.12.0 and later Releases                | In pre-21.12.0 Releases                      | Description   |
|--|--|---|
| qvmc-si_T-<release>.iso.zip                  | qvmc-si_T-<release>.iso                      | <p>Contains the trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>          |
| qvmc-si-template-vmware-<release>.zip        | qvmc-si-template-vmware-<release>.ova        | <p>Contains the VPC-SI binary software image that is used to on-board the software directly into VMware.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>   |
| qvmc-si-template-vmware_T-<release>.zip      | qvmc-si-template-vmware_T-<release>.ova      | <p>Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>                                       |
| qvmc-si-template-libvirt-kvm-<release>.zip   | qvmc-si-template-libvirt-kvm-<release>.tgz   | <p>Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>  |
| qvmc-si-template-libvirt-kvm_T-<release>.zip | qvmc-si-template-libvirt-kvm_T-<release>.tgz | <p>Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>  |
| qvmc-si-<release>.qcow2.zip                  | qvmc-si-<release>.qcow2.gz                   | <p>Contains the VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p>         |
| qvmc-si_T-<release>.qcow2.zip                | qvmc-si_T-<release>.qcow2.gz                 | <p>Contains the trusted VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.</p> <p>In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p> |
| <b>VPC Companion Package</b>                 |  |   |

| In 21.12.0 and later Releases   | In pre-21.12.0 Releases         | Description  |
|---------------------------------|---------------------------------|--|
| companion-vpc-<br><release>.zip | companion-vpc-<br><release>.tgz | <p>Contains numerous files pertaining to this version of the VPC including SNMP MIBs, RADIUS dictionaries, ORBEM clients. These files pertain to both VPC-DI and VPC-SI, and for trusted and non-trusted build variants.</p> <p>In 21.12.0 and later releases, the VPC companion package also includes the signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate.</p> |

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at:

<http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). 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)

© 2020 Cisco Systems, Inc. All rights reserved.