



# Release Notes for StarOS™ Software Version 21.24.0

**First Published:** June 30, 2021

**Last Updated:** June 30, 2021

## Introduction

This Release Note identifies changes and issues related to this software release. This release is the next major feature release since 21.23.0. This release has been qualified for non-CUPS deployments.

## Release Package Version Information

**Table 1 - Release Package Version Information**

| Software Packages | Version              |
|-------------------|----------------------|
| StarOS packages   | 21.24.0, build 81073 |

## Feature and Behavior Changes

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 general 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 **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.

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 see [Table 2](#).

**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><pre>&gt; certutil.exe -hashfile &lt;filename&gt;.&lt;extension&gt; SHA512</pre>  |
| Apple MAC   | Open a terminal window and type the following command<br><br><pre>\$ shasum -a 512 &lt;filename&gt;.&lt;extension&gt;</pre>  |
| Linux   | Open a terminal window and type the following command<br><br><pre>\$ sha512sum &lt;filename&gt;.&lt;extension&gt;</pre> <p>Or</p> <pre>\$ shasum -a 512 &lt;filename&gt;.&lt;extension&gt;</pre> |
| <b>NOTES:</b>   |  |
| <i>&lt;filename&gt;</i> is the name of the file.                    |  |
| <i>&lt;extension&gt;</i> 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 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* |
|---|---|----------------|
| CSCVy14092  | [BP-CUPS] vpmngr crash at vpmngr_get_loc_vpn_chunk_details_by_vpnid                                 | cups-cp        |
| CSCVw58960  | Sessmgr restarts at egtpu_process_tx_setup_req_evt()  | cups-up        |
| CSCVy78471  | [BP-LEGACY]:Rf-SDC does not have CSG info when MBR to enter hyb-sub cell,CCAU send rule trigger CBR | pdn-gw         |
| CSCVy53051  | New CLI to manually set AVP cisco-mpc-protocol-interface  | samog          |
| CSCVy09744  | [CP-SGSN] sessmgr restart seen with function egtpc_handle_del_bearer_cmd_req_evt                    | sgsn           |
| CSCVx98820  | [CUPS-TACACS-IPsec] TCP connection failure with second tacacs server during failover                | staros         |
| CSCVy79548  | bfdmgr does not send keepalive - Intermittent   | staros         |
| * 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* |
|------------|--|----------------|
| CSCVv70527 | "Replay Errors" observed after perform switch over on CP   | cups-cp        |
| CSCVx32019 | "[BP-CUPS] Mid call predef rule changes from rated to free for all components, not charged correctly." | cups-up        |
| CSCVv20041 | Delete counter not incremented proeprly for Monte  | mme            |
| CSCVv20626 | [MONTE] bulkstats counter issue for num-of-ues-in-geographical-area                                    | mme            |

| Bug ID  | Headline  | Product Found* |
|---|---|----------------|
| CSCvq68326  | mmemgr restart is seen in mmemgr_aggregate_msg_to_sessmgr()                             | mme            |
| CSCvw96092  | session manager restarts at pgw_drv_clear_drv_clp_due_to_gngp_ctxt_replacement          | pdn-gw         |
| CSCvs73583  | Assertion failure at ipm_sad_ikesa_free()   | pdn-gw         |
| CSCvw49516  | Sessmgr crash with mbr which includes F-TEID of S1-U eNodeB GTP-U interface.            | pdn-gw         |
| CSCvy03998  | Extend the Peer/IMS server status check mechanism to also include peer-host check       | pdn-gw         |
| CSCvw85418  | [BP-Legacy] EDR's created for ULI CGI_RAI and SGI_RAI contains only MCC MNC info        | pdn-gw         |
| CSCvx22350  | Sessmgr restart with fatal signal tftcpIncomingPacket()                                 | pdn-gw         |
| CSCvy33408  | Reverting CSCvx50403 and CSCvy14382 from integration branch                             | pdn-gw         |
| CSCvy13808  | L2TP authentication difference between 3G and LTE call                                  | pdn-gw         |
| CSCvw59640  | sessmgr_ipv4_process_inet_pkt_part3_pgw_ggsn  | pdn-gw         |
| CSCvw76775  | Many sessmgr restarts seen on virtual PGW   | pdn-gw         |
| CSCvx15261  | Sessmgr crash at PC: [08a14140/X] egtpc_encode_imsi_ie()                                | sae-gw         |
| CSCvy33792  | [VPC-DI] SAMOG Increase cisco-mpc-protocol-interface AVP length for eogre_pmip6         | samog          |
| CSCvx78219  | remove mme peer command is not working as expected                                      | sgsn           |
| CSCvy02569  | Failure message seen on the client server console though the push ssh-key is successful | staros         |
| CSCvy13187  | Reverting the CSCvw56757 non-fraud traffic from hitting http parse-error                | staros         |
| CSCvx49475  | "Effective initial transfer limited by SendQueueBytes" Logs                             | staros         |
| CSCvv68943  | BCF[X] previous instance did not clear  | staros         |
| CSCvx49375  | Following Error after node upgrade " initial-config file has not finished loading"      | staros         |
| * Information in the "Product Found" column identifies the product in which the bug was initially identified. |   |                |

## Operator Notes

### StarOS Version Numbering System

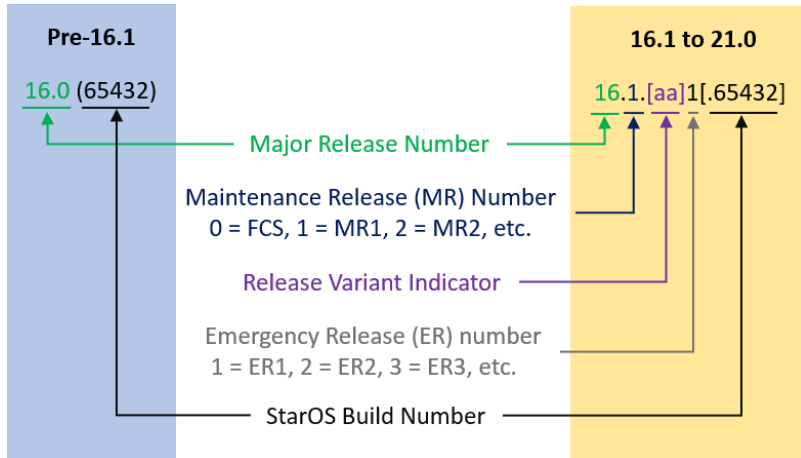
The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5x00 or Cisco Virtualized Packet Core platform.

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.

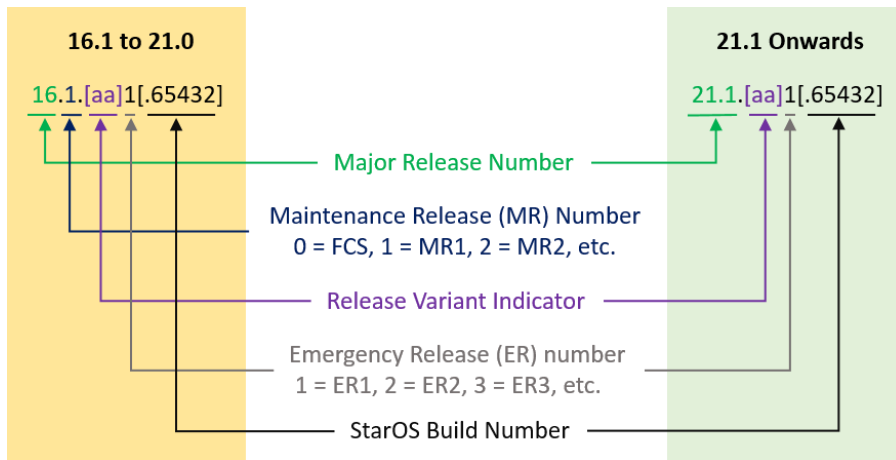
From release 16.1 onwards, the output of the **show version** command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, **show version** will display slightly different information depending on whether or not a build is suitable for deployment.

Operator Notes

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.  |
| <b>StarOS Companion Package</b> |                         |  |
| companion-<release>.zip         | companion-<release>.tgz | 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.<br><br>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. |
| <b>VPC-DI</b>                   |                         |  |
| qvpc-di-<release>.bin.zip       | qvpc-di-<release>.bin   | Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.<br><br>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.  |
| qvpc-di_T-<release>.bin.zip     | qvpc-di_T-<release>.bin | Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.<br><br>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.  |
| qvpc-di-<release>.iso.zip       | qvpc-di-<release>.iso   | Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.<br><br>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.   |
| qvpc-di_T-<release>.iso.zip     | qvpc-di_T-<release>.iso | 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.<br><br>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.   |

| In 21.12.0 and later Releases                | In pre-21.12.0 Releases                      | Description   |
|--|--|---|
| qvmc-di-template-vmware-<release>.zip        | qvmc-di-template-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>   |
| qvmc-di-template-vmware_T-<release>.zip      | qvmc-di-template-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>                                       |
| 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>  |

| In 21.12.0 and later Releases                | In pre-21.12.0 Releases                      | Description   |
|--|--|---|
| 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>                 |
| 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> |



| In 21.12.0 and later Releases      | In pre-21.12.0 Releases     | Description  |
|------------------------------------|-----------------------------|--|
| <b>VPC Companion Package</b>       |                             |  |
| companion-vpc-<release>.zip        | companion-vpc-<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> |
| <b>Ultra Service Platform</b>      |                             |  |
| usp-<version>.iso                  |                             | <p>The USP software package containing component RPMs (bundles).</p> <p>Refer to <a href="#">Table 6</a> for descriptions of the specific bundles.</p>   |
| usp_T-<version>.iso                |                             | <p>The USP software package containing component RPMs (bundles). This bundle contains trusted images.</p> <p>Refer to <a href="#">Table 6</a> for descriptions of the specific bundles.</p>  |
| usp_rpm_verify_utils-<version>.tar |                             | Contains information and utilities for verifying USP RPM integrity.  |

**Table 6 - USP ISO Bundles**

| USP Bundle Name   | Description  |
|---|--|
| usp-em-bundle-<version>-1.x86_64.rpm*                         | The Element Manager (EM) Bundle RPM containing images and metadata for the Ultra Element Manager (UEM) module.   |
| usp-ugp-bundle-<version>-1.x86_64.rpm*                        | The Ultra Gateway Platform (UGP) Bundle RPM containing images for Ultra Packet core (VPC-DI). There are trusted and non-trusted image variants of this bundle. |
| usp-yang-bundle-<version>-1.x86_64.rpm                        | The Yang Bundle RPM containing YANG data models including the VNFD and VNFR.   |
| usp-uas-bundle-<version>-1.x86_64.rpm                         | The Ultra Automation Services Bundle RPM containing AutoVNF, Ultra Web Services (UWS), and other automation packages.  |
| usp-auto-it-bundle-<version>-1.x86_64.rpm                     | The bundle containing the AutoIT packages required to deploy the UAS.  |
| usp-vnfm-bundle-<version>-1.x86_64.rpm                        | The VNFM Bundle RPM containing an image and a boot-up script for ESC (Elastic Service Controller).   |
| ultram-manager-<version>-1.x86_64.rpm*                        | This package contains the script and relevant files needed to deploy the Ultra M Manager Service.  |
| * These bundles are also distributed separately from the ISO. |  |

## 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)

© 2021 Cisco Systems, Inc. All rights reserved.