



# Release Notes for StarOS™ Software Version 21.20.1

**First Published:** July 8, 2020

**Last Updated:** July 8, 2020

## Introduction

This Release Note identifies changes and issues related to this software release. This emergency release is based on release 21.20.0. 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	21.20.1, build 76491

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

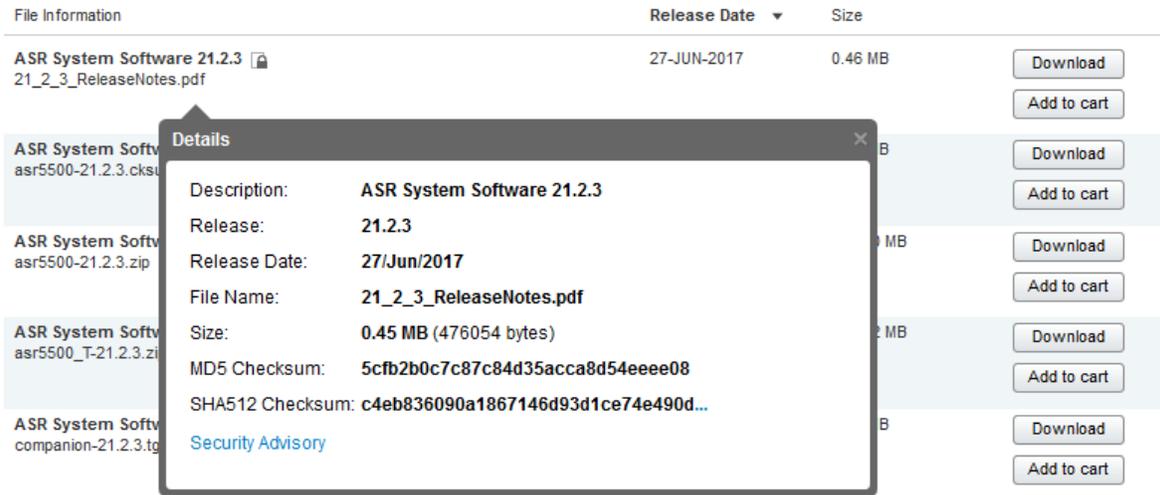
There are no firmware upgrades required for this release.

## 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  > certutil.exe -hashfile <filename>.<extension> SHA512
Apple MAC	Open a terminal window and type the following command  \$ 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  <pre>\$ sha512sum &lt;filename&gt;.&lt;extension&gt;</pre> Or  <pre>\$ shasum -a 512 &lt;filename&gt;.&lt;extension&gt;</pre>
<b>NOTES:</b>  <filename> is the name of the file.  <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*
CSCvu87236	"[BP-CUPS]AF, reload at sess/egtp/egtpc/egtpc_evt_handler_func.c:756 egtpc_handle_abort_proc_cmd_evt()"	cups-cp
CSCvu87058	Calls failing with lpool-ip-validation-failed even though free addresses available	cups-cp
CSCvu86949	[BP-CUPS]: sessmgr restart at acsmgr_allocate_far_id()	cups-cp
CSCvu45618	[BP-CUPS] huge number of session disconnects with reason sxfail-opr-get-usagereport	cups-cp
CSCvt37365	Fatal Signal 6: Aborted pgw_drv_handle_events_from_smgr() snx_pgw_driver_request_control_dispatch()	cups-cp
CSCvu15322	[BP-CUPS]: Huge session disconnect due to &quot;sx-no-response&quot;;	cups-cp

## Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCvu89270	[BP-CUPS]: sessmgr restart at sessmgr_med_data_process_memif_pri()	cups-up
CSCvu14068	[BP_CUPS] : Incorrect i/p o/p data in "sh sub user-plan full all" after SR under specific condition	cups-up
CSCvu37233	On VPC-DI Multiple Sessmgr restarts seen while doing SF card migration from active to standby	mme
CSCvr34106	Assertion Failure for aaamgr_sred occurring frequently	mme
CSCvu80679	MME doesn't handle the Exp Result Code 5511 when received from IWK-SCEF in CIA message	mme
CSCvu82139	[CP-MME]- Post unplanned card failure diamprox/diactrl instances went to over state	mme
CSCvu81466	[MONTE Roaming] On VPC-DI while doing mmemgr restart seen 18K subs drop from total 1.4M	mme
CSCvu36991	BP-ICUPS : Existing flows/throughput impacted when new flows/calls are made	pdn-gw
CSCvu93041	[BP-ICUPS] sessmgr restart at acs_trm_clear_dyn_list	pdn-gw
CSCvu89771	[PLT-ICUPS]: dcardmgr restart followed by sessmgr restarts seen on PXGW stbby on reload	pdn-gw
CSCvu89467	"[PLT-ICUPS]: vpnmgr restart on ASR5500 during reload, with golden PXGW config"	pdn-gw
CSCvu93160	[Smoke2-ICUPS] UBReq sends incorrect AMBR values during QoS merging	pdn-gw
CSCvu93320	BP-ICUPS CRR recovery failures recovery-css-failure sessmgr_gr_ipv4addr_pre_alloc_complete failed	pdn-gw
CSCvu80016	SessMgr crash is observed in S4-SGSN to Gn/GP-SGSN Hard Handover	sgsn
CSCvp05787	sessmgr restart seen with function egtpc_handle_del_bearer_cmd_req_evt()	sgsn
CSCvu68945	Evaluation of staros for Treck ip stack vulnerabilities	staros
CSCvu92937	PLT-ICUPS : npumgr crashes at sn_msg_handle_allocator_alloc_block	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*
CSCvu76479	[BP-CUPS] smp_fp_add_stream_request()	cups-up
CSCvu83433	[N26] NAS Count in 5G to 4G HO scenario is not considered for MME DL NAS Message	mme
CSCvu55766	[BP-ICUPS]: sessmgr restart at acsmgr_sess_gr_uchkpt_accnt_gy_buckets	pdn-gw

Operator Notes

Bug ID	Headline	Product Found*
CSCvu07728	[BP-ICUPS]: sessmgr restart noted during 2XM planned migration	pdn-gw
CSCvu72004	[BP-ICUPS]: sessmgr crashes noted on standby when reloading new PXGW config	pdn-gw
CSCvu45263	[PLT-ICUPS:VzW MPN]: VPP process restart after enabled VPP in golden config	pdn-gw
CSCvu84218	BP-ICUPS : sm deinit causing tcp-stack-disabled failures in CUSP accel of flows	pdn-gw
CSCvu82486	[BP-ICUPS]: IP ToS marking is not getting applied when configured in charging-action.	pdn-gw
CSCvu61381	[BP-ICUPS]: Unable to pass along nat traffiic for MPLS+INET context in MPN set up	pdn-gw
CSCvu54438	[BP-ICUPS]: taking more than 30 minutes to collect SSD on PXGW config system	pdn-gw
CSCvu84580	[BP-ICUPS]: HSLI sessions not coming up on reload on PXGW MPN set up	pdn-gw

\* Information in the "Product Found" column identifies the product in which the bug was initially identified.

## Operator Notes

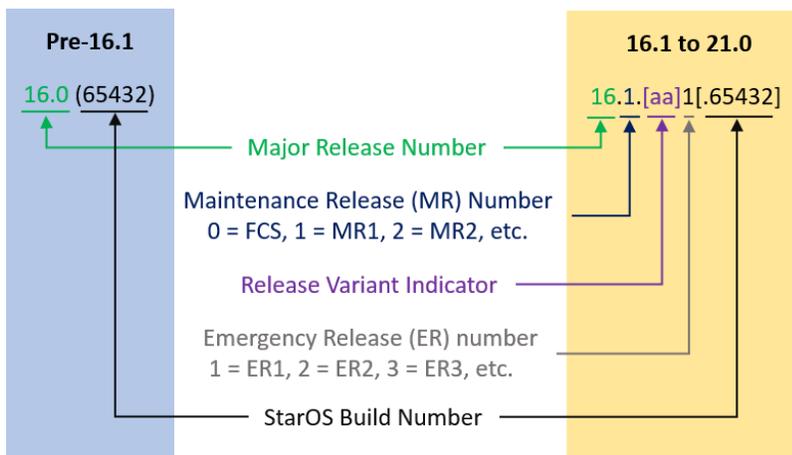
### StarOS Version Numbering System

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.

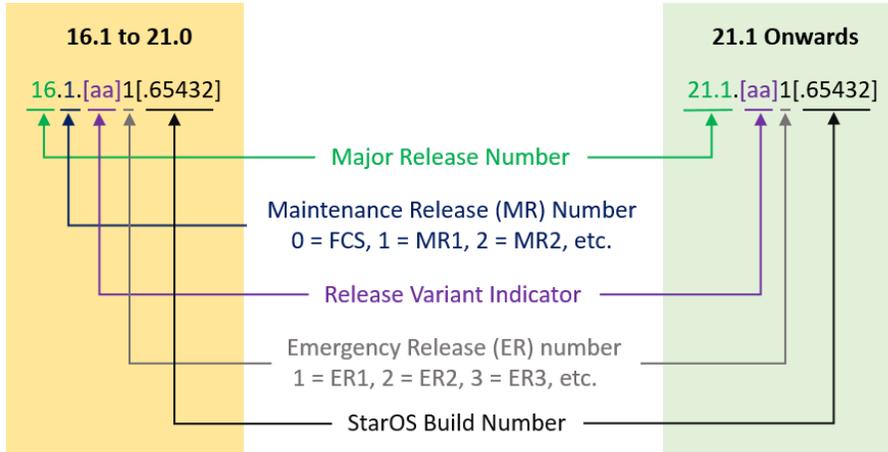
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build 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.
<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.  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.  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_T-<release>.bin.zip	qvmc-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>
qvmc-di-<release>.iso.zip	qvmc-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>
qvmc-di_T-<release>.iso.zip	qvmc-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>
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>

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

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvmc-si-template-libvirt-kvm-<release>.zip	qvmc-si-template-libvirt-kvm-<release>.tgz	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM.  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.
qvmc-si-template-libvirt-kvm_T-<release>.zip	qvmc-si-template-libvirt-kvm_T-<release>.tgz	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM.  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.
qvmc-si-<release>.qcow2.zip	qvmc-si-<release>.qcow2.gz	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.  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.
qvmc-si_T-<release>.qcow2.zip	qvmc-si_T-<release>.qcow2.gz	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.  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.
<b>VPC Companion Package</b>		
companion-vpc-<release>.zip	companion-vpc-<release>.tgz	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.  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.

## 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.