ılıılı cısco

Release Notes for StarOS™ Software Version 21.28.m18

First Published: December 20, 2023 Last Updated: December 20, 2023

Introduction

This Release Note identifies changes and issues related to this software release. These Release Notes identify changes and issues based on 21.28.m17. This release notes is applicable to StarOS and RCM products.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.28.m18, build 92457

Feature and Behavior Changes

Refer to the <u>Release Change Reference</u> 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 <u>http://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html</u>.

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.

Cisco Systems, Inc. www.cisco.com

Installation and Upgrade Notes

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.

File Information			Release Date 💌	Size	
ASR System Softwa 21_2_3_ReleaseNote:	s.pdf		27-JUN-2017	0.46 MB	Download Add to cart
ASR System Softv asr5500-21.2.3.cksi	Details Description: Release:	ASR System Software 21.2.3	_	В	Download Add to cart
ASR System Softv asr5500-21.2.3.zip	Release Date: File Name:	21,2,3 27/Jun/2017 21_2_3_ReleaseNotes.pdf) MB	Download Add to cart
ASR System Softv asr5500_T-21.2.3.zi	Size: MD5 Checksum: SHA512 Checksun	0.45 MB (476054 bytes) 5cfb2b0c7c87c84d35acca8d54 n: c4eb836090a1867146d93d1ce		2 MB	Download Add to cart
ASR System Softv companion-21.2.3.tg	Security Advisory			В	Download Add to cart

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 Ca	Iculations per Operating System	
Operating System	SHA512 checksum calculation command examples	
Microsoft Windows	Open a command line window and type the following command	
	<pre>> certutil.exe -hashfile <filename>.<extension> SHA512</extension></filename></pre>	
Apple MAC	Open a terminal window and type the following command	
	<pre>\$ shasum -a 512 <filename>.<extension></extension></filename></pre>	
Linux	Open a terminal window and type the following command	
	<pre>\$ sha512sum <filename>.<extension></extension></filename></pre>	
	Or	
	<pre>\$ shasum -a 512 <filename>.<extension></extension></filename></pre>	
NOTES:		
<filename> is the nan</filename>	ne of the file.	
<extension> is the file</extension>	e extension (e.gzip or .tgz).	

Table 0. Observes	0-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	
Table 2 - Checksum	Calculations p	er Operating System

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.

Open Bugs in this Release

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 <u>Cisco Bug Search Tool</u>.

Table 3 Open Bugs in this Release

Bug ID	Headline	Product Found*
<u>CSCwi27873</u>	UPF P2P Bulkstats Schema counter value dropped to Zero after all SF card reboot	
CSCwh58126	[cups-up][21.28.Fm12.91299] Fatal Signal 11: 11 PC: [0495e396/X] up- lane_find_app_data_flow()	
CSCwh03670	[CUPS-UP] Downlink total fp packets not shown correctly in case of http out of or- der packet	cups-up
<u>CSCwi26307</u>	[BP_CUPS] Downlink packet is not observed on chassis after removing and adding VLANs related to TS	cups-up
CSCwi32188	[BP-CUPS]: Fatal Signal 11: smp_fp_fill_strm_sfp_mtd() during ICSR switchover with BFD Down	cups-up
CSCwi35960	[CUPS] huge amount of "ICMP packet parse failure" logs in 21.28.m15 with NAT	cups-up
CSCwi52632	[BP-CUPS]egtpu_process_update_req_evt()egtpu_han- dle_user_sap_event()sessmgr_uplane_gtpu_tx_update()	
CSCwi55049	[BP-CUPS]: vppctl errors "Stream operation mis" after SecureNet is enabled	cups-up
CSCwi37280	DNS - MME is not handling dns response in CNAME format properly as expected by customer	mme
<u>CSCwi48857</u>	Sessmgr Assertion failure at egtpc_send_req_msg()	mme
CSCwi51909	mmemgr crash in vMME 01	mme
<u>CSCwi55030</u>	[CP-MME] Observed multiple sessmgr went to warn/over state in 21.28.m18.92419 during regression	mme
CSCwd99519	[UPF-ST] Error logs seen on UPF PDR not found with PDR ID 0x149 and Remove PDR PDR with ID 0x2ce	upf

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 <u>Cisco Bug Search Tool</u>.

Table 4 - Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCwf58498	[CUPS-UP]UL Data packet getting drop while CBresponse is pending and UL data came	cups-cp
CSCwh33064	[CUPS-CP]CP is not sending Outer Header Removal IE for SxA uplink PDR for de- fault bearer	cups-cp
CSCwi37202	[CUPS CP] Memory leak in function sessmgr_ggsn_sx_allocate_trans_info_node()	cups-cp
<u>CSCwi50450</u>	HO failures due to invalid ARP value from PGW	cups-cp
CSCwh71166	Cups CP - Server-Unreachable URR stays active on UP after OCS server recovery	cups-cp
CSCwd66214	[BP-CUPS]: Assertion failure at sess/snx/drivers/sgw/sgw_recovery.c:1277 on ICSR StandBY CP	cups-cp
CSCwh78561	GWC rejects directly CSR for some IMSIs with "no resources available"	cups-cp
CSCwh43745	Assertion failure at sess/egtp/egtpc/egtpc_interface.c:280	cups-cp
CSCwh84055	CDRs are not sent after unplanned SF card migration after fix of CSCwe81062	cups-cp
CSCwe81062	CDRs are not sent after unplanned SF card migration	cups-cp
CSCwh12011	[BP-CUPS]: Multiple sessmgr restarts sgwdrv_epsb_fsm_st_con- nected_evt_s5_disconnected()	cups-cp
CSCwi25128	[BP-CUPS]: Sessmgr restart while clearing the call	cups-cp
CSCwh91993	CP does not pass Subscriber-Params to UP for Pure-S SGW Call	cups-cp
CSCwi24925	[BP-CUPS]: vppctl errors seen on UP after Traffic Steering is enabled	cups-cp
CSCwi21602	[BP-CUPS]: Error log for SGW CDR Duration in future	cups-cp
CSCwi30165	[BP-CUPS] AF at sess/smgr/sessmgr_snx.c:9603 Function: sess- mgr_snx_send_drop_call()	cups-cp
CSCwi11750	Trigger log event and core when bulkstat counter %cc-msg-ccainitaccept% does not increment	cups-cp
CSCwi16517	VPP issues with 21.28.m14	cups-up
CSCwf13605	ipsecdemux crash on asr5500 during crypto call model longevity	epdg
CSCwh63240	sessmgr restart as a resuld of TEID leak when NAS redirection happens	mme
CSCwh87508	ERMI rejected by MME after 5G provisioning done until UE reattach	mme
CSCwi16827	Sess mgr crash during Delete bearer sess procedure	pdn-gw
CSCwi26694	RTP stream is wrongly linked to Default bearer in LI reporting	pdn-gw

CSCwi13992	monpro for gtpp is displaying the response twice	pdn-gw
CSCwh82844	Observing "SESSMGR" asserts with code 21.26.21-89643	pdn-gw
CSCwh84412	[Smoke2_Legacy] User-Location-Information Avp is not changed for GGSN after Handoff	pdn-gw
CSCwi47682	Gy Credit Control Request AVP for Subscription-ID (e.164) contains IMSI instead of MSISDN,	pdn-gw
CSCwi07721	Sessmgr restarted due to counter update for the LMA service processed packets when router with Nemo	pdn-gw
CSCwh93900	RCM should reload old active UP after BGP monitor failure	rcm
CSCwi17348	Call loss during UP Manual Switchover by RCM	rcm
CSCwh85921	session manager restart at function sessmgr_set_pgw_li_info	sae-gw
CSCwh70845	"show apn statistics all" - huge increase of duration of command execution	sae-gw
CSCwi04810	Sessmgr restart at acsmgr_dcca_session_init	sae-gw
CSCwh85877	SGW LMISF not sending buffered IMS signaling packets on S8HR	sgw
CSCwh95823	sessmgr restart at egtpc_adv_validate_msg	sgw
* Information in the "Product Found" column identifies the product in which the bug was initially identified.		

Operator Notes

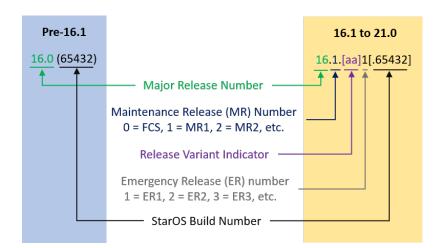
StarOS Version Numbering System

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.

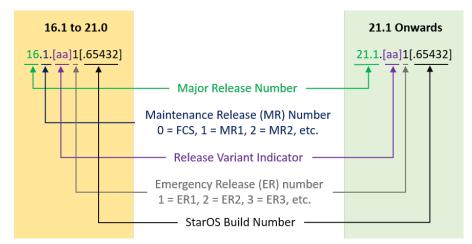
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example "16.0 (55435)". Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build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

In 21.12.0 and later	In pre-21.12.0	Description
Releases	Releases	
ASR 5500		
asr5500- <release>.zip</release>	asr5500- <release>.bin</release>	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</release>	asr5500_T- <release>.bin</release>	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.
StarOS Companion P	ackage	
companion- <release>.zip</release>	companion- <release>.tgz</release>	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.
VPC-DI		
qvpc-di- <release>.bin.zip</release>	qvpc-di- <release>.bin</release>	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.
qvpc-di_T- <release>.bin.zip</release>	qvpc-di_T- <release>.bin</release>	Contains the trusted 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.

Table 3 - Release Package Information

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvpc-di- <release>.iso.zip</release>	qvpc-di- <release>.iso</release>	Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image. In 21.12.0 and later releases, this package also includes the signature file, a verification script, the x509 certificate, and a
qvpc-di_T-	qvpc-di_T-	README file containing information on how to use the script to validate the certificate. Contains the trusted VPC-DI ISO used for new deployments, a
<release>.iso.zip</release>	<release>.iso</release>	 new virtual machine is manually created and configured to boot from a CD image. 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
qvpc-di-template- vmware-	qvpc-di-template- vmware-	validate the certificate. Contains the VPC-DI binary software image that is used to on- board the software directly into VMware.
<release>.zip</release>	<release>.tgz</release>	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-template- vmware_T- <release>.zip</release>	qvpc-di-template- vmware_T- <release>.tgz</release>	Contains the trusted VPC-DI binary software image that is used to on-board the software directly into VMware. 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-template- libvirt-kvm- <release>.zip</release>	qvpc-di-template- libvirt-kvm- <release>.tgz</release>	Contains the same VPC-DI 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.
qvpc-di-template- libvirt-kvm_T- <release>.zip</release>	qvpc-di-template- libvirt-kvm_T- <release>.tgz</release>	Contains the same trusted VPC-DI 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.

In 21.12.0 and later	In pre-21.12.0	Description
Releases qvpc-di- <release>.qcow2.zip</release>	Releases qvpc-di- <release>.qcow2.tgz</release>	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.
		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>.qcow2.zip</release>	qvpc-di_T- <release>.qcow2.tgz</release>	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.
		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.
VPC-SI	1	
qvpc-si- <release>.bin.zip</release>	qvpc-si- <release>.bin</release>	Contains the VPC-SI 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.
qvpc-si_T- <release>.bin.zip</release>	qvpc-si_T- <release>.bin</release>	Contains the trusted VPC-SI 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.
qvpc-si- <release>.iso.zip</release>	qvpc-si- <release>.iso</release>	Contains the VPC-SI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.
		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-si_T- <release>.iso.zip</release>	qvpc-si_T- <release>.iso</release>	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.
		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-si-template- vmware- <release>.ova qvpc-si-template- vmware_T- <release>.ova</release></release>	Contains the VPC-SI binary software image that is used to on- board the software directly into VMware. 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. Contains the trusted VPC-SI binary software image that is used to an based the software directly into VMware.
qvpc-si-template- vmware_T-	signature file, a verification script, the x509 certificate, and a README file containing information on how to use the script to validate the certificate. Contains the trusted VPC-SI binary software image that is used
vmware_T-	
<telease>.0va</telease>	to on-board the software directly into VMware.
	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-si-template- libvirt-kvm-	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM.
<release>.tgz</release>	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-si-template- libvirt-kvm_T-	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM.
<release>.tgz</release>	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-si- <release>.qcow2.gz</release>	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.
qvpc-si_T- <release>.qcow2.gz</release>	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.
	libvirt-kvm- <release>.tgz qvpc-si-template- libvirt-kvm_T- <release>.tgz qvpc-si- <release>.qcow2.gz</release></release></release>

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
companion-vpc- <release>.zip</release>	companion-vpc- <release>.tgz</release>	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.
Ultra Service Platform	1	
usp- <version>.iso</version>		The USP software package containing component RPMs (bundles).
		Refer to <u>Table 6</u> for descriptions of the specific bundles.
usp_T- <version>.iso</version>		The USP software package containing component RPMs (bundles). This bundle contains trusted images.
		Refer to <u>Table 6</u> for descriptions of the specific bundles.
usp_rpm_verify_utils-	<version>.tar</version>	Contains information and utilities for verifying USP RPM integrity.

Table 4 - USP ISO Bundles

USP Bundle Name	Description
usp-em-bundle- <version>-1.x86_64.rpm*</version>	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*</version>	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</version>	The Yang Bundle RPM containing YANG data models including the VNFD and VNFR.
usp-uas-bundle- <version>-1.x86_64.rpm</version>	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</version>	The bundle containing the AutoIT packages required to deploy the UAS.
usp-vnfm-bundle- <version>-1.x86_64.rpm</version>	The VNFM Bundle RPM containing an image and a boot-up script for ESC (Elastic Service Controller).
ultram-manager- <version>-1.x86_64.rpm*</version>	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

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.

Obtaining Documentation and Submitting a Service Request

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 <u>www.cisco.com/go/offices</u>.

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: <u>www.cisco.com/go/trademarks</u>. 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)

© 2023 Cisco Systems, Inc. All rights reserved.