



Release Notes for StarOS™ Software Version 21.28.h3

First Published: October 13, 2023

Last Updated: October 13, 2023

Introduction

This Release Note identifies changes and issues related to this software release. This planned maintenance release is based on release 21.28.h2. This release note is specific to CUPS User Plane only.

Release Package Version Information

Table 1 - Release Package Version Information

Software Packages	Version
StarOS packages	21.28.h3, build 91250

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 the complete list of CUPS documentation available for this release, go to <https://www.cisco.com/c/en/us/support/wireless/virtual-packet-core/products-installation-and-configuration-guides-list.html>.

For the complete list of the corresponding StarOS documentation, go to <https://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.

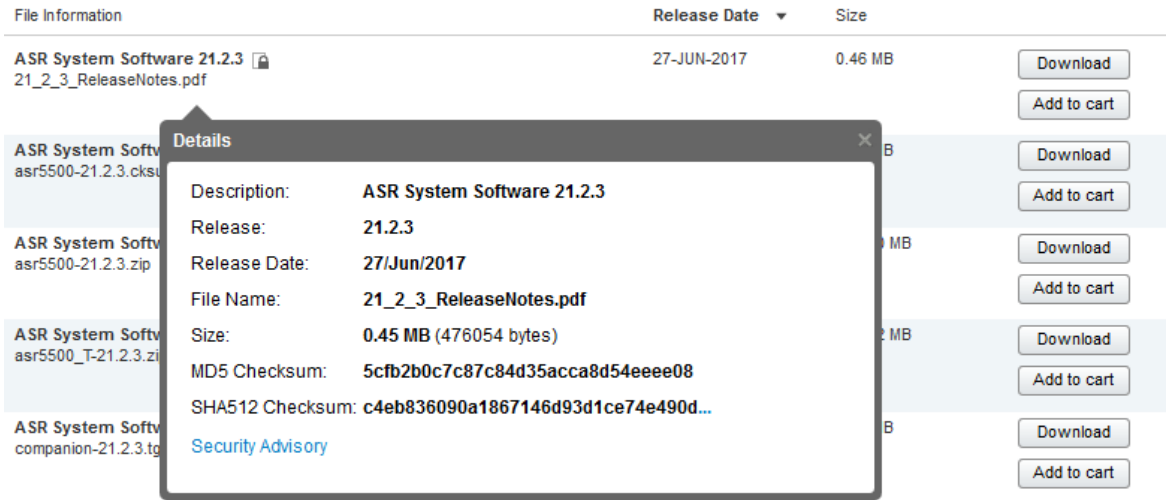
Firmware Updates

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 <pre>> certutil.exe -hashfile <filename>.<extension> SHA512</pre>
Apple MAC	Open a terminal window and type the following command <pre>\$ shasum -a 512 <filename>.<extension></pre>
Linux	Open a terminal window and type the following command <pre>\$ sha512sum <filename>.<extension></pre> <p>Or</p> <pre>\$ shasum -a 512 <filename>.<extension></pre>
NOTES:	
<i><filename></i> is the name of the file.	
<i><extension></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.

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 [Cisco Bug Search Tool](#).

Table 3 - Open Bugs in this Release

Bug ID	Headline	Product Found*
CSCwf99858	SessMgr snap due to race condition	cups-cp
CSCwh81197	[BYTEL / CUPS / LAB / 21.28..h2] DIAMETER PROXY ON SCTP FAILING - WRONG ORIGIN HOST IN CER	cups-cp
CSCwh78561	GWC rejects directly CSR for some IMSIs with "no resources available"	cups-cp
CSCwh16710	CUPS - GX monitoring: overcharging when 4g->3g HO occurs	cups-cp
CSCwe06468	CUPS CP: sessmgr restart seen in Function: sgwdrv_pdn_fsm_st_connected_evt_modify_bearer_ind()	cups-cp
CSCwf26675	[BP-CUPS] Abnormal Release record closure for 3g call with custom38 dictionary	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
CSCwf86398	After WLAN->LTE handover, CP is updating non-existing FAR, leading to handover failure.	cups-cp
CSCwh71166	Cups CP - Server-Unreachable URR stays active on UP after OCS server recovery	cups-cp
CSCwf96709	CLI "event-update send-usage-report reset-usage" sending huge CCR-U msg towards PCRF with 0 usage	cups-cp
CSCwc44211	CUPS UP - Upgrade from 21.23.n9 to 21.23.n10 observed higher RTT/delay between S1U/SGi	cups-up
CSCwh37600	Charging ID inside correlation number is showing 00 00 when using SGW-Service	cups-up
CSCwd70361	Assertion failure at sess/sctrl/sessctrl_uplane_cfg_sync.c:23427	cups-up
CSCwf83239	[S8HR-CUPS] Keepalives information not displayed correctly on UP	cups-up
CSCwh74031	Observed vpp crash in CUPS UP	cups-up

Resolved Bugs in this Release

CSCwh48291	VPP crash resulting in node reload	cups-up
CSCwh85269	SNMP alert/ Error log/ Warning logs every time any sessmgr goes to Pending active or pending standby	cups-up
CSCwh58126	[cups-up][21.28.Fm12.91299] Fatal Signal 11: 11 PC: [0495e396/X] uplane_find_app_data_flow()	cups-up
CSCwh54640	[21.28.Fm12.91254] [cups-up] vpnmgr error messages on UP	cups-up
CSCwh01131	Mon sub feature cases are not working for Pures, Purep and Collapsed call model	cups-up
CSCwh51099	[CUPS] Some DNS requests are not re-addressed when p2p is enabled	cups-up
CSCwe00049	sessmgr memory usage is increasing while number of subscribers remains mostly the same	cups-up
CSCwh20389	EGTUPPathFail not generated in CP node	cups-up
CSCwh03670	[CUPS-UP] Downlink total fp packets not shown correctly in case of http out of order packet	cups-up
CSCwf13605	ipsecdemux crash on asr5500 during crypto call model longevity	epdg
CSCwc65963	sessmgr restart is seen when configuring and unconfiguring Lawful intercept CLIs multiple times	mme
CSCwh63134	sessmgr crash Assertion failure Function: egtpc_send_req_msg()	mme
CSCwh70914	[CP-MME] multiple msgproxy proclat went to over state after sessmgr and mmemgr kill	mme
CSCwf90908	[SAEGW] PGW send EGTP_CAUSE_CONTEXT_NOT_FOUND the 3G -> 4G when handover delay is 2.5 sec or less	pdn-gw
CSCwf87596	On qpc, MPLS/VPN - Staros is reversing the bottom/top labels	pdn-gw
CSCwd17939	In sGWRecord, changeTime appearing as before time from recordOpeningTime and duration showing zero	sae-gw
CSCwf77281	sessmgr restart seen during in SGW during the paging event	sgw
CSCwf84990	[S8HR-Legacy] - Sessmgr memory not recovered back once after Buffered packets flushed out	sgw
CSCwf58771	[S8HR-Legacy] Observed junk values when switch-over to new active chassis and perform SM Recovery	sgw
CSCwe51959	v21.28.mx as the upstream branch :: RHEL-8 Build Issues fix in downstream Dev Branch v21.28.ZVx	staros
CSCwf26822	push config-to-up all takes longer than 5mins to finish	staros
CSCwh73395	VPP restart due to NPUMGR VPP keepalive timeout	upf
CSCwd99519	[UPF-ST] Error logs seen on UPF PDR not found with PDR ID 0x149 and Remove PDR PDR with ID 0x2ce	upf
* 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.

Operator Notes

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*
CSCwf12887	Fatal Signal 11: smgr_uplane_rule_compare_icmp_type()	cups-up
CSCwh47664	CUPS 21.28.hX UPF Mellanox SRIOV interfaces are not applying Service Port MAC address	staros

Operator Notes

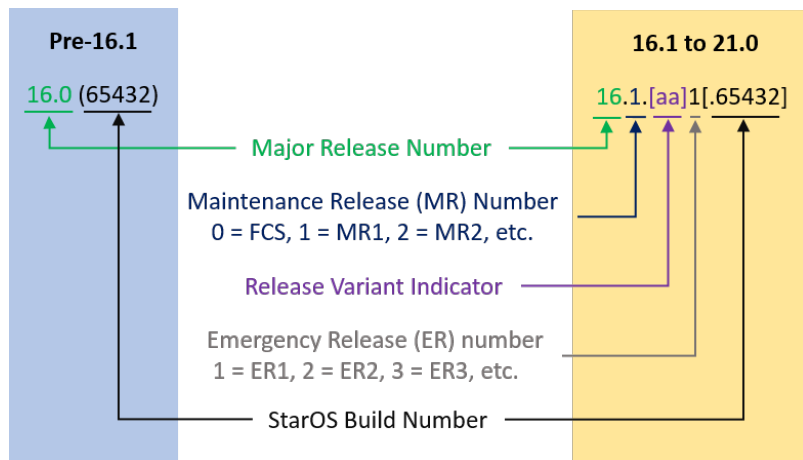
StarOS Version Numbering System

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.

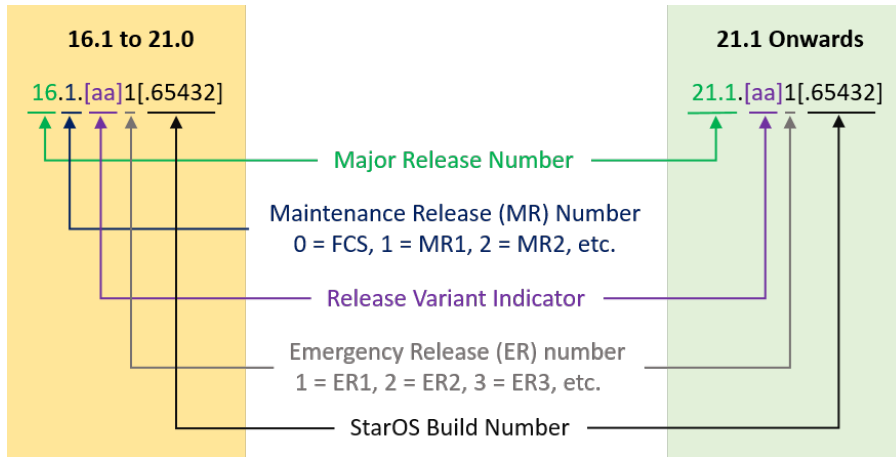
Prior to release 16.1, the *Image Version* field displayed a branch of software including the build number, for example “16.0 (55435)”. Subsequent releases of software for the major release differed only in build number. Lab Quality/EFT releases versus deployment releases also differed only in build 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
ASR 5500		
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.
StarOS Companion Package		
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.
VPC-DI		
qvp-di-<release>.bin.zip	qvp-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.
qvp-di_T-<release>.bin.zip	qvp-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. 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.
qvp-di-<release>.iso.zip	qvp-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. 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.
qvp-di_T-<release>.iso.zip	qvp-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. 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>
VPC-SI		
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>

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qvmc-si_T-<release>.bin.zip	qvmc-si_T-<release>.bin	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.
qvmc-si-<release>.iso.zip	qvmc-si-<release>.iso	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.
qvmc-si_T-<release>.iso.zip	qvmc-si_T-<release>.iso	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.
qvmc-si-template-vmware-<release>.zip	qvmc-si-template-vmware-<release>.ova	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.
qvmc-si-template-vmware_T-<release>.zip	qvmc-si-template-vmware_T-<release>.ova	Contains the trusted 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.
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.

In 21.12.0 and later Releases	In pre-21.12.0 Releases	Description
qypc-si_T- <release>.qcow2.zip	qypc-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.
VPC Companion Package		
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.
Ultra Service Platform		
usp-<version>.iso		The USP software package containing component RPMs (bundles). Refer to Table 6 for descriptions of the specific bundles.
usp_T-<version>.iso		The USP software package containing component RPMs (bundles). This bundle contains trusted images. Refer to Table 6 for descriptions of the specific bundles.
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.

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. 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.