



Release Notes for StarOS™ Software Version 21.11.3 and Ultra Service Platform Version 6.5.2

First Published: May 9, 2019

Last Updated: May 9, 2019

Introduction

This Release Notes identify changes and issues related to this software release. This emergency release is based on release 6.5.1 and StarOS 21.11.3. This Release Notes is applicable to the Ultra Service platforms.

Release Package Version Information

Software Packages	Version
StarOS packages	21.11.3, build 71815
Ultra Service Platform ISO	6_5_2-7121
usp-em-bundle*	6.5.0, Epoch 5171
usp-ugp-bundle*	21.11.3, build 71815, Epoch 6697
usp-yang-bundle	1.0.0, Epoch 5074
usp-uas-bundle	6.5.0, Epoch 6513
usp-auto-it-bundle	5.8.0, Epoch 5282
usp-vnfm-bundle	4.3.0.121, Epoch 5075
ultram-manager RPM*	2.3.0, Epoch 307
USP RPM Verification Utilities	6.5.0
* These bundles are also distributed separately from the ISO.	

Descriptions for the various packages provided with this release are located in _____

Introduction

[Release Package](#) Descriptions.

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:

- StarOS: <https://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides-list.html>
- Ultra Gateway Platform (including the Ultra M Solution): <https://www.cisco.com/c/en/us/support/wireless/ultra-gateway-platform/products-installation-and-configuration-guides-list.html>
- Ultra Automation Services: <https://www.cisco.com/c/en/us/support/wireless/ultra-automation-services/products-installation-and-configuration-guides-list.html>
- Virtual Packet Core (including VPC-SI and VPC-DI): <https://www.cisco.com/c/en/us/support/wireless/virtual-packet-core/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.

Ultra M Hyper-Converged Model Component Versions

HW	SW	6.0	6.1	6.2	6.3	6.4	6.5
	StarOS	21.6.0, Build 68695	21.7.0, Build 68897	21.8.0, Build 69296	21.9.0, Build 69977	21.10.0, Build 70597	21.11.0, Build 70741
	ESC	3.1.0.145	3.1.0.145	4.0.0.104	4.2.0.74	4.3.0.121	4.3.0.121
	RH Kernel	7.3	7.3	7.4	7.5	7.5	7.5
	OSP	10	10	10	10	10	10 or 13 NOTE: OpenStack Platform 13 with RHEL 7.5 is validated only for standalone AutoVNF- based deployments of the UGP VNF.
	BIOS	3.0(3c)	3.0(3c)	3.0(4a)	3.0(4a)	3.0(4a)	3.0(4a)

Installation and Upgrade Notes

UCS C240 M4S SFF (NFVI)	CIMC (BMC)	3.0(3e)	3.0(3e)	3.0(4a)	3.0(4d)	3.0(4d)	3.0(4d)
	MLOM	4.1(3a)	4.1(3a)	4.1(3a)	4.1(3f)	4.1(3f)	4.1(3f)
C2960XR-48TD-I (Management)	Boot Loader	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1	15.2(3r)E1
	IOS	15.2.(2)E5	15.2.(2)E5	15.2.(2)E5	15.2.(2)E5	15.2.(2)E5	15.2.(2)E5
C3850-48T-S (Management)	Boot Loader	3.58	3.58	3.58	3.58	3.58	3.58
	IOS	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E	03.06.06E
Nexus 93180-YC-EX (Leafs)	BIOS	7.59	7.59	7.59	7.59	7.59	7.59
	NX-OS	7.0(3)I5(2)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)
Nexus 9236C (Spines)	BIOS	7.59	7.59	7.59	7.59	7.59	7.59
	NX-OS	7.0(3)I5(2)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)	7.0(3)I7(3)

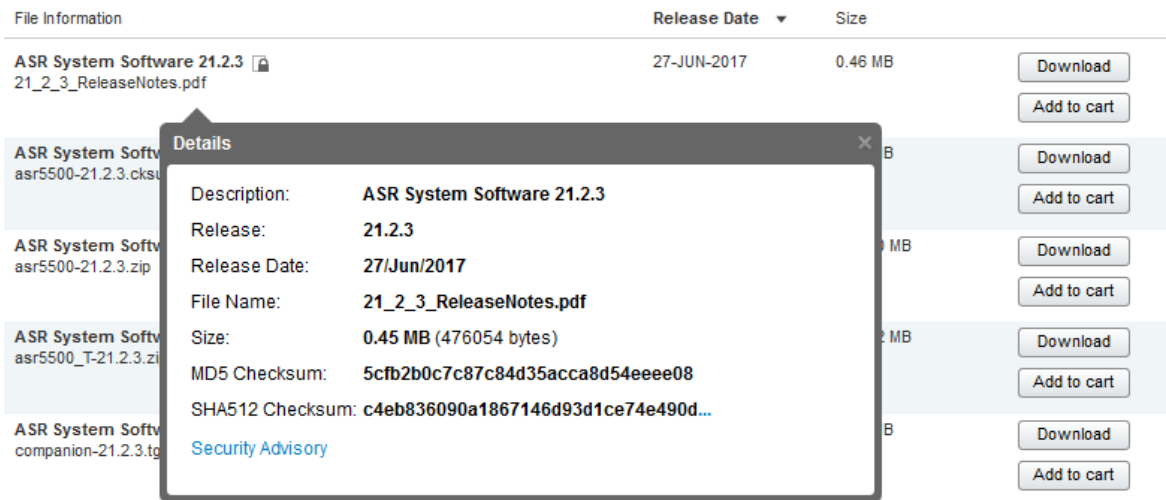
Firmware Updates

There are no firmware updates 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.



Installation and Upgrade Notes

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 1](#) and verify that it matches either the one provided on the software download page.

To calculate a SHA512 checksum on your local desktop, see the following table.

Table 1 – 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>
<p>NOTES:</p> <p><filename> is the name of the file.</p> <p><extension> is the file extension (e.g. .zip or .tgz).</p>	

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

StarOS software images are signed via x509 certificates. USP ISO images are signed with a GPG key. Please view the .README file packaged with the software for information and instructions on how to validate the certificates.

NOTE: Image signing is not currently supported for VPC-SI and/or VPC-DI software packages.

Open Bugs in this Release

The following table lists 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](#).

Bug ID	Headline	Product Found*
CSCvm83524	[BP-CUPS] Assert failure at egtpc_handle_user_sap_event()	cups-cp
CSCvk63958	[PLT-CUPS-ICUPS-VPP]Single user performance blocked due to VPP_MAIN is in over state	cups-up
CSCvn14097	[BP-CUPS] Access Type of Pure-S call is displayed as 'Unknown'	cups-up
CSCvn14202	[BP-CUPS-VPP]Delay charging is having issues with Tear Down packets.	cups-up
CSCvn39767	Unexpected session manager restart- _do_acs_usertcp_event_handler()	pdn-gw
CSCvo32237	[BP-ICUPS]: some UDP streams going to passive post ICSR switchover	pdn-gw
CSCvm65884	PGW-Around 5% increase in sessmgr memory in 21.11.M0.70658 wrt 21.9.M0.69679 baseline CEPS test	pdn-gw
CSCvm83968	[CUSP] need to handle interworking of URL-readdressing and CUSP feature.	pdn-gw
CSCvm82008	[BP-ICUPS]:HTTP volume based offload is not happening after PDN update	sae-gw
CSCvn35333	[BP-ICUPS] uplinkdata and downlinkdata volume values are not correct in PGWCDR after XHDR insertion	sae-gw
CSCvn76706	Sessmgr restarts observed in Cisco ASR5500 after starting the callmodel	sae-gw
CSCvi12541	bfdlc facility instances in warn state on active and standby chassis	sae-gw
CSCvn23275	[PLT-ICUPS] Both DPC2 rebooted upon planned migration	staros
CSCvm98426	[PLT-ICUPS-VPP] Not able to send fragmented packet through VPP.	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 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](#).

Bug ID	Headline	Product Found*
CSCvk58720	Handover rejected (S10 HO) - After congestion is cleared	mme
CSCvn08220	Sessmgr Restart at egtpc_handle_bearer_res_cmd_req_evt	mme
CSCvn59038	Segmentation fault mme_start_procedure() while handling Delete Bearer.	mme

Resolved Bugs in this Release

Bug ID	Headline	Product Found*
CSCvn66416	Assertion failure at sess/mme/mme-app/app/mme_msg_utils	mme
CSCvn74172	SM restarts due to Segmentation fault at egtpc_get_ebi_info_from_pdu during S1 HO	mme
CSCvn82881	MME performs Inter-MME HO when it should be Intra-MME HO	mme
CSCvp32860	SM restarts due to Segmentation fault at egtpc_get_ebi_info_from_pdu during S1 HO in 21.11.Ax	mme
CSCvm09103	mme-service binding was missing due to mismatch in the license.	mme
CSCvm32318	NAS notification (SRVCC handover cancelled) not retransmitted after nasnondeliverynotification	mme
CSCvm63845	Problem with SRVCC after 3G-4G handover during ongoing data session	mme
CSCvn62920	LTE - Wifi - LTE HO fails when ULA does not include MIP6-Agent-Info	mme
CSCvn72982	Sessmgr restart at mme_s1ho_s10_to_4g_send_reloc_resp	mme
CSCv013661	cc overwrite apn remap is case sensitive	mme
CSCv022843	Paging edrx h-sfn should be a 10 bits counter	mme
CSCv033689	inter-rat-nnsf mme-codes parameter missing after reload	mme
CSCv057948	Very inbalanced sessmgr distribution after enabling "sgsn-mme subscriber-data-optimization"	mme
CSCvm42252	StarOS is marking BFD routes down and BGP route learned wrongly after nexus restart for VPC-DI	pdn-gw
CSCvn41573	HTTP Fraud detected with use HTTP HEAD modification	pdn-gw
CSCvk53094	[PGW] [IMSA] [NPLI] - CCR-U doesn't include "UDP-SOURCE-PORT" AVP	pdn-gw
CSCvn97839	Threshold process goes into warn state because of memory	pdn-gw
CSCvp32975	PCC provisioned dynamic rule not enforced when FAPA/TRM activated	pdn-gw
CSCvn33912	PGW sends Update Bearer Request with unknown filters in TFT	pdn-gw
CSCv006323	Sessmgr restart at function xdr_acs_show_sfw_rule_info_t()	pdn-gw
CSCv017281	aaamgr memory leak due to checkpointing	pdn-gw
CSCvj82335	task stop request for BFD sent for Incorrect context	sae-gw
CSCvk43515	Assertion failure at sm_rab_mgmt	sgsn
CSCvk45571	sessmgr restart function: sessmgr_gprs_process_sub_session_idle()	sgsn
CSCvn31717	sessmgr restart on s4_smn_send_egtpc_pdn_local_purge	sgsn
CSCvj51716	Task restart on modify bearer request	sgsn
CSCvj89699	sessmgr Assertion failure in pmm_ms_fsm_invalid_event_handler	sgsn
CSCvn78512	Session manager restarted Fatal Signal 6: Aborted	sgsn
CSCv004661	sessmgr restart- Assertion failure	sgsn
CSCv055588	Session Manager assert during S4 SRNS	sgsn

Operator Notes

Bug ID	Headline	Product Found*
CSCvm93753	MIB Syntax Errors in 21.8.1 (69429) and 21.9.1 (70183)	staros
CSCvn67152	VPC-DI/XL710: Fix port statistic collection time intervals.	staros
CSCvm96218	"ASR5K device sends wrong objects for the traps with ifIndex 1343, 1344, 1345, 1346."	staros
CSCvn09416	GRE tunnels UP when destination is unreachable	staros
CSCvn10317	Standby SFC does not bootup after power off/on demux	staros
CSCvn72221	Kernel crashes and iftask errors seen after FI reload done on UCS	staros
CSCvn94836	VPC-DI: iftask double count for di_tx traffic	staros

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

Operator Notes

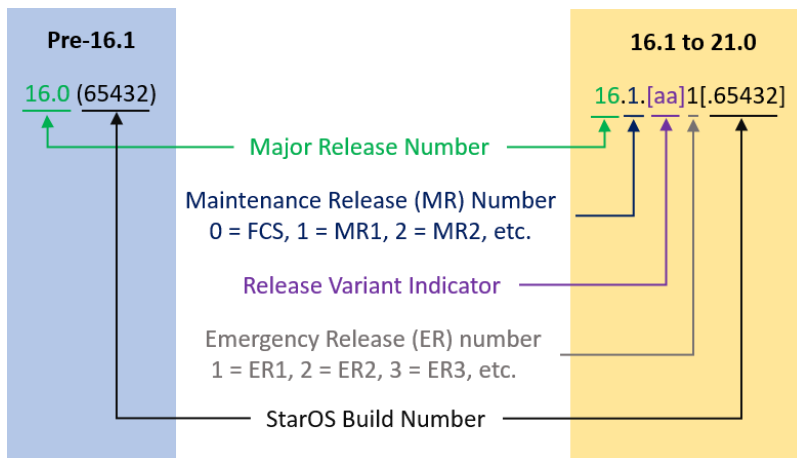
StarOS Version Numbering System

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

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

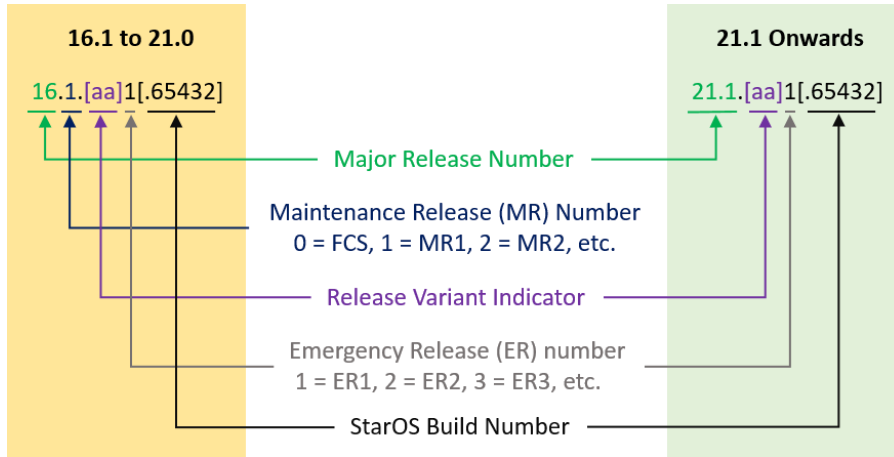
From release 16.1 onwards, the output of the **show version** command, as well as the terminology used to describe the Build Version Number fields, has changed. Additionally, **show version** will display slightly different information depending on whether or not a build is suitable for deployment.

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



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

Operator Notes



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 2](#) lists provides descriptions for the packages that are available with this release.

Table 2 - Release Package Information

Package	Description
ASR 5500	
asr5500-<release>.bin	A zip file containing 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>.bin	A zip file containing 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.
VPC-DI	
qvmc-di-<release>.bin	The VPC-DI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvmc-di_T-<release>.bin	The trusted VPC-DI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvmc-di-<release>.iso	The VPC-DI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvmc-di_T-<release>.iso	The trusted VPC-DI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvmc-di-template-vmware-<release>.tgz	The VPC-DI binary software image that is used to on-board the software directly into Vmware.
qvmc-di-template-vmware_T-<release>.tgz	The trusted VPC-DI binary software image that is used to on-board the software directly into Vmware.
qvmc-di-template-libvirt-kvm-<release>.tgz	This is an archive that includes the same VPC-DI ISO identified above, but additional installation files for using it on KVM.
qvmc-di-template-libvirt-kvm_T-<release>.tgz	This is an archive that includes the same trusted VPC-DI ISO identified above, but additional installation files for using it on KVM.
qvmc-di-<release>.qcow2.tgz	The VPC-DI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.
qvmc-di_T-<release>.qcow2.tgz	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.
VPC-SI	
qvmc-si-<release>.bin	The VPC-SI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.

Operator Notes

Package	Description
qvpc-si_T- <release>.bin	The trusted VPC-SI binary software image which is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-si-<release>.iso	The VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvpc-si_T- <release>.iso	The trusted VPC-SI ISO used for new deployments a new virtual machine is manually created and configured to boot from a CD image.
qvpc-si-template- vmware-<release>.ova	The VPC-SI binary software image that is used to on-board the software directly into Vmware.
qvpc-si-template- vmware_T- <release>.ova	The trusted VPC-SI binary software image that is used to on-board the software directly into Vmware.
qvpc-si-template- libvirt-kvm- <release>.tgz	This is an archive that includes the same VPC-SI ISO identified above, but additional installation files for using it on KVM.
qvpc-si-template- libvirt-kvm_T- <release>.tgz	This is an archive that includes the same trusted VPC-SI ISO identified above, but additional installation files for using it on KVM.
qvpc-si-<release>. qcow2.gz	The VPC-SI binary software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.
qvpc-si_T-<release>. qcow2.gz	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.
StarOS Companion Package	
companion- <release>.tgz	An archive containing 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.
Ultra Service Platform	
usp-<version>.iso	The USP software package containing component RPMs (bundles). Refer to Table 3 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 3 for descriptions of the specific bundles.
usp_rpm_verify_utils- <version>.tar	This package contains information and utilities for verifying USP RPM integrity.

Table 3 - 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.

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 are considered un-controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax 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. (1110R)

© 2018 Cisco Systems, Inc. All rights reserved.