Release Notes for the StarOS™ Software Version 2025.01.gh0

First Published: January 31, 2025

Introduction

This Release Notes identifies changes and issues related to the Classic Gateway, and Control and User Plane Separation (CUPS) software releases.

Products Qualified and Released in this Release

Products	Qualified Yes/No
cups-cp	Yes
cups-up	Yes
mme	Yes
ePDG	Yes
pdn-gw	Yes
saegw	Yes
sgsn	Yes
Platforms	
ASR 5500	No
VPC-DI	Yes
VPC-SI	Yes

Cisco Systems, Inc. www.cisco.com

Release Lifecycle Milestones

Release Lifecycle Milestone	Milestone	Date
First Customer Ship	FCS	31-Jan-2025
End of Life	EoL	31-Jan-2025
End of Software Maintenance	EoSM	01-Aug-2026
End of Vulnerability and Security Support	EoVSS	01-Aug-2026
Last Date of Support	LDoS	31-Aug-2027

Release Package Version Information

Software Packages	Version	Build Number
StarOS Package	2025.01.gh0	21.28.mh25.96732

Descriptions for the various packages provided with this release are available in the Release Package Descriptions section.

Verified Compatibility

Products	Version
ADC P2P Plugin	2.74.h3.2586
ESCA	6.0.0.86
Host OS	RHEL 8.4
RedHat OpenStack	RHOSP 16.2
E810C NIC Version	Driver: ice version: 1.12.6 Firmware: 4.20 0x80018f67 0.387.18
CIMC Version (UCS C220-M6S)	4.3(2.230207)
NED Package	ncs-6.1.11.2-nso-mob-fp-3.5.2-ad74d4f-2024-10-18T1052/ncs-6.1.11.2-nso-mob-fp-3.5.2-ad74d4f-2024-10-18T1052.tar.gz
NSO-MFP	nso-mob-fp-3.5.2

Note: Use only these compatible software versions for the products qualified in this release.

What's New in this Release

Features and Enhancements

This section covers a brief description of the features and enhancements introduced in this release. It also includes links to detailed documentation, where available.

Feature Title	Feature Description	Product
Selection of UP During Session Creation Failures	This feature enhances the UP selection mechanism by marking the UP as "Busy-Out" in case of high volumes of call failures. This keeps the specific UP out of repeated selections and therefore improves the overall user experience. Commands Introduced: A new CLI is introduced to Configure the Parameters to exclude a UP: **exclude-user-plane minimum-call-failures** ***min_callfail_range*** **failure-threshold-percentage** ***fail_threshold_percentage*** **failure-rejection-interval** ***fail_reject_int*** **Default Setting**: Disabled- Configuration Required to Enable	cups
3GPP-Charging-Characteristics AVP Support in R8 Dictionary	This feature aims to address the support of 3GPP-Charging-Characteristics AVP in the r8-gx-standard dictionary, which is critical for differential charging particularly for telecommunication operators seeking to leverage advanced 5G functionalities. A new CLI command "**encode-cc-in-r8- gx-dict**" is introduced to enable the inclusion of 3GPP-Charging-Characteristics AVP in CCR-I messages when using the r8-gx-standard dictionary. **Default Setting**: Disabled- Configuration Required to Enable	cups
Increase the limit for the number of user plane groups in the IP pool management policy	This feature enhances the number of User Plane (UP) groups allowed in the IP pool management policy. The maximum number of UP groups allowed in each IP pool management policy is 100. **Default Setting**: Disabled- Configuration Required to Enable	cups

Ubuntu 22.04 Container Base Image upgrade for VM based RCM	This release recommends upgrading the SMI base image and Cluster Manager to Ubuntu 22.04. Additionally, it is recommended to update the Inception Server to the latest SMI disk ISO and refresh the container images in smi-app, smi-library, smi-build, smi-shared, smi-incubator, and related components.	cups
Handling Final Unit Indication with MSCC Result code 4999	When the Final Unit Indication (FUI) AVP is received with the Multiple Services Credit Control (MSCC) Result Code 4999, the specified action mentioned in FUI, either redirect or terminate, should be applied. Currently, Result Code 4999 is not supported, so the CUPS CP either terminates or continues the call based on the failure handling configuration under Credit Control Configuration mode. To support MSCC Result Code 4999, a new CLI command, **map-mscc-rc-4999-to-2001**, has been introduced. This command maps the MSCC Result Code 4999 to 2001 (DIAMETER_SUCCESS) when the Final Unit Indication AVP is received. This feature benefits customers by allowing session continuation and applying the FUI action specified in the AVP. **Default Setting**: Disabled- Configuration Required to Enable	cups
Enablement of the Network Policy Bit in MME	The feature supports the Network Policy Information Element (IE) in the Attach and Tracking Area Update (TAU) Accept messages. It enhances network security by utilizing operator policies in the MME. Command introduced: **send-network-policy unsec-redir-not-allowed** : In the MME-service and call-control-profile configuration mode, to enable the network policy configuration, use the **send-network-policy unsec-redir-not-allowed** command to configure unsecured redirection to GERAN not allowed. If the **send- network-policy unsec-redir-not-allowed** command is not enabled, the Network Policy IE is not sent in the Attach/TAU Accept message. **Default Setting**: Disabled- Configuration Required to Enable	mme
Implementation of EGTPC/EGTPU IPv6 Path Failure and Clear SNMP Traps	In this feature, the SNMP traps for EGTPC/EGTPU IPv6 Path Failure and Path Failure Clear are implemented on ePDG, specifically for VPC-DI platforms. The ePDG is responsible for generating specific SNMP traps when there is no response for GTPV2	staros

	requests from remote IPv6 peers. This capability is vital for identifying and resolving issues related to control and data path failures in the network. **Default Setting**: Enabled- Configuration Required to Suppress	

Behavior Changes

This section covers a brief description of the behavior changes introduced in this release.

Behavior Change	Description
NTSR Session Hold Time Update	**Previous Behavior**: The maximum range for the NTSR timer that holds the session after path failure detection at the MME is 3600 seconds for all the setups. **New Behavior:** In VPC-DI platform, the maximum range for the NTSR timer that holds the session after path failure detection at the MME is 2 days or 172800 seconds. The maximum range remains the same as 3600 seconds for other platforms.
Mask Credentials in the Output URL of show crash config Command	**Previous Behavior:** The output of the **show crash config** command displays the complete URL for FTP, SFTP, and TFTP servers. **New Behavior**: The output of the **show crash config** command now masks the credentials in the URL for FTP, SFTP, and TFTP servers**.**
Support of 'LTE-M RAT type reporting to PGW' flag in the indication IE for S-GW to pass the LTE-M RAT type to P-GW	**Previous Behavior:** When MME requests the S-GW to pass the LTE-M RAT type to the P-GW, the S-GW sends the LTE-M RAT type to P-GW without receiving the LTEMPI(LTE-M RAT type reporting to P-GW Indication) bit in the indication IE from MME. **New Behavior:** When MME requests the S-GW to pass the LTE-M RAT type to the P-GW, the S-GW sends the LTE-M RAT type to P-GW only if it receives LTEMPI bit in the indication IE from MME in every Create Session, Request message, and Modify Bearer Request message. Otherwise, S-GW sends the WB-E-UTRAN RAT type to P-GW.

Related Documentation

For a complete list of documentation available for this release, go to:

http://www.cisco.com/c/en/us/support/wireless/asr-5000-series/products-installation-and-configuration-guides- list.html

Installation and Upgrade Notes

This Release Note does not contain general installation and upgrade instructions. Refer to the existing installation documentation for specific installation and upgrade considerations.

Synchronizing Boot File for Service Function Cards

To synchronize the boot file for all the Service Function (SF) VPC-DI non-management cards, use the

following: CLI executable command:

```
[local] host_name# system synchronize boot
```

This assures that the changes in boot file are identically maintained across the SF cards.

Ensure that you execute this command before reload for version upgrade from any version less than mh14 to

mh14 or later.

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**.** Click **Linux,** and then choose the Software Image Release Version**.**

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 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 Table 1

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 > certutil.exe -hashfile *<filename>*.*<extension>* SHA512

Apple MAC	Open a terminal window and type the following command $ shasum -a 512 <*filename*>.<*extension*>

Linux	Open a terminal window and type the following command
	$ sha512sum <*filename*>.<*extension*>
	Or
	$ shasum -a 512 <*filename*>.<*extension*>

NOTES: <*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 2024.01 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.

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 for this Release

The following table lists the open bugs in this specific 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 2 - Open Bugs in this Release

Bug ID	Headline	Product Found
CSCwn06583	While performing SGW Relocation getting error as EGTP_CAUSE_PEER_NOT_RESPONDING	cups-cp
CSCwm40394	Sx-IPSec - clear crypto security-association results in Sx failure	cups-cp
CSCwm74110	[CUPS 21.28] Reboot SF Demux leads to BFD sessions DOWN on Standby Card	cups-cp
CSCwk79042	[CUPS-UP] SX path failure is not leading to SRP switchover with sx monitor enabled	cups-up
CSCwm51816	sessmgr task restarted on UP, when LI and S8hr interception call is getting cleared	cups-up
CSCwk65512	ipsecmgr cpu warn/over during make-break sessions with 4096 keysize device certificate	epdg
CSCwn39619	Bulkstats counter not populating any value during sessmgr crash.	epdg

Resolved Bugs for this Release

The following table lists the resolved bugs 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 3 - Resolved Bugs in this Release

Bug ID	Headline	Product Found
CSCwn19334	sessmgr failure at sess/smgr/sessmgr_sgw_recovery	cups-cp
CSCwm91097	[SXA] Charging ID updation not expected 0x0	cups-cp
CSCwn12297	Cannot change monitoring key at session level on CUPS when changing rulebase and ruledef	cups-cp
CSCwn15127	SGW is not assigning dual S1-u IP post X2 HO with SGW change	cups-cp
CSCwm90958	Three second delay in sending CCR-T after 4012 in Gy CCA-Initial	cups-cp
CSCwn54830	[Viettel-vEPC] multiple restarts on GGSN Cisco during migrate traffic	cups-cp
CSCwn12434	SAEGW is ignoring GTPC messages	cups-cp
CSCwn49737	[CUPS-CP] Assertion failure at sess/egtp/egtpc/egtpc_evt_handler_func.c:8069	cups-cp
CSCwm46137	saegw-service statistics wrongly labels initiated PDNs as current PDNs Under sgw function	cups-cp
CSCwm65335	Sessmgr restart observed for CUPS-CP node on version 21.28.m26-94712	cups-cp
CSCwm81665	UDP checksum 0x0 is initiated from PGW for GTPC message	cups-cp

CSCwm47782	UP not sending 'sx session report' to CP when UE goes into Idle state in RA case.	cups-up
CSCwn15344	PGW Personal Stateful Firewall wrongly dropping packets	cups-up
CSCwn63279	Upon multiple card migrations ipsecmgr instance has NULL demux mgr.	epdg
CSCwn38610	Segmentation fault at sessmgr_med_pdif_ipsec_data_receive	epdg
CSCwm57722	SCTP bulkstat counter description is incorrect under mme schema	mme
CSCwm61933	MME rejects UBReq with No Resource available while handling ERMI	mme
CSCwi00493	sessmgr reload at sess/mme/mme-app/app/mme_im_exit_proc.c:3003	mme
CSCwm49685	List corruption in need of debug content	mme
CSCwm63294	Rewriting clear-route-multipath-zero CLI to be inline with other config CLIs	mme
CSCwn29026	sessmgr crash at mme_auth_awt_hss_hss_resp()	mme
CSCwn39799	MME not properly coding "NR UE Security Capabilities" IE to eNB	mme
CSCwm97868	Sessmgr restarts due to assertion failure in mme_pdn_fsm_connect_pending_disconnect	mme
CSCwn59542	Assertion failure in 'mme_app_create_sgw_entry' after modifying TAI objects	mme
CSCwj29750	Sessmgr restart after SW upgrade to 21.28.m19, mme_auth_awt_hss_hss_resp()	mme
CSCwn18588	multiple sessmgr in warn state due to mme_app_allocate_ue_addl_security_cap and SN_cmAlloc	mme
CSCwm39736	Assertion failure at egtpc_handle_context_rsp_msg()	mme
CSCwm62734	Idle timer resetting not working for ipv6 pmip/lma leg	pdn-gw
CSCwm67862	Credit Control Failure Handling is showing UNKNOWN	pdn-gw
CSCwn55113	After vPGW software upgrade (21.28.mh20-95098) customer observing all cards lock state "UNKNOWN"	pdn-gw
CSCwn04769	PGW is sending CCR-U with wrong destination realm/host and will get reject with CC 3003 from OCS	pdn-gw
CSCwn31711	Sessmgr restart at function sessmgr_pgw_allocate_new_sub_session()	pdn-gw
CSCwm47392	Sessmgr restarts after enabling VoLTE for specific inroamer IMSIs ranges	pdn-gw
CSCwn58706	CDRs are stucked when transport problems were observed	sae-gw
CSCwn20357	Incorrect MNC value observed from show subscriber saegw-only full output	sae-gw
CSCwn29559	Wrong display of IMEI in "show lawful-intercept full intercept-id <id>" output in GGSN service	sae-gw
CSCwd55745	Facility Mpls_sig is in over state continously	sae-gw
CSCwm49666	SGW sends LTE-M on S8, though LTEMPI isn't set	sgw
CSCwm99808	snmpEngineBoots not incrementing post CF switchover	staros
CSCwn30975	Unequal distribution of ipsecmgr across SF cards	staros
CSCwn24626	CertValid trap generated with expiration date not matching the certificate	staros
CSCwm44319	Update version number for latest release version numbering	staros
CSCwn18430	Good replacement card for failed standby MIO may fail to boot	staros
CSCwm68602	SW should handle FSC power supply failures better and take a bad FSC card Offline.	staros

Operator Notes

StarOS Version Numbering System

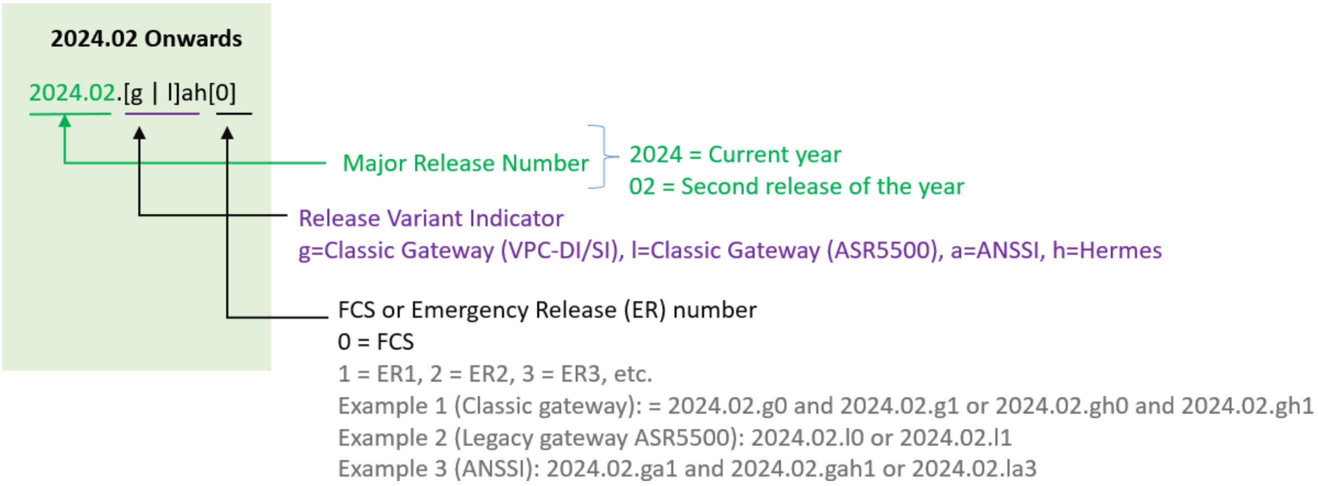
The output of the **show version** command displays detailed information about the version of StarOS currently running on the ASR 5500 or Cisco Virtualized Packet Core platform.

NOTE: Starting 2024.01.0 release (January 2024), Cisco is transitioning to a new release versioning scheme. The release version is based on the current year and product. Refer to **Figure** 1 for more details.

During the transition phase, some file names will reflect the new versioning whereas others will refer to the 21.28.x- based naming convention. With the next release, StarOS-related packages will be completely migrated to the new versioning scheme.

Version Numbering for FCS, Emergency, and Maintenance Releases

Figure 1 – Version Numbering


2024.02 Onwards
2024.02.[g | l]ah[0]
Major Release Number
2024 = Current year
02 = Second release of the year
Release Variant Indicator
g=Classic Gateway (VPC-DI/SI), l=Classic Gateway (ASR5500), a=ANSSI, h=Hermes
FCS or Emergency Release (ER) number
0 = FCS
1 = ER1, 2 = ER2, 3 = ER3, etc.
Example 1 (Classic gateway): = 2024.02.g0 and 2024.02.g1 or 2024.02.gh0 and 2024.02.gh1
Example 2 (Legacy gateway ASR5500): 2024.02.l0 or 2024.02.l1
Example 3 (ANSSI): 2024.02.ga1 and 2024.02.gah1 or 2024.02.la3

Note: For any clarification, contact your Cisco account representative.

StarOS Configuration Recommendations for VPC-DI

Configure the following StarOS-level settings in the **staros_param.cfg** file to set up the day-0 cloud configuration for the VNF.

Enable the boot parameter to move KNI packets over MCDMA threads by setting KNI_ON_MCDMA_THREAD_ENABLE=1.

Troubleshooting Information

Issue: VIP accessibility for VPC-DI instances deployed via ESC on Openstack using the ML2/OVN mechanism driver may be problematic.

Workaround:

1. Identify the CF1 and CF2 ports on the management network within Openstack
2. Configure **allowed_address_pairs** for these ports to match the virtual port IP address (use /32 notation)
3. Avoid using CIDR format IP addresses for **allowed_address_pairs** on these ports
4. Execute the following command to set the allowed address **pairs:openstack port set** <CF-mgmt-port-ID> **-- allowed-address ip-address**=<VIP-address>,**mac-address**=<CF-mgmt-port-MAC-address>

Release Package Descriptions

Table 4 provides examples of packages according to the release. For more information about the release packages up to 21.28.x releases, refer to the corresponding releases of the release note.

Table 4 - Release Package Information

Software Package	Description
ASR 5500	
asr5500-<release>.zip	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	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.
VPC Companion Package	
companion-vpc-<release>.zip For example, companion-vpc-2024.02.gh2.i4.zip	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.
VPC-DI	
qvpc-di-<release>.bin.zip	Contains the VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-di_T-<release>.bin.zip	Contains the trusted VPC-DI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-di-<release>.iso.zip	Contains the VPC-DI ISO used for new deployments, a new virtual machine is manually created and configured to boot from a CD image.
qvpc-di_T-<release>.iso.zip	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.
qvpc-di-template-vmware-<release>.zip	Contains the VPC-DI binary software image that is used to on-board the software directly into VMware.
qvpc-di-template-vmware_T-<release>.zip	Contains the trusted VPC-DI binary software image that is used to on-board the software directly into VMware.
qvpc-di-template-libvirt-kvm-<release>.zip	Contains the same VPC-DI ISO identified above and additional installation files for using it on KVM.

qvpc-di-template-libvirt-kvm_T-<release>.zip	Contains the same trusted VPC-DI ISO identified above and additional installation files for using it on KVM.
qvpc-di-<release>.qcow2.zip	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.
qvpc-di_T-<release>.qcow2.zip	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.
VPC-SI	
intelligent_onboarding-<release>.zip	Contains the VPC-SI onboarding signature package that is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-si-<release>.bin.zip	Contains the VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-si_T-<release>.bin.zip	Contains the trusted VPC-SI binary software image that is used to replace a previously deployed image on the flash disk in existing installations.
qvpc-si-<release>.iso.zip	Contains 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.zip	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.
qvpc-si-template-vmware-<release>.zip	Contains the VPC-SI binary software image that is used to on-board the software directly into VMware.
qvpc-si-template-vmware_T-<release>.zip	Contains the trusted VPC-SI binary software image that is used to on-board the software directly into VMware.
qvpc-si-template-libvirt-kvm-<release>.zip	Contains the same VPC-SI ISO identified above and additional installation files for using it on KVM.
qvpc-si-template-libvirt-kvm_T-<release>.zip	Contains the same trusted VPC-SI ISO identified above and additional installation files for using it on KVM.
qvpc-si-<release>.qcow2.zip	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.
qvpc-si_T-<release>.qcow2.zip	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.
RCM	
rcm-vm-airgap-<release>.ova.zip	Contains the RCM software image that is used to on-board the software directly into VMware.
rcm-vm-airgap-<release>.qcow2.zip	Contains the RCM software image in a format that can be loaded directly with KVM using an XML definition file, or with OpenStack.
rcm-vm-airgap-<release>.vmdk.zip	Contains the RCM virtual machine disk image software for use with VMware deployments.
Ultra Services Platform	

usp-<version>.iso	The USP software package containing component RPMs (bundles). Refer to the Table 5 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 the Table 5 for descriptions of the specific bundles.
usp_rpm_verify_utils-<version>.tar	Contains information and utilities for verifying USP RPM integrity.

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, refer to https://www.cisco.com/c/en/us/support/index.html.

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 ANYKIND, 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 WITHTHE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSEOR 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: 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)