Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 6.6.25

Revised: June 9, 2023

Network Convergence System 5500 Series Routers

Note *This software release has reached end-of-life status. For more information, see the* End-of-Life and End-of-Sale Notices.

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

Cisco IOS XR Release 6.6.25 contains all features released in Cisco IOS XR Release 6.6.1. Release 6.6.1 is limited availability (LA) release. For more information on IOS XR Release 6.6.1, see Release Notes for Cisco NCS 5500 Series Routers, Release 6.6.1

Software Features Introduced in this Release

Explicit Congestion Notification (ECN) Bit Marking

The Expilicit Congestion Notification (ECN) feature is an extension to WRED (Weighted Random Early Detection). This feature will mark packets instead of dropping them when the average queue length exceeds a specific threshold value. When configured, ECN helps routers and end hosts to understand that the network is congested and slow down sending packets.

For more information on this feature, see the *Modular QoS Configuration Guide for Cisco NCS 5500 Series Routers*.

Flow Label Support for EVPN VPWS

The Flow Label support for EVPN VPWS feature enables provider (P) routers to use a flow-based load balancing to forward traffic between the provider edge (PE) devices. Flow-Aware Transport (FAT) pseudowires (PW) over an MPLS packet switched network is used for load-balancing traffic across BGP-signaled pseudowires for an EVPN virtual private wire service (VPWS).

For more information on this feature, see the *EVPN Virtual Private Wire Service (VPWS)* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.6.x.*

LDP-Based VPLS and VPWS FAT Pseudowire

The LDP-based VPLS and VPWS FAT Pseudowire feature enable provider (P) routers to use a flow-based load balancing to forward traffic between the provider edge (PE) devices. Flow-Aware Transport (FAT) of pseudowires (PW) over an MPLS packet switched network is used for load-balancing traffic across LDP-signaled pseudowires for Virtual Private LAN Services (VPLS) and Virtual PrivateWire Service (VPWS).

For more information on this feature, see the *Configure Multipoint Layer 2 Services* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.6.x.*

Three-level Hierarchical QoS

The Three-level Hierarchical QoS (H-QoS) feature enables enforcement of class/service, group/ ethernet flow point (EFP), and port level SLAs.

As earlier, you can apply the regular two-level egress H-QoS policies on the sub-interfaces to achieve class and EFP SLAs at child and parent levels. In addition, with this feature, you can apply a port shaper policy on the main interface to achieve an aggregated port level SLA in a 1+2 H-QoS model.

The advantage of three-level H-QoS is that the parent shaper on the sub-interfaces is allowed to oversubscribe, thus enabling best effort sharing of the aggregate port shaper at the third level.

To know more about the three-level Hierarchical QoS feature, its sample configuration, and other information, see the *Modular QoS Configuration Guide for Cisco NCS 5500 Series Routers*.

Bridge Domain and BVI Scale

The number of bridge domains depends on the number of attachment circuits (ACs) per bridge domain and if the Bridge-Group Virtual Interface (BVI) is configured or not. In Release 6.6.25, only 750 BDs are supported.

MAC Address Withdrawal

The MAC Address Withdrawal feature provides faster convergence by removing MAC addresses that are dynamically learned. This feature uses Label Distribution Protocol (LDP)-based MAC address withdrawal message. A MAC list Type Length Value (TLV) is part of the MAC address withdrawal message.

This feature also supports optimization of MAC address withdrawal. The optimization allows PEs to retain the MAC addresses that are learned from the CE devices over the access side. Only MAC addresses that are learned from peer PEs are flushed out. This avoids unnecessary MAC flushing toward AC side and ensures better utilization of bandwidth and resources.

For more information on this feature, see the *Configure Multipoint Layer 2 Services* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.6.x.*

Static Route Traffic-Steering using SRTE Policy

Earlier, you could associate Segment Routing Label Switched Paths (SR-LSP) with a static route. The Static Route Traffic-Steering using SRTE Policy feature adds support to specify a Segment Routing (SR) policy as an interface type when configuring static routes for MPLS and IPv6 data planes.

For more information about the Static Route Traffic-Steering using SRTE Policy feature, see the Configure SR-TE Policies chapter in the *Segment Routing Configuration Guide for Cisco NCS 5500 Series Routers*.

LDP over Segment Routing Policy

The LDP over Segment Routing Policy feature enables an LDP-targeted adjacency over Segment Routing (SR) policy between two routers. This feature extends the existing MPLS LDP address family neighbor configuration to specify an SR policy as the targeted end-point.

For more information about the LDP over Segment Routing Policy feature, see the Configure SR-TE Policies chapter in the *Segment Routing Configuration Guide for Cisco NCS 5500 Series Routers* .

Smart Licensing for Flexible Consumption Model

The following hardware variants are supported for Smart Licensing on Cisco NCS 5500 Series Router from this release.

Table 1: Flexible Consumption Model Licenses Usage Pattern Supported from this Release

License Name	Hardware Supported	Consumption Pattern
Essential and Advanced Licenses: ESS-100G-RTU-1 ADV-100G-RTU-1	Routers with fixed chassis unit: NCS-55A2-MOD-HD-S, NCS-55A2-MOD-SE-S, and NCS-55A2-MOD-S. Routers with modular chassis unit: NC55-MOD-A-S and NC55-MOD-A-SE-S Line cards: NCS-55A1-36H-SE-S, NC55-6X200-DWDM-S, NCS-55A1-48Q6H, and NC55-36X100G-S	The number of essential or advanced licenses consumed depends on the number of active ports and is reported on per chassis basis.
Hardware Tracking Licenses that support chassis: • NCS-55A1-36HS-TRK • NCS-55A1-48Q6H-TRK • NCS-55A2-MOD-TRK • NCS-55A2-MODH-TRK • NCS-55A2-MODS-TRK	These Tracking licenses are named on the basis of the hardware supported. For example, NCS-5501-TRK licenses support NCS 5501 systems.	The number of licenses consumed depends on the number of chassis in use.
Hardware Tracking Licenses that support line cards: • NC55-DWDM-LC-TRK • NC55-MOD-A-SE-TRK • NC-55-MOD-A-TRK	These Tracking licenses are named on the basis of the line card supported. For example, NC55-36H-LC-TRK licenses support NC-55-36X100G line cards.	The number of licenses consumed depends on the number of line cards in use.
Software Tracking license: • XR-6.5-TRK • XR-6.6-TRK	These Tracking licenses are named on the basis of the software supported. For example, XR-6.3-TRK licenses support IOS XR 6.3.X software image.	The number of licenses consumed depends on the software images used.

For more information on Smart Licensing, see the *System Management Configuration Guide for Cisco NCS 5500 Series Routers*.

Selective Egress Policy-Based Queue Mapping

With selective egress policy-based queue mapping, you can combine traffic class (TC) maps in various permutations at egress.

The primary aim of introducing egress TC mapping is to classify the traffic in the ingress using a single policy and place the classified traffic into queues, by assigning the traffic classes. At the egress, you can support different grouping of traffic classes.

Based on different Service Level Agreements (SLAs) that each customer would have signed up for, you can group the TCs into priority queues for real time (RT) traffic, other TCs into guaranteed bandwidth (BW) traffic, and the rest into best effort (BE) traffic delivery.

To know more about the selective egress policy-based queue mapping feature, its sample configuration, and other information, see the *Modular QoS Configuration Guide for Cisco NCS 5500 Series Routers*.

Ingress Short-Pipe

Usually, DSCP and precedence-based classifications are supported in QoS traffic only when there is no MPLS label in the packet. Using the ingress short-pipe feature, however, you can classify a packet that contains one MPLS label using the type-of-service (ToS) field of the IPv4 or IPv6 header.

With the ingress short-pipe feature, you get increased visibility into traffic packets. Plus, the feature also removes the limitation of classifying MPLS packets that come into IPv4 or IPv6 networks.

To know more about the selective egress policy-based queue mapping feature, see the *Modular QoS Configuration Guide for Cisco NCS 5500 Series Routers*. To see the command reference details, see *match mpls disposition class-map child_pipe* in *Modular QoS Command Reference for Cisco NCS 5500 Series and Cisco NCS 540 Series Routers*.

Minimum Password Length for First User Creation

To authenticate the user for the first time, Cisco router prompts you to create a username and password, in any of the following situations:

- When the Cisco Router is booted for the very first time.
- When the router is reloaded with no username configuration.
- When the already existing username configurations are deleted.

By default, the minimum length for passwords in a Cisco router is limited to 2 characters. Due to noise on the console, there is a possibility of the router being blocked out. Therefore, the minimum length for password has been increased to 6 characters for a first user created on the box, in each of the situations described above. This reduces the probability of the router being blocked out. It avoids the security risks that are caused due to very small password length. For all other users created after the first one, the default minimum length for password is still 2 characters.

For more information about the feature, see *Configuring AAA Services* Chapter of the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*.

ACL Support for PCEP Connection

PCE protocol (PCEP) (RFC5440) is a client-server model running over TCP/IP, where the server (PCE) opens a port and the clients (PCC) initiate connections. After the peers establish a TCP connection, they create a PCE session on top of it.

The ACL Support for PCEP Connection feature provides a way to protect a PCE server using an Access Control List (ACL) to restrict the PCC peers at the time the TCP connection is created based on the source address of client. When a client initiates the TCP connection, the ACL is referenced, and the client source address is compared. The ACL can either permit or deny the address and the TCP connection will proceed or not.

For more information about ACLs, see the Implementing Access Lists and Prefix Lists chapter in the IP Addresses and Services Configuration Guide.

For more information about the ACL Support for PCEP Connection feature, see the Configure Segment Routing Path Computation Element chapter in the *Segment Routing Configuration Guide for Cisco NCS 5500 Series Routers*.

Global Navigation Satellite System

With this release, support for Global Navigation Satellite System (GNSS) is added to NCS-55A2-MOD-SE-S Router variant. GNSS is used to describe the collection of Satellite Systems that are operating or planned.

There are many Satellite constellation systems already available. These constellations allow ground base GNSS receivers to receive radio signals from these satellites and recover accurate location and time. With GNSS receiver, clocking is changed to a flat architecture where access networks can directly take clock from satellites in the sky by using the on-board GPS chips.

Limitations

- GNSS holdover performance is 1us (micro second) in two hours of holdover after 12 hours of GNSS lock time.
- Time deviation (TDEV) fails marginally on NCS-55A2-MOD-SE-S with GNSS input.

For more information, see *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers*.

Ethernet Flow Point Visibility

The Ethernet flow point (EFP) visibility feature enables you to configure multiple VLANs in the same bridge-domain.

The EFP service instance is a logical interface that connects a bridge domain to a physical port or to an EtherChannel group. A VLAN tag identifies the EFP.

Prior to this release, only one EFP is allowed per bridge-domain. With the EFP visibility feature, you can configure a maximum of 600 EFPs per bridge-domain.

For more information refer the chapter *Configure Virtual LANs in Layer 2 VPNs* in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers, Release 6.6.x*

New Hardware Introduced in this Release

This release introduces following new hardware:

- Cisco NCS-55A2-MOD-SE-S—This chassis is a fixed port, high density, one rack unit form-factor router supports 24 SFP/SFP+ ports capable of supporting one Gigabit Ethernet or 10 Gigabit Ethernet, and 16 SFP/SFP+/SFP28 ports capable of supporting one Gigabit Ethernet, 10 Gigabit Ethernet, or 25 Gigabit Ethernet. The router also supports up to 2 modular port adapters (MPA). The router has external TCAM to support expanded Forwarding Information Base (FIB), network Access Control Lists (ACLs), and QoS for scale-enhanced configuration needs.

  For more information, see the *Hardware Installation Guide for Cisco NCS 5500 Series Fixed-Port Routers*.

- Cisco NCS-55A1-48Q6H—This chassis is a fixed port, high density, one rack unit form-factor router that supports 48 x SFP/SFP+/SFP28G ports, each capable of supporting one Gigabit Ethernet or 10 Gigabit Ethernet or 25 Gigabit Ethernet and 6 x QSFP+/QSFP28 ports each, capable of supporting 10/25 Gigabit Ethernet (via cable breakout), 40 Gigabit Ethernet, or 100 Gigabit Ethernet transceivers.

  For more information, see the *Hardware Installation Guide for Cisco NCS 5500 Series Fixed-Port Routers*.

- NC55-5516-FC2—NCS 5516 second-generation Fabric Module
- NC55-5508-FC2—NCS 5508 second-generation Fabric Module
- NC55-5516-FAN2—NCS 5516 second-generation Fan Module
- NC55-5508-FAN2—NCS 5508 second-generation Fan Module

For more information, see the *Hardware Installation Guide for Cisco NCS 5500 Series Modular Routers*.

Release 6.6.25 Packages

This table lists the Cisco IOS XR Software feature set matrix (packages) with associated filenames.

Table 2: Release 6.6.25 Packages for Cisco NCS 5500 Series Router

Composite Package		
Feature Set	**Filename**	**Description**
Cisco IOS XR IP Unicast Routing Core Bundle	ncs5500-mini-x.iso	Contains base image contents that includes: • Host operating system • System Admin boot image • IOS XR boot image • BGP packages
Individually-Installable Optional Packages		
Feature Set	**Filename**	**Description**
Cisco IOS XR Manageability Package	ncs5500-mgbl-3.0.0.0-r6625.x86_64.rpm	Extensible Markup Language (XML) Parser, Telemetry, Netconf, gRPC and HTTP server packages.
Cisco IOS XR MPLS Package	ncs5500-mpls-2.1.0.0-r6625.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r6625.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.
Cisco IOS XR Security Package	ncs5500-k9sec-3.1.0.0-r6625.x86_64.rpm	Support for Encryption, Decryption, Secure Shell (SSH), Secure Socket Layer (SSL), and Public-key infrastructure (PKI)
Cisco IOS XR ISIS package	ncs5500-isis-1.2.0.0-r6625.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf-2.0.0.0-r6625.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs5500-li-1.0.0.0-r6625.x86_64.rpm	Includes LI software images
Multicast Package	ncs5500-mcast-1.0.0.0-r6625.rpm	Support Multicast

Supported Hardware

For a complete list of hardware and ordering information, see the *Cisco NCS 5500 Series Data Sheet*

Use the Cisco Optics-to-Device Compatibility Matrix tool to determine transceivers supported in Cisco hardware devices.

To install the Cisco NCS 5500 router, see *Hardware Installation Guide for Cisco NCS 5500 Series Routers*.

Determine Software Version

To verify the software version running on the router, use **show version** command in the EXEC mode.

```
RP/0/RP0/CPU0:router# show version
Cisco IOS XR Software, Version 6.6.25
Copyright (c) 2013-2019 by Cisco Systems, Inc.

Build Information:
 Built By     : <username>
 Built On     : Wed May 29 06:59:27 PDT 2019
 Built Host   : iox-lnx-029
 Workspace    : /auto/srcarchive13/prod/6.6.25/ncs5500/ws
 Version      : 6.6.25
 Location     : /opt/cisco/XR/packages/

cisco NCS-5500 () processor
System uptime is 1 hour 35 minutes
```

Caveats

Caveats describe unexpected behavior in Cisco IOS XR Software releases. Severity-1 caveats are the most critical caveats; severity-2 caveats are less critical.

Cisco IOS XR Caveats

There are no caveats specific to Cisco IOS XR Software Release.

Caveats Specific to the NCS 5500 Routers

Caveats describe unexpected behavior in Cisco IOS XR Software releases.

Bug ID	Headline
CSCvo13825	SyncE TDEV, 1PPS TDEV are failing for TGM Performance with GNSS input
CSCvo24293	High drifts are reported with GNSS Holdover performance

Determine Firmware Support

Use the **show hw-module fpd** command in EXEC mode to view the hardware components with their current FPD version and status. The status of the hardware must be CURRENT; Running and Programed version must be the same.

```
(sysadmin-vm)#show hw-module fpd
                                                                    FPD Versions
                                                                    =================
Location   Card type         HWver FPD device       ATR Status   Running Programd
-------------------------------------------------------------------------------
0/0        NC55-36X100G-A-SE 1.0   MIFPGA              CURRENT    0.03    0.03
0/0        NC55-36X100G-A-SE 1.0   Bootloader          CURRENT    0.14    0.14
0/0        NC55-36X100G-A-SE 1.0   DBFPGA              CURRENT    0.14    0.14
0/0        NC55-36X100G-A-SE 1.0   IOFPGA              CURRENT    0.21    0.21
```

```
0/0      NC55-36X100G-A-SE 1.0   SATA               CURRENT    5.00    5.00
0/1      NC55-36X100G      1.0   MIFPGA             CURRENT    0.09    0.09
0/1      NC55-36X100G      1.0   Bootloader         CURRENT    1.19    1.19
0/1      NC55-36X100G      1.0   IOFPGA             CURRENT    0.15    0.15
0/2      NC55-36X100G-S    0.4   MIFPGA             CURRENT    0.07    0.07
0/2      NC55-36X100G-S    0.4   Bootloader         CURRENT    1.14    1.14
0/2      NC55-36X100G-S    0.4   IOFPGA             CURRENT    0.11    0.11
0/2      NC55-36X100G-S    0.4   SATA               CURRENT    5.00    5.00
0/5      NC55-36X100G      1.1   MIFPGA             CURRENT    0.09    0.09
0/5      NC55-36X100G      1.1   Bootloader         CURRENT    1.19    1.19
0/5      NC55-36X100G      1.1   IOFPGA             CURRENT    0.15    0.15
0/5      NC55-36X100G      1.1   SATA               CURRENT    5.00    5.00
0/6      NC55-6X200-DWDM-S 0.0   DENALI0            CURRENT   13.48   13.48
0/6      NC55-6X200-DWDM-S 0.0   DENALI1            CURRENT   13.48   13.48
0/6      NC55-6X200-DWDM-S 0.0   DENALI2            CURRENT   13.48   13.48
0/6      NC55-6X200-DWDM-S 0.0   MORGOTH            CURRENT    5.25    5.25
0/6      NC55-6X200-DWDM-S 0.0   MSFPGA0            CURRENT    2.22    2.22
0/6      NC55-6X200-DWDM-S 0.0   MSFPGA1            CURRENT    2.22    2.22
0/6      NC55-6X200-DWDM-S 0.0   MSFPGA2            CURRENT    2.22    2.22
0/6      NC55-6X200-DWDM-S 0.6   Bootloader         CURRENT    1.14    1.14
0/6      NC55-6X200-DWDM-S 0.6   IOFPGA             CURRENT    0.11    0.11
0/6      NC55-6X200-DWDM-S 0.6   SATA               CURRENT    5.00    5.00
0/RP0    NC55-RP-E         0.4   Bootloader         CURRENT    1.20    1.20
0/RP0    NC55-RP-E         0.4   IOFPGA             CURRENT    0.23    0.23
0/RP0    NC55-RP-E         0.4   OMGFPGA            CURRENT    0.48    0.48
0/RP1    NC55-RP-E         0.4   Bootloader         CURRENT    1.20    1.20
0/RP1    NC55-RP-E         0.4   IOFPGA             CURRENT    0.23    0.23
0/RP1    NC55-RP-E         0.4   OMGFPGA            CURRENT    0.48    0.48
0/FC0    NC55-5508-FC      1.1   Bootloader         CURRENT    1.74    1.74
0/FC0    NC55-5508-FC      1.1   IOFPGA             CURRENT    0.16    0.16
0/FC2    NC55-5508-FC      0.205 Bootloader         CURRENT    1.74    1.74
0/FC2    NC55-5508-FC      0.205 IOFPGA             CURRENT    0.16    0.16
0/FC4    NC55-5508-FC      1.1   Bootloader         CURRENT    1.74    1.74
0/FC4    NC55-5508-FC      1.1   IOFPGA             CURRENT    0.16    0.16
0/FC5    NC55-5508-FC      0.106 Bootloader         CURRENT    1.74    1.74
0/FC5    NC55-5508-FC      0.106 IOFPGA             CURRENT    0.16    0.16
0/SC0    NC55-SC           1.5   Bootloader         CURRENT    1.74    1.74
0/SC0    NC55-SC           1.5   IOFPGA             CURRENT    0.10    0.10
0/SC1    NC55-SC           1.4   Bootloader         CURRENT    1.74    1.74
0/SC1    NC55-SC           1.4   IOFPGA             CURRENT    0.10    0.10
```

Note The FPD versions on board shipped by manufacturer may have higher versions than the FPD package integrated in the IOS XR.

Other Important Information

- The total number of bridge-domains (2*BDs) and GRE tunnels put together should not exceed 1518.

  Here the number 1518 represents the multi-dimensional scale value.

- The offline diagnostics functionality is not supported in NCS 5500 platform. Therefore, the **hw-module service offline location** command will not work. However, you can use the **(sysadmin)# hw-module shutdown location** command to bring down the LC.

- The warning message that the smart licensing evaluation period has expired is displayed in the console every hour. There is, however, no functionality impact on the device. The issue is seen on routers that do not have the Flexible Consumption licensing

model enabled. To stop the repetitive messaging, register the device with the smart licensing server and enable the Flexible Consumption model. Later load a new registration token.

To register the device with the smart licensing server, follow the instructions provided in this link: Register and Activate Your Device.

However, if you do not want to enable the Flexible Consumption licensing model then install the CSCvk45026 SMU to stop the repetitive messages.

Supported Transceiver Modules

To determine the transceivers that Cisco hardware device supports, refer to the Transceiver Module Group (TMG) Compatibility Matrix tool.

Supported Modular Port Adapters

For the compatibility details of Modular Port Adapters (MPAs) on the line cards, see the datasheet of that specific line card.

Upgrading Cisco IOS XR Software

Cisco IOS XR Software is installed and activated from modular packages, allowing specific features or software patches to be installed, upgraded, or downgraded without affecting unrelated processes. Software packages can be upgraded or downgraded on all supported card types, or on a single card (node).

The upgrade document (NCS5500_Upgrade_Downgrade_MOP_6.6.25.pdf) is available along with the software images.

Before starting the software upgrade, use the **show install health** command in the admin mode. This command validates if the statuses of all relevant parameters of the system are ready for the software upgrade without interrupting the system.

Related Documentation

The most current Cisco Network Convergence System 5500 Series documentation is located at this URL:

http://www.cisco.com/c/en/us/support/routers/network-convergence-system-5500-series/tsd-products-support-series-home.html

The document containing Cisco IOS XR System Error Messages (SEM) is located at this URL:

https://www.cisco.com/c/en/us/td/docs/ios_xr_sw/error/message/ios-xr-sem-guide.html

Production Software Maintenance Updates (SMUs)

A production SMU is a SMU that is formally requested, developed, tested, and released. Production SMUs are intended for use in a live network environment and are formally supported by the Cisco TAC and the relevant development teams. Software bugs identified through software recommendations or Bug Search Tools are not a basis for production SMU requests.

For information on production SMU types, refer the Production SMU Types section of the IOS XR Software Maintenance Updates (SMUs) guide.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Full Cisco Trademarks with Software License

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.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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.