Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 6.5.1

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 6.5.1 is a limited availability (LA) release. All Cisco IOS XR Release 6.5.1 features are available in Cisco IOS XR Release 6.5.3, which is a general availability (GA) release. For more information on IOS XR Release 6.5.3, see Release Notes for Cisco NCS 5500 Series Routers, Release 6.5.3

Cisco Feature Deployment Recommendation

In evaluating the use of features in the Cisco IOS XR Release 6.5.1, consider the below classification of features before deploying:

- Category 1—Features are ready for full scale deployment.
- Category 2—Feature behavior will be strengthened with a SMU as needed.
- Category 3—Features are recommended only for EFT and Lab Certification. Large scape deployment will be supported in future releases.

Please contact the Cisco Deployment team or your Account Team to understand whether the features you are implementing are ready for deployment in your network.

For detailed list of Category 1, Category 2 and Category 3 features, see List of Cisco Software Features Recommended for Deployment, on page 13.

Software Features Introduced in this Release

Global Weighted SRLG Protection

A shared risk link group (SRLG) is a set of links sharing a common resource and hence shares the same risk of failure. The current implementation of SRLG protection considers only the directly connected links. Hence, if the router that computes the backup path includes a link that is not directly connected but shares the same SRLG, the SRLG protection fails. The global weighted SRLG

protection feature provides better path selection for the SRLG by associating a weight with the SRLG value and using the weights of the SRLG values while computing the backup path.

For more information about configuring the global weighted SRLG protection feature, see *MPLS Configuration Guide for Cisco NCS 5500 Series RoutersRouting Configuration Guide for Cisco NCS5500 Series Routers* .

BGP Flow Specification version 4 and version 6

BGP Flow Specification version 4 and version 6 feature allows you to receive IPv4 and IPv6 traffic flow specifications and actions that need to be taken on that traffic through BGP update. This feature allows you to rapidly deploy and propagate filtering and policing functionality among a large number of BGP peer routers to mitigate the effects of a distributed denial-of-service (DDoS) attack over your network.

For more informnation about the feature, see the chapter *Implementing BGP* in the *BGP Configuration Guide for Cisco NCS 5500 Series Routers*.

Persistent Interface Shutdown

Prior to Cisco IOS XR Release 6.5.1, the configurations committed in a newly created interface are lost when:

- you do not issue **no shutdown** command to remove the default shutdown config, and
- you issue **no shutdown** command and reload the router.

From Release 6.5.1, onwards, automatic shutdown config behavior is persistent and configurations are intact whether or not the default shhutdown config is removed and even if the router is reloaded.

For more information on the feature, see *interface (global)* command in the *Global Interface Commands* chapter of the *Interface and Hardware Component Command Reference for Cisco NCS 5500 and NCS 540 and NCS 560 Series Routers*

Autobandwidth Bundle TE++

The MPLS-TE auto-bandwidth feature allows to resize the tunnels based on the measured traffic load. The autobandwidth bundle TE++ feature is an extension of the auto-bandwidth feature. This feature allows to automatically increase or decrease the number of MPLS-TE tunnels to a destination based on real time traffic needs. Hence, this feature helps to avoid large LSPs and enables load sharing the traffic between source and destination.

For more information about configuring the Autobandwidth bundle TE++ feature, see *MPLS Configuration Guide for Cisco NCS 5500 Series Routers*.

Validate Commit Check

Before committing a configuration, the overall configuration can be validated. This helps remove conflicts when the configurations within a single commit operation are interdependent.

For information about enabling and running the command, see *Bring-up the Router* chapter in System Setup and Software Installation Guide for NCS 5500 Series Routers, IOS XR Release 6.5.x.

MPLS over GRE Hashing

The **hw-module profile load-balance algorithm** command provides the ability to modify the hashing algorithm used for ECMP and bundle member selection. Effective with Cisco IOS XR release 6.5.1, this command is enhanced to include GPRS tunneling protocol (GTP) mode which allows hashing based upon the tunnel id in GTP-U packets.

For more information about the **hw-module profile load-balance algorithm** command, see *Interface and Hardware Component Command Reference for Cisco NCS 5500 and NCS 540 and NCS 560 Series Routers*.

Point-to-Multipoint Traffic-Engineering

Label switched multicast (LSM) is an MPLS technology extension to support multicast using label encapsulation.The label encapsulation could be either point-to-multipoint (P2MP) label switched paths (LSPs) or multipoint-to-multipoint (MP2MP) LSPs. For creating multicast LSPs, two protocol extensions can be used. The RSVP-TE protocol is extended to signal P2MP LSPs across the MPLS networks which is known as P2MP RSVP-TE. Multicast Label Distribution Protocol (MLDP) provides extensions to the label distribution protocol (LDP) for the setup of P2MP and MP2MP LSPs.The point-to-multipoint traffic-engineering (P2MP-TE) feature implements P2MP RSVP-TE on Cisco NCS 5500 series routers.

For more information about configuring the P2MP-TE feature, see *MPLS Configuration Guide for Cisco NCS 5500 Series Routers*.

Global LLDP Knob to Enable LLDP Configuration

Earlier, in IOS-XR platforms, LLDP was enabled only with global LLDP configuration and administrators had to manually disable each interface.

With this feature, you can now enable the global LLDP configuration per-interface basis. To enable the feature, you must make the necessary configuration changes. For more information on the feature, see the *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers*.

QoS Policy Propagation via BGP

QoS Policy Propagation via BGP (QPPB,) is a mechanism that allows propagation of quality of service (QoS) policy and classification by the sending party based on access lists, community lists and autonomous system paths in the Border Gateway Protocol (BGP), thus helping to classify based on destination instead of source address.

With the enablement of this feature, you can configure QPPB on NCS 5500. For more information on the feature, see *Modular QoS Configuration Guide for Cisco NCS 5500 Series Routers*.

MAC Address Scale Increase

A device can contain up to 128K MAC address entries. A bridge domain on a device can contain up to 65K MAC address entries.

Multiple Spanning Tree Access Gateway (MSTAG)

The Multiple Spanning Tree Access Gateway (MSTAG) feature provides a mechanism to block the redundant path to avoid a loop. This feature enables the provider edge (PE) devices to flush the MAC addresses over VPLS network to prevent unreported traffic drops.

For more information on this feature, see the *Configure Multiple Spanning Tree Protocol* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.5.1*.

Resilient Ethernet Protocol Access Gateway (REPAG)

The Resilient Ethernet Protocol Access Gateway (REPAG) feature provides a mechanism to block the redundant path to avoid a loop. This feature enables the provider edge (PE) devices to flush the MAC addresses over VPLS network to prevent unreported traffic drops.

The REPAG feature provides the same functionality as MSTAG, but in REPAG the access network runs REP and not multiple spanning tree (MST) protocol.

For more information on this feature, see the *Configure Multiple Spanning Tree Protocol* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.5.1*.

Service cli submode-exit Configuration

XR-VM supported a global configuration to exit service cli submode on all configuration session for all Virtual Terminal Type lines (VTY) earlier. But, you would need a knob to enable this feature specific to a VTY.

Cisco IOS XR now supports a configuration to exit service cli submode on all interactive configuration sessions for each VTY using terminal commands. The command, **terminal cli submode-exit** lets you enable or disable submode-exit on all interactive configuration sessions for each VTY. You can use the **show cli submode-exit status** command to check the status of the configuration.

Golden ISO

Prior to Cisco IOS XR Release 6.5.1, the Golden ISO image had to be downloaded the second time for gaining access to the required RPMs and XR configurations.

From Cisco IOS XR Release 6.5.1, the required RPMs and XR configurations are embedded in the Initial RAM disk (INITRD) and are available in the first download of the ISO image. Access to all the additional RPMs and XR configurations are available when the system boots on the first download of the ISO image.

iPXE HTTPS

The iPXE HTTPS feature enables the user to network boot an XR image using HTTPS protocol. Prior to Cisco IOS XR Release 6.5.1, only HTTP and TFTP protocols could be used.

G.8275.2 PTP Profile Support

Cisco NCS 5500 Series Routers support G.8275.2 PTP Telecom Profile from Release 6.5.1 onwards. The G.8275.2 is a PTP profile for use in telecom networks where phase or time-of-day synchronization is required. It differs from G.8275.1 in that, it is not required that each device in the network participates in the PTP protocol. Also, G.8275.2 uses PTP over IPv4 and IPv6 in unicast mode.

The G.8275.2 profile is based on the partial timing support from the network. Hence, nodes using G.8275.2 are not required to be directly connected.

For more information on G.8275.2 profile and other related details, see *Configuring Precision Time Protocol* chapter in *System Management Configuration Guide for Cisco NCS 5500 Series Routers*.

Timing Support

Timing features are supported on the following hardware PIDs in Release 6.5.1:

- Chassis: NCS-5504, NCS-5508, NCS-5516, NCS-5501-SE, NCS-55A2-MOD-HD-S, NCS-55A2-MOD-S
- RP: NC55-RP-E
- Line card: NC55-MOD-A-S
- MPA: NC55-MPA-2TH-S, NC55-MPA-1TH2H-S, NC55-MPA-1TH2H-HD-S, NC55-MPA-4H-S, NC55-MPA-4H-HD-S, NC55-MPA-12T-S

For more information on PTP and other related details, see *Configuring Precision Time Protocol* chapter in *System Management Configuration Guide for Cisco NCS 5500 Series Routers*.

RPF Vector Encoding

RPF vector is a PIM proxy that lets core routers without RPF information forward join and prune messages for external sources (for example, a MPLS-based BGP-free core, where the MPLS core router is without external routes learned from BGP). The RPF vector encoding is now compatible with the new IETF encoding. Use the **rpf-vector use-standard-encoding** command to enable the feature.

For more information on RPF, see the *Implementing Layer-3 Multicast Routing* chapter in the *Multicast Configuration Guide for Cisco NCS 5500 Series Routers*

Resilient Hashing and Flow Auto-Recovery

Resilient Hashing and Flow Auto-Recovery feature provides an option to selectively override the default equal cost multipath (ECMP) behavior during a ECMP path failure. This feature enables the redirection of flows through inactive links only and the prevention of all existing flows from being rehashed to a new link. This feature also provides an option to recover a link or a server when it comes back so it can be reused for sessions.

For more informnation about the feature, see the chapter *Implementing BGP* in the *BGP Configuration Guide for Cisco NCS 5500 Series Routers*.

BGP PIC Edge for IP and MPLS-VPN

The BGP PIC (Prefix Independent Convergence) Edge for IP and MPLS-VPN feature improves BGP convergence after a network failure. This convergence is applicable to both core and edge failures and can be used in both IP and MPLS networks. When a failure is detected, the backup or alternate path immediately takes over, thus enabling fast failover.

For more informnation about the feature, see the chapter *Implementing BGP* in the *BGP Configuration Guide for Cisco NCS 5500 Series Routers*.

PCE-Initiated Segment Routing Policies

You can configure an SR-TE policy on the path computation element (PCE) to reduce link congestion or to minimize the number of network touch points.

The PCE collects network information, such as traffic demand and link utilization. When the PCE determines that a link is congested, it identifies one or more flows that are causing the congestion. The PCE finds a suitable path and deploys an SR-TE policy to divert those flows, without moving the congestion to another part of the network. When there is no more link congestion, the policy is removed. The PCE deploys the SR-TE policy using PCC-PCE communication protocol (PCEP).

For more information on this feature, see the Configure SR-TE Policies chapter in the *Segment Routing Configuration Guide for Cisco NCS 5500 Series Router*.

Fallback VRF

Virtual Routing and Forwarding (VRF) is an IP technology that allows multiple instances of a routing table to co-exist on the same router at the same time. In ACL-based forwarding, which forwards traffic to a VRF, a static default is used to direct traffic to the global routing table. However, such traffic, before being directed to the global routing table requires an explicit next hop and creates a sub-optimal routing.

This feature enables the configuration of a fallback VRF. Therefore, when destination prefix of a data packet does not match any routes in the configured VRF, the fallback VRF table can be used to route packets. The fallback VRF can be the global table itself or another non-global VRF.

For more information about the feature, see the chapter *Implementing Network Stack IPv4 and IPv6* in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*.

For more information on the commands on this feature, see the chapter *Network Stack IPv4 and IPv6 Commands* in the *IP Addresses and Services Command Reference for Cisco NCS 5500 Series and NCS 540 and NCS 560 Series Routers*.

MLDP on Edge Routers

The Multicast Label Distribution Protocol (MLDP) feature is enhanced to support the edges; that is, the encapsulation (headend) and the decapsulation (tailend) at the Provider Edge (PE) devices. The MLDP Edge feature enables service providers to extend the existing MPLS backbone network for multicast services. This feature extends the functionality from midpoint to support the edges - the headend and the tailend.

Earlier than Cisco IOS XR Release 6.5.1, MLDP VRF In-band Signaling (profile 6) and Global Inband Signaling (Profile 7) was supported only at the core, now it is supported on the edge as well.

For more information about this feature, see *Implementing Multicast* Chapter of the *Multicast Configuration Guide for Cisco NCS 5500 Series Routers*.

VLAN Switch

The VLAN Switch feature enables you to configure L2 VLAN switching with minimum configuration. This feature allows you to configure L2 bridging without having to configure and manage separate bridge instances and sub-interfaces for each per VLAN L2 forwarding domain.

Prior to implementation of this feature, to configure and manage basic L2 bridging, numerous sub-interfaces were required. Using separate sub-interfaces for each VLAN on a port overloads the system scalability and consumes hardware resources, slows down provisioning, and makes the device harder to manage due to the large number of sub-interface constructs that exists in the system.

For more information on this feature, see the *Configure Virtual LANs in Layer 2 VPNs* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers*.

Split Horizon Group 2

The Split Horizon Group 2 feature allows you to prevent Broadcast, Unknown unicast and Multicast (BUM) and known unicast traffic to be flooded from one attachment circuit (AC) to other AC within the bridge domain. This feature enables efficient bandwidth allocation and resource optimization.

For more information on this feature, see the *Configure Point-to-Point Layer 2 Services* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers*.

G.8032 Ethernet Ring Protection

The G.8032 Ethernet Ring Protection feature provides protection for Ethernet traffic in a ring topology. This feature prevents loops within the ring at the Ethernet layer by blocking either a pre-determined link or a failed link.

For more information on this feature, see the *Configure Point-to-Point Layer 2 Services* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers*.

EVPN MPLS Seamless Integration with VPLS

Seamless integration of EVPN MPLS with VPLS enables the co-existence of PE nodes running EVPN and VPLS for the same VPN instance. VPLS or legacy network can be upgraded to the next generation EVPN network without service disruption. You can introduce EVPN service on all the selected VPLS provider edge (PE) nodes simultaneously. However, to avoid traffic disruption, provision EVPN service on existing VPLS-enabled PEs one by one.

For more information on this feature, see the *EVPN Features* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers*.

EVPN Single-Active Multi-Homing

The EVPN Single-Active Multi-Homing feature supports single-active redundancy mode. In single-active mode, the provider edge (PE) nodes locally connected to an Ethernet Segment load balance traffic to and from the Ethernet Segment based on EVPN service instance (EVI). Within an EVPN service instance, only the Designated Forwarder (DF) PE forwards traffic to and from the Ethernet Segment.

Usability Enhancements for ACL YANG Models

This feature addresses some of the issues identified with native ACL YANG models that affect usability of the YANG model. It improves user-friendliness and standards compliance in the following ACL YANG models:

- Cisco-IOS-XR-es-acl-cfg
- Cisco-IOS-XR-ipv4-acl-cfg
- Cisco-IOS-XR-ipv6-acl-cfg

For more information about issues addressed as part of this enhancement, see *Components to Use Data Models* chapter of the *Programmability Configuration Guide for Cisco NCS 5500 Series Routers*.

Telemetry over gNMI subscribe RPC

Cisco IOS XR supports Google network management interface (gNMI) protocol in dial-in mode where the client establishes a connection to the router. gNMI is an unified mangement protocol for streaming telemetry data using OpenConfig RPC framework. This framework and protocol does not need explicit configuration, but simplifies telemetry configuration on the router by only starting the gRPC server.

In addition, support is provided for transport layer security (TLS) ciphers in gRPC session. Two new gRPC configuration parameters `max-streams` and `max-streams-per-user` are provided to stream only the gRPC-specific requests.

To enable the gRPC server in dial-in mode, see *Configure Model-driven Telemetry* chapter in *Telemetry Configuration Guide for Cisco NCS 5500 Series Routers*.

OSPF Authentication with Keychain

OSPF Authentication with Keychain feature enables the support of Hashed Message Authentication Code (HMAC) during OSPF authentication. New crypto algorithms such as, HMAC-SHA-256 and HMAC-SHA1-96 are added under key-chain infra as part of this feature. These algorithms provide more secured authentication.

Keychains can be configured at different levels of OSPF like at the router level, or the area level, or the interface level.

For more information about OSPF Authentication, see *Implementing OSPF* Chapter of the *Routing Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.5.x*.

For more information about Keychain configuration, see *Implementing Keychain Management* Chapter of the *System Security Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.5.x*

Minimum Remaining Lifetime for IS-IS

The Minimum Remaining Lifetime for IS-IS feature helps to maintain the stability of the network when the *Remaining Lifetime* field in a Link State Protocol (LSP) is corrupted. Corruption of the *Remaining Lifetime* field in a LSP data unit can go undetected. In

certain scenarios, this may cause or exacerbate flooding of LSPs. This feature resolves this problem by enabling IS-IS to reset the *Remaining Lifetime* value of the received LSP, to the maximum LSP lifetime (1200 seconds), if the *Remaining Lifetime* value of the received LSP is less than the maximum LSP lifetime configured in a local node. If the received LSP lifetime value is less than the Zero Age Lifetime (60 seconds), IS-IS generates an error message indicating that it's a corrupted lifetime event.

IS-IS saves the received *Remaining Lifetime* value in LSP database. The value is shown in the **show isis database** command output under the **Rcvd** field.

For more information about the **show isis database** command, see *IS-IS Commands* Chapter of the *Routing Command Reference Guide*.

For more information about this feature, see *Implementing IS-IS* Chapter of the *Routing Configuration Guide for Cisco NCS 5500 Series Routers*.

Layer 2 Adjacency SID

An adjacency SID is typically associated with a Layer 3 adjacency to a neighboring node. If you have Layer 2 bundle interfaces, where multiple physical interfaces form a bundle interface, the individual Layer 2 bundle members are not visible to IGP; only the bundle interface is visible.

The Layer 2 Adjacency SID feature provides adjacency SID functionality for individual bundle members. This feature allows you to track the availability of individual bundle member links and to verify the segment routing forwarding over the individual bundle member links, for Operational Administration and Maintenance (OAM) purposes. A Layer 2 adjacency SID can be allocated dynamically or configured manually.

For more information on this feature, see the Configure Segment Routing for IS-IS Protocol chapter in the *Segment Routing Configuration Guide for Cisco NCS 5500 Series Routers*.

Segment Routing-Specific Drop Counter

When a router is part of an RSVP-TE network and an segment routing (SR) network, the Multiprotocol Label Switching (MPLS) drop counters do not indicate if the dropped packets are in an RSVP-TE network or an SR network. The **show cef mpls drops** command displays MPLS drop counters for packets that belong to a segment routing (SR) network.

The incoming top MPLS label is inspected. If the label belongs to the Segment Routing Local Block (SRLB) or the Segment Routing Global Block (SRGB), an MPLS SR drop counter is incremented for unknown label value.

For more information on this command, see the Cisco Express Forwarding Commands chapter in the *IP Addresses and Services Command Reference for Cisco NCS 5500 Series and NCS 540 Series Routers*.

Purge Originator Identification TLV for IS-IS

At present, an IS-IS purge does not contain any information to identify the Intermediate System (IS) that generates the purge. This makes it difficult to locate the source IS.

To address this issue, the Purge Originator Identification (POI) TLV for IS-IS feature defines a type, length, and value (TLV) that can be added to the purges, to record the system ID of the IS that had initiated the purge. This makes it easier to locate the origin of the purge and its cause. If you are using cryptographic authentication, then the **enable-poi** keyword in **lsp-password** command must be enabled to insert the Purge Originator Identification (POI). If you are not using cryptographic authentication, then the POI is inserted by default. This TLV is also helpful in lab environments.

For more information about this feature, see *Implementing IS-IS* Chapter of the *Routing Configuration Guide for Cisco NCS 5500 Series Routers*.

Master Key Tuple Configuration

This feature specifies the TCP Authentication Option (TCP-AO) that replaces the TCP MD5 option. TCP-AO uses the Message Authentication Codes (MACs), which provides the following:

- protection against replays for long-lived TCP connections
- more details on the security association with TCP connections than TCP MD5
- a larger set of MACs with minimal other system and operational changes.

Cisco provides the MKT configuration by means of the following configurations:

- keychain configuration
- tcp tcp-ao keychain configuration

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

VRRP over BVI

The Virtual Router Redundancy Protocol (VRRP) protocol provides default gateway redundancy. Configuring VRRP enables a group of routers to behave as a single virtual default gateway router in which one router acts as the primary router and other routers act as Backup.

BVI (Bridge-Group Virtual Interface) is a virtual interface which provides L3 or routed functionality to a Bridge Group. L2 functionality is applicable to the interfaces which are part of a Bridge Group and BVI is the routed interface for that Bridge Group.

VRRP sessions run on top of interfaces of the multiple routers which are in the same home network. This feature enables the configuration of a VRRP session over BVI. Therefore, instead of physical interfaces, VRRP sessions can run between BVI interfaces of multiple routers.

For more information about the feature, see the chapter *Configure IPv6 ACL-based LPTS Policers* in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*.

Segment Routing Traffic Engineering Policies with Autoroute Include

Segment Routing Traffic Engineering (SR-TE) policies configured with Autoroute Include allow you to steer specific IGP (IS-IS, OSPF) prefixes over non-shortest paths and to divert the traffic for those prefixes on to the SR-TE policy. Autoroute Include applies Autoroute Announce functionality to the specified destinations or prefixes. The Autoroute SR-TE policy adds the prefixes into the IGP, which determines if the prefixes on the endpoint or downstream of the endpoint are eligible to use the SR-TE policy. If a prefix is eligible, then the IGP checks if the prefix is listed in the Autoroute Include configuration. If the prefix is included, then the IGP downloads the prefix route with the SR-TE policy as the outgoing path.

For more information on this feature, see the Configure SR-TE Policies chapter in the *Segment Routing Configuration Guide for Cisco NCS 5500 Series Router*.

SR-TE Color-Only Steering

A segment routing traffic engineering (SR-TE) policy is identified as an ordered list (head-end, color, end-point). The color-only steering feature is a traffic steering mechanism where a policy is created with a given color, regardless of the endpoint. You can create an SR-TE policy for a specific color that uses a NULL end-point (**ipv4 0.0.0.0** for IPv4 NULL, and **ipv6 ::0** for IPv6 NULL end-point), which minimizes the number of SR-TE policies required at a headend to forward traffic for a given address family.

You can also configure a color-only (CO) flag (**co-flag 00** and **co-flag 01**) for color-only steering (NULL end-point) as part of the color extended community in BGP for overlay routes. The CO flag allows the selection of an SR-TE policy with a matching color, regardless of the endpoint.

For more information on this feature, see the Configure SR-TE Policies chapter in the *Segment Routing Configuration Guide for Cisco NCS 5500 Series Router*.

SR-TE Address-Family Agnostic Steering

Address-family agnostic steering uses an SR-TE policy to steer both labeled and unlabeled IPv4 and IPv6 traffic. This steering mechanism relies on color-only steering and requires support of IPv6 encapsulation (IPv6 caps) over IPV4 endpoint policy, which is enabled automatically when the policy is created in XTC. The result is that you can have a single SR-TE policy to forward traffic, regardless of the address-family.

For more information on this feature, see the Configure SR-TE Policies chapter in the *Segment Routing Configuration Guide for Cisco NCS 5500 Series Router*.

IS-IS Authentication with Keychain

IS-IS Authentication with Keychain feature enables the support of Hashed Message Authentication Code (HMAC) and Cipher-based Message Authentication Code (CMAC) during IS-IS authentication. New cryptographic algorithms such as, AES-128-CMAC-96, HMAC-SHA-256, and HMAC-SHA1-96 are added under Keychain infra as part of this feature. These algorithms provide more secured authentication.

Keychains can be configured at the router level (in case of the **lsp-password** command) and at the interface level (in case of the **hello-password** command) within IS-IS. These commands refer to the global keychain configuration and instruct the IS-IS protocol to obtain security parameters from the global set of configured keychains.

For more information about Keychain configuration, see *Implementing Keychain Management* Chapter of the *System Security Configuration Guide for Cisco NCS 5500 Series Routers*.

Enhancements to Programmability

Cisco IOS XR supports programmability of `OC NI`, `OC local routing`, `OC-MPLS`, `OC-RSVP-SR`, `OC-RPL` and `OC-BGP-Policy` OpenConfig data models for configuration and operational data.

For more information about YANG data models and configuration, see *Using Data Models* chapter in *Programmability Configuration Guide for Cisco NCS 5500 Series Routers*

Enhancements to ZTP

The following enhancements are introduced in Release 6.5.1:

- During the fresh boot, to establish a secured connection with DHCP server, authentication is performed on data ports through DHCP option 43 for IPv4 and option 17 for IPv6. These DHCP options are defined in option space and included within **dhcpd.conf/dhcpd6.conf** configuration files.
- During the fresh boot of a router auto ZTP process is initiated from the management port and switches to data port when:
    - ZTP does not find an active interface,
    - delay in DHCP response, and
    - ZTP encounters an error.

Note The auto breakout mode is not supported.

- During fresh boot of the router or manual invocation of ZTP, IPv6 is enabled on all dataports (in dataport mode).
- The log file **ztp.log** is saved in **/var/log** folder, and a copy of log file is available at **/disk0:/ztp/ztp.log** location using a soft link. However, executing **ztp clean** command clears files saved on disk and not on **/var/log** folder where current ZTP logs are saved. In order to have a log from current ZTP run, you must manually clear the ZTP log file from **/var/log/** folder.
- When ZTP process encounters any error, or when ZTP quits or terminates, it reverts to the initial configuration that exists before starting of ZTP process.

For more information on Auto ZTP feature, see the chapter *Configuring Zero Touch Provisioning* in the *System Management Configuration Guide for Cisco NCS 5500 Series Routers*

Replace Installed Files with Golden ISO

Golden ISO (GISO) upgrades to a version that has a predefined list of software maintenance update (SMUs) with a single operation. However, to update to the same version with a different set of SMUs requires a two-step process. This two-step process can be avoided using the `install update replace` functionality to replace the currently active version with the full package including the image and SMUs from the newly added GISO.

For information about the functionality and configuration, see *Customize Installation using Golden ISO* chapter in the System Setup and Software Installation Guide for NCS5500 Series Routers, IOS XR 6.5.x.

Support for MTU Size 9646 Bytes

Cisco NCS 5500 supports MTU packet size up to 9646 bytes for physical and bundle interfaces.

Pseudowire Redundancy

The Pseudowire Redundancy feature allows you to configure a redundant pseudowire that backs up the primary pseudowire. When the primary pseudowire fails, the PE router switches to the redundant pseudowire. You can elect to have the primary pseudowire resume operation after it becomes functional. The primary pseudowire fails when the PE router fails or when there is a network outage.

For more information on this feature, see the *Configure Point-to-Point Layer 2 Services* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers*.

IS-IS Distribute List

This feature allows users to specify a filter based on destination prefix list or route policy, and use that filter to prevent routes computed by Intermediate System-to-Intermediate System (IS-IS) from being installed in the Routing Information Base (RIB).

When distribute-list in command is configured, some routes that IS-IS computes are not installed in the forwarding plane of the local router, but other IS-IS routers will not be aware of this. This introduces a difference between the forwarding state computed by other IS-IS routers and the actual forwarding state on this router. In some cases, this could lead to traffic being dropped or looped. Hence, be careful about when to use this command.

For more information about the **distribute-list in** command, see *Routing Command Reference Guide*.

For more information about this feature, see *Implementing IS-IS* Chapter of the *Routing Configuration Guide for Cisco NCS 5500 Series Routers*.

NRSSVR Process Infra Hardening on Repeated Configuration Commits

This feature provides resolution to prevent RDSFS process crash, and memory leakage at Name Registration Service (NRS) and Replicated Data Services File System (RDSFS) Server due to *large number of configuration commits*. To achieve this, nrs_purge API is enhanced to purge the NRS handles for files that are already deleted. This resolution provides significant improvements in the following aspects:

- Enables a large number of configuration commits, without any issues
- Ensures lower memory consumption for NRS server and RDSFS processes.
- Prevents the need to reload the router when it has to recover from the following scenarios:
  - Continuous restarting or crashing of RDSFS processes
  - Not being able to commit any configurations

Enhancement to the Port Mode Configuration

From Release 6.5.1 onwards, the following modulations are supported while configuring port mode speed:

- 8qam
- 16qam
- qpsk

For more information on configuring port modes, see the *Configuring Controllers* chapter in the *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers*.

For more information on the **port-mode** command, see the *Controller Commands* chapter in the *Interface and Hardware Component Command Reference for Cisco NCS 5500 and NCS 540 and NCS 560 Series Routers*.

List of Cisco Software Features Recommended for Deployment

Category-1

- 1XCFP2 and 2XQSFP28 MPA
- BGP PIC Edge for IP and MPLS-VPN
- BGP Flow Specification version 4 and version 6
- Dark bandwidth-Reduced telemetry interval (10s)
- Enhancements to Programmability
- Global LLDP Knob to Enable LLDP Configuration
- ISIS Authentication with keychain
- Master Key Tuple Configuration
- MPA - 4XQSFP28
- MPLS over GRE Hashing

- Multiple Spanning Tree Access Gateway (MSTAG)
- NETCONF Install YANG Actions
- NCS-55A2-MOD
- NCS55-MOD-LC
- OSPF Authentication with Keychain
- Persistent Interface Shutdown
- QoS Policy Propagation via BGP
- Remove constraint on number of containers that can be resolved
- Resilient Ethernet Protocol Access Gateway (REPAG)
- Resilient Hashing and Flow Auto-Recovery
- Service CLI Submode-exit Configuration
- Support for BGP, ISIS, Interface, RPL, BMP, Flex CLI, XML config, MPLS-TE
- Telemetry over gNMI subscribe RPC
- Timing Support-G.8275.2, G.8273.2 and G.8275.1 Profile
- Usability Enhancements for ACL YANG Models
- VRRP over BVI

Category-2

- Autobandwidth Bundle TE++
- BGP-PIC Edge
- CFM rewrite EFP (push and pop tag enablement)
- FIB Optimization for SE (ECMP-FEC Reuse)
- Enhancements to ZTP
- Global Weighted SRLG Protection
- G.8032 Ethernet Ring Protection
- IS-IS Distribute List
- MAC Address Scale Increase
- Minimum Remaining Lifetime for IS-IS
- MLDP on Edge Routers
- MPA - 12X10G
- MPLS-Change auto-bandwidth RSVP minimun reservation after tunnel flap
- Point-to-Multipoint Traffic-Engineering

- PCE Initiated LSPs
- Pseudowire Redundancy
- Replace Installed Files with Golden ISO
- Segment Routing-Specific Drop Counter
- SRTE FIB Installation Performance
- Split Horizon Group 2
- SR-TE Color-Only Steering
- SR-PCE: Scalability to 10K Nodes/LSPs, 100K Links, 2K PCEP Sessions
- VLAN Switch

Category-3

- EVPN Single-Active Multi-Homing
- EVPN MPLS Seamless Integration with VPLS
- EVPN RT Constraint

Behavior Change Introduced in this release

Deprecated Commands

- From this release onwards the **interface tunnel-te** *tunnel-id* **path-option pref {dynamic|explicit} segment-routing** command is deprecated. Configure Segment Routing Traffic Engineering (SR-TE) using the **segment-routing traffic-eng** command.

  For more information on the SR-TE commands and configurations, see the *Segment Routing Command Reference* and *Segment Routing Configuration Guide for Cisco NCS 5500 Series Routers*.

RPKI Prefix Validation

Starting from Cisco IOS XR Release 6.5.1, origin-as validation is disabled by default, you must enable it per address family.

See Configure BGP Prefix Validation

Hardware Introduced in Release 6.5.1

This release introduces the following new hardware:

- NCS-55A2-MOD-S and NCS-55A2-MOD-HD-S—These chassis are fixed port, high density, two rack-unit form-factor routers that support 24 SFP/SFP+ ports capable of supporting Gigabit Ethernet or 10 Gigabit Ethernet, and 16 SFP/SFP+/SFP28 ports capable of supporting Gigabit Ethernet, 10 Gigabit Ethernet, or 25 Gigabit Ethernet. The routers also supports up to 2 modular port adapters (MPA). The NCS-55A2-MOD-HD-S is temperature-hardened.

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

- NC55-MOD-A-S—This line card supports 12 SFP/SFP+ ports capable of supporting Gigabit Ethernet or 10 Gigabit Ethernet, and 2 QSFP+ ports capable of supporting 40 Gigabit Ethernet. This line card also supports up to 2 modular port adapters (MPA).

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

- Modular Port Adapters—Supported in the NCS-55A2-MOD-S and NCS-55A2-MOD-HD-S routers and the NC55-MOD-A-S line card:
  - NC55-MPA-4H-S and NC55-MPA-4H-HD-S—The 4-port 40GE/100GE MPA provides 4 ports for 4x25GE (via cable breakout), QSFP+ (40Gbps) or QSFP28 (100Gbps) transceivers. The NCS-NC55-MPA-4H-HD-S is temperature-hardened.
  - NC55-MPA-2TH-S—The 2-port 100GE/200GE MPA provides 2 ports for digital CFP2 transceivers.
  - NC55-MPA-1TH2H-S—The 1-port 100GE/200GE + 2-Port 40GE/100GE combination MPA provides 1 port for digital CFP2 transceivers and 2 ports for 4x25GE (via cable breakout), QSFP+ (40Gbps) or QSFP28 (100Gbps) transceivers.
  - NC55-MPA-12T-S—The 12-port 1GE/10GE MPA provides 12 ports for SFP/SFP+ transceivers, and supports 10G OTN, WAN PHY, and linear DWDM.

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

- CFP2-WDM-DET-1HL and CFP2-WDM-D-1HL pluggable optical modules—The Cisco digital CFP2 pluggable optical modules are the latest addition to the Cisco pluggables portfolio. With the Cisco digital CFP2 pluggable optical module, the Digital Signal Processor (DSP) chip resides directly on the pluggable module, providing a more complete and compact solution that can be used across all platforms with the CFP2 interfaces. The CFP2-WDM-DET-1HL pluggable optical module contains a tunable optics filter (TOF) that allows the pluggable to also be used in DWDM systems.

  The Cisco digital CFP2 pluggable optical modules are supported in the NC55-MOD-A-S line card and the NC55-MPA-2TH-S, NCS-55A2-MOD-S with MPA and NC55-MPA-1TH2H-S modular port adapters.

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*.

Release 6.5.1 Packages

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

Table 1: Release 6.5.1 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-r651.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-r651.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r651.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.
Cisco IOS XR Security Package	ncs5500-k9sec-3.1.0.0-r651.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-r651.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf-2.0.0.0-r651.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs5500-li-1.0.0.0-r651.x86_64.rpm	Includes LI software images
Multicast Package	ncs5500-mcast-1.0.0.0-r651.rpm	Support Multicast

Determine Software Version

Log in to the router and enter the **show version** command:

```
RP/0/RP0/CPU0:router# show version

Cisco IOS XR Software, Version 6.5.1
Copyright (c) 2013-2018 by Cisco Systems, Inc.

Build Information:
 Built By     : <username>
 Built On     : Wed Aug  8 17:10:43 PDT 2018
 Built Host   : iox-ucs-025
 Workspace    : /auto/srcarchive17/prod/6.5.1/ncs5500/ws
 Version      : 6.5.1
 Location     : /opt/cisco/XR/packages/

cisco NCS-5500 () processor
System uptime is 11 hours 8 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

Bug ID	Headline
CSCvj73245	YANG framework detected the fatal condition Backend processing failed for cdp netconf request
CSCvk71334	Failed to obtain hardware interface key for BVI interface after series of 10+ reloads
CSCvk75964	Install Fails if GISO build tool is used from 6.5.x

Caveats Specific to the NCS 5500 Routers

Caveats describe unexpected behavior in Cisco IOS XR Software releases.

Bug ID	Headline
CSCvi36859	Operational Failures are not made available to "Show configurations warnings" CLI

Bug ID	Headline
CSCvi77491	Both PI and PD license UNREGISTERED after HwModuleLocRP0Reload

Determine Firmware Support

Use the **show hw-module fpd** command in Admin 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.

This sample **show hw-module fpd** command output is taken from NCS 5508 chassis:

```
(sysadmin-vm)#show hw-module fpd
                                                                    FPD Versions
                                                                   ==============
Location  Card type         HWver FPD device       ATR Status   Run     Programd
-------------------------------------------------------------------------------
0/0       NC55-24H12F-SE    1.0   Bootloader           CURRENT    1.13    1.13
0/0       NC55-24H12F-SE    1.0   IOFPGA               CURRENT    0.09    0.09
0/0       NC55-24H12F-SE    1.0   SATA                 CURRENT    5.00    5.00
0/4       NC55-36X100G-A-SE 0.210 Bootloader           CURRENT    0.13    0.13
0/4       NC55-36X100G-A-SE 0.210 DBFPGA               CURRENT    0.14    0.14
0/4       NC55-36X100G-A-SE 0.210 IOFPGA               CURRENT    0.21    0.21
0/4       NC55-36X100G-A-SE 0.210 SATA                 CURRENT    5.00    5.00
0/5       NC55-36X100G-A-SE 0.210 Bootloader           CURRENT    0.13    0.13
0/5       NC55-36X100G-A-SE 0.210 DBFPGA               CURRENT    0.14    0.14
0/5       NC55-36X100G-A-SE 0.210 IOFPGA               CURRENT    0.21    0.21
```

```
0/5       NC55-36X100G-A-SE 0.210 SATA               CURRENT    5.00    5.00
0/RP0     NC55-RP           1.1   Bootloader         CURRENT    9.28    9.28
0/RP0     NC55-RP           1.1   IOFPGA             CURRENT    0.09    0.09
0/RP1     NC55-RP           1.1   Bootloader         CURRENT    9.28    9.28
0/RP1     NC55-RP           1.1   IOFPGA             CURRENT    0.09    0.09
0/FC0     NC55-5508-FC      1.0   Bootloader         CURRENT    1.74    1.74
0/FC0     NC55-5508-FC      1.0   IOFPGA             CURRENT    0.16    0.16
0/FC1     NC55-5508-FC      1.0   Bootloader         CURRENT    1.74    1.74
0/FC1     NC55-5508-FC      1.0   IOFPGA             CURRENT    0.16    0.16
0/FC2     NC55-5508-FC      1.0   Bootloader         CURRENT    1.74    1.74
0/FC2     NC55-5508-FC      1.0   IOFPGA             CURRENT    0.16    0.16
0/FC3     NC55-5508-FC      1.0   Bootloader         CURRENT    1.74    1.74
0/FC3     NC55-5508-FC      1.0   IOFPGA             CURRENT    0.16    0.16
0/FC4     NC55-5508-FC      1.0   Bootloader         CURRENT    1.74    1.74
0/FC4     NC55-5508-FC      1.0   IOFPGA             CURRENT    0.16    0.16
0/FC5     NC55-5508-FC      1.0   Bootloader         CURRENT    1.74    1.74
0/FC5     NC55-5508-FC      1.0   IOFPGA             CURRENT    0.16    0.16
0/SC0     NC55-SC           1.6   Bootloader         CURRENT    1.74    1.74
0/SC0     NC55-SC           1.6   IOFPGA             CURRENT    0.10    0.10
0/SC1     NC55-SC           1.6   Bootloader         CURRENT    1.74    1.74
0/SC1     NC55-SC           1.6   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.

- MLD Snooping is not supported until Cisco IOS XR Release 6.5.3. The support will be available in future releases.
- 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.

- Flow-aware transport pseudowire feature is not supported.
- Use **show mrib route summary** command to gather correct number of (S,G) routes.

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).

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.