Release Notes for Cisco NCS 5500 Series Routers, Release 6.2.2

Revised: April 9, 2021

Network Convergence System 5500 Series Routers

Note This product 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.

Software Features Introduced in Cisco IOS XR Software Release 6.2.2

MPLS OAM Using Nil FEC

The Nil-FEC ping and traceroute operations are extensions of regular MPLS ping and traceroute operations used for failure detection and trouble shooting in MPLS networks. Regular MPLS ping and traceroute requires at least one forwarding equivalence class (FEC) in the target FEC stack. In Nil-FEC ping and traceroute operations, an explicit FEC is not associated with the label.

For more information on Nil-FEC ping and traceroute, see *MPLS Configuration Guide for Cisco NCS5500 Series Routers*.

Configuring MPLS Static Labels for IPv6 Prefixes

MPLS labels can be assigned statically or dynamically. Effective with this release, you can also assign static labels to IPv6 prefixes and set the next hop address in the static LSP as an IPv6 address. You can also configure multiple forward paths, back up path sets, and specify outgoing next hops that can resolve with RIB.

For more information about configuring MPLS static labels for IPv6 prefixes, see *MPLS Configuration Guide for Cisco NCS5500 Series Routers*.

BGP Labeled Unicast IPv6 Address-Family

BGP Labeled Unicast IPv6 Address-Family bascially distributes MPLS labels using BGP structures. Thus IPv6 reachability information is exchanged over an IPv4 MPLS core infrastructure. It relies heavily on multiprotocol Border Gateway Protocol (BGP) extensions in the IPv4 network configuration on the provider edge (PE) router to exchange IPv6 reachability information (in addition to an MPLS label) for each IPv6 address prefix.

Explicit BGP SR-TE

Explicit BGP SR-TE uses an SR-TE policy that contains a list of explicit paths with SIDs that correspond to each explicit paths. A BGP speaker signals an explicit SR-TE policy to a remote peer, which triggers the setup of an TE tunnel with specific characteristics and explicit paths. The policy (identified by a unique color ID) contains a list of explicit paths with SIDs that correspond to each explicit paths.

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

BGP BMP Post Inbound Policy

The BGP Monitoring Protocol (BMP) feature enables monitoring of BGP neighbors (called BMP clients). Post inbound policy monitoring is available and configurable from this release.

Multicast Features

Multicast Source Discovery Protocol

Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple PIM sparse-mode domains. MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains.

PIM SSM over IPv6

In this release PIM SSM supports IPv6.

PIM-SM Operations

Typically, PIM in sparse mode (PIM-SM) operation is used in a multicast network when relatively few routers are involved in each multicast. Routers do not forward multicast packets for a group, unless there is an explicit request for traffic. Requests are accomplished using PIM join messages, which are sent hop by hop toward the root node of the tree. The root node of a tree in PIM-SM is the rendezvous point (RP) in the case of a shared tree or the first-hop router that is directly connected to the multicast source in the case of a shortest path tree (SPT). The RP keeps track of multicast groups, and the sources that send multicast packets are registered with the RP by the first-hop router of the source.

As a PIM join travels up the tree, routers along the path set up the multicast forwarding state so that the requested multicast traffic is forwarded back down the tree. When multicast traffic is no longer needed, a router sends a PIM prune message up the tree toward the root node to prune (or remove) the unnecessary traffic. As this PIM prune travels hop by hop up the tree, each router updates its forwarding state appropriately. Ultimately, the forwarding state associated with a multicast group or source is removed. Additionally, if prunes are not explicitly sent, the PIM state will timeout and be removed in the absence of any further join messages.

PIM SM does not support:

- Auto-RP
- Bundle VLAN
- VRF/VPN

For more information about multicast features, see the *Multicast Configuration Guide for Cisco NCS 5500 Series Routers, Release 6.2.x*

Dynamic LPTS Flows

Prior to this release, Cisco IOS XR did not support all flow types for LPTS. With the Dynamic LPTS Flows feature, users can configure LPTS flow types and maximum LPTS entries per flow type in the TCAM. This is enabled by configuring the **lpts pifib hardware dynamic-flows location <node-id>** command in the global configuration mode. The dynamic LPTS flow type configuration is per line card (LC). User can have multiple profiles configured across LCs.

For more information on Dynamic LPTS flow type configuration and commands, see the *Defining Dynamic LPTS Flow Type* section in the *Multicast Configuration Guide for Cisco NCS 5500 Series Routers*, and the respective commands in the *Multicast Command Reference Guide for Cisco NCS 5500 Series Routers.*

Automatic FPD Upgrade

Field-Programmable Devices (FPD) can be automatically upgraded by enabling the **fpd auto-upgrade** command in both Administration configuration and XR configuration mode. FPD images are automatically upgraded when a software upgrade is initiated or when a Line card is inserted / reloaded on a router.

Validating GRE Tunnel Destination

This feature allows you to check whether the GRE tunnel destination is reachable using a prefix-list.

For more information about validating GRE tunnel destination using a prefix-list, see *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers* .

6 Label Hashing

This feature modifies the hashing algorithm to load balance deeper in the payload of the packet.

128K TE Midpoint Tunnels

Effective with Cisco IOS-XR release 6.2.2, Cisco NCS5500 series router supports up to 128K MPLS TE mid-point tunnels. However, re-optimization is supported only for 64K MPLS-TE tunnels at a given instance. Since other MPLS features like LDP also share the same FEC resources, the number of node protected tunnels supported are limited by available FEC resources on the line card and router. Hence, you should take into account the distribution of link and node protected tunnels while deploying 128K MPLS-TE mid-point tunnels. For more information about MPLS-TE, see *MPLS Configuration Guide for Cisco NCS5500 Series Routers*.

Policy-Based Tunnel Selection

Policy-Based Tunnel Selection (PBTS) is now supported on Cisco NCS 5500 Series Routers. PBTS is a method to direct traffic into specific TE-tunnels based on classification criteria of the incoming packets based on Differentiated Services Code Point (DSCP) fields in the packets.

PBTS is implemented by enabling the **forward-class** command in the MPLS-TE configuration mode.

For more information on PBTS, see Implementing MPLS Traffic Engineering chapter in *MPLS Configuration Guide for Cisco NCS 5500 Series Routers, Release 6.2.x*.

DMZ Link Bandwidth

The DMZ link bandwidth of the eBGP link is a community that is advertised to IBGP peers to be used for multipath load balancing. The DMZ Link Bandwidth community is an optional non-transitive attribute, so the community is not advertised to eBGP peers. The DMZ Link Bandwidth feature enables the advertising of the DMZ Link Bandwidth community to an external BGP peer, and also the receiving of the community by an eBGP peer.

For more information, see the *BGP Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.2.x*.

QoS Re-marking of IP Packets in Egress Direction

The router support the marking of IP DSCP bits of all IP packets to zero, in the egress direction. This feature helps to re-mark the priority of IP packets, which is mostly used in scenarios like IP over Ethernet over MPLS over GRE. This functionality is achieved using the ingress policy-map with **set dscp 0** option configured in class-default.

For more information about this feature, see the *Implementing Access Lists and Prefix Lists* chapter in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*.

Matching by Fragment Offset in ACLs

You can configure an access control list (ACL) rule to filter packets by the fragment-offset value. Depending on whether a packet matches the criteria in a permit or deny statement, the packet is either processed or dropped respectively at the interface. Fragment-offset filtering is supported only on ingress direction with compression mode of an ACL.

Configuring ACL Filtering by IP Packet Length

You can configure an access control list to filter packets by the packet length at an ingress interface. Depending on whether a packet matches the packet-length condition in a permit or deny statement, the packet is either processed or dropped respectively at the interface.

For more information about this feature, see the *Implementing Access Lists and Prefix Lists* chapter in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*.For complete command reference, see the *Access List Commands* chapter in *IP Addresses and Services Command Reference for Cisco NCS 5500 Series and NCS 540 and NCS 560 Series Routers*

Enhancement to Zero Touch Provisioning

Zero Touch Provisioning (ZTP) supports auto provisioning of router by running customized scripts using DHCP server over v6.

For more information about ZTP, see the *Perform Disaster Recovery* chapter in the *System Setup and Software Installation Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.2.x*.

Enhancements to Programmability

Data models are a programmatic and standards-based way of configuring and collecting operational data of a network device, replacing the process of manual configuration.

The enhancements includes support for:

- Netconf OC Models
- OC RPC

For more information, see the *Programmability Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.2.x* .

Enhancements to Flexible Packaging

Flexible packaging is an enhancement that modularizes and delivers the Cisco IOS XR operating system as RPM packages.

Flexible packaging supports a customized ISO that includes ISO, RPMs, SMUs and configurations. This customized ISO, called the Golden ISO (GISO) eases installation and eliminates multiple install operations when installing additional packages. To build the customized ISO, use the `gisobuild.py` tool available in the box location at `/pkg/bin` in IOS XR mode.

For more information, see the *Customize Installation using Golden ISO* chapter in the *Flexible Packaging Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.2.x*.

Enhancement to Model-driven Telemetry

Model-driven telemetry supports UDP protocol for dial-out configuration where the router initiates a session to the destinations based on the subscription.

For more information, see the *Configure Model-driven Telemetry* chapter in the *Telemetry Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.2.x* .

Internet Protocol Flow Information Export (IPFIX)

Internet Protocol Flow Information Export (IPFIX) is an IETF standard export protocol for sending Netflow packets. IPFIX is based on Netflow version 9.

The IPFIX feature formats Netflow data and transfers the Netflow information from an exporter to a collector using UDP as transport protocol.

For more information, refer *Netflow Configuration Guide for Cisco NCS 5500 Series Routers*.

MACSec SNMP MIB (IEEE8021-SECY-MIB)

The IEEE8021-SECY-MIB provides Simple Network Management Protocol (SNMP) access to the MAC security entity (SecY) MIB running with IOS XR MACsec-enabled line cards. The IEEE8021-SECY-MIB is used to query on the SecY data, encryption and decryption, and the hardware statistics. The SecY MIB data is queried only on the Controlled Port.

The object ID of the IEEE8021-SECY-MIB is 1.0.8802.1.1.3. The IEEE8021-SECY-MIB contains the following tables that specifies the detailed attributes of the Controlled Port interface and are indexed by the ifindex pointing to the Controlled Port. All of these tables have a read-only access.

Table 1: IEEE8021-SECY-MIB Table

Tables	OID
secyIfTable	1.0.8802.1.1.3.1.1.1
secyTxSCTable	1.0.8802.1.1.3.1.1.2
secyTxSATable	1.0.8802.1.1.3.1.1.3
secyRxSCTable	1.0.8802.1.1.3.1.1.4
secyRxSATable	1.0.8802.1.1.3.1.1.5
secyCipherSuiteTable	1.0.8802.1.1.3.1.1.6
secyTxSAStatsTable	1.0.8802.1.1.3.1.1.7
secyTxSCStatsTable	1.0.8802.1.1.3.1.1.8
secyRxSAStatsTable	1.0.8802.1.1.3.1.1.9
secyRxSCStatsTable	1.0.8802.1.1.3.1.1.10
secyStatsTable	1.0.8802.1.1.3.1.1.11

For more information, see the SecY IEEE MIB at the following URL:

http://www.ieee802.org/1/files/public/MIBs/IEEE8021-SECY-MIB-200601100000Z.txt

Type 6 Encryption Support for MACsec Key Configuration

Using the Type 6 password encryption feature, you can securely store MACsec plain text key string (CAK) in Type 6 encrypted format.

The primary key is the password or key used to encrypt all plain text MACsec key strings (CAK) in the router configuration with the use of an Advance Encryption Standard (AES) symmetric cipher.

The primary key is not stored in the router configuration and cannot be seen or obtained in any way while connected to the router.

The Type 6 password encryption is effective only if a primary key is configured.

For more information, see the *Implementing MACsec Encryption* Chapter of the *System Security Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.2.x*.

URPF Loose Mode

Cisco Network Convergence System 5500 Series supports the use of URPF in loose mode. URPF loose mode is enabled when the router is configured to validate only the prefix of the source IP address in the FIB and not the interface used by the packet to reach the router. By configuring loose mode, legitimate traffic that uses an alternate interface to reach the router is not mistaken to be malicious. URPF loose mode is very useful in multi-homed provider edge networks.

For more information, see the *Configuring URPF Loose Mode* section of the *Implementing Cisco Express Forwarding* chapter in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*.

Configurable LPTS Policers

In Cisco IOS XR, the control packets, which are destined to the Route Processor (RP), are policed using a set of ingress policers in the incoming ports. These policers are programmed statically during bootup by LPTS components. The policers are applied based on the flow type of the incoming control traffic. The flow type is determined by looking at the packet headers. The policer rates for these static ingress policers are defined in a configuration file, which are programmed on the route processor during bootup. You can change the policer values based on the flow types of these set of ingress policers. You are able to configure the rate per policer per node.

For more information on Configurable LPTS Policers configuration, refer *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*

ABF with GRE Tunnel as Destination

Converged networks carry voice, video and data. Users may need to route certain traffic through specific paths instead of using the paths computed by routing protocols. This is achieved by specifying the next-hop address in ACL configurations, so that the configured next-hop address from ACL is used for fowarding packet towards its destination instead of routing packet-based destination address lookup. This feature of using next-hop in ACL configurations for forwarding is called ACL Based Forwarding (ABF).

From Release 6.2.1.1, IPv4 ABF nexthops routed over GRE interfaces are supported.

For more information on ABF with GRE Tunnel as Destination configuration and commands, refer *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*

Configuring Backup Paths for Static LSPs

This feature allows you to configure a back up path for a static LSP to forward traffic if the primary path is not reachable or fails.

For more information about configuring backup paths for MPLS static LSPs, see *MPLS Configuration Guide for Cisco NCS5500 Series Routers*.

Configuring Static LSP Next Hop Resolve

This feature allows you to specify the next hop address for the incoming label in a static LSP with out specifying the interface.

For more information about configuring static LSP next hop resolve, see *MPLS Configuration Guide for Cisco NCS5500 Series Routers*.

Configuring ACLs with QoS Groups

Cisco IOS XR supports the use of QoS groups in an ACL to classify traffic based on a match condition. Before you can configure QoS groups in an ACL, the QoS peering profile must be enabled on the router or the line card.

For more information on this feature, see the *Configuring ACLs with QoS Groups* section in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*.

Object-Group ACLs

Cisco IOS XR provides an option to create object-group ACLs to classify users, devices, or protocols into groups, so you can have a group-level access control policy. Instead of specifying individual IP addresses, protocols, and port numbers in multiple ACEs, a single the object group in a single ACL.

This feature is very beneficial in large scale networks which currently contain hundreds of ACLs. By using the object-group ACL feature, the number of ACEs per ACL are significantly reduced. Object-group ACLs are also more readable, and easier to manage than conventional ACLs. Using object-group ACLs instead of conventional ACLs optimizes the storage needed in TCAM.

For more information on this feature, see the *Understanding Object-Group ACLs* section in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*.

Hardware Introduced in Release 6.2.2

This release introduces the following new hardware:

- Cisco NCS-55A1-36H—This chassis is a fixed port, high density, one rack unit form-factor router that supports port density of 36 x QSFP ports, each capable of supporting 4x10 GE (via cable breakout), 4x25 GE (via cable breakout), 40 GE (QSFP+), or 100 GE (QSFP28) receivers.

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

  For information on the optics supported and other specifications, refer the NCS 5500 Data Sheet.

- NC55-6X200-DWDM-S—This IPoDWDM line card adds DWDM capabilities to the NCS 5500 series modular chassis. The line card has 6 ports that support second-generation Coherent Transceiver Pluggable (CTP2) optics modules (in CFP2 form-factor). Each port can support 100 Gbps (DWDM QPSK), 150 Gbps (DWDM 8 QAM), or 200 Gbps (DWDM 16 QAM) WDM signals with full line rate MACsec capability.

  The NC55-6X200-DWDM-S line card, with ONS-CFP2-WDM long-haul optics, eliminates the need for connecting short-range grey optics to a dedicated optical platform between NCS 5500 series modular chassis, reducing operating expenses and capital cost.

Performance monitoring of optical, optical transport network (OTN), and forward error correction (FEC) parameters can be calculated and collected in 30-second, 15-minute, or 24-hour intervals.

For more information on the NC55-6X200-DWDM-S line card, see the *Hardware Installation Guide for Cisco NCS 5500 Series Routers*.

For information on configuring the NC55-6X200-DWDM-S line card, see the "Configuring Controllers" chapter in the *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers*.

Hardware Enhancements in Release 6.2.2

- The 36-port 100 Gigabit Ethernet MACsec Line Card (NC55-36x100G-S) supports 4x25 (via cable breakout) for QSFP28 modules.

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

- The QSFP-to-SFP+ Adaptor (CVR-QSFP-SFP10G) is supported on modular line cards (NC55-24X100-SE,NCS55-24H12F-SE) with ZR, ER, and DWDM SFP+ optics.

Release 6.2.2 Packages

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

Table 2: Release 6.2.2 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-1.0.0.0-r622.x86_64.rpm	Extensible Markup Language (XML) Parser, Telemetry, Netconf, gRPC and HTTP server packages.
Cisco IOS XR MPLS Package	ncs5500-mpls-1.0.0.0-r622.x86_64.rpm ncs5500-mpls-te-rsvp-1.0.0.0-r622.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.

Cisco IOS XR Security Package	ncs5500-k9sec-1.0.0.0-r622.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*.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf*.rpm	Support OSPF
Multicast Package	ncs5500-mcast-1.0.0.0-r622.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

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

```
RP/0/RP0/CPU0:router# show version
Cisco IOS XR Software, Version 6.2.2
Copyright (c) 2013-2017 by Cisco Systems, Inc.

Build Information:
 Built By     : <username>
 Built On     : Tue Jul 11 15:35:33 PDT 2017
 Build Host   : iox-ucs-027
 Workspace    : /auto/srcarchive13/production/6.2.2/ncs5500/workspace
 Version      : 6.2.2
 Location     : /opt/cisco/XR/packages/

cisco NCS-5500 () processor
System uptime is 1 day, 8 hours, 24 minutes
```

Caveats

There are no caveats in this release.

Identifier	Description
CSCve82062	Observing False min > max commit fail on optical PM threshold value
CSCvf16968	L2 to L3 v4 and v6 traffic drop on a few bundle members
CSCvf04716	admin showtech is saving on line card
CSCvf12070	On commit replace dpa olist objects are not cleared

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.

Table 3: PID and FPD Versions for Release 6.2.2

PID	FPD Device	FPD Versions
NCS55-RP	Bootloader	9.23
	IOFPGA	0.09
NCS55-SC	Bootloader	1.7
	IOFPGA	0.08
NC55-5508-FC	Bootloader	1.7
	IOFPGA	0.16
NC55-36X100G	Bootloader	1.17
	IOFPGA	0.15
	MIFPGA	0.09
NC55-24X100G-SE	Bootloader	1.11
	IOFPGA	0.12
	MIFPGA	0.03
NC55-18H18F	Bootloader	1.11
	IOFPGA	0.22
	MIFPGA	0.03
NC55-36X100G-S	Bootloader	1.11
	IOFPGA	0.09
	MIFPGA	0.06
NC55-24H12F-SE	Bootloader	1.11
	IOFPGA	0.08
	MIFPGA	0.02

PID	FPD Device	FPD Versions
NCS-5501	Bootloader	1.13
	CPU-IOFPGA	1.14
	MB-IOFPGA	1.04
	MB-MIFPGA	1.01
NCS-5501-SE	Bootloader	1.15
	CPU-IOFPGA	1.14
	MB-IOFPGA	1.07
	MB-MIFPGA	1.02
NCS-5502	Bootloader	1.15
	CPU-IOFPGA	1.14
	DC-IOFPGA	1.05
	DC-MIFPGA	1.02
	MB-IOFPGA	1.05
	MB-MIFPGA	1.02
NCS-5502-SE	Bootloader	1.15
	CPU-IOFPGA	1.14
	DC-IOFPGA	1.05
	DC-MIFPGA	1.02
	MB-IOFPGA	1.05
	MB-MIFPGA	1.02
NC55-5516-FC	Bootloader	1.73
	IOFPGA	0.23
NCS-55A1-36H-B	Bootloader	1.05
	CPU-IOFPGA	1.14
	MB-IOFPGA	1
	MB-MIFPGA	1

PID	FPD Device	FPD Versions
NC55-6X200-DWDM-S	Bootloader	1.11
	IOFPGA	0.1
	DENALI	13.48
	MORGOTH	5.13
	MSFPGA	2.21

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.

- PIM on Bundle-Ether subinterface is not supported.

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.

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.

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.