Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 6.6.1

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 6.6.1 is a limited availability (LA) release. All Cisco IOS XR Release 6.6.1 features are available in Cisco IOS XR Release 6.6.25, which is a general availability (GA) release. For more information on IOS XR Release 6.6.25, see *Release Notes for Cisco NCS 5500 Series Routers, Release 6.6.25*

Software Features Introduced in this Release

SRv6 Base

Segment routing can be applied on both MPLS and IPv6 data planes. In a SR-MPLS enabled network, an MPLS label is used as the segment identifier and the source router chooses a path to the destination and encodes the path in the packet header as a stack of labels. However, in a segment routing over IPv6 (SRv6) network, an IPv6 address serves as the segment identifier (SID). The source router encodes the path to destination as an ordered list of segments (list of IPv6 addresses) in the IP packet. This release introduces base support for Segment Routing using IPv6 data plane.

SRv6 IS-IS

Intermediate System-to-Intermediate System (IS-IS) protocol already supports segment-routing with MPLS data plane (SR-MPLS). This feature enables extensions in ISIS to support segment-routing with IPv6 data plane (SRv6). The extensions include exchanging a node's SRv6 capabilities and node and adjacency segments as SRv6 SIDs.

SRv6 Based IS-IS TI-LFA

Topology-Independent Loop-Free Alternate (TI-LFA) provides link protection in topologies where other fast reroute techniques cannot provide protection. TI-LFA with ISIS SR-MPLS is already supported. This feature introduces support for implementing TI-LFA using segment routing over IPv6 (SRv6) for the IS-IS protocol.

L3VPN Support in Segment Routing IPv6

This feature enables Layer 3 Virtual Private Network in Segment Routing in an IPv6 network.

SRv6 and BFDv6 on Bundle

Bidirectional forwarding detection (BFD) provides low-overhead, short-duration detection of failures in the path between adjacent forwarding engines. BFD allows a single mechanism to be used for failure detection over any media and at any protocol layer, with a wide range of detection times and overhead. The fast detection of failures provides immediate reaction to failure in the event of a failed link or neighbor. In BFDv6 hardware offload over bundle, each bundle member link with IPv6 address runs its own BFD session.

SRv6 L3VPNv4 OAM

This feature enables to use the existing Internet Control Message Protocol version 6 (ICMPv6) mechanism for basic Operations, Administration, and Maintenance (OAM) functionality to address the OAM requirements for SRv6 enabled L3VPN networks.

SRv6 OAM with Segment Routing Header

SRv6 OAM with segment routing header (SRH) feature enables to test reachability and isolate faults in a segment routing over IPv6 (SRv6) network using ping and traceroute commands.

BGP Labeled Unicast Multiple Label Stack

The number of BGP Labeled Unicast Multiple Label Stack supported has been increased from three to five.

Smart Licensing

Smart Licensing is a cloud-based, software license management solution that enables you to automate time-consuming, manual licensing tasks. The solution allows you to easily track the status of your license and software usage trends.

Smart Licensing uses Flexible Licensing consumption model which is based on the capacity of ports configured. If you purchase a chassis that supports Flexible licensing, you need to configure flexible licensing to enable it. You can configure Flexible Licensing consumption model through the **license smart flexible-consumption enable** command. Flexible licensing checks usage across all ports of a system on a daily basis and reports license usage results to the Smart Licensing Manager at Cisco.com.

IGMP L2 EVPN State Sync

After IGMP snooping has been enabled, this information has to be synced with the peer using the L2 EVPN sync feature.

IPv4 - Enhanced Designated Forwarder Election for Multicast

After IGMP snooping has been enabled and this information has been synced with the peer, both the peers need to act like a last hop router and send PIM join upstream. Once traffic arrives on both the peers, only one should forward it to the receiver. Designated Forwarder Election elects one peer to do the forwarding.

EVPN: Dual PIM-DR - IPv4

After IGMP snooping has been enabled and this information has been synced with the peer, both the peers need to act like a last hop router and send PIM join upstream.

Hardware timestamp support for QoS

In earlier releases, the timestamp for hardware data collection was synchronized to the time when Cisco telemetry was manually run, and not the time when the hardware *actually* collected the data. This resulted in inaccurate data rate calculation with telemetry data. From Release 6.6.1 onwards, the telemetry timestamp is updated with the timestamp when the hardware collects data. Which means that when you run telemetry, the timestamp in the telemetry data that it collects is in sync with what was collected by the hardware.

CFM on EVPN ELAN

Connectivity fault management (CFM) is a service-level Operations and Maintenance (OAM) protocol that provides tools for monitoring and troubleshooting end-to-end Ethernet services for each VLAN. This includes proactive connectivity monitoring, fault verification, and fault isolation.

Cisco IOS XR Software Release 6.6.1 introduces CFM support for single-homed EVPN Emulated Local Area Network (ELAN) services. This functionality helps you to monitor the ELAN services of users against their contractual service-level agreements (SLAs), thereby providing high speed Layer 2 and Layer 3 services with high resiliency and less operational complexity to different market segments.

Restrictions for CFM on EVPN ELAN

CFM on EVPN ELAN is subjected to these restrictions:

- Supports only single-homed EVPN ELAN.
- Supports single homing with one AC per PW.
- DOWN MEP on AC interface of EVPN-BD is not supported.
- Does not support loss measurement.
- Does not support Y1731.

ERSPAN ACL to Match IPv4/IPv6 and MPLS Labels

With this feature, a new command, *monitor-session ERSPAN ethernet direction rx-only port-level acl* is introduced. The command enables you to configure partial traffic mirroring.

Egress Rate-Limiting for Locally Generated ERSPAN Traffic

With this release, support for rate-limiting of the replicated traffic on ERSPAN has been added. This feature provides rate limiting of the mirroring traffic or the egress traffic. With rate limiting, you can limit the amount of egress traffic to a specific rate, which prevents network and remote ERSPAN destination traffic overloading.

UDLD Support for NCS5500

This feature enables Unidirectional Link Detection (UDLD) support for NCS 5000 that allows you to configure each interface. The interface must be a physical ethernet interface. UDLD is a single-hop physical link protocol for monitoring an ethernet link, including both point-to-point and shared media links. This is a Cisco-proprietary protocol to detect link problems, which are not detected at the physical link layer.

Route Reflector, Pathlist and Prefix Independence Convergence Support for Segment Routing on IPv6

This feature enables the route reflector to support Virtual Private Network(VPN) v4 Segment IDs (SID) on an IPv6 network. The feature also enables Prefix Independent Convergence support for Segment Routing on IPv6.

SR Ingress Counter

This feature enables support for ingress SR per-label counters and thus provides a way for SR label accounting in the MPLS forwarding table.

SR-TE: FIB Programming of Best Candidate-path Only

In the current implementation of SR-TE policy, segment-lists of all candidate paths are pre-programmed in FIB. However, this may limit the number of SR-TE policies possible on the router. This feature enables to include only the segment list of best path in FIB.

SR-TE Egress Statistics: per-segment List Counter

In SR-TE policies, you can specify multiple segment lists that can load share the traffic entering the SR path. Currently, the traffic statistics is aggregated across all the segment lists and exported at the interface level. This feature enables to export the traffic statistics for each segment list in addition to the aggregate mode at interface level.

Segment Routing for IS-IS Flexible Algorithm

Segment Routing (SR) allows a flexible definition of end-to-end paths within IGP topologies by encoding paths as sequences of topological sub-paths, called segments. It also defines an algorithm that defines how the path is computed and provides a way to associate prefix-SID with an algorithm. This allows IGPs to compute the path based on various algorithms and forward the traffic on such a path using the algorithm-specific segments. No additional segments are required for traffic to stay on the computed paths as in the case of the SR-TE.

Segment Routing with OSPFv2

This feature contains the following sub-features for segment routing with OSPFv2:

- segment routing local block (SRLB)
- microloop avoidance
- local unequal cost multipath (UCMP)
- extended traffic engineering (TE) metric type-length-value (TLV)

The segment routing local block (SRLB) feature introduces support for configuring adjacency segment ID (SID) statically for segment routing with OSPFv2. The static adjacency SID helps to force the traffic over a specific link while implementing SR-TE. The segment routing microloop avoidance feature detects if microloops can occur following a topology change. With this enhancement, SRTE tunnel for microloop avoidance is created only if number of labels required for microloop avoidance exceeds the number of labels the router can impose.

Bandwidth based local unequal cost multipath (UCMP) feature allows OSPF to perform load sharing on ECMP or UCMP paths based on configured weights on interface or interface bandwidth.

The extended traffic engineering (TE) metric TLV feature allows OSPF to distribute network performance information including link delay and bandwidth parameters.

AC-Aware VLAN bundle

The AC-Aware VLAN Bundle feature allows you to configure more than one subinterface on the same main port in an EVPN enabled bridge domain. When you configure this feature using the **ac-aware-vlan-bundling** command, the BGP Extended Community (ExtCom) is set to the VLAN of the subinterface on the MAC synchronization routes, which enables you to distinguish between the subinterfaces.

EVPN E-TREE

The EVPN E-Tree feature provides a rooted-multipoint Ethernet service over MPLS core. The EVPN Ethernet Tree (E-Tree) service enables you to define attachment circuits (ACs) as either a root site or a leaf site, which helps in load balancing and avoid loops in a network.

Multicast Route Statistics

Multicast route statistic feature provides information about the multicast routes. The multicast statistics information includes the rate at which packets are received.

Before enabling multicast route statistics, you must configure an ACL to specify which of the IP route statistics to be captured.

Multicast Listener Discovery over BVI

Multicast IPv6 packets received from core, which has BVI as forwarding interface, is forwarded to access over snooped L2 AC or interface.

Note

- As per MLDv2 RFC recommendation the MLDv2 reports should carry the Hop-by-Hop options header for the reports to get punted up.
- MLDv2 is supported over BVI only when BVI is configured as a forwarding interface.

MLD and BVI Overview

Routers use the Internet Group Management Protocol (IGMP) (IPv4) and Multicast Listener Discovery (MLD) (IPv6) to learn whether members of a group are present on their directly attached subnets. Hosts join multicast groups by sending IGMP or MLD report messages.

MLDv1 and MLDv2 are supported on NCS 5500. However, MLDv2 is enabled when you configure MLD by default.

MLDv2 shares feature parity with IGMPv3 with respect to all supported interface types with the exception of PPoE and subinterfaces. MLDv2 enables a node to report interest in listening to packets only from specific multicast source addresses.

A BVI interface is a routed interface representing a set of interfaces (bridged) in the same L2 broadcast domain. MLD join messages coming in or out of this broadcast domain passes through the BVI interface.

Conditional Marking of MPLS Experimental bits for L2VPN Traffic

In earlier releases, conditional marking of MPLS experimental bits was available for L3VPN traffic. From Release 6.6.1 onwards, this feature is also available for L2VPN traffic. You can now set up the conditional marking of MPLS experimental bits for L2VPN traffic on the Provider Edge routers in the imposition direction.

IGMP Snooping on Layer2

IGMP snooping provides a way to constrain multicast traffic at Layer 2. By snooping the IGMP membership reports sent by hosts in the bridge domain, the IGMP snooping application can set up Layer 2 multicast forwarding tables to deliver traffic only to ports with at least one interested member, significantly reducing the volume of multicast traffic.

64 MPLS ECMP Support - Per Level

The Cisco NCS 5500 Series Router currently supports 32-way ECMP and hence you can deploy upto 32 ECMP paths to the next hop. This feature enhances the maximum number of ECMP paths you can deploy on the router to 64.

NetFlow to Report Physical Bundle Member

NetFlow to Report Physical Bundle Member is supported on the NCS 5500 platform from the Cisco IOS XR Release 6.6.1. This feature enables a user to report actual underlying members of the bundle interface which carries the data traffic.

NetFlow to report Physical Bundle Member is useful in cases of capacity planning and for traffic engineering purposes.

VRRP Scale Increase from 16 to 225

The Virtual Router Redundancy Protocol (VRRP) feature allows for transparent failover at the first-hop IP router, enabling a group of routers to form a single virtual router. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group.

The maximum VRRP has been optimized from 16 to 225 from the Cisco IOS XR Release 6.6.x.

IPv6 Multicast Listener Discovery Snooping over BVI

Multicast Listener Discovery (MLD) snooping provides a way to constrain multicast traffic at L2. By snooping the MLD membership reports sent by hosts in the bridge domain, the MLD snooping application can set up L2 multicast forwarding tables. This table is later used to deliver traffic only to ports with at least one interested member, significantly reducing the volume of multicast traffic.

MLDv2 support over BVI enables implementing IPv6 multicast routing over a L2 segment of the network that is using an IPv6 VLAN. The multicast routes are bridged via BVI interface from L3 segment to L2 segment of the network.

MLDv2 snooping over BVI enables forwarding MLDv2 membership reports received over the L2 domain to MLD snooping instead of MLD.

IPv6 Multicast for Multiple Sources

Before this release IPv6 multicast support was limited to a single source for each multicast group. However, when multiple sources were involved then it resulted in duplicating multicast flows of multiple sources to all interested receivers.

From Release 6.6.1 onwards, IPv6 multicast supports multiple sources for a single multicast group.

Note When a router has LCs (with and without external TCAMs), it operates with default IPv6 multicast route scale, which is programmed on the LC without an external TCAM.

Support for 300 Multicast Traffic Sources

From this release onwards support for 300 multicast traffic sources per multicast group in PIM-SM mode is introduced.

The support is available in

- VRF-lite configuration
- Multipath hashing for load splitting for IP multicast traffic

A 300 multicast sources per group is supported with a maximum of 40000 multicast routes. Over that limit, unexpected multicast behavior many result.

Note You should configure an MTU of 5000 to support 300 multicast sources per group.

Multicast IPv4 Source-Specific Multicast Scale

From this release, IPv4 Source-Specific Multicast (SSM) supports 120000 multicast routes.

L3VPN QoS Traffic-class Marking in Segment Routing IPv6

The L3VPN QoS traffic-class marking in Segment Routing IPv6 feature enables the marking of traffic-class headers and propagates the traffic-class from the IPv4 header of incoming traffic. This enables prioritization of traffic for Segment Routing in an IPv6 network.

To enable this feature use the **hw-module profile segment-routing srv6 encapsulation traffic-class** command and reload the router for the configuration to take effect.

IP-tunnel decapsulation statistics (GRE+IPinIP)

Generic Routing Encapsulation (GRE) is a tunnelling protocol that provides a simple generic approach to transport packets of one protocol over another protocol by means of encapsulation. GRE encapsulates a payload, that is, an inner packet that needs to be delivered to a destination network inside an outer IP packet. The GRE tunnel behave as virtual point-to-point link that have two endpoints identified by the tunnel source and tunnel destination address. Encapsulation by the outer packet takes place at the tunnel source whereas decapsulation of the outer packet takes place at the tunnel destination. With this feature, along with encapsulation statistics, decapsulation statistics is available.

DHCPv6 PD Synchronization for All-Active Multihoming using Session Redundancy

The DHCPv6 PD Synchronization for All-Active Multihoming using Session Redundancy feature provides load balancing for both control and data packets. This feature helps in efficient utilization of devices with respect to throughput (line rate) and processing power.

Prior to this release, Session Redundancy (SeRG) mechanism supported active-standby to address access failure, core failure, and node or chassis failures. In all these cases, one active point of attachment (PoA) is responsible to create sessions and synchronize binding information using SeRG across the PoA. This mechanism did not serve the purpose of EVPN all-active multihoming as PoAs are in primary-subordinate mode for a given access-link in SeRG group. This restricts only one node that acts as primary to process control packets, create bindings, and forward data path.

This feature allows you to define both POAs to be active unlike in primary-subordinate mode. Also, there is no need to exchange or negotiate the roles of respective PoAs.

DHCPv6 Relay IAPD on IRB

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Identity Association for Prefix Delegation (IAPD) on IRB feature allows you to manage link, subnet, and site addressing changes. This feature allows you to automate the process of assigning

prefixes to a customer for use within their network. The prefix delegation occurs between a provider edge (PE) device and customer edge (CE) device using the DHCPv6 prefix delegation option. After the delegated prefixes are assigned to an user, the user may further subnet and assign prefixes to the links in the customer's network.

DHCPv4 Relay Synchronization for All-Active Multihoming

DHCPv4 Relay Synchronization for All-active Multihoming feature enables a transitory entity between the end user and DHCPv4 server and does not create any DHCPv4 binding. This feature supports the equal distribution of DHCP control-plane packets among end users across point of attachment (PoA). All DHCP control packets for single users exist on the same DHCPv4 relay (PoA) so that end users can lease IP address allocation without any intervention and delay.

VLAN Bundle Sub Interface Support

The maximum number of supported Ethernet link bundles is increased to 1024 and also the maximum number of supported bundle sub interfaces is increased to 1024.

Use of CRC for Improved BER/LFS on 10G

CRC-BER determines the reliability of a link by polling hardware counters every 5 seconds. It monitors the number of CRC-BER errors that are received and triggers respective actions that are based on the configuration.

This feature supports the following:

- 10g native and channelized interface.
- V1 algorithm runs in parallel with v2 (crc ber).
- Physical interfaces.
- Physical interfaces that are part of a bundle.

DHCPv4 Relay on IRB

The Dynamic Host Configuration Protocol for IPv4 (DHCPv4) Relay on IRB feature provides DHCP support for the end users in EVPN all-active multihoming scenario. This feature enables reduction of traffic flooding, increase in load sharing, faster convergence during link and device failures, and simplification of data center automation.

DHCPv4 relay agent relay request packets coming over access interface towards external DHCPv4 server to request address (/32) allocation for the end user. DHCPv4 relay agent acts as stateless for end users by not maintaining any DHCPv4 binding and respective route entry for allocated address.

SRv6 Services for L3VPN VPNv4 Active-Standby Redundancy using Port-Active Mode

The SRv6 Services for L3VPN VPNv4 Active-Standby Redundancy using Port-Active Mode feature provides all-active per-port loadbalancing support for multihoming. Forwarding of traffic is determined based on a specific interface rather than per-flow across multiple Provider Edge (PE) routers. This feature enables efficient load-balancing and provides faster convergence. In an active-standby scenario, the active PE router is detected using designated forwarder (DF) by modulo calculation and the interface of the standby PE is brought down. For Modulo calculation, byte 10 of the ESI is used.

The number of Ethernet Segments (ES) supported is 13.

IEEE 802.1X Port-Based Authentication

The IEEE 802.1X port-based authentication protects the network from unauthorized clients. It blocks all traffic to and from devices at the interface, until the client is authenticated by the authentication server. After successful authentication, the port is open for traffic.

IAPD Route Distribution and withdrawal in DHCPv6 Relay

This feature enables the propagation of the Attachment Circuit (AC) interface status to the DHCPv6 relay agent. Based on the AC interface status, route distribution and withdrawal towards the core MPLS network takes place. In the EVPN Multi-homing Active-Active Model, this feature prevents traffic block hole for the core-to-subscriber traffic of DHCPv6 IAPD Sessions that are associated with the Attachment Circuits (ACs) that are down. The traffic for the ACs that are down are withdrawn and directed towards the core network.

Bidirectional Forwarding Detection over VRF

In the context of routing, the purpose of Bidirectional Forwarding Detection (BFD) is to detect communication failure between two routers faster than what is supported by routing protocols detection timers. BFD detects the failure by monitoring incoming BFD control packets from neighbor router. If a number of packets are lost in transmission for whatever reason and thus not received by the monitoring router, the monitoring router brings down routing session to the neighbor router.

Cisco NCS 5500 Router supports BFD with VRF context.

BFD Hardware Offload Support for IPv6

This feature enables Bidirectional forwarding detection (BFD) hardware offload support for IPv6.

Bidirectional forwarding detection (BFD) provides low-overhead, short-duration detection of failures in the path between adjacent forwarding engines. BFD allows a single mechanism to be used for failure detection over any media and at any protocol layer, with a wide range of detection times and overhead. The fast detection of failures provides immediate reaction to failure in the event of a failed link or neighbor.

Table 1: The supported BFD minimum-interval and multiplier values

Session type	Values
BLB and BFD multihop session	Minimum 300ms interval with minimum 3 multiplier
All other BFD session types	Minimum 4ms interval with minimum 3 multiplier

TWAMP Light

TWAMP LIGHT defines a flexible method for measuring round-trip IP performance between any two devices and thereby helpsthe customers check the IP SLA compliance. It is a light-weight model of TWAMP (Two-Way Active Measurement Protocol) as it eliminates the need for a TWAMP control session. Thus it removes the overhead of establishing and tearing down a control session, and thereby eliminates the need for a TWAMP server entity to be maintained at the reflector end.

Proactive ARP and ND

This feature ensures that CEF (Cisco Express Forwarding) proactively triggers ARP (Address Resolution Protocol) or ND (Neighbor Discovery) in order to resolve any missing next-hop information, retrying every 15 seconds until the next-hop information is resolved.

Thus, when you configure a static route which has an incomplete next-hop information, this feature automatically triggers ARP or ND resolution.

Revised OC-platform model version

Support for openconfig-platform.yang (OC-platform) model is revised from version 0.4.0 to version 0.11.0. In addition to retreiving basic component information, this revised version of the model extracts additional details such as operational state, available and utilized memory, allocated and used power, temperature, power-supply, fan, linecard and so on.

Support for new XR NETCONF actions

IOS-XR and System admin actions are RPC statements that trigger an operation or execute a command on the router. The following NETCONF actions are introduced in this release:

- copy
- delete

Telemetry support for OC LACP

The OpenConfig-Link Aggregation Control Protocol (OC-LACP) model defined by the OC community, helps manage LACP-enabled bundles and member interfaces. Cisco IOS XR supports OC-LACP version 1.0.2. Currently, the support is extended to version 1.1.0. Telemetry support for (OC-LACP) is provided only for LACP state data at global, bundle and member level.

Enhancement for IEEE Default Profile

The enhancement for IEEE Default Profile enables you to configure the default PTP configuration for hybrid-boundary clocks, on the Cisco NCS 5500 Series Routers. This configuration makes the NCS 5500 Routers compatible with the network that is using the Cisco ASR 920 Routers. Hence, this feature eases the migration from Cisco ASR 920 Routers to NCS 5500 Routers.

Behavior Change Introduced in this release

Depricated Command

From this release onwards the **ispf** command is deprecated.

This command was used to calculate network topology using the incremental shortest path first (iSPF) algorithm.

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*.

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 6.6.1 Packages

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

Table 2: Release 6.6.1 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-r661.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-r661.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r661.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.
Cisco IOS XR Security Package	ncs5500-k9sec-3.1.0.0-r661.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-r661.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf-2.0.0.0-r661.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs5500-li-1.0.0.0-r661.x86_64.rpm	Includes LI software images
Multicast Package	ncs5500-mcast-1.0.0.0-r661.rpm	Support Multicast

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 6.6.1
Copyright (c) 2013-2018 by Cisco Systems, Inc.

Build Information:
Built By     : hlo
Built On     : Thu Dec 20 18:56:08 PST 2018
Built Host   : iox-lnx-029
Workspace    : /auto/srcarchive16/prod/6.6.1/ncs5500/ws
Version      : 6.6.1
Location     : /opt/cisco/XR/packages/
```

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.

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
CSCvn41285	Continuous FIB Error - Action=CREATE Proto=ipv6. BCM SDK - No resources for operation

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        NC55-24H12F-SE    1.0   MIFPGA              CURRENT    0.03    0.03
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 MIFPGA              CURRENT    0.03    0.03
```

```
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 MIFPGA              CURRENT    0.03    0.03
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
0/6/1     NC55-MPA-1TH2H-S  0.4   MPAFPGA             CURRENT    0.53    0.53
0/6/2     NC55-MPA-12T-S    0.1   MPAFPGA             CURRENT    0.27    0.27
0/6       NC55-MOD-A-SE-S   0.201 MIFPGA              CURRENT    0.13    0.13
0/6       NC55-MOD-A-SE-S   0.201 Bootloader          CURRENT    1.00    1.00
0/6       NC55-MOD-A-SE-S   0.201 DBFPGA              CURRENT    0.14    0.14
0/6       NC55-MOD-A-SE-S   0.201 IOFPGA              RLOAD REQ  0.03    0.05
0/RP0     NC55-RP           1.1   Bootloader          CURRENT    9.29    9.29
0/RP0     NC55-RP           1.1   IOFPGA              CURRENT    0.09    0.09
0/RP1     NC55-RP           1.1   Bootloader          CURRENT    9.29    9.29
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.

- 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).

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.