# Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.9.1

Revised: August 22, 2023

# Network Convergence System 5500 Series Routers

## What's New in Cisco IOS XR Release 7.9.1

Cisco IOS XR Release 7.9.1 is a new feature release for Cisco NCS 5500 Series routers. For more details on the Cisco IOS XR release model and associated support, see Guidelines for Cisco IOS XR Software.

For more details on the Cisco IOS XR release model and associated support, see Guidelines for Cisco IOS XR Software.

### New in Documentation

| Product | Description |
|---|---|
| YANG Data Models Navigator | We have launched the tool as an easy reference to view the Data Models (Native, Unified, OpenConfig) supported in IOS XR platforms and releases. You can explore the data model definitions, locate a specific model, and view the containers and their respective lists, leaves, leaf lists, Xpaths, and much more.<br>As we continue to enhance the tool, we would love to hear your feedback. You are welcome to drop us a note here. |

### Software Feature Introduced and Enhanced

Unless specified the following features are not supported on the Cisco 5700 series fixed port routers and the Cisco NCS 5500 series routers that have the Cisco NC57 line cards installed and operating in the native or compatibility mode.

To enable the native mode on Cisco NCS 5500 series routers having Cisco NC57 line cards, use the **hw-module profile npu native-mode-enable** command in the configuration mode. Ensure that you reload the router after configuring the native mode.

| Feature | Description |
|---|---|
| **BGP** | |
| BGP Policy Accounting | Border Gateway Protocol (BGP) policy accounting measures and classifies IP traffic that is received from different peers. You can identify and account for all traffic by customer and bill accordingly.<br>Policy accounting is enabled on an individual input interface basis. Using BGP policy accounting, you can now account for traffic according to the route it traverses.<br>This feature is now supported on routers that have the Cisco NC57 based line cards with external TCAM (eTCAM) and operate in native mode.<br>This feature introduces these changes:<br>• **CLI**: The feature introduces the **hw-module fib bgppa stats-mode** command.<br>• **YANG Data Model**: New XPaths for Cisco-IOS-XR-um-hw-module-profile-cfg.yang (see GitHub, YANG Data Models Navigator) |

| Feature | Description |
|---|---|
| Detect Slow Peer in a BGP Group | BGP peers process the incoming BGP update messages at different rates. A slow peer is a peer that is processing incoming BGP update messages very slowly over a long period of time compared to other peers in the update sub-group.<br>Slow peer handling is important when routes are constantly changing over a long period of time. It is important to clean up stale information in the queue and send only latest state. It is helpful to know if there is a slow peer, which indicates there is a network issue, such as sustained network congestion or a receiver not processing updates on time, that the network administrator can address. |
| **Programmability** | |
| Stream Telemetry Data for ACL Byte Counters | You can stream model-driven telemetry (MDT) data to monitor the ACL statistics such as stopped, matched and denied IPv4 and IPv6 packets using Cisco-IOS-XR-ipv4-acl-oper.yang and Cisco-IOS-XR-ipv6-acl-oper.yang data models. This release lets you stream telemetry data to monitor the statistics using byte counters.<br>Previously, the only option to monitor ACL statistics was to use packet counters.<br>ACL with policer statistics is supported only on Cisco Network Convergence System 5700 Series Routers. |
| Securely retrieve dynamic NACM with LDAP over TLS authentication | You can now securely retrieve the NETCONF Access Control Model (NACM) policies or rules on-demand from a remote Lightweight Directory Access Protocol (LDAP) server to validate each NETCONF operation using Transport Layer Security (TLS) authentication. With TLS authentication, the router and the LDAP server communication is encrypted for security. Before this release, the policies or rules were not encrypted and posed security vulnerabilities. |
| Disable TLS Version 1.0 | Although Transport Layer Security (TLS) provides secure communication between servers and clients, TLS version 1.0 may pose a security threat. You can now disable TLS version 1.0 using the tlsv1-disable command. |
| **Interface and Hardware Component** | |
| Configure lower port speeds for dual-mode optical modules | You can now configure the lower port speed using simple CLI keyword: **speed** or **quad** and switch between the higher and lower speeds without changing the optical module.<br>Earlier, by default, only the higher port speed was available.<br>The feature introduces new XPaths for YANG Data Model: **Cisco-IOS-XR-optics-speed-cfg.yang**<br>(see GitHub, YANG Data Models Navigator.) |
| Support for DP04QSDD-HE0 optical module | This release introduces support for the Cisco 400G QSFP-DD High-Power (Bright) Optical Module, Ethernet Variant.<br>The Cisco 400G QSFP-DD High-Power (Bright) Optical module is an enhanced version of the currently available QSFP-DD ZR+ Optical Module, leveraging the same operational modes but providing as a major enhancement the increase of the Tx Optical Power up to +1dBm. |

| Feature | Description |
| --- | --- |
| Transmission of VLAN-Tagged LLDP Packets | With this release, transmitting VLAN-tagged LLDP packets on the subinterfaces is supported. Earlier, if LLDP is enabled on a subinterface, the LLDP packets are sent without a VLAN tag.<br>VLAN-tagged LLDP packets help to identify unauthorized devices on the network and discover VLANs configured on the network devices. You can monitor and enforce VLAN segregation, ensuring that devices are connected to the correct VLANs and preventing unauthorized access to sensitive network segments.<br>You can enable VLAN tagging for LLDP packets globally or on each subinterface using these commands:<br>• Globally: **lldp subinterfaces-tagged**<br>• Each subinterface: **lldp tagged** |
| Two-pass Forwarding over BVI | With this release, Integrated Routing and Bridging/Bridge-group Virtual Interface (IRB/BVI) supports Layer 2 ACL, QoS, and statistics on BVI-routed packets, using a two-pass forwarding model for packets over BVI.<br>This feature introduces the following changes:<br>• CLI: **hw-module irb**<br>• YANG Data Model: New XPaths for modules Cisco-IOS-XR-fia-hw-profile-cfg.yang and Cisco-IOS-XR-um-hw-module-profile-cfg.yang |
| oFEC Traffic Configuration for QDD-400G-ZRP-S | QDD-400G-ZRP-S optical module can now support the following oFEC traffic configurations:<br>• 400G-TXP-1x1 DAC-16 QAM<br>• 3x100G-MXP-1x1 DAC-8 QAM<br>• 2x100G-MXP-1x1.25 DAC-8 QAM<br>• 2x100G-MXP-1x1.25 DAC-16 QAM<br>This increases the interoperability of the QDD-400G-ZRP-S optical module across network components supporting these formats. |
| **IP Addresses and Services** | |
| DHCP Snooping for Layer 2 networks | With this feature, you can secure your DHCP infrastructure for Bridge Domains. DHCP Snooping operates in the Layer 2 network and prevents unauthorized DHCP servers from accessing your network.<br>This feature mitigates the security risks due to denial-of-service from rogue DHCP servers, which disrupt networks as they compete with legitimate DHCP servers that configure hosts on the network for communication.<br>You can use the following data models to configure this feature:<br>• Cisco-IOS-XR-ipv4-dhcpd-oper.yang<br>• Cisco-IOS-XR-l2vpn-oper.yang<br>• Cisco-IOS-XR-um-dhcp-ipv4-cfg.yang |

| Feature | Description |
| --- | --- |
| Display ACL Statistics in Bytes | We have enabled better visibility of traffic distribution, thus helping you in capacity planning, network optimization, and identifying potential bottlenecks in network planning by displaying ACL statistics in bytes in ingress and egress directions. Previously, the statistics were available only in packet counts. The ACL statistics in bytes addition to packet count, help identify the average package size in the network and detect if the packets are truncated or not.<br><br>You can view the ACL statistics in bytes for ACL-Based Policing only in Cisco NCS 5700 Series Routers and Cisco NC 57 line cards installed and operate in native and compatibility mode.<br><br>The following commands are modified in this feature:<br><br>• **show access-lists ipv4**<br><br>• **show access-lists ipv6** |
| Limit Address Resolution Protocol (ARP) Cache Entries per Interface | In this feature, you can configure the maximum limit for the number of entries of dynamic mapping between IP addresses and media addresses by ARP per interface. Limiting the number of entries provides overflow protections in ARP cache and protects the routers from DOS attacks by preventing memory overuse by cache entries.<br><br>This feature introduces the **arp cache-limit** command. |
| Rate Limiting the Multicast and Broadcast Punted Traffic at Subinterface level | When an Ethernet Virtual Connection (EVC) on a port is stormed with multicast or broadcast punted traffic, it impacts the performance of all the other EVCs on that particular port due to the NPU resource sharing. You can avoid such situations using rate limiting at subinterface level for the multicast and broadcast punted traffic.<br><br>This feature is supported on routers that have the NC57 SE (Services Edge Optimized) version line cards installed and operating in native mode. |
| **L2VPN and Ethernet Services** | |
| Call Admission Control for L2VPN P2P Services over Circuit-Style SR-TE Policies | This feature allows you to configure guaranteed bandwidth for Layer 2 P2P services steered over Circuit-Style SR-TE policies.<br><br>This ensures that a Circuit-Style SR-TE policy has sufficient bandwidth to accommodate a Layer 2 P2P service, while also preventing a L2 P2P service from being steered over a Circuit-Style SR-TE policy when there is insufficient available bandwidth. |
| Dynamic Address Resolution Protocol (ARP) Inspection (DAI) | The routers can now determine the validity of an Address Resolution Protocol (ARP) packet based on valid MAC address to IP address bindings stored in a trusted database built at runtime by DHCP snooping.<br><br>With this feature, the router relays only the valid ARP requests and responses, thus preventing the ARP poisoning attacks.<br><br>This feature introduces the following:<br><br>• **CLI:** New **dynamic-arp-inspection** command.<br><br>• **Yang Data Model**: Cisco-IOS-XR-l2vpn-oper.yang and Cisco-IOS-XR-ipv4-arp-oper.yang |

| Feature | Description |
|---|---|
| IP SourceGuard (IPSG) | You can now achieve source IP address filtering on a Layer 2 port, to prevent a malicious host from manipulating a legitimate host by assuming the legitimate IP address of the host. This feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts.<br>This filtering limits the ability of a host to attack the network by claiming the IP address of a neighbor host.<br>This feature introduces the following:<br>• **CLI:** New **ip-source-guard** command.<br>• **Yang Data Model**: Cisco-IOS-XR-l2vpn-oper.yang |
| Set EVPN Gateway IP Address in EVPN Route Type 5 NLRI | You can now set the EVPN gateway IP address in the EVPN route type 5 network layer reachability information (NLRI) that advertises IPv4 and IPv6 addresses. By setting the EVPN gateway IP address, only one IP-MAC route is withdrawn ensuring fast traffic switchover and reduced convergence time in the event of failure. Furthermore, this feature facilitates optimal traffic load balancing across the Virtual Network Forwarders (VNFs) and minimizes control plane updates when the VNFs or virtual machines (VMs) move.<br>Previously, the NLRI advertisement included the default EVPN gateway IP address of zero, which was represented as 0.0.0.0 for IPv4 and :: for IPv6. This resulted in the withdrawal of all prefixes one by one in the event of a failure, leading to traffic loss.<br>This feature introduces the following new commands:<br>• **set advertise-evpn-gw-ip**<br>• **advertise gateway-ip-disable** |
| **L3VPN** | |
| Resource Optimization for MPLS Inter-AS Option B | You can now preserve MPLS encapsulation ID resources for Inter-AS option B local labels on Cisco NCS 5700 Series routers with Embedded Ternary Content-Addressable Memory (eTCAM) cards without the need to allocate any additional resources for these IDs. This feature is enabled by default and you cannot disable it.<br>Previously, these encapsulation IDs were allocated but left unused. |
| **Multicast** | |
| Load Balancing in Unicast GRE Tunnels | We now support the Equal-Cost Multipath (ECMP) and Link Aggregation Groups (LAG) load-balancing techniques for transporting multicast traffic over unicast GRE tunnels.<br>ECMP and LAG provide higher bandwidth and redundancy, better network performance, and fault tolerance by using all available links. |
| Multicast Traffic Over Layer 2 IPv6 Network | This feature is supported on routers that have the Cisco NC57 line cards installed and operate in native and compatible modes.<br>Routers use Multicast Listener Discovery (MLD) protocol to discover the devices in a network and create route entries or update the route status in an IPv6 multicast network. |
| **Modular QoS** | |

| Feature | Description |
|---|---|
| Additional Routers Supported for ACL with Fragment Match | You can now prevent malicious users from staging denial of service (DoS) attacks for non-initial IP fragments on Cisco NCS 5700 Series Routers and on NCS 5500 Series Routers with line cards other than NC57 line cards.<br>You can achieve this by configuring an ACL with fragment match and specifying QoS match actions to rate-limit noninitial fragments for IPv4 traffic.<br>Previously, this functionality was available only on systems with NC57 line cards running in native mode. |
| **Routing** | |
| Flexible-Algorithm Redistribution in IP Networks | You can now select or filter the prefix-matching algorithm number during route redistribution, so that only the Flex-Algorithms that you configured for specific addresses are redistributed.<br>This feature introduces the **set algorithm** command. |
| Limiting LSA numbers in a OSPF Link-State Database | The nonself-generated link-state advertisements (LSAs) for a given Open Shortest Path First (OSPF) process is limited to 500000. This protection mechanism prevents routers from receiving many LSAs, preventing CPU failure and memory shortages, and is enabled by default from this release onwards. If you have over 500000 LSAs in your network, configure the **max-lsa** command with the expected LSA scale before upgrading to this release or later.<br>This feature modifies the following commands:<br>• **show ospf** to display the maximum number of redistributed prefixes.<br>• **show ospf database database-summary detail** to display the number of LSA counts per router.<br>• **show ospf database database-summary adv-router**router ID to display the router information and the LSAs received from a particular router. |
| Limiting the Maximum Redistributed Type-3 LSA Prefixes in OSPF | By default, the maximum redistributed Type-3 LSA prefixes for a given OSPF process is now limited to 100000. This mechanism prevents OSPF from redistributing a large number of prefixes as Type-3 LSAs and therefore preventing high CPU utilization and memory shortages.<br>Once the number of redistributed prefixes is reached or exceeds the threshold value, the system log message is generated, and no more prefixes are redistributed. |
| **Segment Routing** | |
| IS-IS: Flexible Algorithm Reverse Affinity | This feature enhances the IS-IS Flexible Algorithm link admin group (affinity) constraint to include link colors on links in the reverse direction toward the calculating router.<br>The ability to apply affinity constraints in the reverse direction provides additional control for IS-IS Flexible Algorithm path computation. |
| SR-TE Automated Steering Without Service Label | This feature allows traffic to a BGP service route to be steered over an SR-TE policy using the AS principles, and without imposing the service route's prefix label.<br>This feature enables use-cases such as centralized BGP EPE for 6PE in an SR-MPLS network.<br>This feature introduces the following command:<br>• **bgp prefix-label ignore** |

| Feature | Description |
| --- | --- |
| SR-TE Explicit Segment Lists with Mix of IPv4 and IPv6 Segments | Explicit segment list can be configured to include IPv6 segments, for example IPv6 adjacency SIDs or IPv6 EPE SIDs.<br>This feature enables use-cases such as Centralized BGP EPE for 6PE in an SR-MPLS Network. |
| SRv6 Services: Services with Remote SIDs from W-LIB | This feature enables an SRv6 headend node to receive and install remote SIDs with Wide (32-bit) functions (Remote W-LIB).<br>There is no new CLI to enable this capability at the ingress PE. |
| **System Management** | |
| Auto-Save with Secure File-Transfer and Additional Configurable Parameters | Apart from automatically backing up the running configuration after every commit, you can also do the following with Auto-Save:<br>• Save running configurations to remote systems using Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP).<br>• Configure wait-time between two subsequent auto-saves.<br>• Append time-stamp to the file name of the saved configuration.<br>• Save the encrypted password.<br>• Specify the maximum number of files that you can auto-save.<br>The feature introduces these changes:<br>CLI: Modified the **configuration commit auto-save** command by adding the following keywords:<br>• **filename scp**<br>• **filename sftp**<br>• **wait-time**<br>• **timestamp**<br>• **password**<br>• **maximum**<br>Yang Data Model:<br>• New XPaths for Cisco-IOS-XR-config-autosave-cfg<br>• New XPaths for Cisco-IOS-XR-um-config-commit-cfg |
| FQDN for NTP Server on Non-default VRF | You can now specify a Fully Qualified Domain Name (FQDN) as the hostname for NTP server configuration over non-default VRFs.<br>FQDNs are easy to remember compared to numeric IP addresses. Service migration from one host to another can cause a change in IP address leading to outages.<br>Prior releases allowed FQDN handling in only default VRFs. |

| Feature | Description |
| --- | --- |
| Support for SFTP (Secure File Transfer Protocol) and SCP (Secure Copy Protocol) options in the Copy command | With this feature, the router can transfer data to a remote server on SFTP and SCP by using the underlying SSH protocol implementation. You can use the SFTP and SCP option to facilitate secure transfer of configuration files from the router to an achieve server.<br>This feature modifies the **copy** command. |
| GNSS MIBs Traps for Antenna Open-Circuit, Satellite Visibility and Module Lock Status | Your router uses Global Navigation Satellite System (GNSS) as the satellite system for enhanced timing synchronization of the timing interface. GNSS receiver picks up signals from this satellite system to recalculate position, velocity and local time to high precision.<br>From this release, you can track the GNSS module antenna OC alarm status, status of the GNSS satellite visibility, and specify the lock status of GNSS module.<br>You can useMIB Navigator tool to know more about the following traps introduced in this release:<br>• ciscoGnssAntennaOCAlarmStatus<br>• ciscoGnssSatelliteVisibilityStatus<br>• ciscoGnssModuleLockStatus |
| Enhanced SyncE and extended ESMC | ITU-T G.8262.1 recommendation defines the requirements for timing devices used in synchronizing network equipment. For example, bandwidth, frequency accuracy, holdover, and noise generation.<br>With Enhanced SyncE (eSyncE) and Extended Ethernet Synchronization Message Channel (eESMC) support, the routers are capable of handling the following SyncE clocks on the network:<br>• Enhanced ethernet equipment clock (eEEC)<br>• Enhanced primary reference clock (ePRC)<br>• Enhanced primary reference timing clock (ePRTC)<br>This feature is supported on the following NCS5500 and NCS 5700 variants:<br>• Cisco NCS55A2<br>• Cisco NCS 57C3<br>• Cisco NCS-57B1<br>• Cisco NCS-57C1 |

| Feature | Description |
|---|---|
| New Cisco-NTP-MIB Traps to Monitor NTP server and Improve Timing Accuracy | Cisco-NTP-MIB allows you to monitor NTP on the server and client using SNMP MIB. This release supports new traps, which will help monitor the NTP server and improve timing accuracy . These traps also display the NTP server's current status, the local clock's stratum, the maximum error in seconds, and the delay in round-trip in seconds.Use MIB Navigator to know more about the newly added traps:<br>• cntpSysPeer<br>• cntpSysSrvStatus<br>• cntpSysStratum<br>• cntpSysRootDelay<br>• cntpSysRootDispersion<br>• cntpPeers |
| **System Security** | |
| Accessing Certificate Enrollment URL Using HTTP Proxy via specified Source Interface | With this feature, you can enable the router to use an HTTP proxy to access the certificate enrollment URL. The router uses the already available HTTP proxy configurations to fetch Certificate Revocation List (CRL) to access the certificate enrollment URL. In addition, you can specify a source interface through which the router places the enrollment requests.<br>This feature reduces the enrollment URL access failures when the router fails to reach the enrollment URL directly or when the enrollment URL is only reachable via an HTTP proxy. |
| IEEE 802.1X Port-Based Authentication Support for Multiple Authentication and Multiple Host Modes | The IEEE 802.1X port-based authentication allows only authorized supplicants to access the network. The IEEE 802.1X port-based authentication now supports multiple authentication and multiple host modes to allow multiple hosts or MAC addresses on a single port.<br>Applicable to the following Cisco NCS 5500 Series Routers:<br>• NCS-57C3-MOD-SYS<br>• NC57-36H6D-S<br>• NC57-MOD-S<br>Applicable to the following Cisco NCS 5700 Series Router:<br>• NCS-57C1-48Q6-SYS |

| Feature | Description |
|---|---|
| Secure Key Integration Protocol (SKIP) for Routers | The NCS 5500 Series Routers are now capable of handling the SKIP protocol. With this ability, it can communicate with external quantum devices. This helps in using Quantum Key Distribution (QKD) devices for exchanging MACsec encryption keys between routers to eliminate the key distribution problem in a post quantum world where the current cryptographic systems are no longer secure due to the advent of quantum computers.<br>This feature introduces the following:<br>• **CLI:**<br>• **crypto-sks-kme**<br>• **show crypto sks profile**<br>• **show crypto sks profile stats**<br>• **Yang Data Model**: Cisco-IOS-XR-um-sks-server-cfg.yang<br>For more information on Quantum Key Distribution, see Post Quantum Security Brief. |
| Securely retrieve NACM policies using LDAP over TLS connection | You can now securely retrieve the NETCONF Access Control Model (NACM) policies or rules from a remote Lightweight DirectoryAccess Protocol (LDAP) server using Transport Layer Security (TLS) authentication. With TLS authentication, the communication between the router and the LDAP server is encrypted for security.<br>Before this release, the communication between the LDAP server and the router was not secured. |

## YANG Data Models Introduced and Enhanced

This release introduces or enhances the following data models. For detailed information about the supported and unsupported sensor paths of all the data models, see the Github repository. To get a comprehensive list of the data models supported in a release, navigate to the Available-Content.md file for the release in the Github repository. The unsupported sensor paths are documented as deviations. For example, openconfig-acl.yang provides details about the supported sensor paths, whereas cisco-xr-openconfig-acl-deviations.yang provides the unsupported sensor paths for openconfig-acl.yang on Cisco IOS XR routers.

You can also view the data model definitions using the YANG Data Models Navigator tool. This GUI-based and easy-to-use tool helps you explore the nuances of the data model and view the dependencies between various containers in the model. You can view the list of models supported across Cisco IOS XR releases and platforms, locate a specific model, view the containers and their respective lists, leaves, and leaf lists presentedvisually in a tree structure.

To get started with using data models, see the *Programmability Configuration Guide for Cisco NCS 5500 Series Routers*.

| Feature | Description |
|---|---|
| **Programmability** | |
| Cisco-IOS-XR-config-autosave-cfg | This Cisco native YANG data model enables you to automatically backup the running configuration files after every commit is made. |
| Cisco-IOS-XR-um-config-commit-cfg | This unified data model enables you to automatically back up the running configuration of the routerafter every commit is made. |

| Feature | Description |
| --- | --- |
| openconfig-network-instance.yang Version 0.2.3 | In this release, the installed counter in the OpenConfig data model is enhanced to view the number of routes that are installed in Routing Information Base (RIB) from a specific neighbor per Address Family Identifiers (AFI) or Subsequent Address Family Identifiers (SAFI).<br>The model supports a single instance of BGP with default VRF, and IPv4/IPv6 address family. Cross AFI where an IPv4 route learnt from an IPv6 neighbor, and vice versa, is not supported.<br>You can stream Event-driven telemetry (EDT) and Model-driven telemetry (MDT) data. |
| Cisco-IOS-XR-um-mpls-static-cfg.yang | This Unified data model enables you to configure Label Switched Paths (LSPs) with statically assigned ingress labels that are mapped to prefixes or VRFs and egress paths explicitly defined or mapped to next hops. With this release, you can use the data model to disable the default route to resolve issues with the next hop information.<br>We recommend that you use the data model according to the CLI hierarchy. |
| Cisco-IOS-XR-remote-attestation -agent-oper.yang | This Cisco native data model defines the remote attestation of the routers' security posture to assess the trustworthiness of hardware and software on the router.<br>With this release, you can use the data model to send gNMI requests to retrieve the system integrity information such as secure boot status,Attestation Identity Key (AIK) and Secure Unique Device Identifier (SUDI) certificates.<br>gNMI support is introduced for the show platform security attest certificate command. |
| openconfig-isis.yang Version 1.0.0 | The OpenConfig data model is revised from version 0.6.0 to 1.0.0 to simplify the authentication keychain nodes. With this feature, you can configure the authentication type to limit the establishment of adjacencies and the exchange of LSPs. You can also retrieve the operational state of the authentication nodes. |

| Feature | Description |
|---|---|
| openconfig-network-instance.yang | In this release, the installed counter in the OpenConfig data model is enhanced to view the number of routes that are installed in Routing Information Base (RIB) from a specific neighbor per Address Family Identifiers (AFI) or Subsequent Address Family Identifiers (SAFI).<br>The model supports a single instance of BGP with default VRF, and IPv4/IPv6 address family.<br>**Note** Cross AFI where an IPv4 route learnt from an IPv6 neighbor, and vice versa, is not supported.<br>You can stream Event-driven telemetry (EDT) and Model-driven telemetry (MDT) data. |
| openconfig-bgp.yang Version 9.1.0 | This OpenConfig data model, which is part of the **openconfig-network-instance.yang** data model is revised from version 6.0.0 to 9.1.0. This version introduces the following changes:<br>• Use the **restart-time** node to configure the time interval (in seconds) to reestablish a disconnected BGP session when the maximum prefix limit is exceeded.<br>• Remove the **restart-timer** node that is used to set the maximum restart time for local BGP sessions from global and neighbor Address Family Indicator (AFI) and Subsequent Address Family Indicator (SAFI) sessions. |
| Cisco-IOS-XR-optics-speed-cfg.yang | This Cisco native YANG data model is introduced to configure lower port speeds for dual-mode optical modules. |

## Hardware Introduced

| Hardware Feature | Description |
|---|---|
| Support for QDD-100G-ZR on applicable NCS-5500 | This release launches the following new optics on selective hardware within the product portfolio. For details refer to the Transceiver Module Group (TMG) Compatibility Matrix.<br>• QDD-100G-ZR |
| Support for DP04QSDD-HE0 optical module | This release introduces support for the Cisco 400G QSFP-DD High-Power (Bright) Optical Module, Ethernet Variant.<br>The Cisco 400G QSFP-DD High-Power (Bright) Optical module is an enhanced version of the currently available QSFP-DD ZR+ Optical Module, leveraging the same operational modes but providing as a major enhancement the increase of the Tx Optical Power up to +1dBm.<br>The DP04QSDD-HE0 optical module is supported on the NCS-57C3-MOD-SYS and NCS-57C3-MODS-SYS routers using NC57-MPA-2D4H-S MPA. |

| Hardware Feature | Description |
|---|---|
| Support for various optics on applicable NCS 5500 and NCS 5700 Series Routers | This release supports the following optics on selective hardware within the product portfolio. For details refer to the Transceiver Module Group (TMG) Compatibility Matrix.<br>• QDD-400G<br>• QDD-4X100G<br>• QDD-2X100G<br>• QSFP-100G<br>• QSFP-4SFP25G<br>• QSFP-40G<br>• QSFP-4X10G<br>• QSFP-H40G<br>• SFP-50G<br>• SFP-25G-BX40D-I/-BX40OU-I<br>• SFP-10/25G-BXD-I/-BXU-I |

## Behavior Changes

- Prior to Cisco IOS XR release 7.2.1, a segment of an explicit segment list can be configured as an IPv4 address (representing a Node or a Link) using the **index** *index***address ipv4** *address* command.

  Starting with Cisco IOS XR release 7.2.1, an IPv4-based segment (representing a Node or a Link) can also be configured with the new **index** *index* **mpls adjacency***address* command. The configuration is stored in NVRAM in the same CLI format used to create it. There is no conversion from the old CLI to the new CLI.

  Starting with Cisco IOS XR release 7.9.1, the old CLI has been deprecated. Old configurations stored in NVRAM will be rejected at boot-up.

  As a result, explicit segment lists with IPv4-based segments using the old CLI must be re-configured using the new CLI.

  There are no CLI changes for segments configured as MPLS labels using the **index** *index* **mpls label** *label* command.

- If you are on a release before Cisco IOS XR Release 7.4.1, you can configure SR-ODN with Flexible Algorithm constraints using the **segment-routing traffic-eng on-demand color** *color* **dynamic sid-algorithm** *algorithm-number* command.

  Starting with Cisco IOS XR release 7.4.1, you can also configure SR-ODN with Flexible Algorithm constraints using the new **segment-routing traffic-eng on-demand color** *color* **constraints segments sid-algorithm** *algorithm-number* command.

  From Cisco IOS XR Release 7.9.1, the **segment-routing traffic-eng on-demand color** *color* **dynamic sid-algorithm** *algorithm-number* command is deprecated. Previous configurations stored in NVRAM will be rejected at boot-up.

  Hence, for Cisco IOS XR Release 7.9.1, you must reconfigure all SR-ODN configurations with Flexible Algorithm constraints that use the on-demand dynamic sid-algorithm with the on-demand constraints command.

## Features Supported on Cisco NC57 Line Cards and NCS 5700 Fixed Routers

The following table lists the features supported on Cisco NC57 line cards in compatibility mode (NC57 line cards with previous generation NC55 line cards in the same modular chassis) and native mode (modular chassis with only NC57 line cards and NCS5700 fixed chassis)

***Table 1: Features Supported on Cisco NC57 Line Cards and NCS 5700 fixed routers***

| Feature | Compatible Mode | Native Mode |
|---|---|---|
| Support for Layer 2 IPv6 Multicast Traffic | ✓ | ✓ |
| SRv6 Services: Services with Remote SIDs from W-LIB | × | ✓ |
| Load Balancing in Unicast GRE Tunnels | ✓ | ✓ |
| BGP Policy Accounting | × | ✓ |
| Configure Lower Port Speed of Dual-Mode Optical Modules | ✓ | ✓ |
| Two-pass Forwarding over BVI | ✓ | ✓ |
| Traffic Configuration for QDD-400G-ZRP-S | ✓ | ✓ |
| Cisco-IOS-XR-um-mpls-static-cfg.yang | ✓ | ✓ |
| uRPF in Strict Mode | × | ✓ |
| 802.1X Port-Based Authentication | ✓ | ✓ |
| Monitor ACL Statistics via Byte Counters Telemetry Data | ✓ | ✓ |
| Additional Systems Supported for Configuring an ACL with Fragment Match | ✓ | ✓ |
| Cisco-IOS-XR-attestation-agent-oper.yang | ✓ | ✓ |
| Accessing Certificate Enrollment URL Using HTTP Proxy | ✓ | ✓ |
| GRID Optimization for MPLS Inter-AS Option-B Local Labels | ✓ | ✓ |
| Display ACL Statistics in Bytes | ✓ | ✓ |

For the complete list of features supported on Cisco NC57 line cards until Cisco IOS XR Release 7.9.1. see:

- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.8.2
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.8.1
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.7.2
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.7.1
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.6.1
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.5.3
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.5.2

- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.5.1
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.4.2
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.4.1
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.3.1
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.2.2
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.2.1

# Caveats

There are no caveats in this release.

# Release Package

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

Visit the Cisco Software Download page to download the Cisco IOS XR software images.

***Table 2: Release 7.9.1 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:<br>• Host operating system<br>• System Admin boot image<br>• IOS XR boot image<br>• BGP packages |
| **Individually-Installable Optional Packages** | | |
| **Feature Set** | **Filename** | **Description** |
| Cisco IOS XR Manageability Package | ncs5500-mgbl-3.0.0.0-r791.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-r791.x86_64.rpm<br>ncs5500-mpls-te-rsvp-2.2.0.0-r791.x86_64.rpm | MPLS and MPLS Traffic Engineering (MPLS-TE) RPM. |
| Cisco IOS XR Security Package | ncs5500-k9sec-3.1.0.0-r791.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-r791.x86_64.rpm | Support ISIS |
| Cisco IOS XR OSPF package | ncs5500-ospf-2.0.0.0-r791.x86_64.rpm | Support OSPF |
| Lawful Intercept (LI) Package | ncs5500-li-1.0.0.0-r791.x86_64.rpm | Includes LI software images |
| Multicast Package | ncs5500-mcast-1.0.0.0-r791.rpm | Support Multicast |

***Table 3: Release 7.9.1 TAR files for Cisco NCS 5500 Series Router***

| Feature Set | Filename |
|---|---|
| NCS 5500 IOS XR Software 3DES | NCS5500-iosxr-k9-7.9.1.tar |
| NCS 5500 IOS XR Software | NCS5500-iosxr-7.9.1.tar |
| NCS 5500 IOS XR Software | NCS5500-docs-7.9.1.tar |

***Table 4: Release 7.9.1 Packages for Cisco NCS 5700 Series Router***

| Feature Set | Filename |
|---|---|
| NCS 5700 IOS XR Software | ncs5700-x64-7.9.1.iso |
| NCS 5700 IOS XR Software (only k9 RPMs) | ncs5700-k9sec-rpms.7.9.1.tar |
| NCS 5700 IOS XR Software Optional Package | NCS5700-optional-rpms.7.9.1.tar<br>This TAR file contains the following RPMS:<br>• optional-rpms/cdp/*<br>• optional-rpms/eigrp/*<br>• optional-rpms/telnet/* |

# Determine Software Version

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

```
Router# show version
Cisco IOS XR Software, Version 7.9.1
Copyright (c) 2013-2023 by Cisco Systems, Inc.

Build Information:
 Built By     : ingunawa
 Built On     : Sun Apr  2 01:04:35 PDT 2023
 Built Host   : iox-ucs-047
 Workspace    : /auto/srcarchive15/prod/7.9.1/ncs5500/ws
 Version      : 7.9.1
 Location     : /opt/cisco/XR/packages/
 Label        : 7.9.1

cisco NCS-5500 () processor
System uptime is 19 hours 14 minutes
```

# Determine Firmware Support

Use the **show hw-module fpd** command in EXEC and 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.

**Note** You can also use the **show fpd package** command in Admin mode to check the fpd versions.

This sample output is for **show hw-module fpd** command from the Admin mode:

```
sysadmin-vm:0_RP0# show hw-module fpd
                                                                      FPD Versions
                                                                      ==============
Location  Card type         HWver FPD device       ATR Status      Run      Programd
--------------------------------------------------------------------------------
0/2       NC57-18DD-SE      1.1   Bootloader           CURRENT     1.03      1.03
0/2       NC57-18DD-SE      1.1   DBFPGA               CURRENT     0.14      0.14
0/2       NC57-18DD-SE      1.1   IOFPGA               CURRENT     0.22      0.22
0/2       NC57-18DD-SE      1.1   SATA-INTEL_240G      CURRENT   1132.00   1132.00
0/5       NC57-24DD         1.1   Bootloader           CURRENT     1.03      1.03
0/5       NC57-24DD         1.1   DBFPGA               CURRENT     0.14      0.14
0/5       NC57-24DD         1.1   IOFPGA               CURRENT     0.23      0.23
0/5       NC57-24DD         1.1   SATA-INTEL_240G      CURRENT   1132.00   1132.00
0/RP0     NC55-RP           1.1   Bootloader           CURRENT     9.31      9.31
0/RP0     NC55-RP           1.1   IOFPGA               CURRENT     0.09      0.09
0/RP0     NC55-RP           1.1   SATA-M600-MU         CURRENT     6.00      6.00
0/RP1     NC55-RP           1.0   Bootloader           CURRENT     9.31      9.31
0/RP1     NC55-RP           1.0   IOFPGA               CURRENT     0.09      0.09
0/RP1     NC55-RP           1.0   SATA-M600-MU         CURRENT     6.00      6.00
0/FC0     NC55-5508-FC2     1.0   Bootloader           CURRENT     1.80      1.80
0/FC0     NC55-5508-FC2     1.0   IOFPGA               CURRENT     0.19      0.19
0/FC0     NC55-5508-FC2     1.0   SATA-M5100           CURRENT    75.00     75.00
0/FC1     NC55-5508-FC2     1.0   Bootloader           CURRENT     1.80      1.80
0/FC1     NC55-5508-FC2     1.0   IOFPGA               CURRENT     0.19      0.19
0/FC1     NC55-5508-FC2     1.0   SATA-M5100           CURRENT    75.00     75.00
0/FC2     NC55-5508-FC2     1.0   Bootloader           CURRENT     1.80      1.80
0/FC2     NC55-5508-FC2     1.0   IOFPGA               CURRENT     0.19      0.19
0/FC2     NC55-5508-FC2     1.0   SATA-M5100           CURRENT    75.00     75.00
0/FC3     NC55-5508-FC2     1.0   Bootloader           CURRENT     1.80      1.80
0/FC3     NC55-5508-FC2     1.0   IOFPGA               CURRENT     0.19      0.19
0/FC3     NC55-5508-FC2     1.0   SATA-M5100           CURRENT    75.00     75.00
0/FC5     NC55-5508-FC2     1.0   Bootloader           CURRENT     1.80      1.80
0/FC5     NC55-5508-FC2     1.0   IOFPGA               CURRENT     0.19      0.19
0/FC5     NC55-5508-FC2     1.0   SATA-M5100           CURRENT    75.00     75.00
0/SC0     NC55-SC           1.5   Bootloader           CURRENT     1.74      1.74
0/SC0     NC55-SC           1.5   IOFPGA               CURRENT     0.10      0.10
0/SC1     NC55-SC           1.5   Bootloader           CURRENT     1.74      1.74
0/SC1     NC55-SC           1.5   IOFPGA               CURRENT     0.10      0.10
```

# Important Notes

- 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.
- BGP-Labeled Unicast (LU) Prefix-Independent Convergence (PIC) auto-protection feature may cause equal cost multipath (ECMP) FEC NPU resource exhaustion on BGP peering devices for IPv4/IPv6 addresses. From Cisco IOS XR Release 7.9.1 onwards, the auto-protection feature for BGP-LU multipath PIC is disabled by default. To enable this feature, use the **hw-module fib bgp-mp-pic auto-protect enable** command. After executing the command, you must reload the router.For more information, see *BGP-LU Multipath PIC with Auto Protection* section in *BGP Prefix Independent Convergence* chapter in *BGP Configuration Guide for Cisco NCS 5500 Series Routers.*

## Supported Transceiver Modules

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

## 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.

**Note**

- If you use a TAR package to upgrade from a Cisco IOS XR release prior to 7.x, the output of the **show install health** command in admin mode displays the following error messages:

```
sysadmin-vm:0_RSP0# show install health
. . .
ERROR /install_repo/gl/xr -rw-r--r--. 1 8413 floppy 3230320 Mar 14 05:45 <platform>-isis-2.2.0.0-r702.x86_64
ERROR /install_repo/gl/xr -rwxr-x---. 1 8413 165 1485781 Mar 14 06:02 <platform>-k9sec-3.1.0.0-r702.x86_64
ERROR /install_repo/gl/xr -rw-r--r--. 1 8413 floppy 345144 Mar 14 05:45 <platform>-li-1.0.0.0-r702.x86_64
```

You can ignore these messages and proceed with the installation operation.

- Quad configurations will be lost when you perform a software downgrade on a NCS-55A1-48Q6H device from IOS XR Release 7.5.1 onwards to a release prior to IOS XR Release 7.5.1 due to non-backward compatibility change. The lost configuration can be applied manually after the downgrade.

**Note** A quad is a group of four ports with common speeds, 1G/10G or 25G. You can configure the ports speed fo by using the **hw-module quad** command.

## 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.

## Cisco IOS XR Error messages

To view, search, compare, and download Cisco IOS XR Error Messages, refer to the Cisco IOS XR Error messages tool.

## Cisco IOS XR MIBs

To determine the MIBs supported by platform and release, refer to the Cisco IOS XR MIBs tool.

## Related Documentation

The most current Cisco NCS 5500 router documentation is located at the following URL:

https://www.cisco.com/c/en/us/td/docs/iosxr/ios-xr.html

**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.