Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.7.1

Revised: November 20, 2023

Network Convergence System 5500 Series Routers

What's New in Cisco IOS XR Release 7.7.1

Cisco IOS XR Release 7.7.1 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.

New in Documentation

This release introduces rich and intuitive ways for you to access YANG data models supported in the Cisco IOS XR software.

Product	Description
Cisco IOS XR Error Messages	Search by release number, error strings, or compare release numbers to view a detailed repository of error messages and descriptions.
Cisco IOS XR MIBs	Select the MIB of your choice from a drop-down to explore an extensive repository of MIB information.
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. As we continue to enhance the tool, we would love to hear your feedback. You are welcome to drop us a note here.
Use Case-based Documentation at Learning Labs	You can now quickly explore and experiment on use-cases without setting up any hardware resources with the new Interactive documentation for Cisco 8000 routers on DevNet Learning Labs. Powered by Jupyter, the automated code blocks within the documentation enable you to configure the desired functionality on the routers and retrieve real-time output swiftly. Check out the new interactive documentation here: • End to end 3-stage CLOS Networks for SONiC • Use cases for QoS and Model-driven Telemetry

Software Features Enhanced and Introduced

To learn about features introduced in other Cisco IOS XR releases, select the release from the Documentation Landing Page.

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	

Feature	Description
Allow an AS Path using the router ASN on Cisco Network Convergence System 5700 Series Routers	BGP prevents traffic looping based on the verification of AS numbers in the AS Path. The receiving router drops traffic if it detects its own AS number in the AS Path of the received BGP packet. However, in some instances, such as in a central firewall that requires inter-AS advertising of specific prefixes, you may need a back-and-forth of traffic. For such scenarios, this functionality allows routers to process traffic even if they detect their AS number in the AS path. Configure the **allowas-in** command to allow an AS path for a specific number of times using the router ASN. From this release onwards this functionality is also supported on Cisco Network Convergence System 5700 Series Routers.
BGP Long-lived Graceful Restart Capability on Cisco Network Convergence System 5700 Series Routers	You can retain BGP route information such as IP address, origin packets, destination packets including BGP session failures both in BGP Routing table and forwarding table. BGP Long-lived graceful restart (LLGR) enables the router to retain or maintain stale routes for a longer period after a BGP session fails. LLGR comes into effect after graceful restart (GR) ends. BGP LLGR is also referred as BGP persistence. This feature introduces the following command: • **long-lived-graceful-restart** From this release onwards this functionality is also supported on Cisco Network Convergence System 5700 Series Routers.
Convergence for BGP Labeled Unicast PIC Edge	This feature improves the convergence time of BGP labeled unicast (LU) routes to subseconds when an ingress provider edge router fails or loses PE router connectivity, and another PE router needs to be connected. This feature minimizes traffic drops when the primary paths fail for the BGP LU routes. This feature is now supported on routers that have Cisco NC57 line cards installed and operate in native and compatibility mode`
Install Multiple External and Internal BGP Paths for Load Balancing on Cisco Network Convergence System 5700 Series Routers	You can configure multipath load balancing with both external BGP (eBGP) and internal BGP (iBGP) paths in BGP networks that are configured to use MPLS VPNs A MPLS VPN is a collection of sites that are linked together by an MPLS provider core network. Each location has one or more customer edge (CE) devices that connect to one or more provider edge (PE) devices. PEs communicate with one another using the Multiprotocol-Border Gateway Protocol (MP-BGP). This feature provides improved load balancing deployment and service offering capabilities. It is helpful for multi-homed autonomous systems and PE routers that import both eBGP and iBGP paths from multihomed and stub networks. From this release onwards this functionality is also supported on Cisco Network Convergence System 5700 Series Routers.
OSPF enablement for BGP paths based on IGP metrics on Cisco Network Convergence System 5700 Series Routers	You can enable BGP to choose the shortest path between two nodes based on IGP metrics, even if the nodes are in different autonomous systems (ASs). This is possible because the Accumulated IGP Attribute enables deployments for multiple adjacent BGP ASs. From this release onwards this functionality is also supported on Cisco Network Convergence System 5700 Series Routers.
BGP Peer Group on Cisco Network Convergence System 5700 Series Routers	To avoid applying individual policies for each BGP neighbor residing in a peer group, you can now create a BGP peer group and use a single policy for the group, thus allowing efficient update calculation along with simplified configuration. From this release onwards this functionality is also supported on Cisco Network Convergence System 5700 Series Routers.

Feature	Description
Interface and Hardware Component	
Enhancement to Ethernet SLA Statistics Measurement	You can now configure the size of bins that are used to aggregate the results of Ethernet SLA statistics, in microseconds. The size of the bins is defined by the **width** value of delay and jitter measurement in Ethernet SLA statistics. You can configure the **width** value ranging from 1 to 10000000 microseconds. This enhancement provides granularity to store more accurate results of Ethernet SLA statistics in the aggregate bins. In earlier releases, you could only configure the **width** value for the delay and jitter measurement in milliseconds. This feature introduces the **usec** keyword in the **aggregate** command.
SPAN Filtering on Layer 2 Interfaces for Cisco NC57 Line Cards	SPAN filtering allows you to filter and mirror the incoming (Rx) DNS, HTTP, HTTPS, and TLS Layer 2 interface traffic. To enable the filtering, use the **hw-module profile span-filter l2-rx-enable** command. Thus, providing the user more flexibility to filter, monitor, and troubleshoot the DNS, HTTP, HTTPS, and TLS traffic. This feature is now supported on routers that have the Cisco NC57 line cards installed that operate in the native mode.
IP Addresses and Services	
Egress Hybrid ACL Compression Support	When you configure hybrid ACLs at the egress, you can separate address prefixes and ports into two object groups or access control entries (ACEs). Besides flexibility, using hybrid ACLs offers you granularity in adding multiple object groups at the egress, enhancing your traffic security. Plus, because this functionality uses the internal and external TCAM, the egress ACL has more space and resources for compression, accommodating more ACLs. This feature, enabled on the NC57-24DD and NC57-18DD-SE line cards, introduces the **acl egress compress** option for the `acl ingress compression` command.
L2VPN and Ethernet Services	
Private Line Emulation over EVPN-VPWS Single Homed	You can now configure EVPN VPWS to carry the client traffic from ports like FC, OTN, SDH, SONET, or Ethernet and forward the traffic to the core network by using Private Line Emulation (PLE). PLE emulates the switching capabilities of FC, OTN, SDH, SONET, or Ethernet ports without needing a dedicated equipment and allows interconnecting optical networks with Ethernet networks. This feature introduces the **port-mode** command. This release introduces new and modified YANG data models for PLE. For the list of supported data models, see Supported Yang Data Models for PLE. You can access these data models from the Github repository.
VPLS VFI with BVI as Routed Interface on Cisco 5700 Fixed Routers and Cisco NC57 Line Cards	VPLS virtual forwarding interface (VFI) is a multipoint Layer 2 VPN technology connecting two or more customer devices to perform native bridging functions such as forwarding. Bridged Virtual Interface (BVI) is a virtual interface within the router that acts like a normal routed interface. You can enable BVI on VPLS VFI, where multiple interfaces can be part of a single bridge group. This functionality allows you to route the incoming traffic to the bridge group to L3 interfaces. This feature is now supported on Cisco 5700 Fixed Routers and on routers that have Cisco NC57 line cards installed and operate in native and compatibility modes.

Feature	**Description**
Multicast	
Draft-Rosen Multicast VPN (Profile 0) in PIM spare mode (SM)	Draft-Rosen Multicast VPN (Profile 0) is now supported in PIM sparse mode (PIM-SM) between the PE routers that are running in VRF mode. Prior to this release, Profile 0 was supported only in PIM Source Specific Multicast (SSM) mode.
Mtrace version 2 - Traceroute facility for IP Multicast	Mtrace version2, or Mtrace2, is an IP multicast traceroute facility which allows the tracing of an IP multicast routing path. Based on RFC 8487, Mtrace2 is usually initiated from an Mtrace2 client by sending a Mtracev2 query to a Last-Hop Router (LHR) or to a Rendezvous Point (RP). This feature enables you to: • Trace the path a packet would take from a source to the receiver. • To isolate packet-loss problems. • To isolate configuration problems.
YANG model for Protocol Independent Multicast (PIM) counters	This feature enables you to use YANG models to display traffic counter information for the following PIM counters: • pimInvalidRegister • pimInvalidJoinPrune • pimRPMappingChange
Extending Selective Multicast using IGMP Proxy	The IGMP Proxy function enables PE routers to act as a proxy for the CE routers connected to it. IGMP Proxy function provides the following benefits: • Reduces the flooding of IGMP messages in an EVPN network. • Enables EVPN network to act as a distributed anycast multicast router. • Helps in having selective multicast over EVPN network. Earlier, connecting an external network directly to an EVPN fabric was not possible. With this IGMP Proxy support, it is possible to have seamless connectivity over the EVPN network for its hosts with respect to multicast operations.
Modular QoS	
H-QoS support for EVPN ELAN on Cisco Network Convergence System 5700 Series Routers	You can now apply Hierarchical Modular QoS (H-QoS) on multipoint EVPN service (EVPN ELAN) traffic. You can use H-QoS to specify QoS behavior at multiple levels of hierarchy and allocate specific bandwidth and services to specific users. This feature is now supported on NCS 5700 Series routers operating in native mode (refers to the mode when the router has only NCS 5700 line cards). To enable native mode, use **hw-module profile npu native-mode-enable** in the configuration mode and reload the router. You can verify this configuration in the **show run | in hw** command output.

Feature	Description
QoS Classification Based on Packet Length	You can add an ingress QoS policy on an ACL that filters IPv6 and IPv4 packets based on the packet length. The ACL specifies packet length criteria such as equal to, lesser than, greater than, and so on, to filter packets and prevent distributed-denial-of-service (DDoS) attacks. The QoS policy specifies the forwarding decision. The ACL provides an additional QoS match criteria for IP traffic, thereby providing the combined benefit of network security and traffic classification. This feature is supported on the NCS 5500 Series routers and NCS 5700 Series routers on NC57-18DD-SE and NC57-24DD PIDs.
QoS DSCP Preservation for mLDP	In terms of preserving IP DSCP markings, when you set the MPLS experimental bits (EXP) values (also called Traffic Class values), the IP DSCP markings are now preserved by default in the ingress policies when the MPLS labels are pushed into the packet. Traffic with IP packets with DSCP marking for priority, flows as intended and there's no drop in traffic because of incorrect or missing labels. In previous releases, irrespective of the MPLS label, when the EXP values were copied into the packet header during disposition, even the IP DSCP markings were modified. This modification resulted in traffic drops at the last-hop routers.
QoS IP DSCP Preservation for SR-TE	In terms of preserving IP DSCP markings, this release covers two scenarios for SR-TE traffic: • **For two or less than two topmost or imposition labels:** when you set the MPLS experimental bits (EXP) values (also called Traffic Class values), the IP DSCP markings are now preserved by default in the ingress policies when the MPLS labels are pushed into the packet. • **For more than three imposition labels:** you must enable this functionality to preserve IP DSCP markings. With preservation, traffic with IP packets with DSCP marking for priority, flows as intended and there's no drop in traffic because of incorrect or missing labels. In previous releases, irrespective of the number of MPLS labels, when the EXP values were copied into the packet header during imposition, even the IP DSCP markings were modified. This modification resulted in traffic drops at the next-hop routers in SR-TE tunnels. This feature introduces the **hw-module profile mpls-ext-dscp-preserve v4uc-enable** command.
Routing	
Advertise a Default BGP Route on Cisco Network Convergence System 5700 Series Routers	Your BGP router can now advertise a default route to a specific neighbor irrespective of whether the route is present in the BGP Routing Information Base (RIB). This feature introduces the **default-originate** command that generates and advertises a default route only to the specific BGP peer. From this release onwards this functionality is also supported on Cisco Network Convergence System 5700 Series Routers.

Feature	Description
Multihop BFD over nondefault VRF	You can set a multihop BFD session using IPv4 for a non-default-VRF between a source and destination endpoints that have IP connectivity. This feature provides subsecond forwarding failure detection for a destination more than one hop, and up to 255 hops away. IPv4 Multihop BFD is a BFD session between two nodes, such as a PE and CE node, or between routers that are several TTL hops away. You can extend the BFD session to nondefault VRFs. This feature enables you to extend the BFD session to nondefault VRFs. Thus, the advantage of BFD, low-overhead, and short-duration detection of path failures between routers, is extended to a multihop scenario.
Setting SPF interval in IS-IS to postpone the IS-IS SPF computations	You can now define a standard algorithm to postpone the IS-IS SPF computations by setting an SPF interval. This reduces the computational load and churn on IGP nodes when multiple temporally close network events trigger multiple SPF computations. This algorithm also reduces the probability and the duration of transient forwarding loops during native IS-IS convergence when the protocol reacts to multiple temporally close events. This feature complies with RFC 8405. This feature introduces the **spf-interval ietf** command.
Segment Routing	
SRv6 Traffic Class QoS Enhancement	The modified **hw-module profile segment-routing srv6 mode** command option provides you with better flexibility to customize the optional SRv6 encapsulation parameters. The updated command will now support both L2 and L3 traffic types of SRv6 parameters. Encapsulation is a sub-mode from Release 7.7.1. The **l3-traffic** config supports the additional **policy-map** option that sets SRv6 traffic-class DSCP based on qos-group selected by input policy-map. The following commands are updated: • hw-module profile segment-routing srv6 mode: Mode is a mandatory parameter The following commands are introduced: • encapsulation l2-traffic • encapsulation l3-traffic
System Management	
IPv6 support on NCS-55A1-24Q6H-SS, NCS-55A1-24Q6H-S	Improved scalability, global reachability, better handling of packets and efficient routing are just some of the features that the larger address base of IPv6 offers. You can now avail IPv6 functionality on NCS-55A1-24Q6H-SS and NCS-55A1-24Q6H-S line cards as well.
PTP Double Failure Clock Class	This feature enables you to configure a clock class that will over-ride the existing class during a state of double-failure where PTP and SyncE are lost. This feature introduces the **double-failure-clock-class** command.

Feature	Description
PTP and SyncE support on NC55-MPA-4H-S, NC55-MPA-2TH-S, and NC55-MPA-1TH2H-S	With this release, timing support for PTP and SyncE is available on NC55-MPA-4H-S, NC55-MPA-2TH-S, and NC55-MPA-1TH2H-S.
PTP support on NC55-MPA-4H-S, NC55-MPA-2TH-S, and NC55-MPA-1TH2H-S	Based on the IEEE 1588-2008 standard, Precision Time Protocol (PTP) is a protocol that defines a method to synchronize clocks in a network for networked measurement and control systems. PTP is now supported on the following: • NC55-MPA-4H-S • NCS55-MPA-2TH-S • NC55-MPA-1TH2H-S • NC57-36H6D-S in native mode
SyncE support on NC57-36H6D-S, NC55-MPA-4H-S, NC55-MPA-2TH-S, and NC55-MPA-1TH2H-S	SyncE provides synchronization signals transmitted over the Ethernet physical layer to downstream devices, while the Synchronization Status Message (SSM) indicates the quality level of the transmitting clock to the neighboring nodes, informing the nodes about the level of the network's reliability. Ethernet Synchronization Message Channel (ESMC) is the logical channel that uses an Ethernet PDU (protocol data unit) to exchange SSM information over the SyncE link. SyncE with ESMC and SSM is now supported on the following: • NC55-MPA-4H-S • NCS55-MPA-2TH-S • NC55-MPA-1TH2H-S • NC57-36H6D-S in native mode
Unified Model for FPD: Cisco-IOS-XR-um-fpd-cfg	We have introduced the Cisco-IOS-XR-um-fpd-cfg unified model to enable or disable the automatic reload and automatic upgrade of Field Programmable Devices. You can access this unified model from the Github repository.
Use APTS to Select Timing Source	Assisted Partial Timing Support (APTS) enables you to select timing and synchronization for mobile backhaul networks. APTS is now available on the following routers: • NCS-57C3-MODS-SYS • NCS-57B1-6D24-SYS APTS allows for proper distribution of phase and time synchronization in the network. Some useful information: • ITU-T Telecom Profiles for PTP

Feature	Description
Use PTP Virtual Port to Select Timing Source	You can now select the best available timing source for your routers by using the PTP Virtual Port (VP) feature. This feature allows you to compare, select, and advertise the best clock source between a PTP server and other local timing sources connected to the routers. PTP Virtual Port is now available on the following routers: • NCS-57C3-MODS-SYS • NCS-57B1-6D24-SYS VP is an external frequency, phase, and time input interface on a Telecom Boundary Clock (T-BC), and thus participates in the timing source selection. Some useful information: • ITU-T Telecom Profiles for PTP
System Monitoring	
Out of Resource Handling of Input Logical Interface and Router Interface Resources	You can now reconfigure the threshold level for NPU resources - Input Logical Interface (INLIF) and Router Interface (RIF) by changing the predefined threshold level at which Out of Resource (OOR) situation is triggered. Graceful handling of OOR helps you to minimize traffic loss. You get notified via systemlogs, when the utilization of resources reaches their OOR limit. Also, you can view the utilization of resources by using the following commands: • show controllers npu resources • show grid pool
Traffic Buffer Resource Consumption Alerts	You can now configure threshold values for available traffic buffer resources and get timely syslog alerts on the router console when available resources go below the configured threshold values. These notifications enable you to free up resources or reroute traffic before the router drops traffic packets due to resource exhaustion. In earlier releases, the router dropped traffic without warning when traffic buffer resources got exhausted. This feature is supported on Cisco 5700 Series Routers and routers that have the NC57 line cards installed and operating in either native or compatibility mode. This feature introduces the **hw-module profile qos free-buffer-int-threshold** command
System Security	

Feature	Description
Non-Default SSH Port	We have enhanced the system security to minimize the automated attacks that may target the default Secure Socket Shell (SSH) port on your router. You can now specify a non-default port number for the SSH server on your router. The SSH, Secure Copy Protocol (SCP), and Secure File Transfer Protocol (SFTP) client services can then access your router only through this non-default port. The new port option also enables the SSH, SCP, and SFTP clients on your router to connect to SSH servers on the network that use a wide range of non-default port numbers. In earlier releases, these SSH, SCP, and SFTP connections were established through the default SSH port, 22. The non-default SSH port is supported only on SSH version 2. The feature introduces the **ssh server port** command. The feature modifies these commands to include the **port** option: • **ssh** • **sftp** • **scp**
Password Policy to Restrict Consecutive Characters	We have enhanced the router security by enforcing a strong password policy for all users configured on the router. You can now specify a new password policy for the user that restricts the usage of a specific number of consecutive characters for the login passwords. These characters include English alphabets, the sequence of QWERTY keyboard layout, and numbers, such as, 'abcd', 'qwer', '1234', and so on. Apart from *passwords*, the feature is also applicable for *secrets*–the one-way encrypted secure login passwords that are not easy to decrypt to retrieve the original unencrypted password text. The password policy is applicable only for the users configured on the local AAA server on the router; not those configured on the remote AAA server. The feature introduces the **restrict-consecutive-characters** command.
MACSec Encryption on NC55-32T16Q4H-A	MACSec, the Layer 2 encryption protocol, secures the data on physical media and provides data integrity and confidentiality. MACSec is now supported on NC55-32T16Q4H-A line card, at all port speeds across all ports, including the breakout ports.

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.

Feature	Description
Programmability	

Feature	Description
openconfig-isis Revision 0.6.0	

Feature	Description

	The OpenConfig data model supports to monitor the system performance by checking the packet counter statistics and bandwidth, time, length, and values (TLVs) of IS-IS database using the following XPaths:.
	• `interfaces/interface[interface-id]/bfd/config/bfd-tlv`
	• `global/state/authentication-check`
	• `global/state/maximum-area-addresses`
	• `global/state/poi-tlv`
	• `global/state/iid-tlv`
	• `global/graceful-restart/state/helper-only`
	Root path for system-level counters: `levels/level[level-number]/system-level-counters/state/`
	• `manual-address-drop-from-areas`
	• `part-changes`
	• `auth-fails`
	• `auth-type-fails`
	Root path for TLV type extended-is-reachability counters:
	`levels/level[level-number]/link-state-database/lsp[lsp-id]/tlvs/tlv[type]/extended-is-reachability/ neighbors/neighbor[system-id]/instances/instance[id]/subtlvs/subtlv[type]/`
	Root path for mt-isn counters:
	`levels/level[level-number]/link-state-database/lsp[lsp-id]/tlvs/tlv[type]/mt-isn/neighbors/neighbor[mt-idsystem-id]/ instances/ instance[id]/ subtlvs/subtlv[type]/`
	extended-is-reachability and mt-isn TLV counters:
	• `link-id/state/local`
	• `link-id/state/remote`
	• `link-delay/state/a-bit`
	• `link-delay/state/delay`
	• `min-max-link-delay/state/a-bit`
	• `min-max-link-delay/state/min-delay`
	• `min-max-link-delay/state/max-delay`
	• `link-delay-variation/state/delay`
	• `link-loss/state/a-bit`
	• `link-loss/state/link-loss`
	• `residual-bandwidth/state/bandwidth`
	• `available-bandwidth/state/type`
	• `available-bandwidth/state/bandwidth`

Feature	Description
	• `utilized-bandwidth/state/type` • `utilized-bandwidth/state/bandwidth` Root path for circuit-counters: `interfaces/interface[interface-id]/circuit-counters/state/` • `init-fails` • `auth-type-fails` • `adj-number` Root path for packet counters: `interfaces/interface[interface-id]/levels/level[level-number]/packet-counters/` • `lsp/state/dropped` • `lsp/state/retransmit` • `iih/state/dropped` • `iih/state/retransmit` • `psnp/state/dropped` • `psnp/state/retransmit` • `csnp/state/dropped` • `csnp/state/retransmit` • `unknown/state/received` • `unknown/state/processed` • `unknown/state/dropped` • `unknown/state/sent` • `unknown/state/retransmit` Following statistics always displays the value as ZERO. • `interfaces/interface[interface-id]/circuit-counters/state/init-fails` • `levels/level[level-number]/system-level-counters/state/auth-type-fails` • `interfaces/interface[interface-id]/levels/level[level-number]/packet-counters/iih/state/retransmit` • `interfaces/interface[interface-id]/levels/level[level-number]/packet-counters/csnp/state/retransmit` • `interfaces/interface[interface-id]/levels/level[level-number]/packet-counters/psnp/state/retransmit` • `interfaces/interface[interface-id]/levels/level[level-number]/packet-counters/unknown/state/sent` • `interfaces/interface[interface-id]/levels/level[level-number]/packet-counters/unknown/state/retransmit` This feature introduces **authentication-check disable** command to disable authentication check.

Hardware Introduced

Cisco IOS XR Release 7.7.1 introduces the following hardware support:

Hardware Feature	Description
Optics	Note: Optics support varies across devices (routers, line cards, RPs, and so on). To know if an optics is compatible with a specific Cisco device, refer to the Transceiver Module Group (TMG) Compatibility Matrix. This release launches the following new optics- • Cisco 400GBASE Quad Small Form-Factor Pluggable Double Density (QSFP-DD) • QDD-4X100G-LR-S
NC55-OIP-02 modular port adapter	An 8-port MPA (NC55-OIP-02) that supports SFP+ optical transceivers. This MPA is supported in the NC55A2-MOD-S and NC57C3-MOD-SYS routers and supports Ethernet, FC, OTN, SDH, and SONET port mode options. Refer to the *PLE on EVPN VPWS* section in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 7.7.x* for information on port mode configuration.

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
Accumulated Interior Gateway Protocol Attribute on Cisco Network Convergence System 5700 Series Routers	✕	✓
Allow AS support in BGP to allow an AS path with the PE autonomous system number (ASN) on Cisco Network Convergence System 5700 Series Routers	✕	✓
Install Multiple External and Internal BGP Paths for Load Balancing on Cisco Network Convergence System 5700 Series Routers	✕	✓
OSPF enablement for BGP paths based on IGP metrics on Cisco Network Convergence System 5700 Series Routers	✕	✓
BGP peer group on Cisco Network Convergence System 5700 Series Routers	✕	✓
Convergence for BGP Labeled Unicast PIC Core and Edge	✓	✓
SPAN Filtering on Layer 2 Interfaces	✕	✓
Native Mode H-QoS Support for EVPN ELAN on Cisco NCS 5700 Series Routers	✕	✓

Feature	Compatible Mode	Native Mode
QoS Match Criterion For Packet Length	✗	✓
Advertise a Default BGP Route on Cisco Network Convergence System 5700 Series Routers	✗	✓
PTP and SyncE support on NC55-MPA-4H-S, NC55-MPA-2TH-S, and NC55-MPA-1TH2H-S	✗	✓
Threshold Configurations for Syslog Alerts of Traffic Buffer Resource Consumption	✓	✓
VPLS VFI with BVI as Routed Interface on Cisco 5700 Fixed Routers and Cisco NC57 Line Cards	✗	✓

For the complete list of features supported on Cisco NC57 line cards until Cisco IOS XR Release 7.7.1, see:

- 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 7.5.2
- 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

Table 2: Cisco NCS 5500 Series Routers Specific Bugs

Bug ID	Headline
CSCwb96444	HW_PROG errors : ipnhgroup : EnNotFound error seen post reload on fretta
CSCwb78062	Traffic drop of 4-11 seconds when core bundle is no shut with bundle members on different DCP/LC

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 3: Release 7.7.1 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-r771.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-r771.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r771.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.
Cisco IOS XR Security Package	ncs5500-k9sec-3.1.0.0-r771.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-r771.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf-2.0.0.0-r771.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs5500-li-1.0.0.0-r771.x86_64.rpm	Includes LI software images
Multicast Package	ncs5500-mcast-1.0.0.0-r771.rpm	Support Multicast

Table 4: Release 7.7.1 TAR files for Cisco NCS 5500 Series Router

Feature Set	Filename
NCS 5500 IOS XR Software 3DES	NCS5500-iosxr-k9-7.7.1.tar
NCS 5500 IOS XR Software	NCS5500-iosxr-7.7.1.tar
NCS 5500 IOS XR Software	NCS5500-docs-7.7.1.tar

Table 5: Release 7.7.1 Packages for Cisco NCS 5700 Series Router

Feature Set	Filename
NCS 5700 IOS XR Software	ncs5700-x64-7.7.1.iso

NCS 5700 IOS XR Software (only k9 RPMs)	ncs5700-k9sec-rpms.7.7.1.tar
NCS 5700 IOS XR Software Optional Package	NCS5700-optional-rpms.7.7.1.tar This TAR file contains the following RPMS: • optional-rpms/cdp/* • optional-rpms/eigrp/* • optional-rpms/telnet/*

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 7.7.1
Copyright (c) 2013-2022 by Cisco Systems, Inc.

Build Information:
Built By     : ingunawa
Built On     : Mon Jul 25 02:54:52 PDT 2022
Built Host   : iox-lnx-068
Workspace    : /auto/srcarchive12/prod/7.7.1/ncs5500/ws
Version      : 7.7.1
Location     : /opt/cisco/XR/packages/
Label        : 7.7.1

cisco NCS-5500 () processor
System uptime is 4 hours 21 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
-----------------------------------------------------------------------------------
0/0       NC55-6X200-DWDM-S 1.0   Bootloader           CURRENT     1.20       1.20
0/0       NC55-6X200-DWDM-S 1.0   IOFPGA               CURRENT     0.14       0.14
0/0       NC55-6X200-DWDM-S 1.0   SATA-M600-MCT        CURRENT     5.00       5.00
0/1       NC57-24DD         1.0   Bootloader           CURRENT     1.03       1.03
0/1       NC57-24DD         1.0   DBFPGA               CURRENT     0.14       0.14
0/1       NC57-24DD         1.0   IOFPGA               CURRENT  0.23       0.23
0/1       NC57-24DD         1.0   SATA-M5100           CURRENT    75.00      75.00
0/2       NC55-6X200-DWDM-S 0.502 Bootloader           CURRENT     1.20       1.20
```

```
0/2       NC55-6X200-DWDM-S 0.502 IOFPGA               CURRENT     0.14      0.14
0/2       NC55-6X200-DWDM-S 0.502 SATA-M600-MCT        CURRENT     5.00      5.00
0/3       NC57-36H6D-S      0.300 Bootloader           CURRENT     0.02      0.02
0/3       NC57-36H6D-S      0.300 DBFPGA               CURRENT     0.14      0.14
0/3       NC57-36H6D-S      0.300 IOFPGA               CURRENT     0.46      0.46
0/3       NC57-36H6D-S      0.300 SATA-Micron          CURRENT     1.00      1.00
0/6       NC55-24X100G-SE   1.0   Bootloader           CURRENT     1.20      1.20
0/6       NC55-24X100G-SE   1.0   IOFPGA               CURRENT     0.13      0.13
0/6       NC55-24X100G-SE   1.0   SATA-M600-MCT        CURRENT     5.00      5.00
0/8       NC55-MOD-A-S      0.302 Bootloader           CURRENT     1.03      1.03
0/8       NC55-MOD-A-S      0.302 DBFPGA               CURRENT     0.14      0.14
0/8       NC55-MOD-A-S      0.302 IOFPGA               CURRENT     0.09      0.09
0/8       NC55-MOD-A-S      0.302 SATA-M600-MCT        CURRENT     5.00      5.00
0/9       NC55-32T16Q4H-A   0.12  Bootloader           CURRENT     0.05      0.05
0/9       NC55-32T16Q4H-A   0.12  DBFPGA               CURRENT     0.14      0.14
0/9       NC55-32T16Q4H-A   0.12  IOFPGA               CURRENT     0.89      0.89
0/9       NC55-32T16Q4H-A   0.12  SATA-M5100           CURRENT    75.00     75.00
0/12      NC57-18DD-SE      1.1   Bootloader           CURRENT     1.03      1.03
0/12      NC57-18DD-SE      1.1   DBFPGA               CURRENT     0.14      0.14
0/12      NC57-18DD-SE      1.1   IOFPGA               CURRENT     0.22      0.22
0/12      NC57-18DD-SE      1.1   SATA-M5100           CURRENT    75.00     75.00
0/RP0     NC55-RP2-E        0.201 Bootloader           CURRENT     0.08      0.08
0/RP0     NC55-RP2-E        0.201 IOFPGA               CURRENT     0.50      0.50
0/RP0     NC55-RP2-E        0.201 OMGFPGA              CURRENT     0.52      0.52
0/RP0     NC55-RP2-E        0.201 SATA-M5100           CURRENT    75.00     75.00
0/RP1     NC55-RP2-E        0.202 Bootloader           CURRENT     0.08      0.08
0/RP1     NC55-RP2-E        0.202 IOFPGA               CURRENT     0.50      0.50
0/RP1     NC55-RP2-E        0.202 OMGFPGA              CURRENT     0.52      0.52
0/RP1     NC55-RP2-E        0.202 SATA-M5100           CURRENT    75.00     75.00
0/FC1     NC55-5516-FC2     1.0   Bootloader           CURRENT     1.80      1.80
0/FC1     NC55-5516-FC2     1.0   IOFPGA               CURRENT     0.22      0.22
0/FC1     NC55-5516-FC2     1.0   SATA-M5100           CURRENT    75.00     75.00
0/FC3     NC55-5516-FC2     1.0   Bootloader           CURRENT     1.80      1.80
0/FC3     NC55-5516-FC2     1.0   IOFPGA               CURRENT     0.22      0.22
0/FC3     NC55-5516-FC2     1.0   SATA-M5100           CURRENT    75.00     75.00
0/FC5     NC55-5516-FC2     1.0   Bootloader           CURRENT     1.80      1.80
0/FC5     NC55-5516-FC2     1.0   IOFPGA               CURRENT     0.22      0.22
0/FC5     NC55-5516-FC2     1.0   SATA-M5100           CURRENT    75.00     75.00
0/SC0     NC55-SC           1.4   Bootloader           CURRENT     1.74      1.74
0/SC0     NC55-SC           1.4   IOFPGA               CURRENT     0.10      0.10
0/SC1     NC55-SC           1.4   Bootloader           CURRENT     1.74      1.74
0/SC1     NC55-SC           1.4   IOFPGA               CURRENT     0.10      0.10
```

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.

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.

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.