Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.10.1

Revised: September 17, 2024

Network Convergence System 5500 Series Routers

What's New in Cisco IOS XR Release 7.10.1

Cisco IOS XR Release 7.10.1 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 Software Lifecycle Support Statement - IOS XR.

Software Features Enhanced and Introduced

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

Feature	Description
Application Hosting	
Secure Onboarding of Signed Third-Party Applications	Introduced in this release on: NCS 5500 fixed port routers
	Cisco IOS XR now supports onboarding signed (authenticated) third-party (non-native Cisco IOS XR) applications onto the XR routers securely as per Cisco policies and standards.
	Earlier you could onboard only signed Cisco IOS XR native images and RPMs onto the router.
Programmability	
Improved YANG Input Validator and Get Requests	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])
	The OpenConfig data models provide a structure for managing networks via YANG protocols. With this release, enhancements to the configuration architecture improve input validations and ensure that the Get requests made through gNMI or NETCONF protocols return only explicitly configured OpenConfig leaves.
OpenConfig Metadata for Configuration Annotations	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])
	You can annotate the **OpenConfig-metadata** as part of the OpenConfig **edit-config** request to the Cisco IOS XR router and later fetch using the OpenConfig **get-config** request or delete through gNMI request only.
	The `Set` or `Get` operations can be performed through gNMI only; not through Netconf RPCs.
Prevent Partial Pseudo-Atomic Committed Configurations	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])
	You can now prevent the partially-committed configurations on the router and thus ensure the system database and OpenConfig datastore stay in sync.
	This feature changes how the internal rollback error is handled when a pseudo-atomic commit fails. In such cases, the system database always rolls back the configuration in its datastore thereby ensuring that there is no partially-committed configuration. If there is still inconsistency, the system displays error messages to notify you of various internal rollback failure scenarios based on which you must take rectification action to re-synchronize the data.

Feature	Description
Routing	

[Autonomous System Boundary Router Isolation and Adjacency Control for LSA Overflows](#)	Introduced in this release on NCS 5500 fixed port routers: NCS 5700 fixed port routers
	
	In a network employing an Autonomous System Boundary Router (ASBR) and other routers, you are now assured of uninterrupted traffic flow even if the ASBR generates LSAs that exceed the limit you configured. This is made possible as you can now isolate ASBRs and also control the duration of adjacency in the EXCHANGE or LOADING phase. By isolating the ASBR from its immediate neighbors, the remaining network topology can continue to function without disruption, effectively preventing any adverse impact on traffic flow. This approach also simplifies the recovery process, as manual intervention is only necessary for the immediate neighbors of the ASBR routers.
	
	This feature introduces these changes:
	
	CLI:
	
	   • **max-external-lsa**
	
	   • **exchange-timer**
	
	YANG Data Model:
	
	   • `Cisco-IOS-XR-ipv4-ospf-cfg.yang`
	
	   • `Cisco-IOS-XR-ipv4-ospf-oper.yang`
	
	   • `Cisco-IOS-XR-um-router-ospf-cfg.yang`
	
	(see GitHub, YANG Data Models Navigator)

[Multihop Bidirectional Forwarding Detection on IPv4 and IPv6 Non-Default VRFs](#)	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) (select variants only*) You can now improve the reliability of your network by providing early notification of failures. This is made possible due to extension of Multihop Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 non-default VRFs to process BFD packets encapsulated with MPLS label for a particular VRF. * NCS 5700 line cards in compatibility and native modes support this feature for IPv4 non-default VRFs. Other variants listed here already support this feature for IPv4 non-default VRFs.

Feature	Description
Disable IID-TLV of IS-IS Protocol Instance	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native] You can now disable Instance Identifier Type-Length-Value (IID-TLV) in the Hello and LSP packets when multiple IS-IS protocol instances are configured on the router. Each IS-IS instance has a unique instance-ID set, the TLV of which is sent in the Hello and LSP packets. The IID-TLV attribute helps in uniquely identifying the IS-IS protocol instance as well as the topologies to which the Protocol Data Units (PDUs) apply. The feature introduces these changes: **CLI** New Command: • **iid disable** Modified Commands: • The **hello-padding** command is extended to IS-IS process configuration mode • The **disable (IS-IS)** command is modified with a new **level** keyword, and also extended to interface configuration mode. **YANG Data Model** • New XPaths for `openconfig-isis.yang` (see GitHub, YANG Data Models Navigator)
MPLS	

Automatic Bandwidth Bundle TE++ for Numbered Tunnels	Introduced in this release on: NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5700 line cards [Mode: Compatibility; Native])
	
	We have optimized network performance and enabled efficient utilization of resources for numbered tunnels based on real-time traffic by automatically adding or removing tunnels between two endpoints. This is made possible because this release introduces support for auto-bandwidth TE++ for numbered tunnels, expanding upon the previous support for only named tunnels, letting you define explicit paths and allocate the bandwidth to each tunnel.
	
	The feature introduces these changes:
	
	• **CLI:**
	
	  The **auto-capacity** keyword is added to the **interface tunnel-te** command.
	• **YANG Data Model:**
	
	  New XPaths for `Cisco-IOS-XR-mpls-te-cfg.yang` (see GitHub, YANG Data Models Navigator)

Feature	Description
Multicast Decapsulated Flow Over Static Label Switched Paths Over Single Pass GRE Tunnels	Introduced in this release on: NCS 5500 fixed port routers This feature enables the device to forward the L2 frames payload from decapsulated static label-switched paths (LSPs) over single-pass GRE tunnels. You can now forward only the L2 frames from the decapsulated MPLS static LSPs that are carrying L2 frames. This feature introduces these changes: • The **l2-bypass** keyword is introduced in the **mpls static** command.
Segment Routing	
Configurable Filters for IS-IS Advertisements to BGP-Link State	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) This feature allows you to configure a route map to filter IS-IS route advertisements to BGP-Link State (LS). It also provides a per-area configuration knob to disable IS-IS advertisements for external and propagated prefixes. This configuration of filters hence reduces the amount of redundant data for external and interarea prefixes sent to the BGP - LS clients. The feature introduces **exclude-external** , **exclude-interarea** , and **route-policy** *name* optional keywords in the **distribute link-state** command.
IS-IS Partition Detection and Leakage of Specific Route Advertisements	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) In an open ring topology, a single fiber cut may partition the area or domain into two pieces. With summarization enabled, the area (domain) partition may result in traffic drops. Depending on the configuration in the Area Border Routers (ABRs) or Autonomous System Boundary Routers (ASBRs) that is picked as an entry point to the partitioned area (domain), the traffic is delivered to its destination or dropped as unreachable at ABR or ASBR. IS-IS partition detection and leakage of specific route advertisements features are introduced to retain connectivity for the partitioned area (domain) when summarization is used. The ABRs or ASBRs detect a network partition within an area (domain) and upon detection, ensure that the summary route is replaced with specific route advertisements in IS-IS. The feature introduces these changes: **New Command:** • **partition-detect** **Modified Command:** • The **partition-repair** keyword is introduced in the **summary-prefix** command. **YANG Data Model:** • New XPaths for `Cisco-IOS-XR-um-router-isis-cfg.yang` (see GitHub, YANG Data Models Navigator)

Feature	Description
Multicast VPN: Dynamic Tree-SID Multicast VPN IPv6	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])
	This feature allows Dynamic Tree Segment Identifier (Tree-SID) deployment where IPv6 Multicast payload is used for optimally transporting IP VPN multicast traffic over the provider network, using SR-PCE as a controller. This implementation supports IPv6 only for the Dynamic Tree-SID. Currently, the Static Tree-SID supports IPV4 payloads only, not the IPv6 payloads.
Multicast: Cisco Nonstop Forwarding for Tree-SID	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])
	Starting from this release, Multicast Nonstop Forwarding supports Tree-SID (Tree Segment Identifier). This ensures that traffic forwarding continues without interruptions whenever the active RSP fails over to the standby RSP.
	This feature prevents hardware or software failures on the control plane from disrupting the forwarding of existing packet flows through the router for Tree-SID. Thus, ensuring improved network availability, network stability, preventing routing flaps, and no loss of user sessions while the routing protocol information is being restored.
	The feature modifies the **show mrib nsf private** command.
Reporting of SR-TE Policies Using BGP-Link State	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])
	BGP- Link State (LS) is a mechanism by which LS and Traffic Engineering (TE) information can be collected from networks and shared with external components (such as, Segment Routing Path Computation Element (SR-PCE) or Crossword Optimization Engine (COE)) using the BGP routing protocol.
	The feature gathers the Traffic Engineering Policy information that is locally available in a node and advertises it into BGP-LS updates.
	The operators can now take informed decisions based on the information that is gathered on their network's path computation, reoptimization, service placement, network visualization, and so on.
	The feature introduces these changes:
	CLI:
	• **distribute link-state**
	YANG Data Model:
	• New XPaths for `module Cisco-IOS-XR-infra-xtc-agent-cfg.yang` (see GitHub, YANG Data Models Navigator)
SR Policy Liveness Monitoring - Hardware Offloading	Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards)
	You can now hardware offload the liveness monitoring in performance measurement to the router hardware, which is the Network Processing Unit (NPU). This feature helps you optimize and scale the measurement operation, helping you meet delay-bound Service Level Agreements (SLAs). Previously, this feature was software driven.
	The feature introduces a new keyword **npu-offload** under the **performance-measurement liveness-profile name***liveness profile* command.

Feature	Description
BGP	
Automatically Reestablish a BGP Neighbor Session	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) You can now configure the router to automatically re-establish a BGP neighbor session that has been disabled because the maximum-prefix limit has been exceeded. The feature introduces these changes: **CLI** • **maximum-prefix-restart-time** **YANG Data Model:** • New XPaths for `openconfig-bgp-neighbor.yang`(see GitHub, YANG Data Models Navigator)
BGP Flowspec on Bridge-Group Virtual Interfaces	Introduced in this release on: NCS 5500 modular routers (NCS 5700 line cards [Mode: Native]) You can now effectively employ BGP Flowspec on Bridge-Group Virtual Interface (BVI) to connect to broadcast domains that house host devices, as in the case of enterprise networks. This support means that your customers can safeguard their networks from network threats such as Distributed Denial of Service (DDoS) attacks incoming through the BVI.
Discard Incoming BGP Update Message	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) You can now avoid the session reset when a BGP session encounters errors while parsing the received update message. This is made possible because the feature enables discarding the incoming update message as a withdraw message. **CLI:** • **update in error-handling treat-as-withdraw** **YANG Data Model:** • New XPaths for `openconfig-bgp-neighbor.yang` (see GitHub, YANG Data Models Navigator)
Exclusion of Label Allocation for Non-Advertised Routes	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) We have enabled better label space management and hardware resource utilization by making MPLS label allocation more flexible. This flexibility means you can now assign these labels to only those routes that are advertised to their peer routes, ensuring better label space management and hardware resource utilization. Prior to this release, label allocation was done regardless of whether the routes being advertised. This resulted in inefficient use of label space.

Feature	Description
Protection of Directly Connected EBGP Neighbors through Interface-Based LPTS Identifier	Introduced in this release on: NCS 5500 fixed port routers We have enhanced the network security for directly connected eBGP neighbors by ensuring that only packets originating from designated eBGP neighbors can traverse through a single interface, thus preventing IP spoofing. This is made possible because we've now added an interface identifier for Local Packet Transport Services (LPTS). LPTS filters and polices the packets based on the type of flow rate you configure. The feature introduces the following: **CLI:** • **bgp lpts-secure-binding** **YANG Data Model:** • `Cisco-IOS-XR-um-router-bgp-cfg` (see GitHub, YANG Data Models Navigator)
Reduce Recursions for eBGP Peering on Loopback Address on Bridge-Group Virtual Interface	Introduced in this release on: NCS 5500 modular routers (NCS 5700 line cards [Mode: Native]) You can now achieve eBGP peering on Loopback interfaces on Bridge-Group Virtual Interface (BVI) and reduce the recursion level from three to two. This reduction in the recursion level, achieved by removing the need to use the BVI name in the configuration of static routes, allows faster packet forwarding and better utilization of network resources.
Interface and Hardware Component	
Egress Hybrid ACL-based Traffic Mirroring on Cisco NCS 5700 Series Line Cards and Routers	Introduced in this release on: NCS 5700 fixed port routers (select variants only*); NCS 5700 line cards [Mode: Native] (select variants only*) We've now made it possible for you to narrow down the outgoing (Tx) traffic that you want to mirror and troubleshoot the captured traffic for any anomalous or malicious activity. You can do this by enabling the **capture** option on an L3 interface that has a hybrid ACL configured and Egress Traffic Management (ETM) mode enabled. The traffic matching the rules defined in the egress hybrid ACL gets captured and mirrored. This feature introduces the following changes: **CLI**: The **capture** keyword is introduced in the **ipv4 access-list** and **ipv6 access-list** commands. * This feature is supported on: • NCS-57B1-5DSE-SYS • NCS-57C3-MODS-SYS • NC57-18DD-SE • NC57-36H-SE

Feature	Description
Enhanced Alarm Prioritization, Monitoring, and Management	Introduced in this release on: NCS 5500 fixed port routers NCS 5500 modular routers (NCS 5500 line cards) In this release, we introduce enhanced alarm management that offers improved alarm prioritization, monitoring and management, as listed below: • Suppression of LOL (Loss of Line) alarm when the LOS-P (Loss of Signal-Payload) alarm is generated. This prioritizes the detection and handling of the LOS-P alarm. • Ability to clear alarm static counters using the command **clear counters controller coherentDSP location** . Clearing static counters enables you to monitor alarms generated for a definitive time period. • Suppression of warnings when the respective alarm is triggered. This prevents redundant or repetitive alerts.
Fibre Channel over PLE Transmission Using TTS Auto-Negotiation	Introduced in this release on: NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5700 line cards [Mode: Compatibility; Native]) You can now enhance transmission speed and connectivity between ports with Fibre Channel (FC) over Private Line Emulation (PLE) using Transmitter Training Signal (TTS) with auto-negotiation function. FC over PLE technology facilitates fast and efficient connections and data storage replication between multiple data centers in a Storage Area Network (SAN) spanning different geographical locations. TTS is a feature introduced for the 32G FC ports. The feature introduces these changes: • **CLI:** The **tts** keyword is added to the **controller** command for FC. • **YANG Data Model:** New XPaths for `Cisco-IOS-XR-mpls-te-cfg.yang` (see GitHub, YANG Data Models Navigator)

Feature	Description

QDD Optical Line System	Introduced in this release on: NCS 5500 fixed port routers (select variants only*); NCS 5700 fixed port routers (select variants only*)
	
	The QDD Optical Line System (OLS) is a new pluggable optical amplifier that interconnects two routers or switches for transmitting traffic on a limited number of coherent optical channels over a single span point-to-point link. With the QDD OLS pluggable, it's now possible to obtain the functionality of amplification into a QSFP-DD module that can be plugged into a port of the router or switch.
	
	The benefits of this pluggable are:
	• Provides compact solution for amplification.
	• Provides extended reach.
	• Increases fiber bandwidth.
	• Lowers power dissipation.
	
	This feature introduces the following:
	• **CLI**:
	  • **controller ots (QDD OLS)**
	  • **rx-low-threshold**
	  • **tx-low-threshold**
	  • **ampli-control-mode**
	  • **egress-ampli-gain**
	  • **egress-ampli-power**
	  • **egress-ampli-safety-control-mode**
	  • **egress-ampli-osri**
	  • **show controllers ots (QDD OLS)**
	
	• **YANG Data Model**:
	  • `Cisco-IOS-XR-controller-ots-oper.yang`
	  • `Cisco-IOS-XR-controller-ots-cfg.yang`
	  • `Cisco-IOS-XR-pmengine-oper.yang`
	  • `Cisco-IOS-XR-pmengine-cfg.yang`
	  • `Cisco-IOS-XR-pmengine-clear-act.yang`
	
	* The QDD Optical Line System is now supported on the following hardware:
	• NCS-57B1-6D24-SYS and NCS-57B1-5DSE-SYS routers.
	• On NCS-57C3-MOD and NCS-55A2-MOD routers, the QDD OLS pluggable can be used only through the NC57-MPA-2D4H-S modular port adapter.

Feature	Description
Support for DP04QSDD-ER1 optical module	Introduced in this release on: NCS 5500 modular routers; NCS 5500 line cards(select variants only*)
	This release introduces support for the Cisco DP04QSDD-ER1 Ethernet variant optical module.
	The Cisco DP04QSDD-ER1 optical module is an enhanced version of the currently available QDD-400G-ZR Optical Module. It leverages the same operational modes while providing an extended range of up to 40km using 16QAM transmission.
	* The DP04QSDD-ER1 optical module is supported on Cisco NCS 5500 Series Modular Chassis through the NC57-18DD-SE line card.
Extended Support for DP04QSDD-HE0 optical module	Introduced in this release on: NCS 5500 modular routers (select variants only*); NCS 5700 fixed port routers (select variants only*); NCS 5700 line cards [Mode: Compatibility; Native] (select variants only*)
	This release introduces support for the Cisco 400G QSFP-DD High-Power (Bright) Optical Module, Ethernet Variant on the following routers and line cards-
	* Routers:
	• NCS-57B1-6D24H-S
	• NCS-57B1-5D24-SE
	• NCS-57C1-48Q6-S
	• NCS-57D2-18DD-S
	• NCS-55A2 via NC57-MPA-2D4H-S
	• NC55-MOD via NC57-MPA-2D4H-S
	* Line cards:
	• NC57-24DD
	• NC57-18DD-SE
	• NC57-36H6D-S
	• NC57-MOD-S
	• NC57-48Q2D-S
	• NCS-57B1-6D24H-S
	• NC57-MOD-S via NC57-MPA-2D4H-S
IP Addresses and Services	
Configure ACLs on MPLS Deaggregation Packets	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])
	To ensure that there is no MPLS traffic loss on an interface, you can now apply ACLs on the ingress MPLS deaggregation packets.
	Earlier, the IPv4 or IPv6 ACLs applied on an interface would bypass or block the ingress MPLS packets, resulting in packet loss for MPLS traffic.

Feature	Description

Filter TCP Flags in Egress IPv6 or IPv4 Hybrid ACLs	Introduced in this release on: NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5700 line cards [Mode: Compatibility; Native]) (select variants only*)
	
	We've enhanced the security of the egress traffic by allowing you to restrict and manage traffic on an interface. You can configure an egress IPv6 or IPv4 hybrid ACL such that only the chosen flags are either permited or denied based the TCP flag filters set in the TCP packets. In a TCP header, TCP flags indicate the state of a network connection, provide some additional helpful information for troubleshooting purposes, or how a connection must be handled.
	
	* This feature is supported on:
	
	   • Cisco NCS-57B1-5DSE
	
	   • Cisco NCS-57C3-MODS-SYS
	
	   • NC57-18DD-SE
	
	   • NC57-36H-SE
	
	The following commands are updated:
	
	   • **deny (IPv6)**
	
	   • **permit (IPv6)**

Identify Internal TCAM Entries for Hybrid ACLs	Introduced in this release on: NCS 5500 modular routers (NCS 5700 line cards [Mode: Compatibility; Native]) (select variants only*)
	
	From this release onwards, you'll be able to identify the internal TCAM entries required to create a hybrid ACL, before you attach them to an interface. Because you define the ACLs based on the available internal TCAM resources, you are assured that you can successfully attach the hybrid ACLs to an interface and filter traffic based on the ACEs defined.
	
	Previously, when you'd create an ACL and then attach that ACL to an interface, there was no way to assess upfront if the internal TCAM resources were enough for the ACL to work. In such instances, there was a higher chance of ACLs failing to attach to an interface because of insufficient TCAM resources.
	
	* This feature is supported on:
	
	   • NC57-18DD-SE
	
	   • NC57-24DD
	
	A new keyword, **resource-check** is introduced in the following commands:
	
	   • **show access-lists ipv4**
	
	   • **show access-lists ipv6**

Feature	Description
Single Pass IPv6 Egress ACL	Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers(NCS 5500 line cards)
	You can now experience faster packet processing and save NPU cycles by avoiding the recycling of packets within the router. This is made possible by enabling the single-pass egress ACL which avoids multiple round-trips of packets in the ingress-to-egress path, thereby eliminating the need for additional packet processing. Also, because the match criteria requirement for a single-pass egress IPv6 ACL is reduced, the TCAM key size is reduced.
	This feature introduces the **hw-module profile acl ipv6 single-pass-egress-acl** command.
L2VPN and Ethernet Services	
Advertise EVPN Host IP Routes as IP Unicast Routes	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])
	You can now resume a disrupted video streaming by re-injecting locally learned EVPN host IP routes from multiple bridge domains back into a spine BGP router. The EVPN host routes can be advertised as IPv4 or IPv6 unicast routes to BGP peers. This allows spine BGP routers to install the host routes from a video core source in the Global Routing Table (GRT).
	When there is a link failure, the video streaming is disrupted. The GRT helps to track and locate the video core source, gets the multicast traffic to flow back into the network, and resumes the video streaming.
	The feature introduces these changes:
	CLI:
	• **import from bridge-domain**
	YANG Data Model:
	• New XPaths for `Cisco-IOS-XR-um-router-bgp-cfg.yang` (see GitHub, YANG Data Models Navigator)
EVPN BUM Flood Traffic Optimization	Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards)
	You can save network bandwidth consumption by preventing the replication of Broadcast, Unknown unicast, and Multicast (BUM) traffic towards EVPN core and attachment circuits (AC). This feature not only prevents the replication of BUM traffic but also ensures that only the designated router receives the BUM traffic.
	The feature introduces these changes:
	CLI
	• **hw-module l2-replication core-optimized**
	• **flood mode ac-shg-optimized**
	YANG Data Model:
	• New XPaths for `Cisco-IOS-XR-um-hw-module-profile-cfg.yang` (see GitHub, YANG Data Models Navigator)

Feature	Description
EVPN Link Bandwidth for Proportional Multipath on VNF	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])
	You can now use the EVPN link bandwidth to set proportional multipath on Virtual Network Forwarders (VNFs) connected to Top of Racks (ToRs). You can advertise the link bandwidth extended community attribute for each path in a network. When you enable EVPN link bandwidth on multiple paths, the bandwidth values of these paths are aggregated and the cumulative bandwidth is advertised across the VNFs. The load metrics is installed in Routing Information Base (RIB) and the RIB redistributes nexthop prefixes to the paths to achieve proportional multipath.
	This allows distribution of traffic proportional to the capacity of the links across all the available Virtual Network Forwarders (VNFs) that facilitates optimal traffic load balancing across the VNFs.
	The feature introduces these changes:
	CLI:
	• **evpn-link-bandwidth**
	• **set extcommunity evpn-link-bandwidth**
	• **delete extcommunity evpn-link-bandwidth**
EVPN Port-Active Hot Standby on Bundle Interfaces	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])
	The EVPN port-active mode configuration is now modified to support hot standby. In a hot standby bundle interface, the main and subinterfaces remain up. This functionality ensures fast convergence of standby to active transition.
	Previously, the interfaces in a standby node would be down. During the failure and recovery of active node, the standby node transitions through the Out-of-Service (OOS) state to the Up state.
	If you still want the nodes to transition through the OOS state, use the **access-signal out-of-service** command to revert to the previous behavior.
	The feature introduces these changes:
	CLI:
	• **access-signal out-of-service**
	YANG Data Model:
	• New XPaths for `Cisco-IOS-XR-l2vpn-cfg.yang` (see GitHub, YANG Data Models Navigator)

Feature	Description
ITU-T Y.1731 Compliant EVPN Flexible Cross-Connect Services	Introduced in this release on:NCS 5500 modular routers(NCS 5700 line cards [Mode: Native])(select variants only*)
	EVPN Flexible cross-connect (FXC) services enable aggregation of attachment circuits (ACs) across multiple endpoints in a single Ethernet VPN Virtual Private Wire Service (EVPN-VPWS) service instance, on the same provider edge (PE). This feature now supports ITU-T Y.1731 compliant Delay Measurement Message (DMM) and Synthetic Loss Measurement (SLM) functions.
	Combined with the IEEE-compliant Connectivity Fault Management (CFM), ITU-T Y.1731 provides a comprehensive fault management and performance monitoring solution for EVPN FXC services.
	*This feature is supported on NCS-57D2-18DD-SYS.
Static L2VPN P2P Configuration over MPLS over Single-Pass GRE Tunnel	Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards)
	We help you achieve the designated line rate for your network by enabling a single-pass GRE for static L2VPN point-to-point MPLS over GRE traffic.
	Earlier, you could transport such traffic using two-pass GRE tunnels, which used the recycle functonality to ensure payload transportation while optimizing the line rate.
Modular QoS	
Flexibility to Set a Maximum of One Class Map per Ingress QoS Traffic Policy	Introduced in this release on NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5700 line cards [Mode: Native])
	You can now set a maximum of one class map per ingress QoS traffic policy. In earlier releases, the allowed values for maximum number of class maps per ingress traffic policy were 2, 4, 8, 16, and 32.
	With fewer class maps per traffic policy, the NPU resources required for packet matching are lower. And so this allows you to configure ingress traffic policies on more interfaces of the router.
	This feature modifies the **hw-module profile qos max-classmap-size** command to accept the value of **1** for **max-classmap-size** .
Increase in QoS Policer Scale on Cisco NCS 5700 Series Line Cards and Routers	Introduced in this release on NCS 5700 fixed port routers (select variants only*); NCS 5500 modular routers (NCS 5700 line cards [Mode: Native]) (select variants only*)
	You can now regulate the incoming traffic bursts and manage traffic spikes with the enhanced scale limit of QoS policers for the following fixed port routers and line cards:
	• The Cisco NCS 5700 series fixed port router, NCS-57C3-MOD-SYS, now has an increased scale of 32000 QoS policers, by default
	• The Cisco NCS 5700 series fixed port router, NCS-57B1-6D24-SYS and the Cisco NC57 line card, NC57-24DD installed and operating in native mode, now have an increased scale of 16000 QoS policers, by default

Feature	Description
QoS IP DSCP Preservation for IPv6 SR-TE	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) This release introduces the functionality to preserve IP DSCP markings for IPv6 SR-TE traffic and covers the following scenarios: • **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 IPv6 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 for IPv6 traffic were modified. This modification resulted in traffic drops at the next-hop routers in SR-TE tunnels. This feature introduces a new keyword, **v6uc-enable** , in the **hw-module profile mpls-ext-dscp-preserve** command.
Multicast	
Draft-Rosen Multicast VPN (Profile 0) in PIM Sparse Mode (SM)	Introduced in this release on: NCS 5500 fixed port routers 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. PIM SM provides precise control in cases of large multicast traffic when there is less bandwidth available. This control is possible because it uses a temporary Rendezvous Point (RP) router to connect the multicast traffic source to the next hop router. Prior to this release, Profile 0 was supported only in PIM Source Specific Multicast (SSM) mode.
Protocol Independent Multicast (PIM) SM for Multicast VPN (MVPN) Profile 14	Introduced from this release on: NCS 5700 fixed port routersNCS 5500 modular routers(NCS 5700 line cards [Mode: Compatibility; Native]) With this release, MVPN profile 14 is now extended to support PIM SM mode for IPv4 and static RP.
Netflow	

Feature	Description
Simultaneous L2 and L3 Flow Monitoring using IPFIX	Introduced in this release on: NCS 5500 fixed port routers NCS 5500 modular routers (NCS 5500 line cards)
	This feature introduces support for simultaneous L2 and L3 flow monitoring. Now, you can configure IP Flow Information Export (IPFIX) to actively monitor and record end-to-end L2 and L3 flow information elements from network devices. Previously, only L2 or L3 flow could be monitored at a time.
	This feature introduces these changes:
	CLI: The following sub-menus are introduced for these commands:
	• The **record ipv4** command is modified to support a new optional keyword, **l2-l3**
	• The **record ipv6** command is modified to support a new optional keyword, **l2-l3**
	YANG Data Model:
	• New XPaths for `Cisco-IOS-XR-UM-flow-cfg.yang` (see GitHub, YANG Data Models Navigator)
sFlow Agent Address Assignment	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])
	You can now monitor traffic from a specific source by configuring the sFlow agent ID with the specific IPv4 or IPv6 address.
	Upon configuration, you can determine the source of the sFlow data.
	Earlier, by default, the sFlow agent ID had the source address of the sFlow export packet.
	The feature introduces these changes:
	CLI
	New Command:
	• **router-id**
	Modified Command:
	• The **show flow exporter-map** command is modified to display flow exporter map with router-id information.
	YANG Data Model
	• New XPaths for `openconfig-sampling-sflow.yang` (see GitHub, YANG Data Models Navigator)
System Security	

Feature	Description
Display Username for Failed Authentication for Telnet Protocols	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])
	With this feature, we have enhanced the security of the routers and introduced better tracking functionality to the router.
	The failed authentication sys log now displays the details of users who tried to log in but failed due to authentication failure.
	With this feature provisioned, the router can now display the user ID of both SSH and Telnet protocols.
	In earlier releases, this feature was available only for SSH protocol.
	This feature introduces the following change:
	CLI: **aaa display-login-failed-users** .
	YANG DATA Model: New XPaths for `Cisco-IOS-XR-um-aaa-task-user-cfg` (see Github, YANG Data Models Navigator)
Public Key-Based Authentication of SSH Clients on Cisco IOS XR Routers	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])
	You can now avail cryptographic strength and automated password-less log in while establishing SSH connections with the server. Along with password and keyboard-interactive authentication, Cisco IOS XR routers configured as SSH clients now support public key-based authentication. In this authentication method, passwords need not be sent over the network and hence, it provides an additional layer of security as well as aids in automation processes. This feature is available only for users locally configured on the router, not those configured on remote servers.
	Previous releases supported SSH public key-based authentication only for Cisco IOS XR routers configured as SSH servers.
	The feature introduces these changes:
	• **CLI**:
	• **crypto key generate authentication-ssh rsa**
	• **crypto key zeroize authentication-ssh rsa**
	• **show crypto key mypubkey authentication-ssh rsa**
	• **Yang Data Models**:
	New Xpaths for:
	• `Cisco-IOS-XR-crypto-act.yang`
	• `Cisco-IOS-XR-crypto-cepki-new-oper.yang`
	(see GitHub, YANG Data Models Navigator)
Licensing	

Feature	Description
Cisco Smart Licensing on QDD-400G-ZR-S, QDD-400G-ZRP-S, and DP04QSDD-HE0 optics	Introduced in this release on: NCS 5700 fixed port routers Cisco Smart Licensing is a cloud-based, flexible, automated software licensing model that enables you to activate and manage Cisco software licenses across your organization. Smart Licensing solution allows you to easily track the status of your license and software usage trends. Smart Licensing is now supported on the following optics: • QDD-400G-ZR-S • QDD-400G-ZRP-S • DP04QSDD-HE0
Smart Licensing on NC57-48Q2D-S and NC57-48Q2D-SE-S	Introduced in this release on: NCS 5500 modular routers (NCS 5700 line cards [Mode: Compatibility; Native]) (select variants only*) Cisco Smart Licensing is a cloud-based, flexible and automated software licensing model that enables you to activate and manage Cisco software licenses across your organization. Smart Licensing solution allows you to easily track the status of your license and software usage trends. Smart Licensing is now supported on the following line cards: • NC57-48Q2D-S • NC57-48Q2D-SE-S
System Management	
Auto-Save and Copy Router Configuration Using Public Key Authentication	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) You can now experience passwordless authentication while automatically saving running configurations and securely copying them on the router. The feature uses public key-based authentication, a secure logging method using a secure shell (SSH), which provides increased data security. This feature offers automatic authentication and single sign-on benefits, which also aids in a secure automation process. This feature modifies **configuration commit auto-save** and **copy** command to support password-less authentication.
MACSec Encryption on NCS-57D2-18DD-SYS Routers	Introduced in this release on: NCS 5700 fixed port routers (select variants only*) MACSec, the Layer 2 encryption protocol secures data on physical media and provides data integrity and confidentiality. *This feature is supported on 100G and 400G interfaces of NCS-57D2-18DD-SYS.

Feature	Description
PTP on NC57-48Q2D-S, NC57-48Q2D-SE-S and NCS-57C1-48Q6-SYS	Introduced in this release on: NCS 5500 modular routers (NCS 5700 line cards [Mode: Compatibility]) 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. With this release, PTP Class C and class B performance are now supported on 1G, 10G, 25G, 40G and 100G port speeds for the following hardware: • NC57-48Q2D-S • NC57-48Q2D-SE-S • NCS-57C1-48Q6-SYS
SyncE on NC57-48Q2D-S and NCS-NC57-48Q2D-SE-S	Introduced in this release on: NCS 5500 modular routers (NCS 5700 line cards [Mode: Compatibility]) 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 is now supported on the following hardware: • NC57-48Q2D-S • NC57-48Q2D-SE-S • NCS-57C1-48Q6-SYS
MACSec Encryption on NC57-48Q2D-S and NC57-48Q2D-SE-S	Introduced in this release on: NCS 5700 fixed port routers (select variants only*) With this release, the new *NC57-48Q2D-S and NC57-48Q2D-SE-Sline cards of Cisco NCS 5700 Series Router support MACSec encryption. MACSec, the Layer 2 encryption protocol secures data on physical media and provides data integrity and confidentiality. *This feature is supported on the following hardware: • NC57-48Q2D-S • NC57-48Q2D-SE-S
PTP and SyncE support on breakout ports for NC57-36H6D-S router	Introduced in this release on: NCS 5500 modular routers (NCS 5700 line cards [Mode: Native]) With this release, timing support for PTP and SyncE is extended to 4x10G and 4x25G breakout ports of NC57-36H6D-S and 4x10G breakout port of NC57-36H-SE in native mode. Class B and Class C performances are supported on 4x10G and 4x25G breakout ports in native mode for the NC57-36H6D-S line card and Class B performance is supported on 4x10G breakout port in native mode for the NC57-36H-SE line card. Route Processor: NC55-RP2-E
System Monitoring	

Feature	Description
System Log Facility and Source-address per Remote Server	Introduced in this release on:NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])
	You can now assign a facility number per remote syslog server, which the system inherits to calculate the priority value of the syslog messages sent. You can also configure the source address to choose the interface to send remote syslog packets per remote server.
	The feature introduces these changes:
	Modified Command:
	CLI
	• The keywords **facility** and **source-address** per remote syslog server are introduced in the **logging** command.
	YANG Data Models:
	• New XPaths for `openconfig-system-logging.yang` (see GitHub, YANG Data Models Navigator)

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-crypto-act.yang	The following new leaves are added to this Cisco native data model to enable public key-based authentication of users on Cisco IOS XR routers that are configured as SSH clients:
	• `key-generate-authentication-ssh-rsa-keys`
	• `key-zeroize-authentication-ssh-rsa`
Cisco-IOS-XR-crypto-cepki-new-oper.yang	A new container, `auth-ssh-keys`, is added to this Cisco native data model to display the details of SSH RSA cryptographic keys that are used for public key-based authentication of users on Cisco IOS XR routers that are configured as SSH clients.
Cisco-IOS-XR-l2vpn-cfg.yang	This Cisco native data model is enhanced to support EVPN port-active with hot standby on bundle interfaces.

Feature	Description
Cisco-IOS-XR-um-hw-module-profile-cfg.yang	This Cisco unified data model is enhanced to support optimization of EVPN BUM flood traffic.
Cisco-IOS-XR-um-router-bgp-cfg.yang	This Cisco unified data model is enhanced to advertise EVPN host routes as IPv4 or IPv6 unicast routes.
Cisco-IOS-XR-um-aaa-task-user-cfg	A new container, `display-login-failed-users`, is added to this Cisco unified data model to display username of the users who tried to log in to the router using invalid credentials, in the system logs.
Cisco-IOS-XR-controller-ots-oper.yang	Use this Cisco native data model to view the operational data of the QDD OLS pluggable that you can configure within the optical transport section (OTS) controller mode.
Cisco-IOS-XR-controller-ots-cfg.yang	Use this Cisco native data model to configure the QDD OLS pluggable within the optical transport section (OTS) controller mode.
Cisco-IOS-XR-pmengine-oper.yang	Use this Cisco native data model to view the performance monitoring parameters of the QDD OLS pluggable.
Cisco-IOS-XR-pmengine-cfg.yang	Use this Cisco native data model to configure the performance monitoring parameters of the QDD OLS pluggable.
Cisco-IOS-XR-pmengine-clear-act.yang	Use this Cisco native data model to clear the performance monitoring statistics of the QDD OLS pluggable.
openconfig-ospfv2.yang Version 0.4.0	The OpenConfig data model is introduced as part of the openconfig-network-instance.yang data model to configure OSPF functionalities, such as multiple processes, areas, and interfaces. Event-driven telemetry and Model-driven telemetry are not supported.

Feature	Description
openconfig-bgp-neighbor.yang Version 9.1.0	With this release, the OpenConfig data model introduces the following changes: • The datatype of the timer related leaves in the OpenConfig data model, such as `hold-time`, `keep-alive-interval`, `minimum-advertisement-interval`, `stale-routes-time`, `negotiated-hold-time` are changed. It is changed from `decimal64` to `uint16`. • The new leaf `restart-time` under Neighbor and Peer-group reflects the time interval (in sec) after which the BGP session is re-established. • Introduces the enable or disable capability of `graceful-restart` under Neighbor and Peer-group. • Supports independent configuration of the two leaves: `keepalive` and `hold-time`. • The new leaf `allow-multiple-as` under `global/use-multiple-paths/ebgp/config/`, enables the BGP to choose a path from different neighbouring as multipath. The hop count of the AS-path must match the hop count of the bestpath. You can now program routes with different AS-paths into the forwarding table as equal cost multipath routes. Earlier, for ECMP paths to be eligible, their AS-paths must exactly match the bestpath. • The new leaf `treat-as-withdraw` avoids the session reset when a BGP session encounters errors during parsing of received update message. The leaf discards the incoming update message as a withdraw message and ensures the subsequent actions are done. Event-driven telemetry and Model-driven telemetry are supported.

Feature	Description
opencofig-isis.yang	The OpenConfig data model defines the configuration and state information related to ISIS protocol configuration running on a router. With this release, you can configure the following XPaths: opencofig-network-instance/network-instances/network-instance/protocols/protocol/isis/interfaces/interface/ • `config/hello-padding`: controls the padding type for IS-IS Hello PDUs. • `mpls/igp-ldp-sync/config/enabled`: synchronisation between the LDP and IS-IS. • `levels/level/hello-authentication/config/keychain`: refers to a keychain that should be used for hello authentication. • `enable-bfd/config/enabled`: when this leaf is set to true, BFD is used to detect the liveliness of the remote peer or next-hop. • `levels/level/config/enabled`: when set to true, the functionality within which this leaf is defined is enabled and when set to false it is explicitly disabled. opencofig-network-instance/network-instances/network-instance/protocols/protocol/isis/ • `global/mpls/igp-ldp-sync/config/enabled`: synchronization between the LDP and IS-IS. • `global/config/maximum-area-addresses`: supports maximum area. • `globalconfig/Iid-tlv`: (ISIS Instance Identifier TLV) when set to true, the IID-TLV identifies the unique instance as well as the topology/topologies to which the PDU applies. • `levels/level/authentication/config/keychain`: refers to the keychain that should be used for authenticating IS-IS packets. Event-driven and Model-driven telemetry is supported.

Feature	Description
openconfig-system-logging.yang Version 0.3.1	The OpenConfig data model defines configurations for common logging facilities on network systems. The model is updated with the following XPaths: openconfig-system/logging/ • console/selectors/selector/facility: to configure the facility parameter for console logging of all supported facilities. • remote-servers/remote-server/selectors/selector/facility: to configure the desired facility per remote syslog server. • remote-servers/remote-server/config/source-address: to configure the desired source-address per remote syslog server. You can use the configured facility to calculate the priority field of the remote syslog packet and use the configured source-address to choose the interface to send remote syslog packets. Model-driven telemetry and Event-driven telemetry is not applicable.

Feature	Description

opened-sampling-sflow.yang Version 1.1.0	The OpenConfig data model defines the sampling mechanisms implemented in an sFlow agent for monitoring traffic. This data model augments the openconfig-sampling.yang model. The model is revised from version 0.1.0 to 1.0.0 with the following XPaths:
	
	• `openconfig-sampling-sflow:sampling/sflow/config/`
	  • `agent-id-ipv4` and `agent-id-ipv6`: to configure the agent identifier (ID) with IPv4 or IPv6 address for all collectors. These XPaths are not mandatory. If they are not configured, then the router picks the `source-address` as the agent ID.
	  • `polling-interval`: to configure an interface counter polling-interval for all sFlow enabled interfaces.
	  • `ingress-sampling-rate` and `egress-sampling-rate`: to set the ingress and egress packet sampling rate respectively.
	  • `dscp`: DSCP marking of sFlow export packets generated by the sFlow subsystem on the network device.
	
	• `openconfig-sampling-sflow:sampling/sflow/collectors/collector/config/`
	  • `source-address`: to set the source IPv4 or IPv6 address for sFlow datagrams sent to sFlow collectors. In this release, the XPath is moved from the `config` container to `collectors` container. Upon configuration, the flow exporter-map associated with this collector gets the `source-address` configuration. Earlier, by default, the sFlow agent ID had the source address of the sFlow export packet.
	
	• `openconfig-sampling-sflow:sampling/sflow//interfaces/interface/config/`
	  • `ingress-sampling-rate` and `egress-sampling-rate`: to set the ingress and egress packet sampling rate respectively. In the absence of ingress sampling rate configuration at the interface level, the global `ingress-sampling-rate` will be used. For egress sampling on the interface, `egress-sampling-rate` must be used.
	
	Model-driven telemetry is supported.

Feature	Description
openconfig-system-grpc.yang Version 1.0.0	The OpenConfig data model is revised from version 0.1.1 to 1.0.0. This version enables the gRPC server to listen on any IP address bound to an interface and port of the system or listen for any specific list of IP addresses. The maximum number of supported IP addresses are 32, which may be IPv4 or IPv6, or both. Earlier, the gRPC server had the listen functionality for any IP address on the gRPC port but not to a specific list of listen addresses. Event-driven telemetry and Model-driven telemetry are supported.
openconfig-aft.yang Version 0.6.0	The Abstract Forwarding Table (AFT) OpenConfig data model is enhanced to support the following features: • The gRPC Network Management Interface (gNMI) proto is revised from version 0.7.0 to 0.8.0 to set the atomic flag to send AFT next-hop group notifications in JSON and PROTO encodings using gNMI subscribe RPC. Network events can be represented as multiple updates in the data models. The atomic flag allows NMS to interpret those multiple updates as a single event. • The nodes next-hop-group/state and next-hops/next-hop defines a list of next-hop addresses and a tunnel type for packets that match the specified criteria. Model-driven telemetry and Event-driven telemetry is supported.
Cisco-IOS-XR-infra-xtc-agent-cfg.yang	This Cisco native data model is used for gathering statistics on reporting of SR-Traffic Engineering (TE) policies using BGP-Link State (LS).
Cisco-IOS-XR-um-router-isis-cfg.yang	The latest update to the Cisco-IOS-XR-um-router-isis-cfg.yang unified data model includes the addition of the partition-detect and partition-repair containers. These new containers indicate the configuration of the partition-detect and partition-repair nodes.

Hardware Introduced

Cisco IOS XR Release 7.10.1 introduces the following hardware support:

Hardware Feature	Description

Optics	This release launches the following new optics on selective hardware within the product portfolio. For details, refer to theTransceiver Module Group (TMG) Compatibility Matrix.
	
	Cisco 10GBASE Small Form-Factor Pluggable (SFP+)
	
	  • SFP-10G-SR-I
	
	Cisco 100Gbps QSFP100 SR1.2 BiDi Pluggable
	
	  • QSFP-100G-SR1.2

NC57-48Q2D-S and NC57-48Q2D-SE-S line cards	The NC57-48Q2D-S is a modular line card that supports front panel bandwidth of 2.4 Tbps through fixed optics ports. The front panel consists of the following port:
	
	  • Two QSFP-DD ports of 400GbE
	
	  • 16 SFP56 ports of 50GbE
	
	  • 32 SFP28 ports of 25GbE
	
	The NC57-48Q2D-SE-S line card has additional TCAM for supporting expanded Forwarding Information Base (FIB), network access control lists (ACLs), and QoS for scale-enhanced configuration needs.
	
	The line card can operate in native mode and compatible mode.

Features Supported on Cisco NC5700 Line Cards and NCS 5700 Fixed Port Routers

The following table lists the features supported on Cisco NC5700 line cards in compatibility mode (NC5700 line cards with previous generation NCS 5500 line cards in the same NCS 5500 modular routers) and native mode (NCS 5500 modular routers with only NCS 5700 line cards and NCS 5700 fixed port routers).

To enable the native mode on Cisco NCS 5500 series modular routers having Cisco NCS 5700 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.

Table 1: Features Supported on Cisco NC5700 Line Cards and NCS 5700 fixed port routers

Feature	Compatible Mode	Native Mode
Improved YANG Input Validator and Get Requests	✓	✓
OpenConfig Metadata for Configuration Annotations	✓	✓
Prevent Partial Pseudo-Atomic Committed Configurations	✓	✓
Autonomous System Boundary Router Isolation and Adjacency Control for LSA Overflows	✓	✓
Multihop Bidirectional Forwarding Detection on IPv4 and IPv6 Non-Default VRFs	✕	✓

Feature	Compatible Mode	Native Mode
Disable IID-TLV of IS-IS Protocol Instance	✓	✓
Automatic Bandwidth Bundle TE++ for Numbered Tunnel	✓	✓
Configurable Filters for IS-IS Advertisements to BGP-LS	✓	✓
IS-IS Partition Detection and Leakage of Specific Route Advertisements	✓	✓
Multicast VPN: Dynamic Tree-SID Multicast VPN IPv6	✓	✓
Multicast: Cisco Nonstop Forwarding for Tree-SID	✓	✓
Reporting of SR-TE Policies Using BGP-Link State	✓	✓
Automatically Reestablish a BGP Neighbor Session	✓	✓
BGP Flowspec on Bridge- Group Virtual Interafaces	✗	✓
Discard Incoming BGP Update Message	✓	✓
Exclusion of Label Allocation for Non-Advertised Routes	✓	✓
Reduce Recursions for eBGP Peering on Loopback Address on Bridge-Group Virtual Interface	✗	✓
Egress Hybrid ACL-based Traffic Mirroring on Cisco NCS 5700 Series Line Cards and Routers	✗	✓
Fibre Channel over PLE Transmission Using TTS Auto-Negotiation	✓	✓
QDD Optical Line System	✗	✓
Configure ACLs on MPLS Deaggregation Packets	✓	✓
Filter TCP Flags in Egress IPv6 or IPv4 Hybrid ACLs	✓	✓
Identify Internal TCAM Entries for Hybrid ACLs	✓	✓
Advertise EVPN Host IP Routes as IP Unicast Routes	✓	✓
EVPN Link Bandwidth for Proportional Multipath on VNF	✓	✓
EVPN Port-Active Hot Standby	✓	✓
ITU-T Y.1731 Compliant EVPN Flexible Cross-Connect Services	✗	✓
Flexibility to Set a Maximum of One Class Map per Ingress QoS Traffic Policy	✗	✓
Increase in QoS Policer Scale on Cisco NCS 5700 Series Line Cards and Routers	✗	✓
QoS IP DSCP Preservation for IPv6 SR-TE	✗	✓

Feature	Compatible Mode	Native Mode
Protocol Independent Multicast (PIM) SM for Multicast VPN (MVPN) Profile 14	✓	✓
sFlow Agent Address Assignment	✓	✓
Display Username for Failed Authentication	✓	✓
Public Key-Based Authentication of SSH Clients on Cisco IOS XR Routers	✓	✓
Auto-Save and Copy Router Configuration Using Public Key Authentication	✓	✓
PTP on NC57-48Q2D-S and NC57-48Q2D-SE-S	✓	✕
PTP and SyncE support on breakout ports for NC57-36H6D-S router	✕	✓
MACSec Encryption on NCS-57D2-18DD-SYS Router	✕	✓
SyncE on NC57-48Q2D-S and NCS-NC57-48Q2D-SE-S	✓	✓
Smart Licensing on NC57-48Q2D-S and NC57-48Q2D-SE-S	✓	✓
System Log Facility and Source-address per Remote Server	✓	✓
Extended Support for DP04QSDD-HE0 optical module	✓	✓

For the complete list of features supported on Cisco NC57 line cards until Cisco IOS XR Release 7.10.1. see:

- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.9.2
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.9.1
- 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 7.6.2
- 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

Deprecated features

Starting with Cisco IOS XR release 7.10.1, the performance-measurement **{delay-profile | liveness-profile} {sr-policy | endpoint | interface} name** *name* CLI is deprecated. Old configurations stored in NVRAM will be rejected at boot-up. As a result, performance measurement delay and liveness named profiles using the old CLI must be re-configured using the **performance-measurement {delay-profile | liveness-profile} name** *name* CLI.

> ✎
>
> **Note**　The default performance measurement delay and liveness profiles configured using the **performance-measurement { delay-profile | liveness-profile} { sr-policy | endpoint | interface} default** commands are still valid and unaffected.

For more information, see *CLI Changes for Segment Routing Performance Measurement* section under the *Link Delay Measurement* topic in *Segment Routing Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 7.10.x*.

Caveats

Table 2: Cisco NCS 5500 Series Router Specific Bugs

Bug ID	Headline
CSCwf89722	EVPN VPWS down post migrating from Multi-homing to Single-Homing.
CSCwf81475	Netflow IPv6: The record-ipv6 reports incorrect interfaces with outbundlemember or outphysint options
CSCwf58845	In NC57-18DD-SE, non-fixed QDD ports are not operating as 400G interfaces when DP04QSDD-ER1 optics is used

Behavior Changes

Starting with Cisco IOS XR Software Release 7.10.1, you must configure a name server for Smart Licensing deployment options that use HTTPS for communication with Cisco Smart Software Manager (CSSM). If the system cannot validate that the Common Name (CN) in the X.509 server certificate is a Fully Qualified Domain Name (FQDN), communication with CSSM results in an **Error during SSL communication**. See the *Smart Licensing Chapter* in the *System Management Configuration Guide for NCS 5500 Series Routers* for more information and options to bypass the name server configuration.

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 7.10.1 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-r7101.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-r7101.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r7101.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.
Cisco IOS XR Security Package	ncs5500-k9sec-3.1.0.0-r7101.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-r7101.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf-2.0.0.0-r7101.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs5500-li-1.0.0.0-r7101.x86_64.rpm	Includes LI software images
Multicast Package	ncs5500-mcast-1.0.0.0-r7101.rpm	Support Multicast

Table 4: Release 7.10.1 TAR files for Cisco NCS 5500 Series Router

Feature Set	**Filename**
NCS 5500 IOS XR Software 3DES	NCS5500-iosxr-k9-7.10.1.tar
NCS 5500 IOS XR Software	NCS5500-iosxr-7.10.1.tar
NCS 5500 IOS XR Software	NCS5500-docs-7.10.1.tar

Table 5: Release 7.10.1 Packages for Cisco NCS 5700 Series Router

Feature Set	**Filename**
NCS 5700 IOS XR Software	ncs5700-x64-7.10.1.iso

NCS 5700 IOS XR Software (only k9 RPMs)	ncs5700-k9sec-rpms.7.10.1.tar
NCS 5700 IOS XR Software Optional Package	NCS5700-optional-rpms.7.10.1.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.

```
Router# show version
Cisco IOS XR Software, Version 7.10.1
Copyright (c) 2013-2023 by Cisco Systems, Inc.

Build Information:
 Built By     : deenayak
 Built On     : Wed Aug 16 22:30:10 PDT 2023
 Built Host   : iox-ucs-044
 Workspace    : /auto/srcarchive16/prod/7.10.1/ncs5500/ws
 Version      : 7.10.1
 Location     : /opt/cisco/XR/packages/
 Label        : 7.10.1

cisco NCS-5500 () processor
System uptime is 4 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
--------------------------------------------------------------------------------
0/3       NC57-36H-SE   1.0   Bootloader          CURRENT   1.03    1.03
0/3       NC57-36H-SE   1.0   DBFPGA              CURRENT   0.14    0.14
0/3       NC57-36H-SE   1.0   IOFPGA              CURRENT   0.05    0.05
0/3       NC57-36H-SE   1.0   SATA-Micron         CURRENT   1.00    1.00
0/5       NC57-36H-SE   1.0   Bootloader          CURRENT   1.03    1.03
0/5       NC57-36H-SE   1.0   DBFPGA              CURRENT   0.14    0.14
0/5       NC57-36H-SE   1.0   IOFPGA              CURRENT   0.05    0.05
0/5       NC57-36H-SE   1.0   SATA-Micron         CURRENT   1.00    1.00
```

```
0/7        NC57-36H-SE      1.0    Bootloader          CURRENT     1.03      1.03
0/7        NC57-36H-SE      1.0    DBFPGA              CURRENT     0.14      0.14
0/7        NC57-36H-SE      1.0    IOFPGA              CURRENT     0.05      0.05
0/7        NC57-36H-SE      1.0    SATA-Micron         CURRENT     1.00      1.00
0/RP0      NC55-RP2-E       1.0    Bootloader          CURRENT     0.08      0.08
0/RP0      NC55-RP2-E       1.0    IOFPGA              CURRENT     0.50      0.50
0/RP0      NC55-RP2-E       1.0    OMGFPGA             CURRENT     0.52      0.52
0/RP0      NC55-RP2-E       1.0    SATA-Micron         CURRENT     1.00      1.00
0/RP1      NC55-RP2-E       1.0    Bootloader          CURRENT     0.08      0.08
0/RP1      NC55-RP2-E       1.0    IOFPGA              CURRENT     0.50      0.50
0/RP1      NC55-RP2-E       1.0    OMGFPGA             CURRENT     0.52      0.52
0/RP1      NC55-RP2-E       1.0    SATA-Micron         CURRENT     1.00      1.00
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/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          1.6    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
```

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.

- A kernel upgrade on NCS 5700 Series Routers has introduced some Cisco IOS XR Release 7.10.1-specific upgrade and downgrade caveats. For details, see Release 7.10.1 Caveats.

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.