Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.8.1

Revised: November 29, 2023

Network Convergence System 5500 Series Routers

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

What's New in Cisco IOS XR Release 7.8.1

Cisco IOS XR Release 7.8.1 is a new feature release for Cisco NCS 5500 Series routers. For more details on the Cisco IOS XR release model and associated support, see Guidelines for Cisco IOS XR Software.

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

New in Documentation

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 Feature Introduced and Enhanced

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

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

Feature	Description
System Monitoring	
EEDB Resource Segregation for Encapsulation Types	We have now segregated the Egress Encapsulation Database (EEDB) resources based on different egress encapsulation types, such as attachment circuits (AC), pseudowires, tunnels, and Address Resolution Protocol (ARP). This allows you to examine encapsulation-specific resource details using show commands. When resource usage exceeds the Out of Resource (OOR) threshold levels, the router also alerts you with system log messages. When resource usage exceeds the OOR thresholds, you can avoid traffic loss by taking corrective action to free up resources, such as reducing the scale of interfaces with the related encapsulation. The **show controllers npu resources** command is now modified to include the following optional keywords: • **encapAC** • **encapPWE** • **encaptunnels** • **encapARP** This feature is supported on Cisco 5700 Series Routers and on routers that have the NC57 line cards installed and operating in either native or compatiblity mode

Feature	Description
BGP	
BGP Advertisement without Additional Paths	The route reflector client can now advertise both the best path and the best external path when the locally received route and the route that it received from VRF have different route distinguishers (RDs) without additional paths. Earlier, the router reflector client advertised both the best path and the best external path in the route reflector only when you had configured additional path. This feature is enabled by default and supports both IPv4 and IPv6 prefixes. You cannot disable it.
Programmability	

Feature	Description
gNMI Bundling Size Enhancement	With gRPC Network Management Interface (gNMI) bundling, the router internally bundles multiple gNMI `Update` messages meant for the same client into a single gNMI `Notification` message and sends it to the client over the interface. You can now optimize the interface bandwidth utilization by accommodating more gNMI updates in a single notification message to the client. We have now increased the gNMI bundling size from 32768 to 65536 bytes, and enabled gNMI bundling size configuration through Cisco native data model. Prior releases allowed only a maximum bundling size of 32768 bytes, and you could configure only through CLI. The feature introduces new XPaths to the `Cisco-IOS-XR-telemetry-model-driven-cfg.yang` Cisco native data model to configure gNMI bundling size. To view the specification of gNMI bundling, see Github repository.
gNOI System Service Revision 1.0.0	With the gRPC Network Operations Interface (gNOI) Revision 1.0.0, you can: • Cancel a pending reboot request using the `CancelReboot` RPC • Terminate a process using the `KillProcess` RPC You can access the gNOI system RPC messages from the Github repository.
Routing	
Configure flex-algo IS-IS maximum-path	This feature introduces the new **algorithm 0** command and provides information on the updated **flex-algo** command. These updates enable individual granularity for flex-algo and regular SPF algorithms.
Segment Routing	
Circuit-Style SR-TE Policies	This solution allows Segment Routing to meet the requirements of a connection-oriented transport network, which was historically delivered over circuit-switched SONET/SDH networks. Circuit-style SR-TE policies allow a common network infrastructure to be used for both connection-oriented services and classic IP-based transport. This eliminates the need for multiple parallel networks, which greatly reduces both capital expenditures (CapEx) and operating expenditures (OpEx).
High Availability Support for Dynamic Tree-SID (Multicast VPN)	We have introduced more resilience for building multicast VPN (mVPN) dynamic tree-SIDs by providing High Availability (HA) for the Segment Routing Path Computation Element (SR-PCE). This HA is made possible by adding another SR-PCE to the network. As a result, there's a noncompute or standby PCE for the mVPN dynamic policies. The root Path Computation Element Client (PCC) elects the active SR-PCE. If an active PCE failure occurs, the root PCC delegates the compute role for the mVPN dynamic Tree-SID to the standby SR-PCE.

Feature	Description
Path Tracing Midpoint Node	Path Tracing (PT) provides a log or record of the packet path as a sequence of interface IDs along with its time stamp. In Path Tracing, a node can behave as a source, midpoint, or sink node. The Path Tracing Midpoint feature is implemented in this release which measures the hop-by-hop delay, traces the path in the network and collects egress interface load information and interface Id, and stores them in the Midpoint Compressed Data (MCD) section of Hop-by-Hop Path Tracing (HbH-PT) header. This feature provides visibility to the Path Tracing Midpoint node that handles IPv6 transit in Path Tracing and full characterization of the packet delivery path. It provides real time information and the current status of the network. This feature is supported on Cisco 5700 Series Routers and on routers that have the NC57 line cards installed and operating in native mode. This feature introduces the following command: • **performance-measurement interface**
SR IS-IS Enhancements: max-metric and data plane updates	The new **anomaly** optional keyword is introduced to **affinity flex-algo** command. This keyword helps to advertise the flex-algo affinity when the performance measurement signals a link anomaly, such as an excessive delay on a link. You could use the anomaly option to exclude the link from flex-algo path computations. **affinity flex-algo**
Interface and Hardware Component	
Improved ACL-based Traffic Mirroring with Capture Option Support on Cisco NC57 Line Cards	When you enable **capture** option on a source interface that has an ACL configured, the traffic matching the rules defined in an ACL gets captured. If the ACL configuration uses the **capture** keyword, but the ACL command is not configured on the source interface, then the whole interface traffic is mirrored and the **capture** action does not have any affect. This option not only allows you to narrow down the traffic that you want to mirror but also enables you to troubleshooting the captured traffic for issues, such as packet drops, packet fields getting modified, virus attacks, or any other network threat. This option is introduced in the following commands: • **permit (IPv4)** • **permit (IPv6)** This feature is supported on routers that have the Cisco NC57 line cards installed that operate in the native mode.
SPAN Filtering of Outgoing Traffic on Layer 2 Interfaces for Cisco NC57 Line Cards	This release introduces SPAN filtering on the outgoing (Tx) DNS, HTTP, HTTPS, and TLS Layer 2 interface traffic. Enabling SPAN filtering on outgoing (Tx) traffic provides you more flexibility to monitor and troubleshoot the DNS, HTTP, HTTPS, and TLS traffic. This feature introduces the following command: • **hw-module profile span-filter l2-l3-tx-enable** This feature is supported on routers that have the Cisco NC57 line cards installed that operate in the native mode.

Feature	Description
Support for DP04CFP2-D15 Bidirectional CFP2-DCO Optical Module	In this release, support for DP04CFP2-D15 bidirectional CFP2-DCO optical module is added for NC55-MOD-A-S and NCS-55A2-MOD-S routers with the following MPAs: • NC55-MPA-2TH-S • NC55-MPA-1TH2H-S The bidirectional CFP2-DCO optical module allows for data transmission and reception in both directions over a single fiber of a network, offering a cost and operationally effective method for expanding the network capacity in fiber-restricted networks.
Cisco NC57 Compatibility Mode: Y.1731	This feature is supported on routers that have the Cisco NC57 line cards installed and operate in the compatibility mode. For more information on Y.1731, see Configuring Ethernet OAM.
IP Addresses and Services	
Support for HSRP version 2 Extended Group Range	You can now use HSRP version 2, which has an expanded group IDs up to 4095 with 255 number of (IPv4 and IPv6 combined) HSRP sessions Now, the interoperation with the other routers is supported. Earlier, you could configure only up to 255 group IDs with 255 number of (IPv4 and IPv6 combined) HSRP sessions.
L2VPN and Ethernet Services	
MAC Address Limit Configuration for Static Addresses	You can now configure the MAC address limit for bridge domains to learn only static MAC addresses and to drop traffic from unknown sources. Malicious attackers can spoof a Layer 2 MAC address to change dynamic entries in the MAC table. However, with this functionality enabling you to configure the MAC address limit for bridge domains to learn only static MAC addresses, the dynamic MAC addresses are blocked. In addition, a static entry always overrules dynamic entries. This functionality thus prevents the interception of your data by unauthorized users and improves your network security.
Single Tagged VLAN Range Support for Double Tagged Frames	From this release, L2 subinterface configuration with single tagged VLAN range can be matched with the double tagged frames. Previously, the packet matching was done only with single VLAN ID and the double tagged packets were dropped. With single tagged VLAN range support for double tagged frames, the traffic can reach the VLAN destination safely.
Storm Control Configuration for Subinterfaces	Storm control helps prevent LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm. You can now configure different storm control rates for each subinterface on a physical port. This will give you control at a granular level and prevent flooding of excess traffic at the subinterface level. In earlier releases, storm control could be configured only at the physical port level or only on one subinterface under a main interface. This feature modifies the **hw-module storm-control-combine-policer-bw enable** command to enable per subinterface configuration support for storm control.

Feature	Description
Netflow	
IPFIX Enablement for SRv6 and Services over SRv6 Core	This feature provides improved information about IP traffic flows, through the introduction of sub-menus to two commands. The **record ipv6** command is modified to support a new optional keyword, **srv6** . A new subtype for **ipv4 record** and **ipv6 record** is introduced for **l2-l3** records. For more information, see: • **record ipv6** • **show flow monitor-map**
Modular QoS	
Configure WRED Counters by Class on Cisco NCS 5700 Series Base (Non-SE) Version Line Cards	You can now view WRED statistics per class on Cisco NCS 5700 Series base (non-SE) version line cards operating in native mode. This functionality provides a more accurate and granular statistics profile for packet drops.
Increase in QoS Policer Allocation on Cisco NCS 5700 Series Line Cards	You can now allocate up to a maximum of 64000 policers for QoS by reallocating unused BGP Flowspec policer resources to QoS and increasing the QoS policer count. With more QoS policers, you can apply policies on more sub-interfaces. This feature is supported on NC57-18DD-SE and NC57-36H-SE line cards. This feature introduces the following command: • **hw-module profile qos policer-scale**
System Management	
Flexible Consumption Model on NCS-57D2-18DD-SYS	Flexible Consumption Model (FCM) is now extended to the NCS-57D2-18DD-SYS chassis.
ITU-T G.8275.2 and Default PTP profiles over IPv6	For ITU-T G.8275.2 and the IEEE 1588 default PTP profiles, the encapsulation type for PTP packet transport is now extended to IPv6. This feature modifies the **transport** command to include the keyword **ipv6** .
RSP Slot Location in Syslog	When an RSP switchover occurs, the router logs the active RSP slot location in the syslog message. This helps you quickly identify the active RSP slot from your router's system log messages. In earlier releases, the RSP switchover Syslog message didn't include the active RSP slot location.

Feature	Description
Smart Licensing Per Port for Segment Routing-Traffic Engineering	Cisco Smart Licensing is a cloud-based, flexible software licensing model that enables you to activate and manage Cisco software licenses across your organization. Under the flexible, automated software licensing model, we have Advantage licenses which are required on top of Essential Licenses for ports that use advanced features like L3VPN. This release allows you to allocate the Advantage licenses to the Segment Routing Traffic Engineering (SR-TE) based on the active ports under MPLS or SRV6. Before this release, when you configured SR-TE, all the ports used to consume Advantage licenses. This allows you to manage advantage licenses for SR-TE.
Y.1564 Service Activation Test in Native Mode	Y.1564 - Ethernet Service Activation Test (or performance test methodology) is a testing procedure which tests service turn-up, installation, and troubleshooting of Ethernet-based services. This test methodology was created to have a standard way of measuring Ethernet-based services in the industry. This testing procedure is now supported on Cisco Routers that have the Cisco NCS57 line cards installed and operate in the Native mode.
PTP on NC57-MPA-1FH1D-S and NCS-57D2-18DD-SYS	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 hardware: • NC57-MPA-1FH1D-S • NCS-57D2-18DD-SYS
SyncE on NC57-MPA-1FH1D-S and NCS-57D2-18DD-SYS	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-MPA-1FH1D-S • NCS-57D2-18DD-SYS
Smart Licensing on NCS-57D2-18DD-SYS	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 NCS-57D2-18DD-SYS chassis.
System Monitoring	

Feature	Description
EEDB Resource Segregation for Encapsulation Types	We have now segregated the Egress Encapsulation Database (EEDB) resources based on different egress encapsulation types, such as attachment circuits (AC), pseudowires, tunnels, and Address Resolution Protocol (ARP). This allows you to examine encapsulation-specific resource details using show commands. When resource usage exceeds the Out of Resource (OOR) threshold levels, the router also alerts you with system log messages. When resource usage exceeds the OOR thresholds, you can avoid traffic loss by taking corrective action to free up resources, such as reducing the scale of interfaces with the related encapsulation. The **show controllers npu resources** command is now modified to include the following optional keywords: • **encapAC** • **encapPWE** • **encaptunnels** • **encapARP** This feature is supported on Cisco 5700 Series Routers and on routers that have the NC57 line cards installed and operating in either native or compatiblity mode
System Security	
Dynamic Retrieval of NETCONF Access Control Model Policies	Your router now retrieves the NETCONF Access Control Model (NACM) policies or rules on-demand for an authorized user from a remote Lightweight Directory Access Protocol (LDAP) server to validate each NETCONF operation. As the policies are stored in an external server and retrieved dynamically, this feature eliminates the need to manually update policies on a per-router basis. Before this release, your router supported static NACM, where the NACM policies or rules were stored locally, requiring manual policy updates on each router. This feature introduces the **nacm enable-external-policies** command.
IMA Enforcement	We now use Integrity Measurement Architecture (IMA) to provide a higher level of trust and runtime security for the routers. With IMA appraisal, you can detect modifications to a file or executable within the router. These modifications could be accidental or malicious, carried out remotely or locally. In addition to logging an integrity violation, the IMA policy also enforces an appraisal by blocking any operation (open or run) for a compromised executable. IMA Enforcement is now introduced on Cisco NCS 5700 Series Routers. It is not supported on Cisco NCS 5500 Series Routers.

Feature	Description
Secure Boot Status	You can now verify whether the router is securely booted up with an authentic Cisco software image. We have introduced a **show** command to verify the secure boot status of the router. If the software image was tampered with, then the secure boot fails, and the router does not boot up. Before this release, there was no provision on the router to verify the secure boot status. The feature introduces these: • CLI: **show platform security integrity log secure-boot status** command. • YANG Data Model: `Cisco-IOS-XR-attestation-agent-oper.yang` Cisco native model (see GitHub) The feature is supported only on Cisco NCS 5700 Series Routers.
Secure Boot on NCS-57D2-18DD-SYS	You can ensure that the code that executes on Cisco routers is authentic and unmodified. Cisco hardware-anchored secure boot feature protects the microloader, the first piece of code that boots up, in a tamper-resistant hardware. This functionality thereby establishes a root of trust that helps to prevent Cisco routers from executing tainted network software. This feature is now extended to the following variant of Cisco NCS 5700 Series Router: • NCS-57D2-18DD-SYS
Selective Authentication Methods for SSH Server	You now have the flexibility to choose the preferred SSH server authentication methods on the router. These methods include password authentication, keyboard-interactive authentication, and public-key authentication. This feature allows you to selectively disable these authentication methods. By allowing the SSH clients to connect to the server only through these permitted authentication methods, this functionality provides additional security for router access through SSH. Before this release, by default, the SSH server allowed all these authentication methods for establishing SSH connections. The feature introduces these changes: • **CLI**: New **disable auth-methods** command • **YANG Data Model**: New XPaths for `Cisco-IOS-XR-crypto-ssh-cfg.yang` Cisco native model (see GitHub)
Telemetry	
Stream Telemetry Data for ACL	The Access control List (ACL) is an ordered list of rules used to filter the traffic to increase network performance, and to specify the system resource access permissions either grant or deny to users or systems for security. We have introduced the streaming of ACL statistics to monitor the traffic flow using YANG data and telemetry. It allows you to monitor dropped, matched, and denied packets of IPv4 and IPv6. In earlier releases, you could monitor ACL statistics through CLI. This feature introduces the `Cisco-IOS-XR-ipv4-acl-oper.yang` and `Cisco-IOS-XR-ipv6-acl-oper.yang` models to capture IPv4 and IPv6 ACL statistics on Cisco Network Convergence System 5700 Series Routers.

Feature	Description
Stream Telemetry Data for BGP FlowSpec Statistics	Use Border Gateway Protocol (BGP) FlowSpec to mitigate the effects of distributed denial-of-service (DDoS) attack over the network. We have introduced streaming of BGP FlowSpec statistics using YANG data and telemetry. It allows you to monitor traffic flow match, drop in the traffic, or policing at definite rate for IPv4 and IPv6 parameters such as IP address, port, DSCP, and so on. In earlier releases, you could monitor BGP FlowSpec statistics through CLI. This feature introduces the `Cisco-IOS-XR-flowspec-oper.yang` data models to capture BGP FlowSpec statistics such as matched, dropped, and transmitted packet count on Cisco Network Convergence System 5700 Series Routers.
View Internal TCAM Resource Utilization for Ingress Hybrid ACL	Ternary Content-Addressable Memory(TCAM) is an important and limited resource. This feature, allows you to be mindful of the usage and availability of the resource, before configuring ingress hybrid ACL. You can now fetch the usage data through CLI and Streaming Telemetry. This functionality modifies the following: • **CLI:** The option **status** in the **show controllers npu internaltcam status location** command, displays the possible free and used entries. • **YANG Data Model:** This feature uses the `Cisco-IOS-XR-fia-internal-tcam-oper.yang` to fetch the internal TCAM resource.

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	
Cisco-IOS-XR-attestation-agent-oper.yang	We have introduced this Cisco native data model to verify whether the router is securely booted up with an authentic Cisco software image.
Cisco-IOS-XR-crypto-ssh-cfg.yang	We have introduced the following Xpaths to this Cisco native data model for you to selectively disable the SSH server authentication methods on the router: • `/ssh/server/disable/AuthMethods/Password` • `/ssh/server/disable/AuthMethods/KeyboardInteractive` • `/ssh/server/disable/AuthMethods/PublicKey`

Feature	Description
Openconfig-alarms.yang Revision 0.3.2	The OpenConfig data model, part of the `openconfig-system.yang` data model. The model is revised from 0.3.0 to 0.3.2 to enhance the time the system raises the alarm. This value is expressed relative to the UNIX epoch time. Using this XPath, you can stream Event-driven and Model-driven telemetry data.

Feature	Description
openconfig-sampling-sflow Revision 0.1.0	The OpenConfig data model revision 0.1.0 supports the following XPaths to configure the parameters such as sampling rate, sampling size, the source address of the router, collector port number, IPv4 or IPv6 addresses, and network-instance (VRF) to monitor real-time traffic in data networks using a sampling mechanism in the sFlow agent. `openconfig-sampling-sflow:sampling/sflow` • `config/enabled` • `config/source-address` • `config/sampling-size` • `config/sampling-rate` • `state/enabled` • `state/source-address` • `state/sampling-size` • `state/sampling-rate` • `collectors/collector[address,port]/address` • `collectors/collector[address,port]/port` • `collectors/collector[address,port]/config/address` • `collectors/collector[address,port]/config/port` • `collectors/collector[address,port]/config/network-instance` • `collectors/collector[address,port]/state/address` • `collectors/collector[address,port]/state/port` • `collectors/collector[address,port]/state/network-instance` • `interfaces/interface[name]/name` • `interfaces/interface[name]/config/name` • `interfaces/interface[name]/config/enabled` • `interfaces/interface[name]/config/sampling-rate` • `interfaces/interface[name]/state/name` • `interfaces/interface[name]/state/enabled` • `interfaces/interface[name]/state/sampling-rate` This release introduces **source-address** command.

Feature	Description
openconfig-aft.yang Revision 0.6.0	The OpenConfig data model is revised from version 0.3.0 to 0.6.0. The revised version introduces the support for NMS to receive essential interface characteristics, such as next-hop and next-hop group using the following XPaths to simplify the forwarding process: `openconfig-network-instance/network-instances/network-instance/afts/` • `next-hop-groups/next-hop-group/` • `next-hops/next-hop` To view the operational data of the system, you can stream Event-driven and Model-driven telemetry data.

Hardware Introduced

Hardware Feature	Description
NCS-57D2-18DD-SYS Router	This release introduces a 2-RU fixed port router in the Cisco NCS 5700 series. This high-capacity, low-power-consuming router provides the following support and capabilities: • Up to 7.2 Terabits (Tbps) total port bandwidth and 7.2 Terabits (Tbps) forwarding capacity. • Total of 66 QSFP-DD ports • Support for QSFP28 optics • Synchronous Ethernet (SyncE) • Power supply redundancy
NCS57-MPA-1FH1D-S Modular Port Adapter	This release introduces NCS57-MPA-1FH1D-S, a 2-port 800GbE modular port adapter with one port supporting QSFP-DD and the other supporting CFP2-DCO optical transceivers. This MPA is supported in the NCS-57C3-MODS-SYS router and NC57-MOD-S line card. For more information, see the Cisco Network Convergence System 5700 Series: Modular Port Adapters Data Sheet.
Optics	The NCS-57C3-MODS-SYS and NCS-57C3-MOD-SYS routers now support the following optical modules using the NC57-MPA-2D4H-S modular port adapter (MPA): • QDD-400G-ZR-S • QDD-400G-ZRP-S Combined with routers optimized for 400G port bandwidth (in 4x100G mode), these optical modules offer a simplified high-capacity backhaul and uplink at a lower cost. The NC57-MPA-2D4H-S MPA can co-exist with the other MPAs, including the NC55-MPA-1TH2H-S and NC55-MPA-2TH-S. For more information on these optical modules, see the Cisco 400G Digital Coherent Optics QSFP-DD Optical Modules Data Sheet.

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
Improved ACL-based Traffic Mirroring with Capture Option Support on Cisco NC57 Line Cards	×	✓
SPAN Filtering of Outgoing (Tx) Traffic on Layer 2 Interfaces for Cisco NC57 Line Cards	×	✓
Cisco NC57 Compatibility Mode: Y.1731	✓	×
Configure WRED Counters by Class on Cisco NCS 5700 Series Base (Non-SE) Version Line Cards	×	✓
Increase in QoS Policer Allocation on Cisco NCS 5700 Series Line Cards	✓	✓
Y.1564 Service Activation Test in Native Mode	✓	×
PTP on NC57-MPA-1FH1D-S and NCS-57D2-18DD-SYS	✓	✓
SyncE on NC57-MPA-1FH1D-S and NCS-57D2-18DD-SYS	✓	✓
Smart Licensing on NCS-57D2-18DD-SYS	✓	✓
EEDB Resource Segregation for Encapsulation Types	✓	✓
IMA Enforcement	✓	✓
Secure Boot Status	✓	✓
Secure Boot on NCS-57D2-18DD-SYS	✓	✓
Stream Telemetry Data for ACL	✓	✓
Stream Telemetry Data for BGP FlowSpec Statistics	✓	✓
Configure WRED Counters by Class on Cisco NCS 5700 Series Base (Non-SE) Line Cards	×	✓

For the complete list of features supported on Cisco NC57 line cards until Cisco IOS XR Release 7.8.1, see:

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

- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.5.2
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.5.1
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.4.2
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.4.1
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.3.1
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.2.2
- Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.2.1

Caveats

There are no caveats in this release.

Release Package

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

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

Table 2: Release 7.8.1 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-r781.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-r781.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r781.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.

Cisco IOS XR Security Package	ncs5500-k9sec-3.1.0.0-r781.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-r781.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf-2.0.0.0-r781.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs5500-li-1.0.0.0-r781.x86_64.rpm	Includes LI software images
Multicast Package	ncs5500-mcast-1.0.0.0-r781.rpm	Support Multicast

Table 3: Release 7.8.1 TAR files for Cisco NCS 5500 Series Router

Feature Set	Filename
NCS 5500 IOS XR Software 3DES	NCS5500-iosxr-k9-7.8.1.tar
NCS 5500 IOS XR Software	NCS5500-iosxr-7.8.1.tar
NCS 5500 IOS XR Software	NCS5500-docs-7.8.1.tar

Table 4: Release 7.8.1 Packages for Cisco NCS 5700 Series Router

Feature Set	Filename
NCS 5700 IOS XR Software	ncs5700-x64-7.8.1.iso
NCS 5700 IOS XR Software (only k9 RPMs)	ncs5700-k9sec-rpms.7.8.1.tar
NCS 5700 IOS XR Software Optional Package	NCS5700-optional-rpms.7.8.1.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 7.8.1
Copyright (c) 2013-2022 by Cisco Systems, Inc.
Build Information:
 Built By     : ingunawa
 Built On     : SWed Nov 30 07:45:20 PST 2022
 Built Host   : iox-ucs-053
 Workspace    : /auto/srcarchive16/prod/7.8.1/ncs5500/ws
 Version      : 7.8.1
 Location     : /opt/cisco/XR/packages/
 Label        : 7.8.1
```

```
cisco NCS-5500 () processor
System uptime is 21 hours 58 minutesRP/0/RP0/CPU0:NCS5500#show version
Cisco IOS XR Software, Version 7.8.1
Copyright (c) 2013-2022 by Cisco Systems, Inc.
```

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    Running   Programd
-------------------------------------------------------------------------------------------
0/2        NC57-18DD-SE           1.1   MIFPGA              CURRENT     0.11      0.11
0/2        NC57-18DD-SE           1.1   Bootloader          CURRENT     1.03      1.03
0/2        NC57-18DD-SE           1.1   DBFPGA              CURRENT     0.14      0.14
0/2        NC57-18DD-SE           1.1   IOFPGA              CURRENT     0.22      0.22
0/2        NC57-18DD-SE           1.1   SATA-INTEL_240G     CURRENT   1132.00   1132.00
0/5        NC57-24DD              1.1   MIFPGA              CURRENT     0.11      0.11
0/5        NC57-24DD              1.1   Bootloader          CURRENT     1.03      1.03
0/5        NC57-24DD              1.1   DBFPGA              CURRENT     0.14      0.14
0/5        NC57-24DD              1.1   IOFPGA              CURRENT     0.23      0.23
0/5        NC57-24DD              1.1   SATA-INTEL_240G     CURRENT   1132.00   1132.00
0/RP0      NC55-RP                1.1   Bootloader          CURRENT     9.31      9.31
0/RP0      NC55-RP                1.1   IOFPGA              CURRENT     0.09      0.09
0/RP0      NC55-RP                1.1   SATA-M600-MU        CURRENT     6.00      6.00
0/RP1      NC55-RP                1.0   Bootloader          CURRENT     9.31      9.31
0/RP1      NC55-RP                1.0   IOFPGA              CURRENT     0.09      0.09
0/RP1      NC55-RP                1.0   SATA-M600-MU        CURRENT     6.00      6.00
0/FC0      NC55-5508-FC2          1.0   Bootloader          CURRENT     1.80      1.80
0/FC0      NC55-5508-FC2          1.0   IOFPGA              CURRENT     0.19      0.19
0/FC0      NC55-5508-FC2          1.0   SATA-M5100          CURRENT    75.00     75.00
0/FC1      NC55-5508-FC2          1.0   Bootloader          CURRENT     1.80      1.80
0/FC1      NC55-5508-FC2          1.0   IOFPGA              CURRENT     0.19      0.19
0/FC1      NC55-5508-FC2          1.0   SATA-M5100          CURRENT    75.00     75.00
0/FC2      NC55-5508-FC2          1.0   Bootloader          CURRENT     1.80      1.80
0/FC2      NC55-5508-FC2          1.0   IOFPGA              CURRENT     0.19      0.19
0/FC2      NC55-5508-FC2          1.0   SATA-M5100          CURRENT    75.00     75.00
0/FC3      NC55-5508-FC2          1.0   Bootloader          CURRENT     1.80      1.80
0/FC3      NC55-5508-FC2          1.0   IOFPGA              CURRENT     0.19      0.19
0/FC3      NC55-5508-FC2          1.0   SATA-M5100          CURRENT    75.00     75.00
0/FC5      NC55-5508-FC2          1.0   Bootloader          CURRENT     1.80      1.80
0/FC5      NC55-5508-FC2          1.0   IOFPGA              CURRENT     0.19      0.19
0/FC5      NC55-5508-FC2          1.0   SATA-M5100          CURRENT    75.00     75.00
0/SC0      NC55-SC                1.5   Bootloader          CURRENT     1.74      1.74
0/SC0      NC55-SC                1.5   IOFPGA              CURRENT     0.10      0.10
0/SC1      NC55-SC                1.5   Bootloader          CURRENT     1.74      1.74
0/SC1      NC55-SC                1.5   IOFPGA              CURRENT     0.10      0.10
```

Important Notes

- The total number of bridge-domains (2*BDs) and GRE tunnels put together should not exceed 1518. Here the number 1518 represents the multi-dimensional scale value.
- The offline diagnostics functionality is not supported in NCS 5500 platform. Therefore, the **hw-module service offline location** command will not work. However, you can use the **(sysadmin)# hw-module shutdown location** command to bring down the LC.

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.

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.