Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.5.3

Network Convergence System 5500 Series Routers 2

What's New in Cisco IOS XR Release 7.5.3 2

Caveats 11

Release Package 11

Determine Software Version 12

Determine Firmware Support 12

Important Notes 13

Revised: May 16, 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 7.5.3

Software Features Introduced and Enhanced

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

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

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

Feature	Description
BGP	
Delay BGP Route Advertisements	You can now prevent traffic loss due to premature advertising of BGP routes and subsequent packet loss in a network. You can achieve this by setting the delay time of the BGP start-up in the router until the Routing Information Base (RIB) is synchronized with the Forward Information Base (FIB) in the routing table. This delays the BGP update generation and prevents traffic loss in a network. You can configure a minimum delay of 1 second and a maximum delay of 600 seconds. This feature introduces the **update wait-install delay startup** command.
Interface and Hardware Component	
Decapsulating Multiple Tunneled Packets Using Tunnel Source Direct	With this new **tunnel source direct** option, a single tunnel interface can decapsulate multiple tunnel packets whose outer destination IP is any of the IPv4 or IPv6 address that is locally configured and operationally Up in the switch. Now, you can choose the IP ECMP links when there are multiple IP links between the two switches for decapsulation.

Feature	Description
ERSPAN Traffic to a Destination Tunnel in a Non-Default VRF	In the Cisco IOS XR Release 7.5.3, the tunnels are grouped under the VRFs and you can segregate the traffic towards a specific VRF domain. Encapsulated Remote Switched Port Analyzer (ERSPAN) now transports mirrored traffic through GRE tunnels with multiple VRFs, helping you design your network with multiple Layer 3 partitions. In earlier releases, ERSPAN transported mirrored traffic through GRE tunnels that belonged to only default VRF.
Outer-header hashing support for IPoGREoGUE and MPLSoGREoUDP flows.	This feature specifies the IP hashing profile only on outer IP (L3 and L4) headers for IPoGREoGUE and MPLSoGREoUDP flows.
IP Addresses and Services	
Client ID change in DHCP IPv4 Server Profile	With this release, we've introduced the allow-client-id-change configuration under DHCP IPv4 mode. This option ensures that the client machines have only one binding with DHCP IPv4 server constantly. In scenarios where a client with active binding and valid lease time sends a discover message with a new client id, and the DHCP server approves such requests assuming it as a new client due to different client IDs. This results in multiple bindings for the same client, making the older binding redundant. This feature avoids wastage of DHCP resources due to such multiple bindings.
MPLS	
Self-Ping Probe for Reoptimized LSP	You can now prevent traffic drops on a reoptimized label switch path (LSP) by timely confirmation that it's ready to handle the traffic. This confirmation is made possible by enabling the label edge router (LER) to send self-ping probes over the reoptimized LSP to the ingress LER. As soon the probe reaches the LER, there's confirmation that the RSVP programming is complete along the path. Post this confirmation, the LER switches traffic to the reoptimized LSP with no drop in traffic. This feature introduces the **self-ping** keyword in the **named-tunnels tunnel-te** command.
System Management	
Advanced Secure Hash Algorithm (SHA) for SNMPv3 Authentication	We've added the following SHA algorithms in this release that can be used to authenticate to the SNMPv3 server: • HMAC128SHA224 • HMAC192SHA256 • HMAC256SHA384 • HMAC384SHA512 You can configure the above SHA algorithm for SNMPv3 authentication using the **snmp-server user** command.
System Security	

Feature	Description
Automatic renewal of Public Key Infrastructure (PKI) certificate	You can now enable the router to renew the PKI certificate from the Certificate Authority (CA) by configuring the percentage of the certificate validity, after which the router requests a new certificate from the CA, and the CA authorizes it before certification expiration. This feature eliminates the previously needed manual efforts of certification renewal and avoids interruptions such as MACsec session flaps due to certificate expiry and so on. This feature introduces the following commands: • **auto-enroll** • **renewal-message-type**
OpenSSH Certificate based Authentication for Router	You can now use OpenSSH certificates to authenticate to the remote routers from a client machine. This feature uses the ssh-keygen utility, a standard SSH component to generate and manage authentication keys, available in OpenSSH to create a CA (Certificate Authority) like infrastructure for logging into the router. In this feature, the certificates that are used to authenticate router and client are both signed by the same CA. This automatically establishes trust between router and client, and eliminates the need to establish trust, while using the client for remote logging to router for the first time.

Programmability 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	
Unified Data Model to Configure Encapsulated Ambiguous VLANs	Use the `Cisco-IOS-XR-um-if-encap-ambiguous-cfg.yang` unified data model to configure encapsulated ambiguous VLANs with IEEE802.1ad Provider Bridging (PB) encapsulation type on an access-interface.
Unified Data Model to map script file to the custom OID	Use the `Cisco-IOS-XR-um-script-server-cfg.yang` unified data model to map script file to the custom OID.
Cisco IOS XR unified encap ambiguous cfg yang	Use the unified data model to configure encapsulated ambiguous VLANs with IEEE802.1ad Provider Bridging (PB) encapsulation type on an access-interface.

Feature	Description
openconfig-network-instance.yang Version 0.15.0	The OpenConfig data model is revised from version 0.6.0 to 0.15.0 and supports the following sensor paths to configure and retrieve the Layer 3 forwarding constructs, Layer 2 instances, static routes, forwarding instances, Border Gateway Protocol (BGP) parameters and so on: `openconfig-network-instance/network-instances/network-instance[name]/` • config • state • tables • protocols You can stream Event-driven and Model-driven telemetry data for the operational state of the network instance.
openconfig-system.yang Version 0.7.0	The OpenConfig data model is revised from version 0.6.0 to 0.7.0. This version introduces support to view the statistics of CPU utilization of a component, create a customized banner that is displayed before the username and password login prompts and view the operational state of the system memory using the following sensor paths: `openconfig-system:system/` • cpus • memory/state • config/login-banner Event-driven telemetry is not supported for `openconfig-system:/system/cpus` sensor path. For the other sensor paths, you can stream Event-driven and Model-driven telemetry data for the operational state of the system.

Feature	Description

openconfig-system-terminal.yang Version 0.3.1	The OpenConfig data model is revised from version 0.3.0 to 0.3.1. This version introduces the following config sensor paths to configure the IPv4 or IPv6 telnet server and the number of telnet sessions that are active simultaneously, and state sensor paths to view that the configuration is enabled:
	IPv4:`openconfig-system/system/telnet-server/`
	`oc-term-ext:ipv4/oc-term-ext:vrf[vrf-name]/`
	• oc-term-ext:state/oc-term-ext:enable
	• oc-term-ext:config/oc-term-ext:session-limit
	• oc-term-ext:state/oc-term-ext:session-limit
	IPv6: `openconfig-system/system/telnet-server/`
	`oc-term-ext:ipv6/oc-term-ext:vrf[vrf-name]/`
	• oc-term-ext:state/oc-term-ext:enable
	• oc-term-ext:config/oc-term-ext:session-limit
	• oc-term-ext:state/oc-term-ext:session-limit
	With this release, an extended model `Cisco-IOS-XR-openconfig-system-terminal-ext.yang` is introduced to manage the telnet server configuration.
	You can stream Event-driven and Model-driven telemetry data for the operational state of the system.

openconfig-routing-policy.yang Version 3.2.2	The OpenConfig data model is revised from version 3.1.0 to 3.2.2. You can configure the set-tag operation for local and interior gateway protocol (IGP) tagged routes in a routing policy. This data model is used along with related data models for routing protocols such as border gateway protocol (BGP), interior gateway routing protocol (IGRP) and so on. With this release, the `openconfig-bgp-policy.yang` OpenConfig model is also revised from version 4.0.1 to version 6.0.2. You can configure BGP routes exchanged between two BGP peers using the following sensor paths: `openconfig-routing-policy:routing-policy/` • `policy-definitions/policy-definition` • `defined-sets/tag-sets/tag-set` • `defined-sets/prefix-sets/prefix-set` • `defined-sets/openconfig-bgp-policy:bgpdefined-sets/community-sets/community-set` • `defined-sets/openconfig-bgp-policy:bgpdefined-sets/ext-community-sets/ext-community-set` • `defined-sets/openconfig-bgp-policy:bgpdefined-sets/as-path-sets/as-path-set` You can stream Event-driven and Model-driven telemetry data for the operational state of the routing policy.

Feature	Description
openconfig-local-routing.yang Version 1.2.0	The OpenConfig data model, which is part of the `openconfig-network-instance.yang` data model is revised from version 1.0.1 to 1.2.0. This revision introduces support to configure and retrieve the operational state data for static routes using the following sensor paths: `openconfig-network-instance/network-instances/network-instance[name]/` • `config/enabled` • `protocols/[identifier-name]/static-routes/static/config/description` • `protocols/[identifier-name]/static-routes/static/state/description` You can stream Event-driven and Model-driven telemetry data for the operational state of the static routes.
openconfig-lacp.yang Version 1.2.0	The OpenConfig data model is revised from version 1.1.0 to 1.2.0 and introduces the following sensor paths to monitor the Link Aggregation Control Protocol (LACP) aggregate interface timeouts and the time since the last timeout: `lacp/interfaces/interface[name]/members/member[interface]/state/:` • `last-change` • `counters/lacp-timeout-transitions` You can stream Event-driven telemetry data for the time since the last change of a timeout, and Model-driven telemetry data for the number of times the state has transitioned with a timeout. The state change is monitored since the time the device restarted or the interface was brought up, whichever is most recent.
openconfig-interfaces.yang Version 2.5.0	The OpenConfig data model is revised from version 2.4.3 to 2.5.0. This version introduces support to configure the interface to connect the system to an out-of-band management network and enable the system CPU to handle traffic using the following sensor paths: `openconfig-interfaces/interfaces/interface[name]/state/` • `state/management` • `state/cpu` • `subinterfaces/subinterface[index]/state/management` • `subinterfaces/subinterface[index]/state/cpu` You can stream Event-driven and Model-driven telemetry data for the operational state of the interface.

Feature	Description

openconfig-if-ethernet.yang Version 2.12.1	The OpenConfig data model is revised from version 2.8.1 to 2.12.1 to support the following sensor paths to manage the Forward Error Correction (FEC) configuration and state of Ethernet interfaces:
	Configuration sensor path:
	`openconfig-interfaces:interfaces/interface[name="interface-name"]/`
	`openconfig-if-ethernet:ethernet/config/fec-mode`
	State sensor paths supported on half-duplex interfaces:
	`openconfig-interfaces:interfaces/interface[name="interface-name"]/`
	`openconfig-if-ethernet:ethernet/state/`
	• `in-carrier-errors`
	• `in-interrupted-tx`
	• `in-late-collision`
	• `in-single-collision`
	State sensor paths supported on half-duplex and full-duplex interfaces:
	`openconfig-interfaces:interfaces/interface[name="interface-name"]/`
	`openconfig-if-ethernet:ethernet/state/`
	• `in-mac-errors-rx`
	• `in-symbol-error`
	• `out-mac-errors-tx`
	• `in-maxsize-exceeded`
	You can stream Model-driven telemetry data for the operational state of the Ethernet interfaces.

openconfig-alarms.yang Version 0.3.2	The `openconfig-alarms.yang` OpenConfig data model is part of the `openconfig- system.yang` data model. The model is revised from 0.3.0 to 0.3.2 to enhance the time at which the alarm was raised by the system. This value is expressed relative to the UNIX Epoch time. Using this sensor path, you can stream Event-driven and Model-driven telemetry data.
openconfig-platform-cpu.yang Version 0.1.1	The OpenConfig data model is revised from version 0.1.0 to 0.1.1 and introduces the following sensor paths to view the CPU utilization statistics of the fan components: • `openconfig-platform:components/component/cpu/openconfig-platform-cpu:utilization/state` • `openconfig-platform:components/component[name=<node-name>]/cpu/openconfig-platform-cpu:utilization/state` The *node-name* indicates the location of the RP/CPU node.

Feature	Description
openconfig-bgp.yang Version 6.0.0	The OpenConfig data model is revised from version 3.0.1 to 6.0.0. This version introduces the following changes: • Added new BGP mappings to the data model openconfig-network-instance.yang • Normalized timestamp units to nanoseconds • Removed obsolete model mappings • Managed model mappings with the same semantics but with different names that are absent in the new openconfig-network-instance.yang data model. For example, the name of the leaf under shutdown-threshold-pct container is changed to prefix-limit -pct. warning-threshold • Added new sensor paths for Event-based telemetry
openconfig-rib-bgp.yang Version 0.7.0	The OpenConfig data model is revised from version 0.2.0 to 0.7.0. This version introduces the following changes: • Managed model mappings for BGP Routing Information Base (RIB) in the `openconfig-network-instance.yang` data model • Updated changes related to importing segment-routing module
oc-if-aggregate.yang Version 2.4.3	The OpenConfig data model is revised from version 1.0.2 to 2.4.3. This version does not add or modify leaves. Use this data model to manage the link bundles where one or more ports are aggregated together and treated as a single interface to provide increased bandwidth.
openconfig-bfd.yang Version 0.2.3	The OpenConfig data model is revised from version 0.2.2 to 0.2.3, the current latest version from the OC community. Event-driven telemetry and Model-driven telemetry is not supported for the sensor paths.
openconfig-telemetry.yang Version 0.5.1	The OpenConfig data model is revised from version 0.2.0 to 0.5.1, the latest published version from the OC community. Use this data model to configure telemetry sessions on the router.
openconfig-messages.yang Version 0.0.1	The data model introduces the following sensor path to retrieve the operational state of syslog messages: `openconfig-system:system/messages` The severity of syslog messages varies from the highest severity level 0 (for emergencies) to the lowest severity level 7 (for debugging). Depending upon a specified severity level, the router streams data to the telemetry server, starting from the chosen severity level and higher. This enables you to limit the streamed syslog to the most significant ones. Before you subscribe to the sensor path, you must configure the severity level either through the CLI or YANG: • **CLI**: **`Router(config)#logging yang severity-level`** • **YANG**: `openconfig-system/messages/config/severity` This release does not support the debug-entries container.

Feature	Description
openconfig-lldp.yang Version 0.2.1	You can now override the system default values of some of the mandatory LLDP Type-Length-Values (TLVs) that are advertised by routers to their directly connected neighboring devices. While advertising their identity and capabilities, routers can assign user-defined meaningful names instead of autogenerated values. Using the NETCONF RPC or CLI you can specify these user-defined values. The following leaves support user-defined values for the LLDP TLVs: • `OC-lldp:lldp/config/system-name` • `OC-lldp:lldp/config/system-description` • `OC-lldp:lldp/config/chassis-id-type` • `OC-lldp:lldp/config/chassis-id` The data model also supports the following sensor paths to retrieve the operational state of LLDP packets that are sent and received by a specified interface: • `OC-lldp:lldp/state/counters/last-clear` • `OC-lldp:lldp/state/counters/tlv-accepted` • `OC-lldp:lldp/interfaces/interface/state/counters` • `OC-lldp:lldp/interfaces/interface/neighbors/neighbor/state/age` • `OC-lldp:lldp/interfaces/interface/neighbors/neighbor/state/last-update`
openconfig-isis Version 0.6.0	With the revised version of this model, you can now monitor the system performance by checking the packet counter statistics and bandwidth, time, length, and values (TLVs) of IS-IS database. The revised model updates the leaf nodes in the following paths: • Configuration • Global Mode • System-level • Interface
openconfig-macsec.yang Version 0.2.0	The OpenConfig data model for MACsec now includes viewing error counter for Protocol Data unit (PDU) and Secure Association Key (SAK) in the MKA (MACSecKey Agreement) protocol in the `mka/state/counter` sensor path that was previously deviated. Using this sensor path, you can stream Event-driven and Model-driven telemetry data.

Hardware Introduced

No new hardware introduced in this release.

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

The following table lists the parity 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).

There are no parity features for Cisco NC57 Line Cards and NCS 5700 Fixed Routers in this release.

For the complete list of parity features supported on Cisco NC57 line cards until Cisco IOS XR Release 7.5.3,, see:

- 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 7.4.1
- 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

These caveats are applicable for Cisco IOS XR Software:

Table 1: Cisco NCS 5500 Series Routers Specific Bugs

Bug ID	Headline
CSCwd10994	tty_ltrace_initt FAILED floods on the console
CSCwd13245	show yang operational CLIs may fail by multiple clients simultaneously quering in parallel

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 7.5.3 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-r753.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-r753.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r753.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.
Cisco IOS XR Security Package	ncs5500-k9sec-3.1.0.0-r753.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-r753.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf-2.0.0.0-r753.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs5500-li-1.0.0.0-r753.x86_64.rpm	Includes LI software images
Multicast Package	ncs5500-mcast-1.0.0.0-r753.rpm	Support Multicast

Table 3: Release 7.5.3 TAR files for Cisco NCS 5500 Series Router

Feature Set	Filename
NCS 5500 IOS XR Software 3DES	NCS5500-iosxr-k9-7.5.3.tar
NCS 5500 IOS XR Software	NCS5500-iosxr-7.5.3.tar
NCS 5500 IOS XR Software	NCS5500-docs-7.5.3.tar

Determine Software Version

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

```
RP/0/RP0/CPU0:router# show version
Cisco IOS XR Software, Version 7.5.3
Copyright (c) 2013-2022 by Cisco Systems, Inc.

Build Information:
 Built By     : ingunawa
 Built On     : Tue Sep 27 03:05:21 PDT 2022
 Built Host   : iox-ucs-101
 Workspace    : /auto/srcarchive16/prod/7.5.3/ncs5500/ws
 Version      : 7.5.3
 Location     : /opt/cisco/XR/packages/
 Label        : 7.5.3

cisco NCS-5500 () processor
System uptime is 16 hours 53 minutes
```

Determine Firmware Support

Use the **show hw-module fpd** command in EXEC and Admin mode to view the hardware components with their current FPD version and status. The status of the hardware must be CURRENT; Running and Programed version must be the same.

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

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

```
sysadmin-vm:0_RP0# show hw-module fpd
                                      FPD Versions
                                     ======================
Location  Card type         HWver FPD device       ATR Status      Run     Programd
--------------------------------------------------------------------------------
0/0       NC55-36X100G      1.1   Bootloader           CURRENT     1.22      1.22
0/0       NC55-36X100G      1.1   IOFPGA               CURRENT     0.15      0.15
0/0       NC55-36X100G      1.1   SATA-M600-MCT        CURRENT     5.00      5.00
0/1       NC55-36X100G-S    1.1   Bootloader           CURRENT     1.20      1.20
0/1       NC55-36X100G-S    1.1   IOFPGA               CURRENT     0.11      0.11
0/1       NC55-36X100G-S    1.1   SATA-M600-MCT        CURRENT     5.00      5.00
0/2       NC55-36X100G-S    1.1   Bootloader           CURRENT     1.20      1.20
0/2       NC55-36X100G-S    1.1   IOFPGA               CURRENT     0.11      0.11
0/2       NC55-36X100G-S    1.1   SATA-M600-MCT        CURRENT     5.00      5.00
0/3       NC55-36X100G-S    1.2   Bootloader           CURRENT     1.20      1.20
0/3       NC55-36X100G-S    1.2   IOFPGA               CURRENT     0.11      0.11
0/3       NC55-36X100G-S    1.2   SATA-M600-MCT        CURRENT     5.00      5.00
0/4       NC55-36X100G-S    1.2   Bootloader           CURRENT     1.20      1.20
0/4       NC55-36X100G-S    1.2   IOFPGA               CURRENT     0.11      0.11
0/4       NC55-36X100G-S    1.2   SATA-M600-MCT        CURRENT     5.00      5.00
0/6       NC55-24H12F-SE    1.0   Bootloader           CURRENT     1.20      1.20
0/6       NC55-24H12F-SE    1.0   IOFPGA               CURRENT     0.09      0.09
0/6       NC55-24H12F-SE    1.0   SATA-M600-MCT        CURRENT     5.00      5.00
0/7       NC55-36X100G-S    1.2   Bootloader           CURRENT     1.20      1.20
0/7       NC55-36X100G-S    1.2   IOFPGA               CURRENT     0.11      0.11
0/7       NC55-36X100G-S    1.2   SATA-M600-MCT        CURRENT     5.00      5.00
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/RP1     NC55-RP           1.1   Bootloader           CURRENT     9.31      9.31
0/RP1     NC55-RP           1.1   IOFPGA               CURRENT     0.09      0.09
0/RP1     NC55-RP           1.1   SATA-M600-MU         CURRENT     6.00      6.00
0/FC0     NC55-5508-FC      1.0   Bootloader           CURRENT     1.74      1.74
0/FC0     NC55-5508-FC      1.0   IOFPGA               CURRENT     0.16      0.16
0/FC1     NC55-5508-FC      0.304 Bootloader           CURRENT     1.74      1.74
0/FC1     NC55-5508-FC      0.304 IOFPGA               CURRENT     0.16      0.16
0/FC3     NC55-5508-FC      1.0   Bootloader           CURRENT     1.74      1.74
0/FC3     NC55-5508-FC      1.0   IOFPGA               CURRENT     0.16      0.16
0/FC4     NC55-5508-FC      1.0   Bootloader           CURRENT     1.74      1.74
0/FC4     NC55-5508-FC      1.0   IOFPGA               CURRENT     0.16      0.16
0/FC5     NC55-5508-FC      1.0   Bootloader           CURRENT     1.74      1.74
0/FC5     NC55-5508-FC      1.0   IOFPGA               CURRENT     0.16      0.16
0/SC0     NC55-SC           1.4   Bootloader           CURRENT     1.74      1.74
0/SC0     NC55-SC           1.4   IOFPGA               CURRENT     0.10      0.10
0/SC1     NC55-SC           1.4   Bootloader           CURRENT     1.74      1.74
0/SC1     NC55-SC           1.4   IOFPGA               CURRENT     0.10      0.10
```

Important Notes

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

Supported Transceiver Modules

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

Supported Modular Port Adapters

For the compatibility details of Modular Port Adapters (MPAs) on the line cards, see the datasheet of that specific line card.

Upgrading Cisco IOS XR Software

Cisco IOS XR Software is installed and activated from modular packages, allowing specific features or software patches to be installed, upgraded, or downgraded without affecting unrelated processes. Software packages can be upgraded or downgraded on all supported card types, or on a single card (node).

Before starting the software upgrade, use the **show install health** command in the admin mode. This command validates if the statuses of all relevant parameters of the system are ready for the software upgrade without interrupting the system.

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.

Use user-class Option 'xr-config' Instead Of 'exr-config' To Provision ZTP

In Cisco IOS XR Release 7.3.1 and earlier, the system accepts the device sending **user-class = "exr-config"**; however starting Cisco IOS XR Release 7.3.2 and later, you must use only **user-class = "xr-config"**.

In Cisco IOS XR Release 7.3.2 and later, use:

```
host cisco-rp0 {
   hardware ethernet e4:c7:22:be:10:ba;
   fixed-address 172.30.12.54;
   if exists user-class and option user-class = "iPXE" {
      filename = "http://172.30.0.22/boot.ipxe";
   } elsif exists user-class and option user-class = "xr-config" {
      filename = "http://172.30.0.22/scripts/cisco-rp0_ztp.sh";
```

```
    }
}
```

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.