Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.1.1

Network Convergence System 5500 Series Routers 2

What's New in Cisco IOS XR Release 7.1.1 2

Caveats 9

Supported Packages and System Requirements 10

Other Important Information 12

Full Cisco Trademarks with Software License 14

Revised: June 13, 2023

Network Convergence System 5500 Series Routers

Note *This software release has reached end-of-life status. For more information, see the* End-of-Life and End-of-Sale Notices.

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 7.1.1

Cisco is continuously enhancing the product with every release and this section covers a brief description of key features and enhancements. It also includes links to detailed documentation, where available.

Software

Ping and Traceroute for Segment Routing Flexible Algorithm

Flexible Algorithm validation method is based on segment identifier (SID) label and label assigner, instead of being based on IP address. The assigner is validated against the topology prefix information provided by the SR-PCE database. If the assigner is valid, then the label given is also validated against the SR-PCE database. On the egress side, the destination label is contained in a new SR Label sub-TLV. This label is verified against a SID list provided by the SR-PCE.

See Segment Routing Ping and Traceroute for Flexible Algorithm .

Segment Routing Flexible Algorithm Affinity Constraints for IS-IS

This feature introduces support for “include-all” and “include-any” affinity constraints for configuring Segment Routing Flexible Algorithm for IS-IS.

See the Configuring Flexible Algorithm .

Segment Routing Conditional Prefix Advertisement for IS-IS

Anycast routing enables the steering of traffic toward multiple advertising nodes, providing load-balancing and redundancy. Packets addressed to an Anycast address are forwarded to the topologically nearest nodes. If an advertising node becomes unavailable or unreachable while still advertising its Anycast SID, traffic could still be routed to the node and, as a result, get dropped.

The Segment Routing Conditional Prefix Advertisement for IS-IS feature allows a node to advertise its loopback address when it's connected to the domain, and to track the loopback addresses of the other nodes in the domain. If a node becomes unavailable or unreachable, it will stop advertising its loopback address, allowing for a new path to be computed.

See the Conditional Prefix Advertisement .

Segment Routing Label Edge Router ECMP-FEC Optimization

ECMP-FECs are used for any ECMP programming on the system, such as unlabeled ECMP, MPLS LSP ECMP, VPN multipath, and EVPN multi-homing.

The Segment Routing Label Edge Router (LER) ECMP-FEC Optimization feature allows ECMP-FEC optimization originally developed for Label Switched Router (LSR) nodes (MPLS P) to be enabled on LER (Layer 3 MPLS PE) routers.

The SR ECMP-FEC optimization solution minimizes ECMP-FEC resource consumption during underlay programming for an SR-MPLS network. This feature supports sharing the same ECMP-FEC, regular FEC, and Egress Encapsulation DB (EEDB) entries for all /32 IPv4 Segment Routing prefixes with the same set of next hops.

See Segment Routing ECMP-FEC Optimization.

CFM Adaptive Bandwidth Notifications

Modern microwave devices support adaptive modulation schemes to prevent a complete loss of signal. Adaptive modulation schemes allow the devices to continue to operate during periods of degradation, but at a reduced bandwidth. However, to fully take advantage of this, it's necessary to convey the decrease in bandwidth to the head-end router so that appropriate actions can be taken. Otherwise, the link may become saturated and traffic dropped arbitrarily.

A generic solution to this is a Connectivity Fault Management (CFM) extension to send Bandwidth Notifications Messages (BNM) to Maintenance Endpoints (MEPs) on the corresponding interface on the head-end router. To be flexible in the actions taken, the choice of solution uses Embedded Event Manager (EEM) to invoke operator written TCL scripts

See CFM Adaptive Bandwidth Notifications

BFD-triggered Fast-Reroute

BFD-triggered Fast Reroute feature allows you to obtain link and node protection by using the Bidirectional Forwarding Detection (BFD) protocol to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators.

See BFD-Triggered FRR.

Per-VLAN Rapid Spanning Tree

The Per-VLAN Rapid Spanning Tree (PVRST) is the IEEE 802.1w (RSTP) standard implemented per VLAN. PVRST uses point-to-point wiring to provide rapid convergence of the spanning tree. The spanning tree reconfiguration occurs in less than one second with PVRST.

See Per-VLAN Rapid Spanning Tree.

Multiple Spanning Tree Protocol

The Multiple Spanning Tree Protocol (MSTP) is a Spanning tree protocols (STP) variant that allows you to create multiple and independent spanning trees over the same physical network. You can configure the parameters for each spanning tree separately. You can select different network devices as the root bridge or different paths to form the loop-free topology. Therefore, you can block a given physical interface for some of the spanning trees and unblocked for others.

See Multiple Spanning Tree Protocol and Multiple Spanning Tree Protocol Commands

Highest Random Weight Mode for EVPN DF Election

The Highest Random Weight (HRW) Mode for EVPN DF Election feature provides optimal load distribution of Designated Forwarder (DF) election, redundancy, and fast access. It ensures a nondisruptive service for an Ethernet Segment (ES) irrespective of the state of a peer DF.

See Highest Random Weight Mode for EVPN DF Election.

EVPN Single-Active Multihoming for Anycast Gateway IRB

The EVPN Single-Active Multihoming for Anycast Gateway IRB feature supports single-active redundancy mode. In this mode, the provider edge (PE) nodes locally connected to an Ethernet Segment load balance traffic to and from the Ethernet Segment based on EVPN service instance (EVI). Within an EVPN service instance, only one PE forwards traffic to and from the Ethernet Segment (ES). This feature supports intersubnet scenario only.

See EVPN Single-Active Multihoming for Anycast Gateway IRB

Ingress Short-Pipe Mode to Set DSCP

With this feature, in addition to setting ingress action such as traffic class and QoS group, you can also mark DSCP in the packet header at ingress.

See Ingress Short-Pipe.

Rewrite of Priority Tag

The Rewrite of Priority Tag feature allows you to configure rewrite tag for a priority-tagged VLAN. This feature removes the priority-tagged VLAN in the ingress direction and adds the priority-tagged VLAN in the egress direction.

See Rewrite of Priority Tag.

Support for HSRP v4/v6

Hot Standby Router Protocol (HSRP) is supported. The HSRP is an IP routing redundancy protocol designed to allow for transparent failover at the first-hop IP router. HSRP provides high network availability, because it routes IP traffic from hosts on networks without relying on the availability of any single router. HSRP is used in a group of routers for selecting an active router and a standby router. An active router is the router of choice for routing packets whereas a standby router is a router that takes over the routing duties when an active router fails, or when pre-set routing conditions are met.

See Implementing HSRP .

See HSRP Commands.

EVPN Bridging and VPWS Services over BGP-LU Underlay

The EVPN Bridging and VPWS Services over BGP-LU Underlay feature allows you to configure end-to-end EVPN services between data centers (DCs). This feature allows you to perform ECMP at three-levels: transport, BGP- LU, and service.

This feature supports the following services:

- IRB VRF over BGP-LU over IGP (SR or non-SR (LDP, IGP))
- EVPN Aliasing over BGP-LU over IGP (SR or non-SR (LDP, IGP))
- VPWS over BGP-LU over IGP

See EVPN Bridging and VPWS Services over BGP-LU Underlay .

BFD on Bridge Group Virtual Interface

BFD on Bridge Group Virtual Interface (BVI) feature, with the IRB functionality, provides the ability to route between a bridged domain and a routed domain.

Using the Integrated Routing Bridging (IRB) functionality, you can configure a router for routing and bridging the same network layer protocol, on the same interface. This functionality allows the VLAN header to be maintained on a frame while it transits a router from one interface to another. The BVI is a virtual interface within the router that acts like a normal routed interface that does not support bridging but represents the comparable bridge group to routed interfaces within the router.

See BFD over BVI.

Multisegment Pseudowire

The Multisegment Pseudowire feature allows you to extend L2VPN pseudowires across an inter-AS boundary or across two separate MPLS networks. A multisegment pseudowire connects two or more contiguous pseudowire segments to form an end-to-end multi-hop pseudowire as a single point-to-point pseudowire. These segments act as a single pseudowire, allowing you to:

- Manage the end-to-end service by separating administrative or provisioning domains.
- Keep IP addresses of provider edge (PE) nodes private across interautonomous system (inter-AS) boundaries. Use IP address of autonomous system boundary routers (ASBRs) and treat them as pseudowire aggregation routers. The ASBRs join the pseudowires of the two domains.

See Multisegment Pseudowire.

FIB Per-Prefix Out of Resource Handling Improvement

Forwarding Information Base (FIB) Per-Prefix Out of Resource (OOR) Handling Improvement feature enables you to create a graceful out of resource handling for Forwarding Equivalence Class (FEC) resources.

See FIB Per-Prefix Out of Resource Handling Improvement.

Ingress Classification and Ingress and Egress Marking on L3 Subinterfaces

Beginning this release, you can:

- classify packets at the ingress on L3 subinterfaces for (CoS, DEI) for IPv4, IPv6, and MPLS flows.
- perform Layer 2 marking of Ethernet packets for (CoS, DEI) for IPv4, IPv6, and MPLS flows in the egress direction on L3 subinterfaces.

See Packet Classification Overview and QoS L2 Re-Marking of Ethernet Packets on L3 Flows in Egress Direction on L3 sub-interfaces.

The command, hw-module profile qos ipv6 short-l2qos-enable is introduced.

IPv4 BFD Multihop over MPLS Core and Segment Routing

IPv4 BFD Multihop feature is supported in MPLS LDP and Segment Routing.

See IPv4 Multihop BFD.

Set discard-class to Drop Packets at Ingress

On ingress direction, after matching the traffic based on either the IP Precedence or DSCP value, you can set it to a particular discard-class. At the egress, a congestion avoidance technique such as weighted random early detection (WRED) then uses the assigned discard-class value to determine the probability that a packet is dropped. With the introduction of this feature, if you now set a discard-class of 3, the packet is dropped at ingress itself.

See Packet Marking.

The command, set discard-class is modified.

VPLS VFI with BVI as Routed Interface

The VPLS VFI with BVI as Routed Interface feature allows you to route the VPLS PW traffic dynamically over BVI interface.

Integrated routing and bridging (IRB) enables you to route the packets received from a host on a bridge group and a routed interface using a Bridge-Group Virtual Interface (BVI). The BVI is a virtual interface configured on the router which acts as a gateway routed interface towards the core network.

See VPLS VFI with BVI as Routed Interface.

Interior Gateway Protocol (IGP) Destination-based Load Balancing (DLB)

Currently, the router supports upto 2K labelled prefixes with Equal Cost Multi Path (ECMP). From this release onwards, with the introduction of the Interior Gateway Protocol (IGP) Destination-based Load Balancing (DLB) feature, the router can support higher scale of labelled prefixes.

See Interior Gateway Protocol (IGP) Destination-based Load Balancing (DLB).

CEF Enhancement

This feature enables you to provide the names of the database, for example LPM, EXT-TCAM, and LEM, in which any prefix of any packet is updated. With this feature, you can efficiently manage your network resources because it allows you to understand the scaling of prefixes. This feature also helps you to understand why a particular IP address configuration for a device fails and thereby helps you in debugging.

See Implementing Cisco Express Forwarding.

See Cisco Express Forwarding Commands .

Flooding Disable

The Flooding Disable feature prevents forwarding of Broadcast, Unknown-unicast and Multicast (BUM) traffic on the bridge domain. You can disable flooding of BUM traffic at the bridge level or at the interface level. By disabling flooding at the bridge level, you can prevent forwarding of BUM traffic on attachment circuit (AC) and pseudowire (PW).

You can also disable only unknown unicast traffic at the bridge level or at the interface level. By disabling flooding of unknown unicast traffic at the bridge level, you can prevent forwarding of unknown unicast traffic on attachment circuit (AC) and pseudowire (PW).

By disabling flooding of unknown unicast traffic at the interface level, you can prevent forwarding of unknown unicast traffic on AC alone.

See Flooding Disable.

Notification Alerts for TLS Certificate Expiry

Support for a notification mechanism using SNMP trap and syslog messages when a TLS certificate is approaching its expiry.

The notifications are sent at the following intervals:

- First notification—This notification is sent 60 days before the expiry of the certificate.
- Repeated notifications—After the first notification, subsequent notifications are sent every week until a week before the expiry of the certificate. In the last week, notifications are sent every day until the certificate expiry date.

See Expiry Notification for PKI Certificate .

Congestion Management for Telemetry Data

A congestion management system for telemetry data allows each destination a maximum of 4000 outstanding messages. The events are throttled when the outstanding messages exceed 3000; throttling of cadence messages happen when outstanding messages exceed 250. Events have higher priority than cadence messages.

See Congestion Management for Telemetry Data.

Revised OpenConfig Data Models for Network Programmability

The OpenConfig (OC) data models are defined by the OC community to create configuration and retreive operational state data of the network. The following data models are revised to provide additional capabilities:

- The OC Integrated Intermediate System-to-Intermediate System data model, `oc-isis`, is enahnced to provide support for additional paths in the data model.
- The `oc-policy` data model contains general data definitions for use in routing policy. It can be imported by modules that contain protocol-specific policy conditions and actions.
- Enhancement of gNMI specification to include updates from version 0.4.0 to version 0.6.0. Support is extended for the following gNMI features:
    - gNMI support for multiple client roles and primary arbitration
    - Path Target
    - gNMI service registration with the gRPC reflection service to allow clients to determine that gNMI is available on the target

See Revised OpenConfig Data Models for Network Programmability

gNOI Enhancements

gRPC Network Operations Interface (gNOI) defines a set of gRPC-based microservices for executing operational commands on network devices.

gNOI supports for the following remote procedure calls (RPCs):

- System
    - Ping
    - Traceroute
    - Time
    - SwitchControlProcessor
- File
    - Stat
    - Put
    - TransferToRemote
- Cert

- Rotate
- Install
- GetCertificates
- RevokeCertificates
- CanGenerateCSR

See gRPC Network Operations Interface

ITU-T Y.1564

Y.1564 or Ethernet Service Activation (or performance test methodology) is a testing procedure which tests service turn-up, installation and troubleshooting of Ethernet-based services.

Y.1564 allows simultaneous testing of multiple Ethernet services and measures. It validates the different service level agreements (SLAs) to ensure the service meets guaranteed performance settings in a controlled test time. It helps to ensure all the services carried by the network meet the SLA objectives at the maximum committed rate proving that under maximum load, the network devices and paths can support the traffic as designed, even under stress.

See Y.1564 - Ethernet Service Activation Test .

Retrieve Process Data at Thread Level

Support to retrieve information at thread level to identify heavy processes on the system that can be optimized through network design. A thread is a sequence of instructions to be executed within a program.

- Enhanced `Cisco-IOS-XR-wdsysmon-fd-oper.yang` data model to include CPU utilization at thread level for each running process
- Support `Cisco-IOS-XR-procthreadname-oper.yang` data model to query thread-level details such as thread name, priority, state, stack size of a running processes

See Retrieve Process Data at Thread Level.

Native Data Model for MLDP

The native Multicast Label Distribution Protocol (mldp) model defines configuration and operational state data for the MLDP protocol.

See Native Data Model for MLDP.

OpenConfig Data Models for Network Programmability

The OpenConfig (OC) data models are defined by the OC community to create configuration and retreive operational state data of the network. This release introduces support for the following OC models:

- The OC Bidirectional Forwarding Detection data model, `oc-bfd`, defines the BFD protocol in multi-vendor environment to configure and get operational state data for the BFD protocol.
- The `oc-platform` data model supports streaming operational and configuration state data that are related to the underlying characteristics of the device.

See OpenConfig Data Models for Network Programmability *Programmability Configuration Guide for Cisco NCS 5500 Series Routers*.

Behavior Change Introduced in this release

Deprecated Commands

From this release onwards the **lacp period short receive** and **lacp period short transmit** commands are deprecated.

You can now configure LACP receive and transmit time in a single CLI. Use the **lacp period <*time in milliseconds*>** command in the interface config mode.

You must first enable Cisco extension feature before configuring **lacp period** command. Use the **lacp cisco enable** command in the bundle interface mode. In the absense of Cisco extension feature, even if you have configured a **lacp period** the members transmits at a standard time of 1 second.

See lacp period short command.

H-QoS with G8032

You can configure HQoS on an AC interface that is part of the G.8032 ring. However, this functionality has a limitation on the G.8032 convergence. The convergence depends on the number of AC interfaces used in a G.8032 ring. This limitation is applicable when the HQOS mode is enabled at the system level or at the G.8032 AC level.

See G.8032 Ethernet Ring Protection.

Sub-Interface as EVPN Core Interface

From this release onwards, the EVPN core interface can be a sub-interface.

See EVPN Overview.

Hardware

No new hardware features are introduced in this release.

Hardware Enhancements

This release introduces following hardware enhancements:

- QSFP-40/100G-SRBD—Cisco 100G and 40G SR-BiDi QSFP Transceiver optic (QSFP-40/100G-SRBD) is a dual-mode optic. By default, the optic works in 100G mode. QSFP-40/100G-SRBD optical transceiver is supported on Cisco NCS 5500 series fixed port and modular port routers.

Caveats

Caveats describe unexpected behavior in Cisco IOS XR Software releases. Severity-1 caveats are the most critical caveats; severity-2 caveats are less critical.

Caveats Specific to the NCS 5500 Series Routers

Caveats describe unexpected behavior in Cisco IOS XR Software releases. These caveats are speicifc to NCS 5500 Series Routers:

Bug ID	Headline
CSCvs21179	25G interface taking longer time to come up after unshut and Multiple RX_FAULT logs are seen

Supported Packages and System Requirements

For a complete list of supported optics, hardware and ordering information, see the *Cisco NCS 5500 Series Data Sheet*

To install the Cisco NCS 5500 router, see *Hardware Installation Guide for Cisco NCS 5500 Series Routers*.

Release 7.1.1 Packages

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

Table 1: Release 7.1.1 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-r711.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-r711.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r711.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.
Cisco IOS XR Security Package	ncs5500-k9sec-3.1.0.0-r711.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-r711.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf-2.0.0.0-r711.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs5500-li-1.0.0.0-r711.x86_64.rpm	Includes LI software images
Multicast Package	ncs5500-mcast-1.0.0.0-r711.rpm	Support Multicast

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 7.1.1
Copyright (c) 2013-2020 by Cisco Systems, Inc.

Build Information:
Built By     : <username>
Built On     : Mon Jan 27 01:36:26 PST 2020
Built Host   : iox-lnx-076
Workspace    : /auto/srcarchive15/prod/7.1.1/ncs5500/ws
Version      : 7.1.1
Location     : /opt/cisco/XR/packages/
Label        : 7.1.1

cisco NCS-5500 () processor
System uptime is 1 day 1 hour 21 minutes
```

Determine Firmware Support

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

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

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

```
RP/0/RP0/CPU0:router# show hw-module fpd
                                                                      FPD Versions
                                                                     ===============
Location  Card type         HWver FPD device       ATR Status    Run     Programd
-------------------------------------------------------------------------------
0/0       NC55-36X100G-A-SE 1.0   Bootloader           CURRENT    0.14    0.14
0/0       NC55-36X100G-A-SE 1.0   DBFPGA               CURRENT    0.14    0.14
0/0       NC55-36X100G-A-SE 1.0   IOFPGA               CURRENT    0.26    0.26
0/0       NC55-36X100G-A-SE 1.0   SATA                 CURRENT    5.00    5.00
0/1       NC55-36X100G      1.0   Bootloader           CURRENT    1.19    1.19
0/1       NC55-36X100G      1.0   IOFPGA               CURRENT    0.15    0.15
0/2       NC55-36X100G-S    0.4   Bootloader           CURRENT    1.14    1.14
0/2       NC55-36X100G-S    0.4   IOFPGA               CURRENT    0.11    0.11
0/2       NC55-36X100G-S    0.4   SATA                 CURRENT    5.00    5.00
0/5       NC55-36X100G      1.1   Bootloader           CURRENT    1.19    1.19
0/5       NC55-36X100G      1.1   IOFPGA               CURRENT    0.15    0.15
0/5       NC55-36X100G      1.1   SATA                 CURRENT    5.00    5.00
0/6       NC55-6X200-DWDM-S 0.6   Bootloader           CURRENT    1.14    1.14
0/6       NC55-6X200-DWDM-S 0.6   IOFPGA               CURRENT    0.14    0.14
0/6       NC55-6X200-DWDM-S 0.6   SATA                 CURRENT    5.00    5.00
0/RP0     NC55-RP-E         0.4   Bootloader           CURRENT    1.21    1.21
0/RP0     NC55-RP-E         0.4   IOFPGA               CURRENT    0.23    0.23
0/RP0     NC55-RP-E         0.4   OMGFPGA              CURRENT    0.48    0.48
0/RP1     NC55-RP-E         0.4   Bootloader           CURRENT    1.21    1.21
0/RP1     NC55-RP-E         0.4   IOFPGA               CURRENT    0.23    0.23
0/RP1     NC55-RP-E         0.4   OMGFPGA              CURRENT    0.48    0.48
0/FC0     NC55-5508-FC      1.1   Bootloader           CURRENT    1.74    1.74
0/FC0     NC55-5508-FC      1.1   IOFPGA               CURRENT    0.16    0.16
0/FC2     NC55-5508-FC      0.205 Bootloader           CURRENT    1.74    1.74
0/FC2     NC55-5508-FC      0.205 IOFPGA               CURRENT    0.16    0.16
0/FC4     NC55-5508-FC      1.1   Bootloader           CURRENT    1.74    1.74
```

```
0/FC4     NC55-5508-FC      1.1   IOFPGA              CURRENT    0.16    0.16
0/FC5     NC55-5508-FC      0.106 Bootloader          CURRENT    1.74    1.74
0/FC5     NC55-5508-FC      0.106 IOFPGA              CURRENT    0.16    0.16
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           1.4   Bootloader          CURRENT    1.74    1.74
0/SC1     NC55-SC           1.4   IOFPGA              CURRENT    0.10    0.10
```

Note The FPD versions on board shipped by manufacturer may have higher versions than the FPD package integrated in the IOS XR.

Other Important Information

- 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.

- The warning message that the smart licensing evaluation period has expired is displayed in the console every hour. There is, however, no functionality impact on the device. The issue is seen on routers that do not have the Flexible Consumption licensing model enabled. To stop the repetitive messaging, register the device with the smart licensing server and enable the Flexible Consumption model. Later load a new registration token.

  To register the device with the smart licensing server, follow the instructions provided in this link: Register and Activate Your Device.

- **NCS55A1-36H-SE-S** – Under Secure Domain Router (SDR) configuration, when you change the size of the RP VM memory from 12 GB (default) to 14 GB and commit your changes, the system reloads. When the system is brought back up, it can crash with a core dump by LC XR VM.

  ```
  0/RP0/ADMIN0:Oct 15 12:19:30.280 : dumper[3046]: %INFRA-CALVADOS_DUMPER-6-HOST_COPY_SUCCESS : Copied host
   file /misc/scratch/core/default-sdr--2.20201015-191552.core.0_RP0.lxcdump.tar.lz4 to 0/RP0:/misc/disk1
  0/RP0/ADMIN0:Oct 15 12:19:30.389 : dumper[3046]: %INFRA-CALVADOS_DUMPER-6-HOST_REMV_SUCCESS : Deleted HostOS
   file /misc/scratch/core/default-sdr--2.20201015-191552.core.0_RP0.lxcdump.tar.lz4
  ```

  This is a one-time reload. Other than the additional time required for the LC XR VM to reload, there is no impact to system functionality.

  After the configuration is applied, we recommend that you reload the chassis when prompted to ensure all VMs and host OS are in sync.

- LFA FRR feature is not supported.

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.

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

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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.