Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 7.2.1

Revised: January 11, 2024

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 7.2.1

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

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.

Segment Routing Path Computation Element Support for RSVP-TE Tunnels

The Path Computation Element (PCE) Support for MPLS Traffic Engineering Label Switched Paths (MPLS-TE LSPs) feature allows Cisco's SR-PCE to act as a PCE for MPLS-TE LSPs.

For more information, see PCE Support for MPLS-TE LSPs.

Segment Routing TI-LFA Support for GRE Tunnels

The Segment Routing TI-LFA (Topology independent Loop-free alternate) Support for GRE Tunnels feature extends the TI-LFA logic to span different instances or different IGP domains by using a Generic Routing Encapsulation (GRE) tunnel that runs between two ABRs as a backup path for TI-LFA protection in an SR Core. GRE is a tunneling protocol that provides a simple generic approach to transport packets of one protocol over another protocol by means of encapsulation.

For more information, see SR-MPLS over GRE as TI-LFA Backup Path.

Segment Routing Tree SID Bud Node Support

With multicast distribution trees, a Bud node is a node that acts as a Leaf (egress) node as well as a midpoint (transit) node toward the downstream subtree.

In this release, the tree computation algorithm on the SR-PCE has been enhanced to detect a Bud node based on knowledge of the Leaf set and to handle Leaf/Transit node transitions to the Bud node.

For information, see Bud Node Support.

Segment Routing Tree SID Delay Optimization Objective

This release introduces delay metric as an optimization objective on the SR-PCE in its Tree-SID path computation to minimize a link delay.

For information, see Segment Routing Tree Segment Identifier.

SRv6 IS-IS Flexible Algorithm Summarization

This feature introduces support for SRv6 IS-IS Flexible Algorithm Summarization. SRv6 leverages longest-prefix-match IP forwarding. Massive-scale reachability can be achieved by summarizing locators at ABRs and ASBRs. This feature allows summarizing SRv6 Flexible Algorithm locators at the IS-IS level boundary by the level-1-2 routers.

For more information, see Configuring SRv6 IS-IS Flexible Algorithm.

TCP Authentication Option for Segment Routing Path Computation Element

TCP Message Digest 5 (MD5) authentication is used for authenticating PCEP (TCP) sessions by using clear text or encrypted password. This feature introduces TCP Authentication Option (TCP-AO), which replaces the TCP MD5 option. TCP-AO is compatible with Master Key Tuple (MKT) configuration. TCP-AO also protects connections when using the same MKT across repeated instances of a connection. TCP-AO protects the connections by using traffic key that are derived from the MKT, and then coordinates changes between the endpoints.

For more information, see TCP Authentication Option.

SRv6 IS-IS Microloop Avoidance with Flexible Algorithm

This feature introduces support SRv6 IS-IS Microloop Avoidance with Flexible Algorithm.

Microloop Avoidance paths for a Flexible Algorithm are computed using the same constraints as the calculation of the primary paths for such Flexible Algorithm. These paths use Prefix-SIDs advertised specifically for such Flexible Algorithm in order to enforce a microloop avoidance path.

For more information, see Configuring SRv6 IS-IS Microloop Avoidance.

SR-TE IS-IS Delay Normalization

Performance measurement (PM) measures various link characteristics like packet loss and delay. IS-IS can use such characteristics as a metric for Flexible Algorithm computation. Delay is measured in microseconds. If delay values are taken as measured and used as link metrics during the IS-IS topology computation, some valid ECMP paths might be unused because of the negligible difference in the link delay.

The SR-TE IS-IS Delay Normalization feature takes the delay values of different low-latency links and computes a normalized delay value. The normalized value is advertised and used as a metric during the Flexible Algorithm computation.

For more information, see Delay Normalization.

Manual BGP Peering SIDs for Segment Routing Egress Peer Engineering

This release introduces support for manually configured BGP Egress Peer Engineering (EPE) Peer SIDs. The ability to manually configure BGP-EPE peer SIDs allows for persistent EPE label values. Manual BGP-EPE SIDs are advertised through BGP-LS and are allocated from the Segment Routing Local Block (SRLB).

For more information, see Configuring Manual BGP-EPE Peering SIDs.

DHCPv4 Relay Agent and Proxy Support on SRv6-VPN PE

Currently, DHCPv4 clients do not get an IP address when there is pure IPv6 configured on the core-facing interfaces and a session is established over Segment Routing over IPv6 (SRv6). For IPv6-only environments, DHCPv4 relay agent and proxy are now supported to handle and process new clients and sessions on SRv6 IPv4 L3VPN scenarios.

For more information, see DHCPv4 Relay Agent and Proxy Support for SRv6 IPv4 L3VPN.

Segment Routing On-Demand Next Hop for EVPN

Segment Routing On-Demand Next Hop (SR-ODN) allows a service head-end router to automatically instantiate an SR policy to a BGP next-hop when required (on-demand). SR-ODN provides per-destination steering behaviors where a prefix, a set of prefixes, or all prefixes from a service can be associated with a desired underlay SLA. The functionality applies equally to single-domain and multidomain networks.

An on-demand SR policy is created dynamically for BGP global or VPN (service) routes. This release introduces SR-ODN support for EVPN services with either single-homing or multi-homing configurations.

For more information, see On-Demand SR Policy – SR On-Demand Next-Hop.

Segment Routing On-Demand Next Hop for EVPN-VPWS with Multi-Homing

Segment Routing On-Demand Next Hop (SR-ODN) allows a service head-end router to automatically instantiate an SR policy to a BGP next-hop when required (on-demand). SR-ODN provides per-destination steering behaviors where a prefix, a set of prefixes, or all prefixes from a service can be associated with a desired underlay SLA. The functionality applies equally to single-domain and multi-domain networks.

An on-demand SR policy is created dynamically for BGP global or VPN (service) routes. This release introduces SR-ODN support for EVPN-VPWS services with multi-homing configurations.

For more information, see On-Demand SR Policy – SR On-Demand Next-Hop.

Per-Flow Automated Steering

Currently, the steering of traffic through a Segment Routing (SR) policy is based on the candidate paths of that policy. For a given policy, a candidate path specifies the path to be used to steer traffic to the policy's destination. The policy determines which candidate path to use based on the candidate path's preference and state. The candidate path that is valid and has the highest preference is used to steer all traffic using the given policy. This type of policy is called a Per-Destination Policy (PDP).

Per-Flow Automated Traffic Steering introduces a way to steer traffic on an SR policy based on the attributes of the incoming packets, called a Per-Flow Policy (PFP). A PFP provides up to 8 "ways" or options to the endpoint. With a PFP, packets are classified by a classification policy and marked using internal tags called forward classes (FCs). The FC setting of the packet selects the "way". For example, this "way" can be a traffic-engineered SR path, using a low-delay path to the endpoint. The FC is represented as a numeral with a value of 0 to 7.

For more information, see Per-Flow Automated Steering.

Segment Routing BGP Peer-Set SID

Segment routing egress peer engineering (EPE) uses a controller to instruct an ingress provider edge, or a content source (node) within the segment routing domain, to use a specific egress provider edge (node) and a specific external interface to reach a destination. BGP peer SIDs are used to express source-routed interdomain paths. BGP peer SID types include Peer Node SIDs and Peer Adjacency SIDs.

This release adds support for a new type of BGP peering SID, called BGP Peer Set SID. A BGP Peer Set SID is a group or set of BGP peer SIDs, and can be associated with any combination of Peer Node SIDs or Peer Adjacency SIDs. Peer Set SIDs provide load balancing over BGP neighbors (nodes) or links (adjacencies).

For more information, see Segment Routing Egress Peer Engineering.

Global Weighted SRLG Protection for OSPF

This feature introduces support for Global Weighted Shared Risk Link Group (SRLG) Protection for OSPF. An SRLG is a set of links sharing a common resource and hence shares the same risk of failure. The current implementation of SRLG protection considers only the directly connected links. Hence, if the router that computes the backup path includes a link that is not directly connected but shares the same SRLG, the SRLG protection fails. The global weighted SRLG protection feature provides better path selection for the SRLG by associating a weight with the SRLG value and using the weights of the SRLG values while computing the backup path.

For more information, see Configuring Global Weighted SRLG Protection.

SRv6 Anycast Locator

This feature introduces support for SRv6 Anycast Locator. An SRv6 Anycast locator is a type of locator that identifies a set of nodes (END SIDs). SRv6 Anycast Locators and their associated END SIDs may be provisioned at multiple places in a topology. Anycast routing enables the steering of traffic toward multiple advertising nodes. Packets addressed to an Anycast address are forwarded to the topologically nearest nodes.

One use case is to advertise Anycast END SIDs at exit points from an SRv6 network. Any of the nodes that advertise the common END SID could be used to forward traffic out of the SRv6 portion of the network to the topologically nearest node.

For more information, see Segment Routing over IPv6 Overview.

SR-PCE Inter-Domain Path Computation Using SID Redistribution

A Path Computation Element (PCE) computes SR-TE that is paths based on the SR-topology database that stores the connectivity, state, and TE attributes of SR network nodes and links. BGP Labeled Unicast (BGP-LU) provides MPLS transport across IGP boundaries by advertising the loopbacks and label binding of edge and border routers across IGP boundaries.

The SR-PCE Inter-Domain Path Computation Using SID Redistribution feature adds new functionality to the SR-PCE that enables it to compute a path for remote non-SR end-point devices that are distributed by BGP-LU.

For more information, see Inter-Domain Path Computation Using Redistributed SID.

Segment Routing Path Computation Element Flexible Algorithm Multi-Domain Path Computation

Currently, a Flexible Algorithm definition is unknown to the Segment Routing Path Computation Element (SR-PCE). In order to select a Flexible Algorithm across domains, Flexible Algorithm definition can now be distributed to a PCE topology database from the gateway ABR/ASBR. The SR-PCE Flexible Algorithm Multi-Domain Path Computation feature incorporates the following changes:

- BGP-LS has been augmented to carry a Flexible Algorithm definition (FAD)
- PCEP vendor-specific objects have been added to indicate SR policy Flexible Algorithm constraints to the PCE and to request a path computation based on the Flexible Algorithm number

- PCE algorithms have been augmented to compute paths based on a Flexible Algorithm constraint

For more information, see SR-PCE Flexible Algorithm Multi-Domain Path Computation.

File Mirroring

File mirroring feature enables the router to copy files or directories automatically from `/harddisk:/mirror` location in active RP to `/harddisk:/mirror` location in standby RP or RSP without user intervention or EEM scripts.

For more information, see Introduction to File Mirroring.

The command, mirror enable is introduced.

WAN PHY Supported on 10G MPA

WAN-PHY is now supported on 10G MPA cards. WAN-PHY support in Cisco IOS XR software is based on the IEEE 802.3ae standard.

In this release WAN-PHY is only supported on NC55-MPA-12T-S cards and on SFP-10G-LR-X optics.

The purpose of WAN-PHY is to render 10 Gigabit Ethernet compatible with the SONET STS-192c format and data rate, as defined by ANSI, as well as the SDH VC-4-64c container specified by ITU.

For more information, see Configuring WAN-PHY Controllers .

Commands introduced or modified:

- port-mode sonet framing WIS
- show controller OC192
- show controller STS192c
- show controllers

BFD over Bundle with IPv4 Unnumbered Interface

BFD over Bundle with IPv4 Unnumbered Interface feature enables BFD to run on IP unnumbered interfaces, which take the IP address from the loopback address. This feature saves IP addresses space or range. The same loopback address is used on multiple interfaces.

For more information, see BFD over Bundle with IPv4 Unnumbered Interface.

Support for Packet Filtering on External TCAM of NC57-18DD-SE Line Cards

Traditional IPv4 and IPv6 ACLs programming utilizes the external TCAM of NC57-18DD-SE line cards instead of the internal TCAM. Configuration of ACLs on the external TCAM provides more space in the internal TCAM for other configurations.

Packet-length filtering of IPv4 and IPv6 packets are supported on the default TCAM key of NC57-18DD-SE line cards in the traditional ACL mode without using User Defined Keys. Fragment offset filtering of IPv4 packets are also supported on the default TCAM key of NC57-18DD-SE line cards in the traditional ACL mode without using User Defined Keys.

For more information, see *Understanding Access Lists*, *Matching by Fragment Offset in ACLs*, and *Configuring ACL Filtering by IP Packet Length*, in chapter Implementing Access Lists and Prefix Lists.

BFD Support on HSRP/VRRP

With the introduction of the BFD support on HSRP/VRRP, HSRP/VRRP will use BFD to detect a link failure and facilitate fast failover times without excessive control packet overhead.

With this feature, you can:

- Identify failure detection in less than one second.
- Support all types of encapsulation.
- Have support for almost all routing protocols.

For more information, see:

- Implementing HSRP
- Implementing VRRP

Support for Chained ACLs

In Cisco NCS 5500 Series Routers, you can configure only one ACL per direction on an interface. With the feature, Chained ACLs, you can apply more than one IPv4 or IPv6 ACL (common-acl and interface acl) on an interface for packet filtering at the ingress direction of a router. This feature enables you to separate various types of ACLs for management and other reasons, yet apply both of them on the same interface, in a defined order.

For more information, see Configuring Chained ACLs.

Commands modified for this feature:

- ipv4 access-group
- ipv6 access-group

ACL Support for IPv6 Fragments

This feature enables you to filter packets through IPv6 extended access lists with fragment control. Most DoS (Denial of Service) attacks work by flooding the network with fragmented packets. By filtering the incoming fragments of the IPv6 packets in a network, an extra layer of protection is added against such attacks.

For more information, see *Configuring ACLs with Fragment Control*, *Configuring an IPv4 ACL to Match on Fragment Type*, and *Matching by Fragment Offset in ACLs* in chapter Implementing Access Lists and Prefix Lists.

Support for DHCPv6 Client Options

This feature enables the support of DHCPv6 client on BVI interfaces. You can configure different types of DHCP IPv6 client options to enable different types of functionalities for clients as required.

For more information, see Enabling DHCP Client on an Interface.

The command, ipv6 address dhcp-client-options is introduced.

Enhancement for IPv6 Extension Headers

For traffic flows with extension headers, authentication headers, encapsulation security payloads, and mobility headers, filtering of packets based on layer 4 data is not supported through IPv6 ACLs. For NC57 line cards, hop by hop options, encapsulation security payload, authentication header, destination options, mobility header, and fragment headers are handled in the hardware (instead of software).

For more information, see Filtering Packets with IPv6 Extension Headers.

Set Peak Burst Size for Egress Shaping

From Release 7.2.1 onwards, you can configure peak burst size for egress shaping. This configuration gives your router interface the ability to manage the traffic burst for a particular traffic class such that the peer node can accommodate the burst and does not drop packets either due to lower burst policing or due to shorter queue depth.

For more information, see Configure Traffic Shaping.

The command, shape average is modified.

Conform Aware Hierarchical Policy

Traditional Hierarchical QoS (H-QoS), while allowing for granular and multi-level management of traffic, does not allow for conforming traffic from a child-level policy to a parent-level policy to get priority. This inability means that in case of excess traffic, the parent policer drops conforming traffic packets as well.

With the conform-aware hierarchical policy feature, the parent policer is prevented from dropping any conforming traffic from child policers, thus increasing traffic throughput and efficiency.

For more information, see Conform Aware Hierarchical Policy Overview.

The command, hw-module profile qos conform-aware-policer is introduced.

Ability to Create an ACL with Fragment Match

With the ability to configure an ACL with a fragment match, you now have more granular control over non-initial IP fragments of a packet. You specify the fragments keyword in an ACL and then attach that ACL to specific class maps. When you run this configuration, the ACL applies only to non-initial IP fragments of packets, and enables rate-limiting these packets.

For more information, see Configuring an ACL with Fragment Match.

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

Shared Policer Feature

With the shared policer feature, you can now share a policer bucket among two or more classes. You can also view the statistics in aggregated mode or per-class mode.

For more information, see Shared Policer.

The command, hw-module profile qos shared-policer-per-class-stats is introduced.

EVPN Convergence Improvements

With the introduction of the EVPN convergence improvements for BGP PIC, the following networks are supported, which rides over BGP PIC as transport:

- LxVPN
- EVPN
- 6PE
- 6VPE

For more information, see BGP PIC Implementation Considerations.

BGP PIC Multipath (IPv4/IPv6) with Interface Peering and Loopback Peering

With the introduction of the BGP PIC multipath IPv4/IPv6 with interface peering support, BGP control plan installs multiple primary paths and one backup path for all primary paths in the BGP routing table. If one of the primary paths doesn't work, the system adds a backup into the primary path.

For more information, see BGP PIC Implementation Considerations.

GTP Load Balancing

The GPRS Tunneling Protocol (GTP) Load Balancing feature enables efficient distribution of traffic in mobile networks, and provides increased reliability and availability for the network.

GTP load balancing is performed on IPv4 or IPv6 incoming packets with GTP payloads and on MPLS incoming labeled packets. This feature supports GTP hashing only when the GTP UDP port is 2152.

The number of MPLS label stack in the transport layer is limited to three for GTP hashing. GTP hashing is not considered when the MPLS label stack exceeds three.

For more information, see GTP Load Balancing.

BVI with Double-Tagged AC Support

The Bridge-group Virtual Interface (BVI) with Double-Tagged AC Support feature allows you to configure the attachment circuit (AC) with double-VLAN tag encapsulation on the BVI. You must specify the rewrite ingress pop 2 symmetric option when you configure the AC on the BVI with double-VLAN tag encapsulation.

For more information, see Configure VLAN Sub-Interfaces.

Network Convergence Using Core Isolation Protection

The Network Convergence using Core Isolation Protection feature allows the router to converge fast when remote links and local interfaces fail. This feature reduces the duration of traffic drop by rapidly rerouting traffic to alternate paths. This feature uses Object Tracking (OT) to detect remote link failure and failure of connected interfaces.

Tracking interfaces can only detect failure of connected interfaces and not failure of a remote router interfaces that provides connectivity to the core. Tracking one or more BGP neighbor sessions along with one or more of the neighbor's address-families enables you to detect remote link failure.

For more information, see Network Convergence using Core Isolation Protection.

The command, if track is is introduced.

Support for DHCPv4 and DHCPv6 Client on BVI

The Support for DHCPv4 and DHCPv6 Client over the BVI feature allows you to configure DHCPv4 and DHCPv6 client on the Bridged Virtual Interface (BVI). You can configure a BVI, and request DHCP IPv4 or IPv6 address on the BVI. This configiration allows your customer's device to have initial connectivity to your network without any user intervention in the field. After the device is connected to your network, the customer devices can push a node-specific configuration with static IP addresses on a different BVI for a customer deployment.

For more information, see Support for DHCPv4 and DHCPv6 Client over BVI.

Queueing Support for BUM Traffic on Attachment Circuits

This feature allows you to add BUM traffic queueing support for attachment circuits in a bridge domain. BUM traffic is replicated through Ingress Replication, and the replicated packets use the Ingress VOQ. This feature is only supported on single NPU devices, and not on devices with multiple NPUs or line cards.

For more information, see Queueing Support for BUM Traffic on Attachment Circuits.

The command, flood mode ac-ingress-replication is introduced.

Bridge Domain Scale

You can configure a maximum of 2000 bridge domains. There is an increase in the bridge domain scale from 1500 to 2000. However, there is no change in scale numbers for attachment circuit (AC), pseudowire (PW), and Bridge-group Virtual Interface (BVI).

You can configure BVIs only for 1500 bridge domains out of the 2000 bridge domains. You can configure a maximum of 1500 BVIs with a maximum of one AC per bridge domain. Increasing ACs per bridge reduces BVIs.

EVPN Automatic Unfreezing of MAC and IP Addresses

The EVPN Automatic Unfreezing of MAC and IP Addresses feature unfreezes the permanently frozen MAC and IP addresses automatically. This feature provides a configurable option to enable a MAC or IP address to undergo infinite duplicate detection and recovery cycles without being frozen permanently. The MAC or IP address is permanently frozen when duplicate detection and recovery events occur three times within a 24-hour window. If any of the duplicate detection events happen outside the 24-hour window, the MAC or IP address undergoes only one duplicate detection event and all previous events are ignored.

Commands introduced for this feature:

- host ipv4-address duplicate-detection
- host ipv6-address duplicate-detection
- host mac-address duplicate-detection

EVPN E-Tree Using RT Constraints

The EVPN E-Tree using Route Target (RT) constraints feature enables you to configure BGP RT import and export policies for an attachment circuit (AC). This feature allows you to define communication between the leaf and root nodes. The provider edge (PE) nodes can receive L2 traffic either from the attachment circuit (AC) of a bridge domain (BD) or from the remote PE node. For a given BD, L2 communication can only happen from a root to leaf and leaf to root nodes. This feature does not allow any L2 communication between the ACs of two or more leafs.

This feature provides the following benefits:

- Achieve efficiency of the BGP MAC routes scale
- Reduce the consumption of hardware resources
- Utilize the link bandwidth efficiently

The command, etree rt-leaf is introduced.

Slow Tracking

After you configure the PTP profile on a T-BC or a T-TSC, any change in PTP offset from the T-GM clock triggers an immediate reaction in the servo. With the Slow Tracking feature enabled, the servo corrects any change in the phase offset in steps. The correction is based on the configured value which can be slower than the normal correction rate.

For more information, see Slow Tracking.

Route Processor Fail Over (RPFO)

The Route Processor Fail Over (RPFO) or Stateful Switchover (SSO) feature is supported on the Profile G.8275.1 on the Telecom Boundary Clock. Over a switchover, the time error might jump to a high value after losing lock with the T-GM clock. With this feature enabled, the time error won't increase by more than 400 nanoseconds over a switchover.

For more information, see G.8275.1.

Smart License Updates

This release introduces following updates:

- Support for Smart License feature is now available on NC57 line cards.
- The new license that is introduced in this release is:
  - XR-7.2-TRK
  - NCS-55A1-24Q6-TRK

For more information, see Flexible Consumption Model Licensing Usage Pattern.

802.1X Control for VLAN Tag Subinterfaces with Multi-host and Multi-auth Capability

Previously, by default, 802.1X allowed only one MAC address on each port at a time. This lead to major constraint in current network deployments where multiple hosts or MAC addresses were connected on a single port. Now, multi-auth and multi-host modes are supported by 802.1X to allow multiple hosts or MAC addresses on a single port. By default, dot1x configured port is in multi-auth mode. However, this behaviour can be altered by changing the host mode under dot1x profile. 802.1X port-control is also supported on pre-configured VLAN sub-interfaces along with multi-auth and multi-host modes. For VLAN sub-interfaces with VLAN IDs to be pre-configured, VLAN tagged traffic is allowed only after successful 802.1X authentication of the port.

For more information, see Protect Network using IEEE 802.1X Port-Based Authentication.

The command, dot1x host-mode is introduced.

Password Policy for User Secret

The Cisco IOS XR Software extends the existing password policy support for the user authentication to all types of user secret. The types of secret include Type 5 (**MD5**), 8 (**SHA256**), 9 (**sCrypt**) and 10 (**SHA512**). Prior to this release, the support for a password policy was only for the Type 7 passwords. The new policy is common to both password and secret of the user. Using irreversible hashed-secrets have the benefit that the other modules in the device cannot retrieve the clear-text form of these secrets. Thus, the enhancement provides more secure secrets for the user names. This policy for user secrets is applicable for local and remote users.

For more information, see Password Policy for User Secret.

Commands introduced or modified for this feature are:

- aaa password-policy
- policy(AAA)
- username

Stream Telemetry Data at Leaf-Level

The router streams telemetry data at predefined gather points in the data model even if sensor-path configuration is to an individual leaf. The gather points are collection units; collection always happens at that level for operational data.

Starting from release 7.2.1, the router supports the following sensor-path resolutions:

- Streaming data at the leaf-level or at the container-level under a gather point for cadence-based subscriptions.
- For event-driven subscriptions, streaming is always at the gather point in the model, even if specific leaves or leaf is configured as sensor-path.

See Sensor Path.

gNMI TARGET_DEFINED Subscription Mode

gRPC Network Management Interface (gNMI) defines 3 modes for a streaming subscription that indicates how the router must return data in a subscription: `SAMPLE`, `ON_CHANGE`, and `TARGET_DEFINED`.

When a client creates a subscription specifying the `TARGET_DEFINED` mode, the target, here, the router, determine the best type of subscription to be created on a per-leaf basis. If the path specified within the message refers to some leaves which are event-driven, then an `ON_CHANGE` subscription is created.

In Cisco IOS XR Release 7.2.1, the `TARGET_DEFINED` subscription mode is supported only for sensor paths of OpenConfig model; native model is not supported. The supported models are: OC Interfaces, OC Telemetry, OC Shell Util, OC System NTP, and OC Platform.

See gRPC Network Management Interface.

Retrieve Default Data From Data Nodes Using with-Defaults Capability

The default parameters of a data node can be retrieved using a NETCONF operation that includes the `<with-defaults>` capability.

This capability indicates which default-handling mode is supported by the server. It also indicates support for additional defaults retrieval modes. These retrieval modes allow a NETCONF client to control whether the server returns the default data.

The <get>, <get-config>, <copy-config> and <edit-config> operations support with-defaults capability. Currently, the <with-defaults> capability is supported only for openconfig-interface.yang data model.

See Retrieve Default Parameters Using with-defaults Capability.

Enhancements to Programmability Features

The following enhancements are supported for programmability features:

- New additions to CLI-based data models.
- Export LLDP output via gRPC.
- Support to display the label information about the software version for the `oc-platform` data model.
- gNOI supports for the following new remote procedure calls (RPCs):
  - Interface
    - SetLoopbackMode
    - GetLoopbackMode
    - ClearInterfaceCounters
  - Layer2
    - ClearLLDPInterface

- BGP
    - ClearBGPNeighbor

For more information, see New and Changed Feature Information.

Egress Interface Published as Part of Ingress NetFlow

With the introduction of egress interface published as part of ingress NetFlow, you can capture traffic flow for IP packets on the egress interface or on the outgoing interface of a router.

For more information, see IPFIX 315 Implementation Considerations.

IPv6 Support in MPLS LDP

This feature provides IPv6 protocol support in MPLS LDP. Most of the LDPv4 functions are extended to LDPv6. The LDP control plane can run IPv6 to setup LSPs for IPv6 prefixes.

For more information, see Configuring LDPv6.

UCMP Over MPLS-TE

With this feature, you can lperform oad-balance for incoming traffic over multiple paths of varying costs. UCMP applies a weight to a path, and adds more forwarding instances to a path that has a higher weight (or larger bandwidth). This feature results in an equal load distribution over paths of varying bandwidths (and costs).

For more information, see UCMP Over MPLS-TE.

Hardware

- Cisco NCS-55A1-24Q6H-SS fixed port chassis.

  For more details on this chassis, see the Hardware Installation Guide for Cisco NCS 5500 Series Fixed-Port Routers.

- NC55-RP2-E— Cisco NC55-RP2-E route processor card with SyncE supports enhanced timing operations. For more details, see the Route Processor Card Overview.

- The Cisco NCS-5501, Cisco NCS-5501-SE, Cisco NC55-MPA-12T-S, Cisco NC55-MOD-A-S, Cisco NC55-MOD-A-SE-S, Cisco NCS-55A2-MOD-S, Cisco NCS-55A2-MOD-HD-S, Cisco NCS-55A2-MOD-HX-S, Cisco NCS-55A2-MOD-SE-S, and Cisco NCS-55A2-MOD-SE-H-S chassis support the following optical modules:
    - GLC-BX80-D-I
    - GLC-BX80-U-I
    - GLC-BX40-D-I
    - GLC-BX40-DA-I
    - GLC-BX40-U-I
    - GLC-EX-SMD
    - GLC-BX-D
    - GLC-BX-U

- QSFP to Four SFP+ copper break-out cable (QSFP-4SFP10G-CU1M) and QSFP to Four SFP+ active optical breakout cable (MPU-4x10G) are introduced in this release.

For additional details on the optical modules and cables, refer to the Transceiver Module Group (TMG) Compatibility Matrix Tool.

Behavior Change Introduced

Behavior change refers to any modification of an existing software feature, configuration, or a command. This release introduces following behavior change:

Guidelines for Enabling FIPS

You must follow these guidelines while enabling FIPS mode:

- You must configure the session with a FIPS-approved cryptographic algorithm. A session configured with non-approved cryptographic algorithm for FIPS (such as, MD5 and HMAC-MD5) does not work. This is applicable for OSPF, BGP, RSVP, ISIS, or any application using key chain with non-approved cryptographic algorithm, and only for FIPS mode (that is, when **crypto fips-mode** command is configured).
- If you are using any HMAC-SHA algorithm for a session, then you must ensure that the configured key-string has a minimum length of 14 characters. Otherwise, the session goes down. This is applicable only for FIPS mode.
- If you try to execute the telnet configuration on a system where the FIPS mode is already enabled, then the system rejects the telnet configuration.
- If telnet configuration already exists on the system, and if FIPS mode is enabled later, then the system rejects the telnet connection. But, it does not affect the telnet configuration as such.
- It is recommended to configure the **crypto fips-mode** command first, followed by the FIPS-related commands in a separate commit. The list of commands related to FIPS with non-approved cryptographic algorithms are:
  - **key chain** *key-chain-name* **key** *key-id* **cryptographic-algorithm MD5**
  - **key chain** *key-chain-name* **key** *key-id* **cryptographic-algorithm HMAC-MD5**
  - **router ospfv3 1 authentication ipsec spi 256 md5** *md5-value*
  - **router ospfv3 1 encryption ipsec spi 256 esp des** *des-value*
  - **router ospfv3 1 encryption ipsec spi 256 esp des** *des-value* **authentication md5** *md5-value*
  - **snmp-server user** *username* *usergroup-name* **v3 auth md5 priv des56**
  - **ssh server algorithms key-exchange diffie-hellman-group1-sha1**
  - **telnet vrf default ipv4 server max-servers** *server-limit*

Guidelines for Configuring MACsec Keychain

You must follow this guideline while configuring MACsec:

- The MACsec key IDs (configured through CLI using the **macsec key** command under the key chain configuration mode) are considered to be case insensitive. These key IDs are stored as uppercase letters. Whereas, prior to this release, the key IDs were treated as case sensitive. These key IDs are now stored as uppercase letters. Whereas, prior to this release, the key IDs were treated as case sensitive. Hence, two key IDs with the same value, but of different case (one in uppercase and other in lowercase) were treated as two separate IDs in previous releases. However, the support for this case insensitive IDs is applicable only for

the configurations done through CLI, and not for configurations done through Netconf protocol. Hence it is recommended to have unique strings as key IDs for a MACsec key chain to avoid flapping of MACsec sessions.

For more information, see Guidelines for Configuring MACsec Keychain.

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.

Cisco IOS XR Caveats

Bug ID	Headline
CSCvv05221	BGP session with TCP AO auth stays down post reload on standby

Caveats Specific to the NCS 5500 Series Routers

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

Table 1:

Bug ID	Headline
CSCvu42516	Slow tracking engages very early when servo is in FL state, making sevo erratic.
CSCvu61856	L3VPN vrf traceroute broken--IP vrf TTL1 packet punting with rif 0 for sub-interface
CSCvv26537	IPv6 egress qos is not working fine, when we have egress ACL & QoS

Features Supported on Cisco NC57 Line Cards

The Cisco NC57 line cards operate under two modes:

- Compatible Mode—Used when the chassis contains combination of Cisco NC57 and older generation line cards. This is the default mode.
- Native Mode—Used when the chassis contains only Cisco NC57 line cards. To enable the native mode, use the **hw-module profile npu native-mode-enable** command in the configuration mode. Reload the router to switch to native mode.

  The native mode support is introduced in Release 7.2.1

Following table lists all the features supported on Cisco NC57 line cards as of Release 7.2.1:

Table 2: Parity Features Supported on Cisco NC57 Line Cards

Feature	Supported in Compatible Mode	Supported in Native Mode
4x10G Breakout	✓	✓
802.1Q Trunking	✓	✓
Link Bundling (LACP)	✓	✓
Mixed Bundle (10/40/100/400)	✓	✓
LACP fallback	✓	✓
Ethernet Improved BER/LFS	✓	✓
IP unnumbered interface IPv4/v6	✓	✓
Support for MTU Size 9600 Bytes	✓	✓
OSPF, ISIS, BGP, LDP	✓	✓
QoS (8 queues/port): • Classification/Marking • Policing (2R3C) • Shaping/RED/WRED • On bundle links	✓	✓
OSPF HMAC-SHA-256 authentication	✓	✓
ISIS Purge Originator Identification TLV	✓	✓
BGP 4-byte ASN	✓	✓
BGP Large Community String	✓	✓
BGP MD-5 Authentication	✓	✓
Local AS No-Prepend, Replace-AS	✓	✓
BGP RFC5549	✓	✓
L3VPN (6PE/6VPE)	✓	✓
NCS-5500 BGP per VRF/CE label allocation for 6PE	✓	✓
MPLS Static Label	✓	✓
MPLS over GRE	✓	✓
BGP-LU	✓	✓

Feature	Supported in Compatible Mode	Supported in Native Mode
BGP-LU support for adding multiple labels	✓	✓
BGP LU IPv6 AF	✓	✓
RSVP-TE **Note** 128K MPLS TE Mid-Point	✓	✓
MPLS-TE end to end Path Protection	✓	✓
Autoroute Announce	✓	✓
LDPoTE	✓	✓
LDP over TE for Edge Role	✓	✓
Segment Routing (ISIS/OSPF)	✓	✓
Segment Routing-TE	✓	✓
BGP SR-TE Explicit	✓	✓
RSVP-TE Dark Bandwidth Accounting	✓	✓
SR : Dark bandwidth : Separate flooding thresholds	✓	✓
SR : ISIS – Local w-ECMP, Manual SRTE policy	✓	✓
SR-TI-LFA (Phase 1)	✓	✓
SR TE - TI/FLA	✓	✓
6PE/L3VPN support over SR with TI-LFA	✓	✓
TI-LFA + SR/LDP interworking	✓	✓
TI LFA uLoop avoidance (SR and MPLS)	✓	✓
BGP-SR/BGP link state	✓	✓
SR: BGP prefix-SID proxy	✓	✓
Segment Routing ODN	✓	✓
BGP-TE - v4/v6 (BGP-LS)	✓	✓
VRF-LITE	✓	✓
Fallback VRF (Virtual Routing and Forwarding)	✓	✓
Static GRE	✓	✓

Feature	Supported in Compatible Mode	Supported in Native Mode
TE – PBTS (v4/v6)	✓	✓
ABF	✓	✓
ABF with GRE tunnel as destination	✓	✓
PIC Core	✓	✓
BGP PIC Edge	✓	✓
IP FRR with Remote LFA	✓	✓
BGP v4/v6 FlowSpec / QPPB	✓	✓
GRE decap	✓	✓
uCMP	✓	✓
IPinIP decap	✓	✓
PIM-ECMP	✓	✓
GTP Load balancing	✓	✓
Sticky ECMP	✓	✓
PIM-SM; PIM RPF Vector/ASM	✓	✓
PIM-SSM, IGMPv3	✓	✓
PIM SSM v6 **Note** Supported on SE varient of cards	✓	✓
MLD, MSDP, Anycast RP	✓	✓
v4/v6 Static mroute	✓	✓
RPF Vector TLV. RFC5496	✓	✓
PIM BSR RFC5059	✓	✓
Multicast over VRF LITE **Note** 100 sources per group for VRF LITE MCAST	✓	✓
PIM BFD/PIM-ECMP	✓	✓
Multicast - mLDP for Core **Note** 100 mLDP trees in core	✓	✓

Feature	Supported in Compatible Mode	Supported in Native Mode
P2MP-TE Core for Profile 22 **Note** Support a maximum of 100 P2MP-TE in the core	✓	✓
Per Flow LPTS	✓	✓
uRPF v4/v6 Loose Mode	✓	✓
IPv4/v6 Ingress ACL	✓	✓
Scaled security ACLs; Scaled ACLs - QoS match	✓	✓
Frag Offset Match in ACLs	✓	✓
v6 Pktlen Match in ACLs	✓	✓
IPv6 Egress ACL over main and bundle interfaces	✓	✓
SPAN	×	✓
ERSPAN	×	✓
Classification/Marking	✓	✓
DSCP/EXP classification	✓	✓
Policing (2R3C)	✓	✓
Shaping/RED/WRED	✓	✓
QoS on bundled links	✓	✓
H-QoS (under main interface)	✓	✓
Egress Marking	✓	✓
QoS Re-marking of IP Packets in Egress Direction	✓	✓
QoS: IPv6 Egress marking (Uniform/Pipe mode)	✓	✓
Netflow v9	✓	✓
Netflow v10 (IPFIX) with MPLS	✓	✓
Netflow on VLAN subinterface	✓	✓
IPv4 BFD/BoB	✓	✓
IPv6 BFD (Static)	✓	✓

Feature	Supported in Compatible Mode	Supported in Native Mode
BFD Dampening	✓	✓
MPLS OAM	✓	✓
MPLS OAM for SR (BGP,OSFP,ISIS)	✓	✓
YANG and NETCONF	✓	✓
Telemetry and M2M	✓	✓
Cisco IOS XR 64-bit OC	✓	✓
LLDP YANG Model hooked into Event-Driven Telemetry	✓	✓
Dark bandwidth : Reduced telemetry interval	✓	✓
VRRP v4/V6	✓	✓
TWAMP Responder	✓	✓
Automatic ZTP on a network interfaces	✓	✓
Smart License	✓	✓
Non-Stop forwarding	✓	✓

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 7.2.1 Packages

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

Table 3: Release 7.2.1 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-r721.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-r721.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r721.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.
Cisco IOS XR Security Package	ncs5500-k9sec-3.1.0.0-r721.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-r721.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf-2.0.0.0-r721.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs5500-li-1.0.0.0-r721.x86_64.rpm	Includes LI software images
Multicast Package	ncs5500-mcast-1.0.0.0-r721.rpm	Support Multicast

Table 4: Release 7.2.1 TAR files for Cisco NCS 5500 Series Router

Feature Set	Filename
NCS 5500 IOS XR Software 3DES	NCS5500-iosxr-k9-7.2.1.tar
NCS 5500 IOS XR Software	NCS5500-iosxr-7.2.1.tar
NCS 5500 IOS XR Software	NCS5500-docs-7.2.1.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 7.2.1
Copyright (c) 2013-2020 by Cisco Systems, Inc.

Build Information:
Built By     : gopalk2
Built On     : Wed Aug 12 06:43:35 PDT 2020
Built Host   : iox-ucs-013
Workspace    : /auto/srcarchive13/prod/7.2.1/ncs5500/ws
Version      : 7.2.1
Location     : /opt/cisco/XR/packages/
Label        : 7.2.1-Renum2
cisco NCS-5500 () processor

System uptime is 9 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   Running Programd
--------------------------------------------------------------------------------------
0/2        NC55-36X100G-S        0.4   MIFPGA               CURRENT    0.07    0.07
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
0/4/1      NC55-MPA-1TH2H-S      1.0   MPAFPGA              CURRENT    0.53    0.53
0/4/2      NC55-MPA-2TH-HX-S     0.1   MPAFPGA              CURRENT    0.53    0.53
0/4        NC55-MOD-A-S          1.0   MIFPGA               CURRENT    0.13    0.13
0/4        NC55-MOD-A-S          1.0   Bootloader           CURRENT    1.03    1.03
0/4        NC55-MOD-A-S          1.0   DBFPGA               CURRENT    0.14    0.14
0/4        NC55-MOD-A-S          1.0   IOFPGA               CURRENT    0.09    0.09
0/5        NC55-18H18F           1.0   MIFPGA               CURRENT    0.03    0.03
0/5        NC55-18H18F           1.0   Bootloader           CURRENT    1.14    1.14
0/5        NC55-18H18F           1.0   IOFPGA               CURRENT    0.22    0.22
0/5        NC55-18H18F           1.0   SATA                 CURRENT    5.00    5.00
0/6/1      NC55-MPA-12T-S        0.4   MPAFPGA              CURRENT    0.27    0.27
0/6/2      NC55-MPA-12T-S        0.1   MPAFPGA              CURRENT    0.27    0.27
0/6        NC55-MOD-A-SE-S       0.201 MIFPGA               CURRENT    0.13    0.13
0/6        NC55-MOD-A-SE-S       0.201 Bootloader           CURRENT    1.03    1.03
0/6        NC55-MOD-A-SE-S       0.201 DBFPGA               CURRENT    0.14    0.14
0/6        NC55-MOD-A-SE-S       0.201 IOFPGA               CURRENT    0.09    0.09
0/7/1      NC55-MPA-12T-S        0.1   MPAFPGA              CURRENT    0.27    0.27
0/7/2      NC55-MPA-12T-S        0.1   MPAFPGA              CURRENT    0.27    0.27
0/7        NC55-MOD-A-S          0.302 MIFPGA               CURRENT    0.13    0.13
0/7        NC55-MOD-A-S          0.302 Bootloader           CURRENT    1.03    1.03
0/7        NC55-MOD-A-S          0.302 DBFPGA               CURRENT    0.14    0.14
0/7        NC55-MOD-A-S          0.302 IOFPGA               CURRENT    0.09    0.09
0/7        NC55-MOD-A-S          0.302 SATA                 CURRENT    5.00    5.00
0/9        NC55-36X100G-A-SE     0.303 MIFPGA               CURRENT    0.03    0.03
0/9        NC55-36X100G-A-SE     0.303 Bootloader           CURRENT    0.15    0.15
0/9        NC55-36X100G-A-SE     0.303 DBFPGA               CURRENT    0.14    0.14
0/9        NC55-36X100G-A-SE     0.303 IOFPGA               CURRENT    0.26    0.26
0/9        NC55-36X100G-A-SE     0.303 SATA                 CURRENT    5.00    5.00
0/13       NC55-6X200-DWDM-S     2.3   CFP2_PORT_2          CURRENT    5.52    5.52
0/13       NC55-6X200-DWDM-S     0.0   DENALI0              CURRENT   13.48   13.48
0/13       NC55-6X200-DWDM-S     0.0   DENALI1              CURRENT   13.48   13.48
0/13       NC55-6X200-DWDM-S     0.0   DENALI2              CURRENT   13.48   13.48
0/13       NC55-6X200-DWDM-S     0.0   MORGOTH              CURRENT    5.26    5.26
0/13       NC55-6X200-DWDM-S     0.0   MSFPGA0              CURRENT    2.22    2.22
0/13       NC55-6X200-DWDM-S     0.0   MSFPGA1              CURRENT    2.22    2.22
0/13       NC55-6X200-DWDM-S     0.0   MSFPGA2              CURRENT    2.22    2.22
0/13       NC55-6X200-DWDM-S     0.502 Bootloader           CURRENT    1.14    1.14
0/13       NC55-6X200-DWDM-S     0.502 IOFPGA               CURRENT    0.14    0.14
0/13       NC55-6X200-DWDM-S     0.502 SATA                 CURRENT    5.00    5.00
0/RP0      NC55-RP2-E            1.0   TimingIC-A           CURRENT    2.88    2.88
0/RP0      NC55-RP2-E            1.0   TimingIC-B-0         CURRENT    2.88    2.88
```

```
0/RP0      NC55-RP2-E            1.0   TimingIC-B-1         CURRENT    2.88    2.88
0/RP0      NC55-RP2-E            0.201 Bootloader           CURRENT    0.07    0.07
0/RP0      NC55-RP2-E            0.201 IOFPGA               CURRENT    0.50    0.50
0/RP0      NC55-RP2-E            0.201 OMGFPGA              CURRENT    0.31    0.31
0/RP1      NC55-RP2-E            1.0   TimingIC-A           CURRENT    2.88    2.88
0/RP1      NC55-RP2-E            1.0   TimingIC-B-0         CURRENT    2.88    2.88
0/RP1      NC55-RP2-E            1.0   TimingIC-B-1         CURRENT    2.88    2.88
0/RP1      NC55-RP2-E            0.301 Bootloader           CURRENT    0.07    0.07
0/RP1      NC55-RP2-E            0.301 IOFPGA               CURRENT    0.50    0.50
0/RP1      NC55-RP2-E            0.301 OMGFPGA              CURRENT    0.31    0.31
0/FC0      NC55-5516-FC          0.216 Bootloader           CURRENT    1.75    1.75
0/FC0      NC55-5516-FC          0.216 IOFPGA               CURRENT    0.26    0.26
0/FC1      NC55-5516-FC          0.216 Bootloader           CURRENT    1.75    1.75
0/FC1      NC55-5516-FC          0.216 IOFPGA               CURRENT    0.26    0.26
0/FC2      NC55-5516-FC          0.216 Bootloader           CURRENT    1.75    1.75
0/FC2      NC55-5516-FC          0.216 IOFPGA               CURRENT    0.26    0.26
0/FC3      NC55-5516-FC          0.216 Bootloader           CURRENT    1.75    1.75
0/FC3      NC55-5516-FC          0.216 IOFPGA               CURRENT    0.26    0.26
0/FC4      NC55-5516-FC          0.216 Bootloader           CURRENT    1.75    1.75
0/FC4      NC55-5516-FC          0.216 IOFPGA               CURRENT    0.26    0.26
0/FC5      NC55-5516-FC          0.216 Bootloader           CURRENT    1.75    1.75
0/FC5      NC55-5516-FC          0.216 IOFPGA               CURRENT    0.26    0.26
0/PM3      NC55-PWR-3KW-2HV      0.2   DT-LogicMCU          CURRENT    3.01    3.01
0/PM3      NC55-PWR-3KW-2HV      0.2   DT-PriMCU            CURRENT    3.00    3.00
0/PM3      NC55-PWR-3KW-2HV      0.2   DT-SecMCU            CURRENT    3.01    3.01
0/PM6      NC55-PWR-3KW-2HV      0.2   DT-LogicMCU          CURRENT    3.01    3.01
0/PM6      NC55-PWR-3KW-2HV      0.2   DT-PriMCU            CURRENT    3.00    3.00
0/PM6      NC55-PWR-3KW-2HV      0.2   DT-SecMCU            CURRENT    3.01    3.01
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
```

Other Important Information

- Remotely triggered black hole (RTBH) feature is supported only on NC57 line cards with TCAM.
- 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.
- **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).

The upgrade document NCS5500_Upgrade_Downgrade_MOP_7.2.1.pdf is available along with the Release 7.2.1 software images downloaded from the software download page.

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

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.