Release Notes for Cisco NCS 5000 Series Routers, IOS XR Release 7.2.1

Revised: January 11, 2024

Network Convergence System 5000 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.

Release 7.2.1 Packages

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

Table 1: Release 7.2.1 Packages for Cisco NCS 5000 Series Router

Composite Package		
Feature Set	**Filename**	**Description**
Cisco IOS XR IP Unicast Routing Core Bundle	ncs5k-mini-x.iso	Contains base image contents that includes: • Host operating system • System Admin boot image • IOS XR boot image • Alarm co-relation
Individually-Installable Optional Packages		
Feature Set	**Filename**	**Description**
Cisco IOS XR Manageability Package	ncs5k-mgbl-3.0.0.0-r721.x86_64..rpm	XML, Parser, HTTP Server, Telemetry, and gRPC.

Cisco IOS XR MPLS Package	ncs5k-mpls-3.1.0.0-r721.x86_64.rpm	Label Distribution Protocol (LDP), MPLS forwarding , MPLS operations , Administration and maintenance (OAM), Layer3-vpn , layer-2 vpn.
Cisco IOS XR MPLS RSVP TE package	ncs5k-mpls-te-rsvp-1.1.0.0-r721.x86_64.rpm	Supports MPLS RSVP-TE (Resource Reservation Protocol with Traffic Engineering extensions)
Cisco IOS XR Security Package	ncs5k-k9sec-3.2.0.0-r721.x86_64.rpm	Support for Encryption, Decryption, and Secure Shell (SSH),
Cisco IOS XR Multicast Package	ncs5k-mcast-2.2.0.0-r721.x86_64.rpm	Multicast routing protocols (PIM, IGMP, Auto-rp, BSR) and infrastructure (Multicast routing information Base) , Multicast forwarding (mfwd)
Cisco IOS XR ISIS package	ncs5k-isis-2.2.0.0-r721.x86_64.rpm	Supports ISIS
Cisco IOS XR OSPF package	ncs5k-ospf-2.0.0.0-r721.x86_64.rpm	Supports OSPF

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

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:

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

Support for VRRP Over BVI Interfaces

This feature enables you configure Virtual Router Redundancy Protocol (VRRP) over Bridge-Group Virtual Interface (BVI). Therefore, instead of physical interfaces, VRRP sessions can run between BVI interfaces of multiple routers providing increased efficiency and functionalities.

See Understanding VRRP over BVI and Configure VRRP over BVI.

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.

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 JSON Encoding Support

Cisco IOS XR routers support gNMI remote procedure calls (RPCs). The gNMI `subscribe` RPC supports JSON encoding in addition to the previously supported `proto` encoding format.

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.

Telemetry Domain Name Support

The destination for dial-out configuration supports IP address (Ipv4 or IPv6), and fully qualified domain name (FQDN) using domain name services (DNS). To use FQDN, you must assign IP address to the domain name.The domain name is limited to 128 characters. If DNS lookup fails for the provided domain name, the internal timer is activated for 30 sec. With this, the connectivity is continually tried every 30 sec until the domain named is looked-up successfully. DNS provides an address list depending on the address-family being requested. For example, on the router, the IP address for domain name is set using the following commands for ipv4 and ipv6 respectively:

```
domain ipv4 host abcd 172.x.x.1 172.x.x.2
```

```
domain ipv6 host abcd fd00:xx:xx:xx:1::1 fd00:xx:xx:xx:1::3
```

See Monitor CPU Utilization Using Telemetry Data to Plan Network Infrastructure.

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.

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*

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 5000 Routers

Caveats describe unexpected behavior in Cisco IOS XR Software releases. These caveats are specific to NCS 5000 Routers:

There are no caveats in this release.

Supported Packages and System Requirements

Supported Hardware

For a complete list of supported optics, hardware and ordering information for NCS 5001 and NCS 5002 series router, see the *Cisco NCS 5000 Series Data Sheet*

For a complete list of supported optics, hardware and ordering information for NCS 5011 router, see the *Cisco NCS 5011 Series Data Sheet*

To install the Cisco NCS 5000 series routers, see *Hardware Installation Guide for Cisco NCS 5000 Series Routers*.

Other Important Information

- Country-specific laws, regulations, and licenses—In certain countries, use of these products may be prohibited and subject to laws, regulations, or licenses, including requirements applicable to the use of the products under telecommunications and other

laws and regulations; customers must comply with all such applicable laws in the countries in which they intend to use the products.

- Exceeding Cisco testing—If you intend to test beyond the combined maximum configuration tested and published by Cisco, contact your Cisco Technical Support representative to discuss how to engineer a large-scale configuration for your purpose.

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.

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.