Release Notes for Cisco NCS 4000 Series, Cisco IOS XR Release 6.1.42

First Published: 2018-07-23

Release Notes for Cisco NCS 4000 Series, Cisco IOS XR Release 6.1.42

Note Come to the Content Hub at content.cisco.com, where, using the Faceted Search feature, you can accurately zoom in on the content you want; create customized PDF books on the fly for ready reference; and can do so much more...

So, what are you waiting for? Click content.cisco.com now!

And, if you are already experiencing the Content Hub, we'd like to hear from you!

Click the **Feedback** icon on the page and let your thoughts flow!

The release notes contain information about the new features introduced in the Cisco NCS 4000 Series. For detailed information regarding features, capabilities, hardware, and software introduced with this release, see the guides listed in the *Additional References* section.

Revision History

Date	Notes
July 2018	This is the first release of this publication.

Software and Hardware Requirements

Before you begin to install the software, you must check whether your system meets the minimum software and hardware requirements.

- Hardware—Intel Core i5, i7, or faster processor. A minimum of 4 GB RAM, 100 GB hard disk with 250 MB of available hard drive space.
- One of these operating System:
  - Windows 7, Windows Server 2008, or later.
  - Apple Mac OS X
  - UNIX workstation with Solaris Version 9 or 10 on an UltraSPARC-III or faster processor, with a minimum of 1 GB RAM and a minimum of 250 MB of available hard drive space.

    - Ubuntu 12.10

- Java Runtime Environment—Java Runtime Environment Version 1.8.
- Browser:
    - Internet Explorer
    - Mozilla
    - Safari
    - Google Chrome

New Features for Release 6.1.42

Note Before you dive into this release's features, we invite you to content.cisco.com to experience the features of the Cisco Content Hub. Here, you can, among other things:

- Create customized books to house information that's relevant only to you.
- Collaborate on notes and share articles by experts.
- Benefit from context-based recommendations.
- Use faceted search to close in on relevant content.

And, if you are already experiencing the Content Hub, we'd like to hear from you!

Click the **Feedback** icon on the page and let your thoughts flow!

This section highlights new NCS 4000 features for Release 6.1.42 :

Software

The following software features have been introduced in Release 6.1.42:

Bidirectional Forwarding Detection (BFD)

BFD is a detection protocol designed 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.

BFD provides fast BFD peer failure detection times for Interior Gateway Protocols (IGP) - OSPF and IS-IS. BFD sends rapid failure detection notices to the routing protocols in the local router to initiate the routing table recalculation process. This results in significantly reducing the overall network convergence time.

BGP Route Reflect (RR)

Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) that allows you to create loop-free interdomain routing between autonomous systems.

BGP requires that all internal BGP (iBGP) speakers to be fully meshed. However, this requirement does not scale well when there are many iBGP speakers. Configuring the route reflectors is one method to reduce the iBGP mesh in the network and allow all iBGP speakers within an autonomous network to learn about the available routes without introducing loops.

To configure a route reflector you have to tell the router whether the other iBGP router is a client or non-client. A client is an iBGP router that the route reflector will “reflect” routes to and the non-client is just a regular iBGP neighbor.

CFM/Y.1731, Link OAM

Ethernet Connectivity Fault Management (CFM) is an end-to-end, per-service-instance Ethernet layer operations, administration, and maintenance (OAM) protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet MANs and WANs. "End-to-end" can mean PE-to-PE or CE-to-CE. A service can be identified as a service provider VLAN (S-VLAN) or an Ethernet Virtual Connection (EVC) service.

Link OAM allows network operators to monitor and troubleshoot a single Ethernet link. It is an optional sublayer implemented in the Data Link Layer between the Logical Link Control (LLC) and MAC sublayers of the Open Systems Interconnect (OSI) model. You can monitor a link for critical events and, if needed, put a remote device into loopback mode for link testing. Link OAM also discovers unidirectional links, which are created when one transmission direction fails.

Channelization

Channelization is used to create multiple lower order ODU from higher order ODU for bandwidth sharing. This release supports channelization with packet interfaces.

Ethernet Local Management Interface

Ethernet Local Management Interface (E-LMI) is an asymmetric protocol that runs on the Provider Edge (PE) to Customer Edge (CE) link. The user-facing Provider Edge (uPE) device uses E-LMI to communicate status and configuration parameters of Ethernet Virtual Circuits (EVCs) available on the User-Network Interface (UNI) to the CE device. E-LMI defines the message formats and procedures for conveying the information from uPE to CE.

Ethernet Remote Port Shutdown

Ethernet virtual circuits (EVCs) define a Layer 2 bridging architecture that supports Ethernet services. An EVC is defined by the Metro-Ethernet Forum (MEF) as an association between two or more user network interfaces that identifies a point-to-point or multipoint-to-multipoint path within the service provider network. An EVC is a conceptual service pipe within the service provider network.

Flex-LSP

Flex LSP also known as Associated Bidirectional LSPs is the combination of static bidirectional MPLS-TP and dynamic MPLS-TE. Flex LSP provides bidirectional label switched paths (LSPs) set up dynamically through Resource Reservation Protocol–Traffic Engineering (RSVP-TE). It does not support non-co routed LSPs. Flex Label Switched Paths are LSP instances where the forward and the reverse direction paths are setup, monitored and protected independently and associated together during signaling. You use a RSVP Association object to bind the two forward and reverse LSPs together to form either a co-routed or non co-routed associated bidirectional TE tunnel. You can associate a protecting MPLS-TE tunnel with either a working MPLS-TE LSP, protecting MPLS-TELSP, or both. The working LSP is the primary LSP backed up by the protecting LSP. When a working LSP goes down, the protecting LSP is automatically activated. You can configure a MPLS-TE tunnel to operate without protection as well.

Frequency synchronization

Frequency synchronization is the ability to distribute precision frequency around the network. Precision frequency is required in the next generation networks for applications such as circuit emulation. To achieve compliance to ITU specifications for TDM, differential method circuit emulation must be used, which requires a known, common precision frequency reference at each end of the emulated circuit.

IS-IS

The Intermediate System-to-Intermediate System (IS-IS) routing protocol is an Interior Gateway Protocol (IGP) standardized by the Internet Engineering Task Force (IETF) and commonly used in large Service Provider networks. IS-IS may also be deployed in extremely large Enterprise networks. IS-IS is a link-state routing protocol, providing fast convergence and excellent scalability. Like all link-state protocols, IS-IS is very efficient in its use of network bandwidth.

IS-IS uses OSI protocols to deliver its packets and establish its adjacencies. IS-IS routers need to be assigned OSI addresses, which they use as a Router ID to create network structure.

L2Xconnect/VLAN/EVC

Layer 2 Virtual Private Network (L2VPN) emulates the behavior of a LAN across an L2 switched, IP or MPLS-enabled IP network, allowing Ethernet devices to communicate with each other as they would when connected to a common LAN segment. Point-to-point L2 connections are vital when creating L2VPNs.

Link Aggregation

Link Aggregation (LAG) is a mechanism used to aggregate physical interfaces or ports to create a logical entity called link bundle. LAG is a trunking technology that groups together multiple full-duplex Ethernet interfaces to provide fault-tolerant high-speed links between switches, routers, and servers. This release supports only L2 LAG.

Following are supported with LAG:

- VLAN subinterfaces on ethernet link bundles
- LAG through Link Aggregation Control Protocol (LACP)
- Connectivity Fault Management (CFM) protocol with ethernet bundles
- QoS over Bundles

MPLS-TE

MPLS-TE software enables an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. MPLS-TE is essential for service provider and Internet service provider (ISP) backbones. Such backbones support a high use of transmission capacity, and the networks must be very resilient so that they can withstand link or node failures. MPLS-TE provides an integrated approach to traffic engineering. With MPLS, traffic engineering capabilities are integrated into Layer 3, which optimizes the routing of IP traffic.

Orchestrated Line Card Reload (OLR)

Hitless upgrade(s) using ISSU is possible only when the SDKs are compatible. For packet-features, a software upgrade includes a change in the SDK resulting in the traffic getting affected. OLR is a solution wherein, the user can upgrade the software without an impact on the traffic, even when the SDKs are not compatible. For OTN-only nodes, OLR is not required.

OSPF/IPV4

Open Shortest Path First (OSPF). OSPF is an Interior Gateway. Protocol (IGP) developed by the OSPF working group of the Internet Engineering Task Force (IETF). OSPF was designed expressly for IP networks and it supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.

QoS

Quality of Service (QoS) is the technique of prioritizing traffic flows and providing preferential forwarding for higher-priority packets. The fundamental reason for implementing QoS in a network is to provide better service for certain traffic flows. A traffic flow can be defined as a combination of source and destination addresses, source and destination socket numbers, and the session identifier. The traffic flow must be identified, classified, and prioritized on all routers and passed along the data forwarding path throughout the network to achieve end-to-end QoS delivery. The key QoS techniques are:

- QoS Classification - involves categorizing a packet within a specific group (or class) and assigning it a traffic descriptor to make it accessible for QoS handling on the network. The traffic descriptor contains information about the forwarding treatment (quality of service) that the packet should receive.
- Policing - allows the user to control the maximum rate of traffic sent or received on an interface and to partition a network into multiple priority levels or class of service (CoS).
- Qos Marking - Marking is a process, which helps to modify QOS fields incoming and outgoing packets. Unconditional and conditional packet marking feature provides users with a means for efficient packet marking by which the users can differentiate packets based on the designated markings.
- Dropping technologies (Tail Drop and WRED) - Tail drop is a congestion avoidance technique that drops packets when an output queue is full until congestion is eliminated. WRED drops packets selectively based on IP precedence.
- Shapers and policers - are needed to ensure that a packet adheres to a contract and service. A policer typically drops traffic flow; whereas, a shaper delays excess traffic flow using a buffer, or queuing mechanism, to hold the traffic for transmission at a later time.

  For more information about QoS, see the *Quality of Service Configuration Guide for Cisco NCS 4000 Series*.

SRLG

Announce SRLG : Enabling SRLG Announce on Ethernet Terminated ODU to pass on the SRLG from OTN layer to packet interfaces.

SRLG Inheritance : SRLG values configured for optics controllers get inherited to underlying ethernet interfaces and sub-interfaces.

VPWS

Virtual Private Wire Services (VPWS), also known as Ethernet-over-MPLS (EoMPLS), allow two L2VPN Provider Edge (PE) devices to tunnel the Ethernet traffic through an MPLS-enabled L3 core and encapsulates Ethernet protocol data units (PDUs) inside MPLS packets (using label stacking) to forward them across the MPLS cloud. The two L2VPN PEs are typically connected at two different sites with an MPLS core between them. The two attachment circuits (ACs)connected at each L2VPN PE are linked by a pseudo wire (PW) over the MPLS network, which is the MPLS PW. The pseudo wire is a virtual point-to-point circuit. The two PEs establish an MPLS LDP targeted session between themselves so they can establish and control the status of the PW. An MPLS LDP targeted session is a label distribution session between routers that are not directly connected. When you create an MPLS traffic engineering tunnel interface, you need to establish a label distribution session between the tunnel headend and the tailend routers.

You can use the Pseudowire Call Admission Control (PW CAC) process to check for bandwidth constraints and ensure that after the path is signaled, the links (pseudowires participating in the bidirectional LSP association have the required bandwidth. Only pseudowires with sufficient bandwidth are admitted in the bidirectional LSP association process. The PW CAC feature works only when the PW is configured with a L2VPN preferred path tunnel.

VPWS Scale

1000 VPWS sessions are supported on each line card and 4000 VPWS sessions are supported on a node.

For more information on the above software features, see the *Configuration Guide for Cisco NCS 4000 Series*.

Hardware

The following hardware has been introduced in Release 6.1.42:

NCS4009-FC2F-S Fabric Card

The NCS4009-FC2F-S fabric card and the NCS4009-FAN-FC auxiliary fan tray are introduced for the Cisco NCS 4009 chassis. The NCS4009-FC2F-S fabric card is a 400G fabric card and enables 400G traffic using the 400G line card. The auxiliary fan tray is attached to the NCS4009-FC2F-S fabric card in the front and provides cooling to the chassis components. The air filter supported for the NCS4009-FC2F-S fabric card is NCS4009-FTF-2 .

For more information, see the *Hardware Installation Guide for Cisco NCS 4000 Series*.

External Caveats

External Bugs in Release 6.1.42

The following list contains known issues for Release 6.1.42:

Caveat ID Number	Description
CSCvc07972	There should be intelligence to identify and select far end controller, once near end is selected
CSCvf40494	CFP2 Optics FEC default threshold need to be changed for 15-min / 24-hour bucket
CSCvf84158	handle the ungraceful FIA driver crash in DNX/DPA & WB recovery

Caveat ID Number	Description
CSCvg10302	Traffic glitch seen for primary tunnels when link in backup path fails
CSCvh50871	[6142 16I]XR ISSU From 6136 to 6142 16I, after PON reset packet interface flap
CSCvh51358	NCS4K: LAG: 900ms bundle vpws convergence with LC OIR/reload
CSCvh62767	Traffic drop seen even after configuring OH, drops on DIGI because of no flow control

Supported FPD Versions

The following table lists the FPD versions supported in Release 6.1.42

Card Type	FPD Description	Req. Reload	S/W Version	Min. Req. S/W Version
NCS4009-FC-S	CCC-FPGA CCC-Power-On PLX-8608 SB Certificates	No No Yes No	1.05 1.03 0.03 1.00	1.05 1.03 0.03 1.00
NCS4009-FC2-S	CCC-FPGA CCC-Power-On PLX-8714 SB Certificates	No No Yes No	2.05 1.02 0.03 1.00	2.05 1.02 0.03 1.00
NCS4009-FC2-SP	CCC-FPGA CCC-Power-On PLX-8608 SB Certificates	No No Yes No	1.11 1.02 0.03 1.00	1.11 1.02 0.03 1.00
NCS4009-FC2F-S	CCC-FPGA CCC-Power-On PLX-8714 SB Certificates	No No Yes No	2.05 1.02 0.03 1.00	2.05 1.02 0.03 1.00
NCS4016-FC-M	CCC-FPGA CCC-Power-On PLX-8649 SB Certificates	No No Yes No	4.40 1.12 0.08 1.00	4.40 1.12 0.08 1.00

NCS4016-FC-S	CCC-FPGA	No	5.07	5.07
	CCC-Power-On	No	1.01	1.01
	PLX-8649	Yes	0.08	0.08
	SB Certificates	No	1.00	1.00
	CCC-FPGA	Yes	0.05	0.01
	CCC-Power-On	Yes	1.12	1.08
	PLX-8649	Yes	0.08	0.08
	SB Certificates	No	1.00	1.00
NCS4016-FC2-M	CCC-FPGA	No	1.35	1.35
	CCC-Power-On	No	1.01	1.01
	LTC2978_420848_ISP	Yes	1.00	1.00
	PLX-8649	Yes	0.14	0.14
	SB Certificates	No	1.00	1.00
NCS4K-2OT-O-S	Backup-ZYNQ	Yes	1.68	1.00
	CCC-FPGA	No	3.27	3.27
	CCC-Power-On	No	1.17	1.17
	DIGI1	Yes	2.03	2.03
	DIGI2	Yes	2.03	2.03
	Ethernet - Switch	Yes	1.40	1.40
	GENNUM	Yes	3.01	3.01
	PLX-8618	Yes	0.09	0.09
	Primary-ZYNQ	No	1.68	1.68
	SB Certificates	No	1.00	1.00
NCS4K-24LR-O-S	Backup-ZYNQ	Yes	4.15	0.01
	CCC-FPGA	No	4.39	4.39
	CCC-Power-On	No	1.18	1.18
	Ethernet - Switch	Yes	1.37	1.37
	PLX-8618	Yes	0.11	0.11
	Primary-ZYNQ	No	4.17	4.17
	SB Certificates	No	1.00	1.00

NCS4K-2H-O-K	Backup-ZYNQ	Yes	1.55	0.01
	CCC-FPGA	No	3.38	3.38
	CCC-Power-On	No	1.17	1.17
	DIGI1	Yes	2.03	2.03
	DIGI2	Yes	2.03	2.03
	Ethernet - Switch	Yes	1.40	1.40
	GENNUM	Yes	3.01	3.01
	LEPTON	No	4.02	4.02
	PLX-8618	Yes	0.10	0.10
	Primary-ZYNQ	No	1.56	1.56
	SB Certificates	No	1.00	1.00
NCS4K-2H-W	Backup-ZYNQ	No	1.53	1.00
	CCC-FPGA	No	4.34	4.34
	CCC-Power-On	No	1.17	1.17
	EAGLE-0-FPD	No	5.05	5.05
	EAGLE-1-FPD	Yes	5.05	5.05
	Ethernet - Switch	Yes	1.35	1.35
	GN2411-FPD-1	Yes	3.05	3.05
	GN2411-FPD-2	Yes	3.05	3.05
	GN2411-FPD-3	Yes	3.05	3.05
	GN2411-FPD-4	Yes	3.05	3.05
	PLX-8608	Yes	0.10	0.10
	Primary-ZYNQ	No	1.53	1.53
	SB Certificates	No	1.00	1.00
NCS4K-2H10T-OP-KS	Backup-ZYNQ	Yes	1.91	1.00
	CCC-FPGA	No	1.49	1.49
	CCC-Power-On	No	1.11	1.11
	DIGI1	Yes	2.03	2.03
	DIGI2	Yes	2.03	2.03
	Ethernet - Switch	Yes	1.02	1.02
	GRIMA	Yes	1.51	1.51
	PLX-8649	Yes	0.11	0.11
	Primary-ZYNQ	No	1.91	1.91
	SB Certificates	No	1.00	1.00

NCS4K-4H-OP-K	Backup-ZYNQ	Yes	0.09	0.09
	CCC-FPGA	Yes	2.02	2.02
	CCC-Power-On	Yes	1.06	1.06
	DIGI1	No	2.03	2.03
	DIGI2	No	2.03	2.03
	Ethernet - Switch	Yes	1.01	1.01
	LEPTON	No	5.00	5.00
	PLX-8649	Yes	0.01	0.01
	Primary-ZYNQ	No	1.09	1.09
	SB Certificates	No	1.00	1.00
NCS4K-4H-OPW-QC2	Backup-MELKOR	Yes	5.22	5.22
	Backup-ZYNQ	No	3.30	3.30
	CCC-FPGA	No	0.29	0.29
	CCC-Power-On	No	1.09	1.09
	DENALI	No	13.48	13.48
	DIGI1	Yes	2.02	2.02
	DIGI2	Yes	2.02	2.02
	Ethernet-Switch	Yes	1.51	1.51
	PLX-8750	Yes	0.09	0.09
	Primary-MELKOR	No	5.22	5.22
	Primary-ZYNQ	No	3.30	3.30
	SB Certificates	No	1.00	1.00
	SMAUG	Yes	0.08	0.08

NCS4K-AC-PSU	AB-PriMCU	No	1.31	1.31
	AB-Sec54vMCU	No	1.49	1.49
	AB-Sec5vMCU	No	1.43	1.43
	DT-PriMCU	No	3.00	3.00
	DT-PriMCU	No	1.06	1.06
	DT-PriMCU	No	2.01	2.01
	DT-Sec54vMCU	No	4.00	4.00
	DT-Sec54vMCU	No	2.03	2.03
	DT-Sec54vMCU	No	3.02	3.02
	DT-Sec5vMCU	No	3.01	3.01
	DT-Sec5vMCU	No	1.09	1.09
	DT-Sec5vMCU	No	2.02	2.02
NCS4K-CRAFT	Craft-NCS4009	No	1.03	1.03
	Craft-NCS4016	No	1.04	1.04
NCS4K-DC-PSU-V1	AB-PriMCU	No	3.01	3.01
	AB-Sec54vMCU	No	3.01	3.01
	AB-Sec5vMCU	No	3.02	3.02
	DT-Pri2MCU	No	3.02	3.02
	DT-Pri2MCU	No	2.02	2.02
	DT-PriMCU	No	3.02	3.02
	DT-PriMCU	No	2.02	2.02
	DT-Sec54v2MCU	No	3.01	3.00
	DT-Sec54v2MCU	No	2.05	2.05
	DT-Sec54vMCU	No	3.01	3.00
	DT-Sec54vMCU	No	2.05	2.05
	DT-Sec5vMCU	No	3.04	3.02
	DT-Sec5vMCU	No	2.06	2.06
NCS4K-ECU	ECU-FPGA	No	3.01	3.01
NCS4K-FTA	Fantray-FPGA	No	3.01	3.01

NCS4K-RP	BACKUP-BIOS	Yes	14.02	1.00
	Backup-CCC-PwrOn	Yes	1.22	1.00
	Backup-Ethswitch	Yes	1.36	1.00
	Backup-Timing	Yes	3.50	3.00
	BP-FPGA	No	3.21	3.21
	CCC-Bootloader	Yes	4.28	4.08
	CCC-FPGA	Yes	4.28	4.28
	CCC-Power-On	Yes	1.22	1.22
	CPU-Complex-BckKey	Yes	1.00	1.00
	CPU-Complex-Boot	Yes	2.09	2.04
	CPU-Complex-FPGA	Yes	2.09	2.09
	CPU-Complex-PriKey	Yes	1.00	1.00
	Ethernet - Switch	Yes	1.36	1.36
	PLX-8649	Yes	0.08	0.08
	PLX-8696	Yes	0.05	0.05
	Primary-BIOS	Yes	14.03	14.03
	SB Backup Key	No	1.00	1.00
	SB Certificates	No	1.00	1.00
	SB Primary Key	No	1.00	1.00
	SMART - iSATA	No	7.05	7.05
	SMART - SATA	No	7.05	7.05
	Timing FPGA	Yes	3.50	3.50
P-S-FANTRAY	Fantray-FPGA	No	2.04	2.04

Cisco Bug Search Tool

Use the Bug Search Tool (BST) to view the list of outstanding and resolved bugs in a release.

BST, the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The tool allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has provision to filter bugs based on credentials to provide external and internal bug views for the search input.

Search Bugs in BST

Procedure

Step 1 Go to https://tools.cisco.com/bugsearch/. You will be prompted to log into Cisco.com. After successful login, the Bug Toolkit page open.

Step 2 Enter the bug ID in the Search For: field. To search for release bugs, enter the following parameters in the page:

a) Search For — Enter NCS4k in the text box.
b) Releases — Enter the release number.
c) Show Bugs — Select Affecting or Fixed in these Releases

Step 3 Press Enter.

- By default, the search results include bugs with all severity levels and statuses, and bugs that were modified during the life cycle of the bug. After you perform a search, you can filter your search results to meet your search requirements.
- An initial set of 25 search results is shown in the bottom pane. Drag the scroll bar to display the next set of 25 results. Pagination of search results is not supported.

Additional References

Related Documentation

Use the release notes with the following publications:

Document Title	Description
Hardware Installation Guide for Cisco NCS 4000 Series	Provides installation information about the Cisco NCS 4009 and Cisco NCS 4016 chassis.
Cisco Network Convergence System 4000 Series Unpacking, Moving, and Securing Guide	Provides instructions for unpacking the Cisco NCS 4009 and Cisco NCS 4016 chassis, moving the chassis to its permanent location, and mounting the chassis in a rack.
Regulatory Compliance and Safety Information for the Cisco NCS 4000 Series	Provides the international agency compliance, safety, and statutory information that apply to Cisco NCS 4009 and Cisco NCS 4016 chassis.
Configuration Guide for Cisco NCS 4000 Series	Provides background and reference material, procedures to configure and maintain the Cisco NCS 4009 and Cisco NCS 4016 chassis.

Document Title	Description
Command Reference for Cisco NCS 4000 Series	Provides the various commands available to configure and maintain the Cisco NCS 4009 and Cisco NCS 4016 chassis.
System Setup and Software Installation Guide for Cisco NCS 4000 Series	Provides instructions to set up the system and perform software installation.
Alarms Troubleshooting Guide for Cisco NCS 4000 Series	Provides a description, severity, and troubleshooting procedure for each commonly encountered NCS 4000 alarm and condition.
Cisco IOS XR System Error Message Reference Guide	Provides a list of the Cisco IOS XR system error messages for all Cisco IOS XR platforms
Quality of Service Configuration Guide for Cisco NCS 4000 Series	Provides features available to configure and maintain Quality of Service (QoS) for the Cisco NCS 4000 Series Routers.
Quality of Service Command Reference for Cisco NCS 4000 Series	Provides various commands available to configure and maintain Quality of Service (QoS) for the Cisco NCS 4000 Series Routers.
Migration of Single Chassis to Multi Chassis for Cisco NCS 4000 Series	Provides configuration procedures for the supported multi chassis configurations.

Technical Assistance

Link	Description
http://www.cisco.com/cisco/web/support/index.html	The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.