Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.2

Revised: April 9, 2021

Network Convergence System 5500 Series Routers

Note This product 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.

Cisco IOS XR Release 6.3.2 contains all features released in Cisco IOS XR Release 6.3.1. Release 6.3.1 is a limited availability (LA) release. For more information on IOS XR Release 6.3.1 features, see Release Notes for Cisco NCS 5500 Series Routers, Release 6.3.1

Cisco Feature Deployment Recommendation

In evaluating the use of features in the Cisco IOS XR Release 6.3.2, consider the below classification of features before deploying:

- Category 1—Features are ready for full scale deployment.
- Category 2—Feature behavior will be strengthened with a SMU as needed.
- Category 3—Features are recommended only for EFT and Lab Certification. Large scape deployment will be supported in future releases.

Please contact the Cisco Deployment team or your Account Team to understand whether the features you are implementing are ready for deployment in your network.

For detailed list of Category 1, Category 2 and Category 3 features, see List of Cisco Software Features Recommended for Deployment , on page 10.

Software Features Introduced in Cisco IOS XR Software Release 6.3.2

Smart Licensing

Smart Licensing is a cloud-based, software license management solution that enables you to automate time-consuming, manual licensing tasks. The solution allows you to easily track the status of your license and software usage trends.

Note

- By default Smart Licensing is enabled.
- Only non-consumption model Smart Licensing is supported.

For information on configuring Smart Licensing, see the chapter *Software Entitlement* in the *System Management Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.x*

BFD Transparency

BFD transparency feature enables Bidirectional Forwarding Detection (BFD) sessions between CEs connected over L2VPN network to come up seamlessly without BFD packets getting processed or dropped in the L2VPN Core.

For more information, see the *Routing Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.x*.

Egress IPv4 ACLs on BVIs

Bridge Virtual Interfaces (BVIs) provide a bridge between the routing and bridging domains on a router. A BVI is configured with an IP address and operates as a regular routed interface. You can configure an ACL on a BVI to filter the traffic for the network that uses the interface.

To know how to configure an IPv4 egress ACL on a BVI, see the *ACLs on Bridge Virtual Interfaces* section in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*.

IPv4 ACL Matching on Fragment Type

Most DoS (Denial of Service) attacks work by flooding the network with fragmented packets. By filtering the incoming fragments of the packet in a network, an extra layer of protection can be added against such attacks. You can configure an IPv4 ACL to match on the fragment type, and perform an appropriate action.

For information about configuring an IPv4 ACL to match by the various fragment types, see *Configuring an IPv4 ACL to Match on Fragment Type* section in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*. For information about the various fragment types to match on, see the following command pages in the *IP Addresses and Services Command Reference for Cisco NCS 5500 Series Routers*.

- **dont-fragment**
- **is-fragment**
- **first-fragment**
- **last-fragment**

IP-MIB Support for IPv4

IOS-XR implementation of IP-MIB now supports IPv4 statistics as per RFC4293. Refer to the SNMP OID Navigator for a list of new OIDs added for iPv4 statistics.

IS-IS VRF Aware Lite

The feature adds the possibility to run an Integrated Intermediate System-to-Intermediate System (IS-IS) process in the context of a non-default VPN routing and forwarding (VRF). Both IPv4 and IPv6 are supported. The implementation is more suitable for VRF-lite scenarios.

For more information, see the *Routing Configuration Guide for Cisco NCS 5000 Series Routers, IOS XR Release 6.3.x*.

ACLs Matching on TTL Value

You can configure ACLs to match on the TTL value specified in the IPv4 or IPv6 header. You can specify the TTL match condition to be based on a single value, or multiple values. You can also rewrite the TTL value in the IPv4 or IPv6 header by using the **set ttl** command. TTL matching is supported only for ingress ACLs.

ACLs that are shared across interfaces and use the same TCAM space are known as shared ACLs. However, you can configure only 31 unique, shared ACLs. To configure more unique ACLs, ACL sharing must be disabled by using the **interface-based** command. By making the ACLs unique for an interface, you can configure more than 31 ACLs.

For information on configuring ACLs to match on TTL values and configuring unique ACLs, see the *Configuring TTL Matching for IPv4 ACLs* and *Configuring TTL Matching for IPv6 ACLs* sections in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*.

Explicit Binding Segment Identifier (BSID)

A binding segment is a local segment that identifies an SR-TE policy. Each SR-TE policy is associated with a binding segment ID (BSID). By default, a BSID is allocated automatically for each SR-TE policy when the SR-TE policy is instantiated.

The Explicit BSID feature allows you to request that the SR-TE policy uses a BSID value that you provide. Explicit BSIDs are allocated from the segment routing local block (SRLB) or the dynamic range of labels. You can also specify how the BSID allocation behaves if the BSID value is not available.

For more information on this feature, see the Configure SR-TE Policies chapter in the Segment Routing Configuration Guide for NCS 5500 Series Aggregation Services Routers.

BGP Commit Replace for Neighbour Groups

BGP commit replace for neighbour groups feature allows you to move an autonomous system from a BGP neighbour to a BGP neighbour group in a single IOS-XR commit.

Conditional Marking of MPLS Experimental bits for L3VPN Traffic

Conditional Marking of MPLS Experimental bits for L3VPN Traffic feature enables the user to configure the conditional marking of MPLS Experimental bits for L3VPN Traffic on the Provider Edge routers in the imposition direction.

For more information on this feature, see the *Configuring Modular QoS Service Packet Classification* chapter in the *Modular QoS Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.x*

BER and LFS Optimization on 10/40/100Gbps Interfaces"

Bit Error Rate (BER) is a number of bit errors per unit time that determines the reliability of a link. The system supports BER on 10/40/100 GE interfaces. The system raises an alarm or brings down the TX of an interface once the error value crosses the configured threshold value.

Link fault signalling (LFS) is a physical layer protocol that enables communication on a link between Ethernet devices. When you configure a device on a network, the port can detect and report fault conditions on transmit and receive ports.

For more information, see the *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers* guide.

10G DWDM Tunable Optics

This feature provides tunable support for the dense wavelength-division multiplexing (DWDM) wavelengths of the DWDM-XFP-C module on the Cisco NCS 5500 Series Aggregation Services Routers. You can configure the DWDM ITU wavelengths by using the itu channel command in the interface configuration mode.

For more information, see the *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers* guide.

DWDM Optics with Limiting Electrical Receiver

This features provides support for DWDM optics PID. The itu channel command ensures that the traffic continues to flow. The modules have the operating wavelengths according to ITU-T G.692 at 100GHz grids in C-band.

For more information, see the *Interface and Hardware Component Configuration Guide for Cisco NCS 5500 Series Routers* guide.

LLDP Support on the MGMT Interface

With the introduction of this feature, the system supports the IOS XR LLDP enablement over the Management Interfaces on Cisco NCS 5500. This feature requires support from SPIO as LLDP uses SPIO for both transmission and reception of the frames.

For more information, see the Using Data Models chapter in *Programmability Configuration Guide for Cisco NCS 5500 Series Routers*.

MPLS Static LSP over BVI

By using a bridge-group virtual interface (BVI), you can convert multiple interfaces as members of a common broadcast domain. MPLS static over BVI feature allows you to specify a BVI interface as nexthop while setting up a static label-switched path (LSP).

For more information about configuring MPLS static over BVI feature, see *MPLS Configuration Guide for Cisco NCS 5500 Series Routers, Release 6.3.x.*

LDP over MPLS-TE

LDP over MPLS-TE feature combines the benefits of both LDP and RSVP protocols which are used to set up LSPs. While LDP is easy to configure, RSVP has traffic engineering capabilities which help to avoid traffic congestions. In LDP over MPLS-TE, an LDP signalled label-switched path (LSP) runs through a TE tunnel established using RSVP-TE.

For more information about configuring LDP over MPLS-TE feature, see *MPLS Configuration Guide for Cisco NCS 5500 Series Routers, Release 6.3.x.*

MPLS-TE Path Protection

Path protection provides an end-to-end failure recovery mechanism for MPLS-TE tunnels. A secondary Label Switched Path (LSP) is established, in advance, to provide failure protection for the protected LSP that is carrying a tunnel's TE traffic. When there is a failure on the protected LSP, the source router immediately enables the secondary LSP to temporarily carry the tunnel's traffic.

For more information about configuring MPLS-TE path protection, see *MPLS Configuration Guide for Cisco NCS 5500 Series Routers, Release 6.3.x.*

BGP Large Community String

BGP communities provides a way to group destinations and apply routing decisions such as acceptance, rejection, preference, or redistribution on a group of destinations using community attributes. BGP community attributes are variable length attributes consisting of a set of one or more 4-byte values which are split into two parts of 16 bits to represent AS number and a locally defined value. BGP large community is a 12 byte optional attribute which can accommodate 4 byte ASNs which cannot be accommodated by the BGP community or the BGP extended community.

For more information about configuring BGP large community feature, see *Routing Configuration Guide for Cisco NCS 5500 Series Routers* .

L2VPN VPLS or VPWS over SR-TE Preferred Path

L2VPN VPLS or VPWS over SR-TE Preferred Path feature allows you to set the preferred path between the two end-points for L2VPN Virtual Private LAN Service (VPLS) or Virtual Private Wire Service (VPWS) using SR-TE policy.

For more information on this feature, see the *L2VPN Preferred Path over Segment Routing for Traffic Engineering Policy* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.2*.

MPLS L3VPN Services using Segment Routing

The MPLS L3VPN Services using Segment Routing feature allows you to achieve better resilience and convergence for the network traffic, by transporting MPLS L3VPN services using Segment Routing (SR), instead of MPLS LDP. Segment routing can be directly applied to the MPLS architecture without changing the forwarding plane.

For more information on this feature, see the *Implementing MPLS Layer 3 VPNs* chapter in the *L3VPN Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.2*.

DHCPv6 Relay Agent

A DHCPv6 relay agent is a host that forwards DHCP packets between clients and servers that do not reside on a shared physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router where IP datagrams are switched between networks transparently.

DHCP clients use User Datagram Protocol (UDP) broadcasts to send DHCP DISCOVER messages when they lack information about the network to which they belong.

If a client is on a network segment that does not include a server, a relay agent is needed on that network segment to ensure that DHCP packets reach the servers on another network segment. UDP broadcast packets are not forwarded, because most routers are not configured to forward broadcast traffic. You can configure a DHCPv6 relay agent to forward DHCP packets to a remote server by configuring a DHCPv6 relay profile and configure one or more helper addresses in it. You can assign the profile to an interface or a VRF.

For more information, see *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.x*.

BGP Dynamic Neighbor Authentication

BGP dynamic neighbor support allows BGP peering to a group of remote neighbors that are defined by a range of IP addresses. Each range can be configured as a subnet IP address.

In larger BGP networks, implementing BGP dynamic neighbors can reduce the amount and complexity of CLI configuration and save CPU and memory usage. Both IPv4 and IPv6 peering are supported.

The BGP dynamic neighbor authentication support enhances security by enabling authentication while forming BGP dynamic neighbors.

For more information, see *BGP Dynamic Neighbors* chapter of the *BGP Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.x*.

MACSec Fallback Pre-Shared Key

Fallback is a session recovery mechanism when primary PSK fails to bring up secured MKA session. It ensures that a PSK is always available to perform MACSec encryption and decryption.

- In CAK rollover of primary keys, if latest active keys are mismatched, system performs a hitless rollover from current active key to fallback key, provided the fallback keys match.
- If a session is up with fallback, and primary latest active key configuration mismatches are rectified between peers, system performs a hitless rollover from fallback to primary latest active key.

For more information, see *System Security Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.x*.

Management Plane Protection for Third-Party Applications

Management Plane Protection (MPP) provides a mechanism for securing management traffic on the router. Without MPP, if the service is enabled, the Cisco IOS XR allows the service traffic to pass through any interface with a network address.

MPP configuration for third-party application (TPA) enables to filter the traffic of TPA component, for example, gRPC component. The addition of gRPC component controls the management protocol traffic and supports the management protocols for the TPA, for example, gRPC. It also helps to control the gRPC application and filter the gRPC traffic through MPP configuration.

For more information, see *MPP for Third Party Applications* chapter of the *System Security Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.x*.

MACSec Data Delay Protection

MACSec data delay protection allows MKA participants to ensure that the data frames protected by MACSec are not delayed by more than 2 seconds. Each SecY uses MKA to communicate the lowest packet number (PN) used for transmission with the Secure Association Key (SAK) within two seconds. Traffic delayed longer than 2 seconds are rejected by the interfaces enabled with delay protection.

This provides additional security in preventing any man-in-the-middle attack (MITM) or replay attack.

For more information, see *Creating a User-Defined MACsec Policy* section of the *Configure MACSec* Chapter of the *System Security Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.x*.

BGP Labeled Unicast with Multiple Label Stack

BGP Labeled Unicast Multiple Label Stack feature enables the user to make the XR router receive and advertise BGP LU updates with a stack of one or more labels associated with the encoded prefix.

This feature provides the ability for a controller to push a multiple label stack through BGP labeled unicast session onto the headend.

For information about configuring BGP Labeled Unicast with Multiple Label Stack feature, see the *BGP Configuration Guide for Cisco NCS 5500 Series Routers*.

BPDU Transparency with MACSec

BPDU Transparency with MACSec feature enables you to create tunnel between a source customer edges (CE) device and destination CE devices and use this tunnel to carry traffic between these two CEs.

For more information on this feature, see the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.2*.

IP Fast Reroute with Remote Loop Free Alternate (LFA)

Some topologies (for example the commonly used ring-based topology) require protection that is not afforded by Loop-Free Alternate (LFA) Fast Reroute (FRR) alone. In such cases, use the Label Distribution Protocol (LDP)-based FRR Remote LFA feature where IGPs compute non-directly connected neighbor, which are more than one hop away, as LFA backup path to protect the given prefix's primary path. The LDP sets up labeled backup LSP with the remote next-hop for the protected prefix. LDP also sets up another transport LSP to tunnel traffic to remote next-hop without exposing the LFA backup label as learnt from remote node.

For information about configuring Fast Reroute Remote Loop-Free Alternate feature, see the *Routing Configuration Guide for Cisco NCS 5500 Series Routers*.

Static LSP Next Hop Resolve with Recursive Prefix

Static LSP next hop resolve with recursive prefix feature supports resolution of recursive routes for static LSPs. This feature enables you to specify a next-hop which is not directly connected for a static LSP destination.

For more information about configuring static LSP next hop resolve with recursive feature, see *MPLS Configuration Guide for Cisco NCS 5500 Series Routers* .

RPM Signing and Verification

Cisco IOS XR supports RPM signing and signature verification for Cisco IOS XR RPM packages in the ISO and upgrade images. All RPM packages in the Cisco IOS XR ISO and upgrade images are signed to ensure cryptographic integrity and authenticity. This guarantees that the RPM packages have not been tampered with and the RPM packages are from Cisco IOS XR. The private key, used for signing the RPM packages, is created and securely maintained by Cisco.

Enhancements to Programmability

Cisco IOS XR supports `Network-Instance`, `LLDP`, and `ISIS` Open Config Models. These models have YANG models defined for configuration and operational data.

For more information about YANG data models and configuration, see *Using Data Models* chapter in Programmability Configuration Guide for Cisco NCS 5500 Series.

IP Flow Information Export (IPFIX) 315 Format

Internet Protocol Flow Information Export (IPFIX) is an IETF standard export protocol (RFC 7011) for sending IP flow information. Cisco NCS 5500 Router supports IPFIX 315 format to export flow information. IPFIX 315 format facilitates sending ‘n’ octets frame information starting from ethernet header till trasport header of the traffic flow over the network. IPFIX 315 supports sending variable size packet record with variable payload information such as IPv4, IPv6, MPLS, and Nested packets like OuterIP-GRE-InnerIP etc. The process includes sampling and exporting the traffic flow information. Along with the ethernet frame information, IPFIX 315 format exports information of incoming and outgoing interface of the sampled packet.

For information on configuring IPFIX 315, see *Netflow Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.x*.

USB Golden ISO Boot

Golden ISO (GISO) is a customized installable image. GISO supports booting from PXE and USB.

For information about installing Golden ISO and booting options, see *Customize Installation using Golden ISO* chapter in System Setup and Software Installation Guide for Cisco NCS 5500 Series Routers.

LLDP YANG Models

Link Layer Discovery Protocol (LLDP) YANG model supports configuring event-driven telemetry.

For an example about configuring event-driven telemetry for LLDP, see *Configure Model-driven Telemetry* chapter in Telemetry Configuration Guide for Cisco NCS 5500 Series Routers .

NETCONF Transport for Event-Driven Telemetry

Support for NETCONF as a transport for event-driven telemetry.

For information about NETCONF notifications, see *Configure Model-driven Telemetry* chapter in Telemetry Configuration Guide for Cisco NCS 5500 Series Routers .

IPv4 Multihop BFD

The IPv4 Multihop BFD feature provides sub-second forwarding failure detection for a destination more than one hop, and up to 255 hops, away. The **bfd multihop ttl-drop-threshold** command can be used to drop BFD packets coming from neighbors exceeding a certain number of hops. BFD multihop is supported on all currently supported media-type for BFD singlehop.

. For more information on the IPv4 Multihop BFD feature, see the *Routing Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.2*.

EVPN VPWS over SR-TE Preferred Path

EVPN VPWS over SR-TE Preferred Path feature allows you to set the preferred path between the two end-points for EVPN VPWS pseudowire (PW) using SR-TE policy.

For more information on this feature, see the *L2VPN Preferred Path over Segment Routing for Traffic Engineering Policy* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.2*.

EVPN Multiple Services per Ethernet Segment

EVPN Multiple Services per Ethernet Segment feature allows you to configure multiple services over single Ethernet Segment (ES). Instead of configuring multiple services over multiple ES, you can configure multiple services over a single ES. With this feature you can optimize the use of resources, especially bandwidth and reduce the cost of hardware.

For more information on this feature, see the *EVPN Features* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.2*.

EVPN Support for V6 Hosts with Mobility

EVPN Support for V6 Hosts with Mobility feature enables you to provide EVPN IPv6 service over IPv4-MPLS core network. This feature supports all-active multihoming and virtual machine (VM) or host move.

For more information on this feature, see the *Configure EVPN IRB* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.2*.

EVPN VPWS On-Demand Next Hop with SR-TE

The EVPN VPWS On-Demand Next Hop with SR-TE feature enables you to fetch the best path to send traffic from the source to destination in a point-to-point service using IOS XR Traffic Controller (XTC).

For more information on this feature, see the *L2VPN Preferred Path over Segment Routing for Traffic Engineering Policy* chapter in the *L2VPN and Ethernet Services Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.2*.

BFD for Protocol Independent Multicast

The BFD Support for Multicast (PIM) feature, also known as PIM BFD, registers PIM as a client of BFD. PIM can then utilize BFD to initiate a session with an adjacent PIM node to support BFD's fast adjacency failure detection in the protocol layer. PIM registers with BFD. When PIM BFD is enabled, BFD notifies PIM about failures.

For more information about configuring PIM BFD feature, see *Routing Configuration Guide for Cisco NCS 5500 Series Routers, Release 6.3.x.*

PIM on Bundle-Ethernet subinterface

The support for PIM on Bundle-Ethernet subinterface is introduced in this release.

IPv4 BFD for BGP on a Bundle Interface

IPv4 BFD for BGP over Bundle Interface feature, also known as Bidirectional Forwarding Detection (BFD) over Logical Bundle feature implements and deploys BFD over bundle interfaces based on RFC 5880. The BFD over Logical Bundle (BLB) feature replaces the BVLAN feature and resolves certain interoperability issues with other platforms that run BFD over bundle interface in pure RFC5880 fashion.

For more information on this feature, see the *Routing Configuration Guide for Cisco NCS 5500 Series Routers, IOS XR Release 6.3.2*.

IPv6 Egress ACLs on Physical and Bundle Interfaces

Support has been provided for IPv6 egress ACLs on gigabit ethernet and bundle interfaces. To know more about the configuration prerequisites and steps, see *Configuring IPv6 ACLs* in the *IP Addresses and Services Configuration Guide for Cisco NCS 5500 Series Routers*.

List of Cisco Software Features Recommended for Deployment

Category-1

- 100Mbps Copper SFP Support
- 10G DWDM Tunable Optics
- ACL Matching on TTL Value
- Affinity Support with Anycast SID for Segment Routing TE
- BER and LFS Optimization on 10/40/100Gbps Interfaces
- BGP commit replace for neighbor groups
- BGP Dynamic Neighbor Authentication

- BGP Labeled Unicast with Multiple Label Stack
- System metrics monitoring (disk space, CPU usage, memory usage, load averages, etc)
- BPDU Transparency MACSec
- Conditional Marking of MPLS Experimental Bits for L3VPN Traffic
- DHCPv6 Relay Agent
- DWDM Optics with Limiting Electrical Receiver
- Egress IPv4 ACLs on BVI
- Explicit Binding Segment Identifier (BSID)
- IP Fast Reroute with Remote Loop Free Alternate (LFA
- IP Flow Information Export (IPFIX) 315 Format
- IPv4 ACL Matching on Fragment Type
- ISIS OpenConfig Model
- IS-IS VRF Aware-Lite
- ITU-T G.8275.1
- L2VPN VPLS or VPWS over SR-TE Preferred Path
- L3VPN, 6PE Support on Segment Routing
- LLDP OpenConfig Model
- LLDP Support on the Management Interface
- LLDP YANG model support for Event-Driven Telemetry
- MACSec Data Delay Protection
- MACSec Fallback Pre-shared Key
- Management Plane Protection for Third-Party Applications
- Manual SR TE Policy Configuration
- mLDP for Core Deployments
- MPLS Static LSP over BVI
- MPLS-TE Path Protection
- Multicast over VRF-Lite
- NETCONF Transport for Event-Driven Telemetry
- Network-Instance IS-IS Extension OpenConfig Model
- Network-Instance OpenConfig Model
- Prefix-based GRE Tunnel Destination for Load Balancing
- Protocol Independent Multicast (PIM) Equal Cost Multipath (ECMP)

- PW Ping over Segment Routing
- RPM Signing and Verification
- Smart Licensing
- Static LSP Next Hop Resolve with Recursive Prefix
- Sync E. ESMC
- Topology Independent Loop Free Alternate (TI-LFA)
- Topology Independent Loop Free Alternate (TI-LFA) Microloop Avoidance
- USB Golden ISO Boot

Category-2

- EVPN VPWS over SR-TE preferred-path
- BFD Dampening
- BFD for Protocol Independent Multicast (PIM)
- EVPN Multiple Services per Ethernet Segment
- EVPN support IPv6 Hosts with Mobility
- EVPN VPWS On-Demand Next Hop (ODN) with SR-TE
- IPv4 BFD for BGP on a Bundle Interface
- IPv4 Multihop BFD
- IPv6 Egress ACLs on Physical and Bundle Interfaces
- LDP over TE for Core Deployments

Category-3

- IGMP Snooping
- IPv4 Multicast and PIM over BVI”
- Multicast on a VLAN over a Bundle

For the category defination, refer to the Cisco Feature Deployment Recommendation, on page 2 section.

Behavior Change Introduced in Cisco IOS XR Release 6.3.2

From this release onwards **address-family** is a mandatory keyword for the **show tech-support multicast** command. The command syntax is:

```
show tech multicast address-family <ipv4/ipv6>.
```

For more information, refer the *show tech-support multicast* command in the *Tech-Support Commands* chapter of the *Advance System Command Reference for Cisco NCS 5500 Series Routers.*

New Hardware Introduced in Cisco IOS XR Release 6.3.2

This release introduces the following new hardware:

- Cisco NCS-55A1-36H-SE—This chassis is a fixed port, high density, one rack unit form-factor router that supports port density of 36 x QSFP ports, each capable of supporting 4x10 GE (via cable breakout), 4x25 GE (via cable breakout), 40 GE (QSFP+), or 100 GE (QSFP28) receivers. The router has additional TCAM to support large prefix scale.

  For more information, see the *Hardware Installation Guide for Cisco NCS 5500 Series Fixed-Port Routers*.

  For information on the optics supported and other specifications, refer to the *Cisco Network Convergence System 5500 Series: 55A1 Fixed Chassis Data Sheet*.

- NC55-PWR-3KW-2HV—Dual-input high voltage AC-input or DC-input (HVAC/HVDC) power supply that provides 3.15KW with either 1 or 2 input power lines. This power supply is supported in the NCS 5500 modular chassis and provides *n*+*n* line redundancy mode in a single power supply for the Cisco NCS 5516 router.

  For more information, see the *Hardware Installation Guide for Cisco NCS 5500 Series Modular Routers*.

The support for below 10G and 1G optics is extended on the line cards listed in the table below:

Table 1: 10G Optics

Optics	Supported on LC
SFP-10G-SR, and –S	NCS-55A1-36H-S, NCS-55A1-24H, NCS-5502-SE
SFP-10G-LR, and –S	NCS-55A1-36H-S, NCS-55A1-24H, NCS-5502-SE
SFP-10G-ER, and –S	NC55-36X100G, NC55-36X100G-A-SE
SFP-10G-ZR, and –S	NC55-36X100G, NC55-36X100G-A-SE
DWDM-SFP10G-xxxx (fixed)	NC55-36X100G, NC55-36X100G-A-SE

Table 2: 1G Optics

Optics	Supported on LC
GLC-TE (1000BASE-T)	NC55-24H12F-SE
GLC-SX-MMD	NC55-24X100-SE, NC55-24H12F-SE, NC55-36X100G, NCS-55A1-24H
GLC-LH-SMD	NC55-24X100-SE, NC55-24H12F-SE, NC55-36X100G, NCS-55A1-24H

Supported Hardware

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

Use the Cisco Optics-to-Device Compatibility Matrix tool to determine transceivers supported in Cisco hardware devices.

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

Release 6.3.2 Packages

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

Table 3: Release 6.3.2 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-r632.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-r632.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r632.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.
Cisco IOS XR Security Package	ncs5500-k9sec-3.1.0.0-r632.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-r632.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf-2.0.0.0-r632.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs5500-li-1.0.0.0-r632.x86_64.rpm	Includes LI software images
Multicast Package	ncs5500-mcast-1.0.0.0-r632.rpm	Support Multicast

Determine Software Version

Log in to the router and enter the **show version** command:

```
RP/0/RP0/CPU0:router# show version

Cisco IOS XR Software, Version 6.3.2
Copyright (c) 2013-2017 by Cisco Systems, Inc.
```

```
Build Information:
 Built By     : username
 Built On     : Wed Mar 28 20:50:18 PDT 2018
 Build Host   : iox-ucs-025
 Workspace    : /auto/srcarchive17/prod/6.3.2/ncs5500/ws
 Version      : 6.3.2
 Location     : /opt/cisco/XR/packages/

cisco NCS-5500 () processor
System uptime is 3 minutes
```

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
CSCvh18580	Convergence delay of upto 15sec with main/sub interface shutdown
CSCvh69102	FRR shutdown notification not processed on sub-interface

Caveats Specific to the Cisco NCS 5500 Routers

Caveats describe unexpected behavior in Cisco IOS XR Software releases.

Determine Firmware Support

Use the **show hw-module fpd** command in 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.

Table 4: PID and FPD Versions for Release 6.3.2

PID	FPD Device	FPD Versions
NCS55-RP	Bootloader	9.25
	IOFPGA	0.09
NCS55-SC	Bootloader	1.74
	IOFPGA	0.10
NC55-5508-FC	Bootloader	1.74
	IOFPGA	0.16

PID	FPD Device	FPD Versions
NC55-36X100G	Bootloader	1.17
	IOFPGA	0.15
	MIFPGA	0.09
NC55-24X100G-SE	Bootloader	1.11
	IOFPGA	0.13
	MIFPGA	0.03
NC55-18H18F	Bootloader	1.11
	IOFPGA	0.22
	MIFPGA	0.03
NC55-36X100G-S	Bootloader	1.11
	IOFPGA	0.1
	MIFPGA	0.06
NC55-24H12F-SE	Bootloader	1.11
	IOFPGA	0.09
	MIFPGA	0.03
NCS-5501	Bootloader	1.16
	CPU-IOFPGA	1.14
	MB-IOFPGA	1.05
	MB-MIFPGA	1.01
NCS-5501-SE	Bootloader	1.16
	CPU-IOFPGA	1.14
	MB-IOFPGA	1.11
	MB-MIFPGA	1.02

PID	FPD Device	FPD Versions
NCS-5502	Bootloader	1.16
	CPU-IOFPGA	1.14
	DC-IOFPGA	1.05
	DC-MIFPGA	1.02
	MB-IOFPGA	1.05
	MB-MIFPGA	1.02
NCS-5502-SE	Bootloader	1.16
	CPU-IOFPGA	1.14
	DC-IOFPGA	1.05
	DC-MIFPGA	1.02
	MB-IOFPGA	1.05
	MB-MIFPGA	1.02
NC55-5516-FC	Bootloader	1.75
	IOFPGA	0.23
NCS-55A1-36H-B	Bootloader	1.07
	CPU-IOFPGA	1.14
	MB-IOFPGA	1.01
	MB-MIFPGA	1.02
NC55-6X200-DWDM-S	Bootloader	1.12
	IOFPGA	0.11
	DENALI	13.48
	MORGOTH	5.17
	MSFPGA	2.22
	CFP2_PORT	5.23
NC55-36X100G-A-SE	MIFPGA	0.03
	Bootloader	0.13
	DBFPGA	0.14
	IOFPGA	0.21

PID	FPD Device	FPD Versions
NC55-5504-FC	Bootloader	1.75
	IOFPGA	0.07
NC55-RP-E	Bootloader	1.14
	IOFPGA	0.21
	OMGFPGA	0.48
NCS-55A1-24H	Bootloader	1.07
	CPU-IOFPGA	1.14
NCS-55A1-36H-SE-S	Bootloader	1.07
	CPU-IOFPGA	1.14
	MB-IOFPGA	1.01
	MB-MIFPGA	1.02
N540-24Z8Q2C-M	Bootloader	1.07
	CPU-IOFPGA	0.03
	MB-IOFPGA	0.16
	MB-MIFPGA	0.04

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

Other Important Information

- The total number of bridge-domains (2*BDs) and GRE tunnels put together should not exceed 1518.

  Here the number 1518 represents the multi-dimensional scale value.

- MLD Snooping is not supported until Cisco IOS XR Release 6.5.3. The support will be available in future releases.
- The offline diagnostics functionality is not supported in NCS 5500 platform. Therefore, the **hw-module service offline location** command will not work. However, you can use the **(sysadmin)# hw-module shutdown location** command to bring down the LC.
- The **hw-module profile mfib statistics** configuration command is not supported in this release.

Upgrading Cisco IOS XR Software

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

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

Related Documentation

The most current Cisco Network Convergence System 5500 Series documentation is located at this URL:

http://www.cisco.com/c/en/us/support/routers/network-convergence-system-5500-series/tsd-products-support-series-home.html

The document containing Cisco IOS XR System Error Messages (SEM) is located at this URL:

https://www.cisco.com/c/en/us/td/docs/ios_xr_sw/error/message/ios-xr-sem-guide.html

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.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Full Cisco Trademarks with Software License

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

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

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

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

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

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

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

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

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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