What's New for Cisco IOS XE 17.15.x

This chapter describes the new hardware and software features that are supported on the Cisco NCS 4201 and Cisco NCS 4202 Series routers.

For information on features supported for each release, see Feature Compatibility Matrix.

What's New in Hardware for Cisco IOS XE 17.15.3b

There are no new hardware features introduced for this release.

What's New in Software for Cisco IOS XE 17.15.3b

Feature	Description
IP Addressing	
Optimizing security and CPU utilization using software ACL in VRF traffic management	The Software ACL (SW ACL) is a platform-specific feature designed to control Layer 3 VRF traffic, such as ICMP, SSH, and Telnet, by managing traffic punted to the CPU. This feature enhances security and optimizes CPU utilization by allowing only explicitly permitted traffic to reach the CPU. The software ACLs enhances reliable and secure VRF-based services in enterprise networks and service provider networks. Command introduced: **platform sw_acl enable interface {icmp | ssh | telnet}**
MPLS	

Feature	Description
Support for Co-routed Inter-area Flex-LSP Tunnels in Point-to-Point OSPF network	Co-routed Flex LSP tunnels now support an inter-area and multiple areas in a Point-to-Point OSPF network. For example, in an inter-area OSPF network, both the head-end or tail-end for a bidirectional LSPs that are in different areas learn the network topology and perform the automatic path redundancy when there is a network link failure.

What's New in Hardware for Cisco IOS XE 17.15.2

There are no new hardware features introduced for this release.

What's New in Software for Cisco IOS XE 17.15.2

Feature	Description
Chassis	
NCCS 3GPP IP Specification Compliance for Interfaces	The router adheres to and complies with the IP specification guidelines as outlined by the National Centre for Communication Security (NCCS) certification, which is based on the 3rd Generation Partnership Project (3GPP) standards. This compliance ensures that the router meets rigorous security and performance benchmarks, providing users with a reliable and secure networking solution that aligns with industry best practices and regulatory requirements.
SNMP Dying Gasp support over IPv6 BGP Labeled Unicast Network	In addition to IPv4, SNMP dying gasp over FPGA is now extended to IPv6 BGP-Labeled Unicast (BGP-LU) network scenarios. This enhancement allows administrators to maintain and monitor their networks more effectively and robustly, ensuring reliable notification and management of critical network events across both IPv4 and IPv6 environments.

What's New in Hardware for Cisco IOS XE 17.15.1

Optics	Description
Management Port LED Status Indicators	The right LED indicator for the management port on the router now displays the link status and activity of the management port. You can monitor and troubleshoot the status and activity of the management port more effectively when the LED indicator turns green or in the Off state. For more details on the link status and activity, see the CPU Management Port LED Indication table.

What's New in Software for Cisco IOS XE 17.15.1

Feature	Description
Alarm Configuring and Monitoring	
SONET Alarms for APS	• With Automatic Protection Switching (APS), SONET alarms soaking as per the recommendation from GR-253. • Alarm is raised or cleared during APS manual, force, and lock out switch actions. • When traffic is switched to an alternate link in the APS group, the severity of the alarms is affected based on service impact.
SD-BER and SF -BER Alarms for T1/E1 and T3/E3 services	Signal Failure-Bit Error Rate (SF-BER) and Signal Degrade-BER (SD-BER) alarms are declared when there is a signal failure or signal degradation that happens in the traffic. These alarms may be raised when the error rate of a given entity exceeds the user-configured BER threshold value. This helps the administrator to take corrective actions.
CEM OCx	
DDS DS0 Remote Latching Loopback	DS0 loopback is used for testing and troubleshooting the T1 or E1, T3 or E3, and OCx channel over PSN. You can configure DS0 loopback on these controllers for remote devices.
Protection Switching Count for Protected SONET Interface	In SONET with redundancy, an Automatic protection switching (APS) occurs between working and standby protection networks due to reasons like a circuit failure. Whenever the switching happens, the switching count is tracked using a Protection Switching Count (PSC) parameter. Depending on the PSC count, you can debug the network to identify the reason for extensive switching and work on the corrective actions.
TCAM and NFT Commands	

Feature	Description
TCAM and NFT Commands	New commands have been introduced for the Ternary Content-Addressable Memory (TCAM) and NFT. **TCAM** You can now view the Ternary Content-Addressable Memory (TCAM) utilization for each control plane TCAM entry. Command: show platform hardware pp active tcam utilization control-plane-sessions **NFT** • You can now enable the collection of the packets punted to the CPU from the NFT hash table. Command: platform nft-summarization enable • Once the above command is enabled, you can use a timer to clean up the NFT hash table. Command: platform nft-summarization timer-value • You can view a summary of the packets punted to the CPU from the NFT hash table. Command: show platform hardware pp active infrastructure pi nft summary