What's New for Cisco IOS XE 17.15.x

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	
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	
Alarms to Monitor Unsupported Slot Compatibility in IM	When an interface module (IM) is inserted into an unsupported slot, an **IM_NOT_SUPPORTED** syslog message is generated. Additionally, new unsupported alarms such as **IM_NOT_SUPPORTED**, **INVALID_COMBINATION**, **INVALID_MODE**, and**SPA_MISMATCH** are asserted when an IM is inserted into a router slot that is not supported. You can view the alarm status and unsupported slot information using the **show facility-alarm status** CLI command. This enhancement ensures administrators are promptly alerted to any compatibility issues, enabling them to take corrective action and maintain network stability.
Suppressing Extraneous Alarms for Admin-Down Interfaces	Extraneous alarms along with SNMP traps, can be generated on TDM or Ethernet interfaces even when these interfaces are in an administratively down state. These unnecessary alarms can lead to redundant monitoring and troubleshooting efforts. These alarms are suppressed by default. To mitigate this issue, you can disable this feature or unsuppress these alarms using the following command the router: **platform enable-transceiver-sensor-alarm-on-admin-down** This ensures that only relevant alarms are captured and displayed. This helps streamline network management and improves operational efficiency.
Performance Routing	
Hardware Resource and Scale Monitoring	A new command has been introduced for hardware resource and scale monitoring. You can now view the current utilizations and the maximum capacities available in the hardware for various resources. Command: show platform hardware pp active resource-usage monitor

What's New in Hardware for IOS XE 17.15.1b

There are no new hardware features introduced for this release.

What's New in Software for IOS XE 17.15.1b

Feature	Description
Alarms	
New APS Alarms and Conditions	New APS alarms and conditions have been introduced to enhance network monitoring and management. These alarms are raised or cleared during APS manual, forced, and lockout switch actions, providing real-time alerts on network changes. This advanced alerting mechanism ensures that network operators are immediately informed of any alterations, enabling them to swiftly respond to and manage network conditions, thereby maintaining optimal performance and reliability.
SONET Alarms for APS	In APS scenarios, the existing SONET alarms follow the GR-253 standard for alarm soaking. This standardization helps filter out transient conditions by defining specific assertion and clearing times for alarms.
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 administrator to take corrective actions.
CEM	
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.
Protected TAP on FRR Protected Core	You can now monitor CEM traffic through protected TAP and split TAP sessions on the protected Fast Reroute (FRR) core interface. During events such as link failure or connectivity issues, the automatic switching happens from active to standby path. Thus, you can monitor and debug the issue without affecting the traffic on these FRR protected core interfaces.
Protection Switching Count for Protected SONET Interface	In SONET networks with redundancy, Automatic Protection Switching (APS) seamlessly transitions traffic between working and standby protection links, typically due to circuit failures or other disruptions. Each switching event is tracked using the Protection Switching Count (PSC) parameter. This parameter allows network operators to monitor and analyze the frequency of these switches in real-time. By examining the PSC count, users can diagnose the network to identify the root causes of frequent switching events and implement necessary corrective actions. This advanced capability significantly enhances network reliability and performance, offering users a robust and efficient solution for maintaining optimal service quality.

Feature	Description
Clear Counters command	• Unlike the previous release, where the **clear counters** command reset the old dataset, from this release onwards, the command resets all the PMON datasets, including the current dataset. • You can clear the PMON data for a specific interface module on the device using the **clear controller hw-module** command
GR-820-CORE specific Performance Monitoring	The **show controller tabular** enables you to view the performance monitoring details in tabular form as per GR-820-Core standards.
Chassis	
Alarms to Monitor Standby RSP Upgrade During IOS Version Mismatch	During an upgrade, for a high availability setup, if the IOS version of the active Route Switch Processor (RSP) does not match the IOS version of the standby RSP, a Syslog message, **IPC: IOS versions do not match** is printed on the console. The upgrade process is aborted and there are no alarms to notify the IOS version mismatch or the progress of the standby upgrade. From Cisco IOS XE 17.15.1, show commands have been enhanced to display Syslog messages for any active and standby RSP version mismatch, and the IOS XE image from the active RSP is copied to the standby RSP. You can execute the following show commands on the active RSP to monitor the progress of the upgrade: • **show facility-alarm status** • **show facility-condition status** The NCS 4206/16-RSP3 module supports this feature. See the High Availability Configuration Guide for the upgrade process.
Alarm for Incompatible SFP	When an incompatible SFP is used in Ethernet interface modules on the RSP3 node, a *Transceiver NOT_COMPATIBLE* alarm is raised.
High Availability	
Monitoring alarms for standby RSP management interface	In addition to Active RSP, alarms are now generated for the management interface of the Stand-by RSP. You can monitor these alarms in Cisco's Evolved Programmable Network Manager (EPNM) and take the appropriate action to fix the problem.
In-Service Software Upgrade (ISSU) Enhancements	During the ISSU upgrade, the system verifies if the new software image is already available in the active and standby boot flash before the binary image expansion. This helps to reduce the ISSU upgrade time on multiple devices. Syslog messages are generated during this ISSU upgrade for each stage. If alarms are generated, they are captured at each stage and sent to SNMP. You can monitor the ISSU process using the show facility-alarm status CLI command. These enhancements are supported only on RSP3 modules.
QoS	

Feature	Description
Displaying ASIC QoS Policer Values for Egress Traffic	In addition to Ingress traffic, you can now view the programmed hardware (ASIC) values of the QoS features configured for Egress traffic. Use the following command to enable ASIC values: **platform qos-egress-hw-param enable** The programmed hardware (ASIC) value may differ from the configured software value due to hardware limitations. Now, you can compare the actual QoS policer value programmed in the hardware with the value you configured in the software for egress traffic.
Timing and Synchronization	
Improved Network Synchronization Redundancy with an External BITS Clock	The T4 PLL in the route processor can now send a SyncE signal through the BITS port to an external clocking device. If equipped with a high-quality oscillator, the external clocking device can clean up the timing signal to reduce the jitter. When returned to the T0 PLL through the same BITS port, the cleaned-up signal can be sent to other nodes to propagate network synchronization. This functionality is useful when an external BITS clock cannot receive timing inputs from a Primary Reference Source (PRS). The system can fall back on using the SyncE signal received from a peer router to provide redundancy to the network synchronization operation. Command introduced: **network-clock timing-source** bits Compliance: BITS implementation and SyncE recommendations from GR-436 and G.8264 standards Supported Interface Module: RSP3

What's New in Hardware for Cisco IOS XE 17.15.1

There are no new hardware features introduced for this release.

What's New in Software for Cisco IOS XE 17.15.1

Feature	Description
Alarms	
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.

Feature	Description
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	
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 links 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	
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