



What's New in Cisco IOS XE 17.14.x

- [Hardware Features in Cisco IOS XE 17.14.1, on page 1](#)
- [Software Features in Cisco IOS XE 17.14.1, on page 1](#)
- [Hardware and Software Behavior Changes in Cisco IOS XE 17.14.1, on page 2](#)

Hardware Features in Cisco IOS XE 17.14.1

There are no new hardware features in this release.

Software Features in Cisco IOS XE 17.14.1

Feature Name	Description
IP SLA Probe Configuration Modification Capability	Introduces support to reconfigure the parameters of a scheduled IP SLA session using the configure replace command.
mDNS Protocol Options	The mDNS protocol option is introduced in the device sensor filter spec command. This allows the user to apply the mDNS protocol TLV filter list to the device sensor output. The device sensor filter list mdns command is introduced to create a mDNS protocol filter containing a list of Type-Length-Value (TLV) fields that can be included or excluded in the device sensor output. The tlv command is introduced to configure the list of Type Length Value (TLVs) in mDNS protocol configuration mode.
OSPF Local RIB Path Limit Enhancement	The OSPF Local RIB Path Limit feature is designed to restrict the number of paths stored by OSPF in its Local RIB, offering enhanced control over network path selection. With the maximum-paths command enabled, the network administrators can now control the number of paths OSPF installs in the Local RIB for a specific prefix.
Precision Time Protocol	Precision Time Protocol (PTP) is defined in IEEE 1588 as Precision Clock Synchronization for Networked Measurements and Control Systems, and was developed to synchronize the clocks in packet-based networks that include distributed device clocks of varying precision and stability. This feature is implemented on the Cisco Catalyst 9200CX Compact Series Switches.

Feature Name	Description
Programmability: <ul style="list-style-type: none"> • gNMI: Stream Subscriptions with on-Change Mode • gNMI: SubscribeResponse with sync_response • YANG Data Models • YANG Support for Mutiple Next-Hops 	The following programmability features are introduced in this release: <ul style="list-style-type: none"> • gNMI: Stream Subscriptions with on-Change Mode: gNMI telemetry supports on-change subscriptions on the same set of models as other telemetry protocols. • gNMI: SubscribeResponse with sync_response: The sync_response is a boolean field that is part of the SubscribeResponse response message. The sync_response message is sent after the first update message. • YANG Data Models: For the list of Cisco IOS XE YANG models available with this release, navigate to: https://github.com/YangModels/yang/tree/main/vendor/cisco/xe/17141. • YANG Support for Mutiple Next-Hops: A new container is added under the next-hop-options choice node to retrieve all next-hops for a given route or prefix. Also, an uptime leaf node is added to provide the timestamp for each next hop.
show reload history command	The show reload history command is introduced. It displays the reason for device reload and its history.
spanning-tree bpdud sender-conflict command	This feature allows the user to enable spanning tree protocol BPDU sender conflict feature using the spanning-tree bpdud sender-conflict command. When the device is in RSTP mode, BPDU packets are transmitted every two seconds from a designated port to a non-designated port. When you use the spanning-tree bpdud sender-conflict command, if there is any change in the RSTP mode due to sender conflict, the device generates a notification.

New on the WebUI

There are no new WebUI features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE 17.14.1

Behavior Change	Description
Switch Integrated Security Features (SISF) – Enhanced Throttling Limit for ARP Packets	<p>In Cisco IOS XE Amsterdam 17.3.1, a throttling limit was introduced to mitigate high CPU utilization scenarios. In a five second window, a maximum of 50 ARP broadcast packets per source IP were processed by SISF.</p> <p>In Cisco IOS XE 17.14.1, this limit is increased to a maximum of 100 ARP broadcast packets for each source IP. When the limit is reached, incoming ARP packets are dropped.</p>