



What's New in Cisco IOS XE Dublin 17.12.x

- [Hardware Features in Cisco IOS XE Dublin 17.12.4, on page 1](#)
- [Software Features in Cisco IOS XE Dublin 17.12.4, on page 1](#)
- [Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.4, on page 2](#)
- [Hardware Features in Cisco IOS XE Dublin 17.12.3, on page 2](#)
- [Software Features in Cisco IOS XE Dublin 17.12.3, on page 2](#)
- [Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.3, on page 2](#)
- [Hardware Features in Cisco IOS XE Dublin 17.12.2, on page 2](#)
- [Software Features in Cisco IOS XE Dublin 17.12.2, on page 2](#)
- [Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.2, on page 3](#)
- [Hardware Features in Cisco IOS XE Dublin 17.12.1, on page 3](#)
- [Software Features in Cisco IOS XE Dublin 17.12.1, on page 4](#)
- [Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.1, on page 6](#)

Hardware Features in Cisco IOS XE Dublin 17.12.4

There are no new hardware features in this release.

Software Features in Cisco IOS XE Dublin 17.12.4

Feature Name	Description
Link Debounce	<p>The Link Debounce Timer delays notification of a link up or down status change. Delayed notification of a link status change can decrease traffic loss due to network reconfiguration when network ethernet port experiences minor faults in the link. The Link Debounce Up Timer is a new enhancement of the feature which delays notification of a link from down to up status change.</p> <p>The feature was implemented on Cisco Catalyst 9600 Series Supervisor 2 Module at the global level only. Per port configuration is not supported.</p>

Feature Name	Description
Enabling Third-Party Optics During AutoInstall	<p data-bbox="448 289 1484 541">During AutoInstall, the system will detect, third-party optics automatically. Unlike the default boot up process, the third-party optics will not move to err-disabled state during AutoInstall. In the default boot up process, you need to configure the service unsupported-transceiver command to detect the third party optics after system boot. When AutoInstall is successful, the third-party optics are enabled. In all other cases, these optics will be in the err-disabled state. The service unsupported transceiver command is not saved into the startup configuration, and when the configuration is saved using the write memory command, and the system is reloaded, the third-party optics will move into the err-disabled state.</p> <p data-bbox="448 562 1484 625">This feature is enabled by default. You can use the no service unsupported-transceiver command to disable the third-party optics, after the auto install is complete.</p>

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.4

There are no behavior changes in this release.

Hardware Features in Cisco IOS XE Dublin 17.12.3

There are no new hardware features in this release.

Software Features in Cisco IOS XE Dublin 17.12.3

There are no new software features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.3

There are no behavior changes in this release.

Hardware Features in Cisco IOS XE Dublin 17.12.2

There are no new hardware features in this release.

Software Features in Cisco IOS XE Dublin 17.12.2

There are no new software features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.2

There are no behavior changes in this release.

Hardware Features in Cisco IOS XE Dublin 17.12.1

Feature Name	Description
Cisco 100GBASE QSFP-100G Modules	<p>Supported transceiver module product numbers:</p> <ul style="list-style-type: none"> • QSFP-100G-SR1.2 <p>Compatible line cards:</p> <ul style="list-style-type: none"> • C9600-LC-24C, C9600-LC-40YL4CD and C9600X-LC-32CD line cards on Cisco Catalyst 9600X Supervisor Module 2 (C9600X-SUP-2) • C9600-LC-24C and C9600-LC-40YL4CD line cards on Cisco Catalyst 9600 Supervisor Module 1 (C9600-SUP-1) <p>For information about the modules, see Cisco 100GBASE QSFP-100G Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.</p>
	<p>Supported transceiver module product numbers:</p> <ul style="list-style-type: none"> • QSFP-100G-ZR4-S <p>Compatible line cards:</p> <ul style="list-style-type: none"> • C9600-LC-24C, C9600-LC-40YL4CD and C9600X-LC-32CD line cards on Cisco Catalyst 9600X Supervisor Module 2 (C9600X-SUP-2) <p>For information about the modules, see Cisco 100GBASE QSFP-100G Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.</p>

Software Features in Cisco IOS XE Dublin 17.12.1

Feature Name	Description
BGP EVPN VXLAN <ul style="list-style-type: none"> • ARP inspection and DHCP Rogue Server Protection in VXLAN Environment (L2 VNIs) • BGP EVPN VRF Auto RD and Auto RT 	<p>The following BGP EVPN VXLAN features are introduced in this release:</p> <ul style="list-style-type: none"> • ARP inspection and DHCP Rogue Server Protection in VXLAN Environment (L2 VNIs): BGP EVPN VXLAN fabric now supports ARP inspection and DHCP Rogue Server Protection. To configure these features, enable ARP inspection and DHCP Snooping on the VTEPs of the EVPN VXLAN fabric. • BGP EVPN VRF Auto RD and Auto RT: BGP EVPN Layer 3 overlay VRF configuration is simplified with the introduction of new CLIs to auto generate the route distinguisher (RD) and route target (RT) for a VRF. <p>You can enable the auto generation of RD either at a global level, using the vrf rd-auto command or specifically for a VRF, using the rd-auto [disable] command in the VRF submode.</p> <p>To enable auto assignment of RT for a VRF, use the vnid vni-id command in the VRF submode.</p> <p>You can also choose to disable the auto RD and RT features by using the no form of the command.</p>
DSCP marking for RADIUS packets for administrative sessions	Allows you to configure DSCP marking for RADIUS packets for administrative sessions such as SSH and Telnet.
Interface ID Option in DHCPv6 Relay Message	Introduces support for interface ID option in DHCPv6 Relay message. With this, the physical interface details of the client interface are included along with the VLAN number in the message.
Interface Template Support for IPv6 DHCP Guard	Enables you to add the ipv6 dhcp guard attach-policy policy_name global configuration command to an interface template. IPv6 DHCP Guard is then enabled and the policy is applied, wherever the template is applied.
IP DHCP Server Changes to Limit IP Assignment to Next Hop only	Allows you to assign DHCP IP address only to the neighbouring device in an interface using the ip dhcp restrict next hop command. When this command is enabled, the DHCP server in the interface uses the MAC addresses in the DHCP packet and compares it with the addresses in the Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP) cache table. If the MAC addresses match, then the DHCP IP address is assigned to that device.

Feature Name	Description
Modified Trustpoints for Secure Unique Device Identity (SUDI) Certificates	<p>Starting from Cisco IOS XE Dublin 17.12.1, the following changes have been introduced for trustpoints.</p> <ul style="list-style-type: none"> Trustpoint names for existing SUDI certificates <p>If your device supports Cisco Manufacturing CA III certificate and is not disabled, the trustpoint names are as follows.</p> <ul style="list-style-type: none"> For <i>Cisco Manufacturing CA III</i> certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA3_SUDI For <i>Cisco Manufacturing CA SHA2</i> certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA2_SUDI <p>If your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled using no platform sudi cmca3 command, the trustpoint names are as follows.</p> <ul style="list-style-type: none"> For <i>Cisco Manufacturing CA SHA2</i> certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA2_SUDI For <i>Cisco Manufacturing CA</i> certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA_SUDI <ul style="list-style-type: none"> Hardware SUDI certificates <ul style="list-style-type: none"> If your device supports <i>High Assurance SUDI CA</i> certificate, this certificate is loaded under CISCO_IDEVID_SUDI trustpoint. If your device does not support <i>High Assurance SUDI CA</i> certificate, <i>ACT2 SUDI CA</i> certificate is loaded under CISCO_IDEVID_SUDI trustpoint. <ul style="list-style-type: none"> show ip http server status command output <p>If you configure the trustpoint for the HTTP server as CISCO_IDEVID_SUDI, the output of show ip http server status command displays the operating trustpoint along with the configured trustpoint.</p> <p>The following example shows a sample output of show ip http server status command with both the configured and the operating trustpoint names. Note that if your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled, the operating trustpoint in the below output displays CISCO_IDEVID_CMCA2_SUDI.</p> <pre>Device# show ip http server status ... HTTP secure server trustpoint: CISCO_IDEVID_SUDI HTTP secure server operating trustpoint: CISCO_IDEVID_CMCA3_SUDI</pre>
Optimized Layer 2 Overlay Multicast for IPv4 and IPv6 traffic	<p>Optimized Layer 2 Overlay Multicast forwards multicast traffic within the Layer 2 Virtual Network Instance (L2VNI).</p> <p>Support for optimized Layer 2 overlay multicast was introduced on the Cisco Catalyst Series Supervisor 2 Module (C9600X-SUP-2).</p>

Feature Name	Description
Programmability: <ul style="list-style-type: none"> • NETCONF-SSH Algorithms • YANG Data Models 	The following programmability features are introduced in this release: <ul style="list-style-type: none"> • NETCONF-SSH Algorithms: The NETCONF-SSH server configuration file contains the list of all supported algorithms. From this release onwards, you can enable or disable these algorithms at runtime by using Cisco IOS commands or YANG models. • YANG Data Models: For the list of Cisco IOS XE YANG models available with this release, navigate to: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/17121.
show idprom tan command	The show idprom tan command was introduced. It displays the top assembly part number and top assembly part revision number for the identification programmable read-only memory.

New on the WebUI

There are no new WebUI features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.1

Behavior Change	Description
ip mtu command	On the C9600X-SUP-2 Supervisor Module, the ip mtu command has been modified to perform IPv4 and IPv6 fragmentation on the specified IP MTU value.
BDPU Guard and Root Guard Syslogs	The BDPU guard and root guard syslogs have been modified to include client bridge ID information.