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

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

There are no new hardware features in this release.

Software Features in Cisco IOS XE Dublin 17.12.1

Feature Name	Applicable Models	Description
BGP EVPN VXLAN • ARP inspection and DHCP Rogue Server Protection in VXLAN Environment (L2 VNIs) • BGP EVPN VRF Auto RD and Auto RT	All Models	The following BGP EVPN VXLAN features are introduced in this release: • 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. 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. To enable auto assignment of RT for a VRF, use the **vnid** *vni-id* command in the VRF submode. You can also choose to disable the auto RD and RT features by using the **no** form of the command.

Feature Name	Applicable Models	Description
DSCP marking for RADIUS packets for administrative sessions	All Models	Allows you to configure DSCP marking for RADIUS packets for administrative sessions such as SSH and Telnet.
Interface ID Option in DHCPv6 Relay Message	All Models	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	All Models	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	All Models	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	Applicable Models	Description
Modified Trustpoints for Secure Unique Device Identity (SUDI) Certificates	All Models	

Feature Name	Applicable Models	Description
		Starting from Cisco IOS XE Dublin 17.12.1, the following changes have been introduced for trustpoints. • Trustpoint names for existing SUDI certificates If your device supports Cisco Manufacturing CA III certificate and is not disabled, the trustpoint names are as follows. • For *Cisco Manufacturing CA III* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA3_SUDI • For *Cisco Manufacturing CA SHA2* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA2_SUDI 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. • For *Cisco Manufacturing CA SHA2* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA2_SUDI • For *Cisco Manufacturing CA* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA_SUDI • Hardware SUDI certificates • If your device supports *High Assurance SUDI CA* certificate, this certificate is loaded under CISCO_IDEVID_SUDI trustpoint. • If your device does not support *High Assurance SUDI CA* certificate, *ACT2 SUDI CA* certificate is loaded under CISCO_IDEVID_SUDI trustpoint. • **show ip http server status** command output 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. 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. `Device# show ip http server status` …

Feature Name	Applicable Models	Description
		`HTTP secure server trustpoint: CISCO_IDEVID_SUDI` `HTTP secure server operating trustpoint: CISCO_IDEVID_CMCA3_SUDI`
Optimized Layer 2 Overlay Multicast for IPv4 and IPv6 traffic	9500X	Optimized Layer 2 Overlay Multicast forwards multicast traffic within the Layer 2 Virtual Network Instance (L2VNI). Support for optimized Layer 2 overlay multicast was introduced on the Cisco Catalyst 9500X Series Switches.
Programmability: • NETCONF-SSH Algorithms • YANG Data Models	All Models	The following programmability features are introduced in this release: • 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	All Models	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.
Support for NetFlow Version 5 and 32-bit Autonomous System Number Field	9500H	Support was introduced for Netflow Version 5 protocol and the 32-bit Autonomous System Number field.

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 Catalyst 9500X Series Switches, the **ip mtu** command has been modified to perform IPv4 and IPv6 fragmentation on the specified IP MTU value.

Behavior Change	Description
BDPU Guard and Root Guard Syslogs	The BDPU guard and root guard syslogs have been modified to include client bridge ID information.
ROMMON and FPGA Auto-upgrade	On the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models of the Cisco Catalyst 9500 Series Switches, support for auto-upgrade of the ROMMON and field-programmable gate array (FPGA) have been introduced. Auto-upgrade to this release is supported only if the bootloader version is 17.10.1r or a later release.