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

Feature Name	Description

Cisco Catalyst 9400 Series 12-Port 40G/100G Module (C9400-LC-12QC)	A 12-port fiber optic Ethernet switching module with these key hardware and software features:
	
	Hardware Features:
	
	• Can be installed on Cisco Catalyst C9404R, C9407R, and C9410R chassis. See Cisco Catalyst 9400 Series Switches Hardware Installation Guide.
	
	• Supports a maximum bandwidth of 480 Gbps. See Cisco Catalyst 9400 Series Switch Line Cards Data Sheet.
	
	• Compatible with supervisor modules C9400X-SUP-2 and C9400X-SUP-2XL only. See Cisco Catalyst 9400 Series Line Card Installation Note.
	
	• Supports 10, 25, 40, and 100 Gbps connectivity.
	
	    • Port nos. 1 through 12 can be used interchangeably as 10 or 40 Gbps ports, with a suitable transceiver installed.
	
	    • Port nos. 9 through 12 can also be configured as 25 or 100 Gbps ports, with a suitable transceiver and the required software configuration. When a port is configured to operate at 100 Gbps or 25 Gbps, one port from 5 to 8 and belonging to the same port group, is disabled. For example, if port no. 9 is configured to operate at 100 Gbps speeds, port no. 5 is disabled.
	
	  See Example: 100 Gbps and 40 Gbps Configuration on C9400-LC-12QC.
	
	Software Features:
	
	• For 25 or 100 Gbps support on port nos. 9 through 12, configure the **enable mode 100G** command in interface configuration mode. See Configuring Interface Characteristics and Interface and Hardware Commands.
	
	• Supports Cisco StackWise Virtual on all ports. See Configuring Cisco StackWise Virtual. When Cisco StackWise Virtual is configured on ports 9 through 12, they can operate only at 100 Gbps speeds

Feature Name	Description

Cisco Catalyst 9400 Series 24-Port 10G/25G Module (C9400-LC-24XY)	A 24-port fiber optic Ethernet switching module with these key hardware and software features:
	
	Hardware Features:
	
	• Can be installed on Cisco Catalyst C9404R, C9407R, and C9410R chassis. See Cisco Catalyst 9400 Series Switches Hardware Installation Guide.
	
	• Supports a maximum bandwidth of 480 Gbps. See Cisco Catalyst 9400 Series Switch Line Cards Data Sheet.
	
	• Compatible with supervisor modules C9400X-SUP-2 and C9400X-SUP-2XL only. See Cisco Catalyst 9400 Series Line Card Installation Note.
	
	• Supports 1, 10, and 25 Gbps connectivity.
	
	    • Port nos. 1 through 4 can be used interchangeably as 1 or 10 Gbps ports, with a suitable transceiver installed.
	
	    • Port nos. 5 through 24 can be used interchangeably as 1 or 10 or 25 Gbps ports, with a suitable transceiver installed.
	
	See Example: 25 Gbps and 10 Gbps Connectivity on C9400-LC-24XY.
	
	Software Features:
	
	• Supports Cisco StackWise Virtual on all ports. See Configuring Cisco StackWise Virtual.

Software Features in Cisco IOS XE Dublin 17.12.1

Feature Name	Description
BGP EVPN VXLAN • ARP inspection and DHCP Rogue Server Protection in VXLAN Environment (L2 VNIs) • BGP EVPN VRF Auto RD and Auto RT	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	Description
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.
EPC support of AppGigabitEthernet	Introduces support for configuring the AppGigabitEthernet port as an interface for Embedded Packet Capture (EPC).
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	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 … HTTP secure server trustpoint: CISCO_IDEVID_SUDI HTTP secure server operating trustpoint: CISCO_IDEVID_CMCA3_SUDI ```

Feature Name	Description
Programmability: • NETCONF-SSH Algorithms • YANG Data 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	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
BDPU Guard and Root Guard Syslogs	The BDPU guard and root guard syslogs have been modified to include client bridge ID information.
C9400-LC-48XS Linecard idprom value for max_power	For some C9400-LC-48XS linecards with hardware version less than 3.1 (use the **show module** command to check), the idprom value for max_power is incorrectly programmed to 360. The correct value is 250. This will cause the device to overbudget by ~100W for each of these linecards. No field failures have been observed due to this issue. However, rare scenarios exist where the device can run out of power budget.