Whats New in Cisco IOS XE Dublin 17.11.x

Hardware Features in Cisco IOS XE Dublin 17.11.99SW

There are no new hardware features in this release.

Software Features in Cisco IOS XE Dublin 17.11.99SW

Feature Name	Description
Tenant Routed Multicast over BGP EVPN VXLANv6	Tenant Routed Multicast over BGP EVPN VXLANv6 enables the delivery of IPv4 and IPv6 multicast host traffic in BGP EVPN overlay multi-tenant fabric in an efficient and resilient manner. The new software capability enables IPv4 and IPv6 multicast in overlay with underlay network infrastructure natively running single-stack IPv6. The Tenant Routed Multicast over BGP EVPN VXLANv6 is supported over IPv6 Default MDT group. For more information, see Configuring Tenant Routed Multicast over BGP EVPN VXLANv6.

New on the WebUI
There are no new WebUI features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.11.99SW

There are no behavior changes in this release.

Hardware Features in Cisco IOS XE Dublin 17.11.1

Feature Name	Description
Cisco 100GBASE QSFP-100G Modules on Cisco Catalyst 9500 Series Switches - High Performance and 9500X Series Switches	Supported transceiver module product numbers: • QSFP-100G-FR-S For information about the module, see Cisco 100GBASE QSFP-100G Modules. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Software Features in Cisco IOS XE Dublin 17.11.1

Feature Name	Description
BGP EVPN VXLAN • Cisco StackWise Virtual Support in BGP EVPN VXLAN • Dynamic BGP Peering for EVPN • EVPN Microsegmentation • EVPN Route Map Support • Layer 3 TRM with Data MDT • Multi-Homing in a BGP EVPN VXLAN Fabric	The following BGP EVPN VXLAN features are introduced in this release: • Cisco StackWise Virtual Support in BGP EVPN VXLAN: Introduces support for Cisco StackWise Virtual with BGP EVPN VXLAN on the Cisco Catalyst 9500X Series Switches. • Dynamic BGP Peering for EVPN: Introduces support for BGP dynamic neighbor sessions to the L2VPN EVPN address family. • EVPN Microsegmentation: BGP EVPN VXLAN integrates Cisco TrustSec to provide microsegmentation and end-to-end access control with the propagation of the security group tag (SGT). Using security group-based access control lists (SGACLs), you can control the operations that a user can perform, based on the security group assignments and destination resources in a VXLAN campus fabric. • EVPN Route Map Support: The Leaf, Spine, and Border nodes of a BGP EVPN fabric now support route map for the L2VPN address-family. With route map support, the BGP attributes and their values can be modified to customize the routing policy based on the requirement. The routing policy can be applied for both inbound and outbound EVPN routes. • Layer 3 Tenant Routed Multicast (TRM) with Data Multicast Distribution Tree (MDT): Introduces support for Layer 3 TRM with Data MDT on the Cisco Catalyst 9500X Series Switches. • Multi-Homing in a BGP EVPN VXLAN Fabric: BGP EVPN is enhanced to restrict the ethernet segment operations to the EVPN-controlled VLANs on the trunk port. This allows traditional Layer 2 domains to co-exist with Layer 2 VNI-enabled VLANs at access layer. It also allows selective VLAN migration to overlay VXLAN segmentation.
Cisco StackWise Virtual	Cisco StackWise Virtual is a network system virtualization technology that pairs two switches into one virtual switch to simplify operational efficiency with a single control and management plane. Starting with this release, the feature is supported on the C9500X-60L4D model of Cisco Catalyst 9500X Series Switches.
Custom EtherTypes	Introduces support for configuring 0x9100 and 0x88a8 custom ethertypes. Use **switchport dot1q ether type** command in the interface configuration mode to configure this feature. This feature is supported only on Cisco Catalyst 9500X Series Switches.
Default Limits for redistributed routes and LSA in OSPF	Default values have been assigned to the number of redistributed routes and LSAs in OSPF to prevent the device being flooded with routes. The default values for redistributed routes is 10240 routes. The default value for LSAs is 50,000 LSAs. You can customize the default values.

Feature Name	Description
Deprecation of Weak Ciphers	The minimum RSA key pair size must be 2048 bits. The compliance shield on the device must be disabled using the **crypto engine compliance shield disable** command to use the weak RSA key.
IPv6 support for SGACL	Introduces support for IPv6 addressing of SGT and SGACL on the C9500X-28C8D. This allows dynamic learning of mappings between IP addresses and SGTs for IPv6 addresses.
LAN MACsec over MPLS	Introduces support for MACsec with MPLS. This feature allows MPLS packets to be encrypted with a MACsec tag. This feature is not supported on Cisco Catalyst 9500X Series Switches.
MPLS VPN Inter-AS Option A	Introduces support for MPLS VPN Inter-AS Option A on the C9500X-28C8D. Inter-AS Option A is the simplest to configure, and it provides back to back virtual routing and forwarding (VRF) connectivity.
NETCONF support for PTPv2	Introduces support for configuring PTPv2 with NETCONF. NETCONF provides a mechanism to install, manipulate, and delete the configuration of network devices.
Policy- Based Routing (PBR)	Introduces support for policy-based routing on Cisco Catalyst 9500X Series Switches. You can use PBR to configure a defined policy for traffic flows.

Feature Name	Description
Programmability • gNMI Dial-Out Telemetry • Multicast Routing Support on the AppGigabitEthernet Port • PROTO Encoding • Secure Zero-Touch Provisioning • YANG Data Models	The following programmability features are introduced in this release: • gNMI Dial-Out Telemetry: This feature introduces a tunnel service for gNMI dial-out connections. Using this feature, you can use the device (that acts as a tunnel client) to dial out to a collector (that acts as a tunnel server). The tunnel server forwards requests from gNMI or gNOI clients. • Multicast Routing Support on the AppGigabitEthernet Port: Multicast traffic forwarding is supported on the AppGigabitEthernet interface. Applications can select the networks that allow multicast traffic. This feature is supported only on Cisco Catalyst 9500 Series Switches - High Performance. • PROTO Encoding: gNMI protocol supports PROTO encoding. The gnmi.proto file represents the blueprint for generating a complete set of client and server-side procedures that instantiate the framework for the gNMI protocol. • Secure Zero-Touch Provisioning: Secure ZTP is a technique to securely provision a device, while it is booting in a factory-default state. The provisioning updates the boot image, commits an initial configuration, and executes customer-specific scripts. The provisioned device can establish secure connections with other systems. This feature is supported only on Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance. • 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/17111.
Pseudowire Redundancy	Introduces support for L2VPN pseudowire redundancy Cisco Catalyst 9500X Series Switches. This feature allows you to configure your network to detect a failure in the network and reroute the Layer 2 service to another endpoint that can continue to provide service.
show aaa dead-criteria radius enhancement command	The **show aaa dead-criteria radius enhancement** command allows you to use the configured radius server name as the input to identify the unique server in the server group and print the server dead criteria configuration.
show access-session command	The **info** keyword was introduced for the **show access-session** command.
Silent Host Handling	The **silent-host-detection** keyword was introduced for the following commands: • **database-mapping** • **show lisp instance-id ipv4 database** • **show lisp instance-id ipv6 database** • **show lisp instance-id ipv4 server** • **show lisp instance-id ipv6 server**

Feature Name	Description
Support for RFC8781 - PREF64 in IPv6 RA	Introduces the **ipv6 nd ra nat64-prefix** command to configure NAT64 prefix information in an IPv6 router advertisement (RA) on an interface. This feature can be enabled only if NAT64 is already configured on the device.
TCN Flood	The **no ip igmp snooping tcn flood** command was introduced to disable the flooding of multicast traffic during a spanning-tree Topology Change Notification (TCN) event.

New on the WebUI
There are no new WebUI features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.11.1

Behavior Change	Description
Deprecation of **snmp-server enable traps license** global configuration command	The command was deprecated. The associated MIB, CISCO-LICENSE-MGMT-MIB, is also no longer supported. In place of the deprecated command and unsupported MIB, use CISCO-SMART-LIC-MIB. On devices where In-Service Software Upgrade (ISSU) is supported, before you perform an ISSU upgrade, you must manually remove the **snmp-server enable traps license** global configuration command if it is present in startup configuration. If the command is present in the configuration during an ISSU upgrade, it causes an ISSU configuration synchronization failure. Enter the **no** form of the command to remove it from the configuration and save changes by entering the **copy running-config startup-config** command in privileged EXEC mode.
New flag for the IPv6 SGACL monitor mode	A new flag has been introduced for the IPv6 SGACL monitor mode. This was introduced to address hardware limitation of a single counter shared for IPv4 and IPv6 traffic. The HW_Monitor counter gets incremented irrespective of the type of traffic, which in turn updates the monitor mode flag. With a separate flag for IPv6 and IPv4 SGACL monitor mode, only the corresponding protocol flag is updated depending on the type of traffic.
show power and **show power detail** command output	The **show power** and **show power detail** command outputs are modified to display the correct power information of the standby switch.