What's New for Cisco IOS XE Dublin 17.11.x

This chapter describes the new hardware and software features supported in Cisco IOS XE Dublin 17.11.x.

For information on features supported for each release, see Feature Compatibility Matrix .

What's New in Hardware for Cisco IOS XE Dublin 17.11.1a

There are no new features in this release.

What's New in Software for Cisco IOS XE Dublin 17.11.1a

Feature	Description
CEM	
Support for 3-in-24 BERT patterns	Support for 3-in-24 BERT patterns on the following interface modules and modes: • 48-port T1 or E1 interface module • 48-port T3/E3 interface module • 1-Port OC-48 or 4-Port OC-12/OC-3 interface module • NCS 4200 Combo 8-Port SFP GE and 1-Port 10 GE 20G Interface Module (NCS4200-1T8S-20CS) • STS-1 mode

Feature	Description
System CESoP NxDS0 BERT	You can configure BERT patterns at the DS0 level on the following interface modules for both the system and line directions. • 48-Port T1 or E1 CEM interface module • 48-Port T3 or E3 CEM interface module • 1-port OC-48/STM-16 or 4-port OC-12/OC-3 / STM-1/STM-4 + 12-port T1/E1 + 4-port T3/E3 CEM interface module • NCS 4200 Combo 8-port SFP GE and 1-port 10 GE 20G interface module You can configure speed with bandwidth of 56 kbps or 64 kbps along with the BERT pattern. With DS0 level BERT configuration, you can verify the end-to-end connectivity.
Frame Relay Port Mode	Frame Relay (FR) port mode provides transport between two Provider Edge (PE) devices, where the complete FR frame is transported using the same encapsulation configured for the HDLC or FR pseudowire. On the PE device, the multiple FR Virtual Circuits (VCs) are carried over a single interface and the traffic is passed into a single transparent HDLC or FR pseudowire in an MPLS network. Thus with port mode, there are many-to-one mappings between multiple FR VCs and a pseudowire in a secure manner. You can configure HDLC or FR port mode on the following interface modules: • NCS4200-3GMS and NCS4200-1T8S-20CS
Layer 3 Termination for Frame Relay	You can configure layer 3 termination on the Frame Relay (FR) and Mulitlink Frame Relay (MFR) sub interface for the following interface modules: • NCS4200-3GMS • NCS4200-1T8S-20CS You can assign IP address on the FR sub interface and terminate the Layer 3 traffic where ever required in the network. • Layer 3 Termination for Frame Relay • Multilink Frame Relay (MFR) Layer 3 Termination
IP Routing: BFD	
Micro BFD Support on Port Channel with EFPs	A Micro Bidirectional Forwarding Detection (Micro-BFD) session can detect failures in member links of a port channel. You can now enable Micro-BFD sessions for a port channel on which Ethernet flow Point (EFP) or service instance is configured. This feature ensures that traffic is forwarded to a member link only when the micro-BFD session for that member link is in the UP state. As part of this feature, the **source-service-instance** *number* keyword has been added to the **port-channel bfd** command. The specified service instance provides the source IP address for the micro-BFD session.

Feature	Description
Timing and Synchronization	
NTP Support for IPv6 Networks	Network Time Protocol (NTP) synchronizes device clocks across networks to maintain system accuracy. In this release, NTP supports IPv6 multicast networks. The NTP server sends clock updates as multicast messages to the clients across IPv6 networks. As NTP packets are sent only to the intended clients, it reduces timing traffic in the network.
Programmability	
gNMI Dial-Out Using gRPC Tunnel Service	This feature allows you to configure a network device (tunnel client) to register certain targets (preapproved services) with a gRPC tunnel server through the CLI. These targets are defined as ports on the network device. You can use the gRPC tunnel server to forward connections from external clients, such as gRPC Network Management Interface (gNMI)/gRPC Network Operations Interface (gNOI), to connect to the network device without establishing a direct connection. The following commands are introduced for the tunnel and target configurations respectively: • **gnxi grpctunnel destination** *server name* • **gnxi grpctunnel target**
Software Activation	
No License Snapshot Support	License snapshot won't be generated starting from this release and the software relies only on the existing snapshot for any PAK license information.
Strong Crypto Algorithms	
Strong Crypto Algorithms	We strongly recommend stronger cryptographic algorithms instead of weak cryptographic algorithms, such as RSA keys of less than 2048 bits, MD5 for authentication, DES, and 3DES for encryption. Soon, such weak algorithms will no longer be allowed by default. An explicit configuration is required to continue using such weak algorithms. For SNMP v3 users with weak cryptographic properties, the SNMP operations to the device will fail, resulting in loss of management access to device through SNMP. Similarly, if the RSA key pair is not updated to be at least 2048 bits for SSH, the SSH server will be disabled, resulting in loss of remote access to the device through SSH. For more information on how to migrate to stronger cryptographic algorithms for SNMP, see the Field Notice Number: FN72509. For more information on how to migrate to stronger cryptographic algorithms for SSH, see Field Notice Number: FN72511.
YANG	

Feature	Description
YANG Support for show l2vpn atom vc detail Command	The Cisco-IOS-XE-l2vpn-oper native model is a collection of YANG definitions for L2VPN services operational data. Additional leaves and lists are now supported in the following sensor path: **Cisco-IOS-XE-l2vpn-oper\l2vpn-oper-data\l2vpn-services\l2vpn-atom-vc-info** With this model, you can get detailed information, such as the L2VPN service name, service type, interface name, peer address, status, encapsulation type, virtual circuit ID, and packet information by using a NETCONF RPC. In earlier releases, you could perform this action by using the following CLI: **show l2vpn atom vc detail** **Note** There is existing YANG support for the following related CLIs in the **Cisco-IOS-XE-l2vpn-oper** native model: • **show l2vpn service xconnect peer peer_id vcid vcid** • **show l2vpn atom commands** 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. Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same GitHub location highlights changes that have been made in the release.