Limitations and Restrictions

Limitations and Restrictions

- Control Plane Policing (CoPP)—The **show run** command does not display information about classes configured under `system-cpp policy`, when they are left at default values. Use the **show policy-map system-cpp-policy** or the **show policy-map control-plane** commands in privileged EXEC mode instead.
- Hardware limitations
  - Management Port—You cannot modify the configured port speed, duplex mode and flow control and disable auto-negotiation on the Ethernet Management port (GigabitEthernet0/0). Port speed and duplex mode can only be changed from a peer port.
  - Network Module — When the C9200-NM-4X network module is plugged into the C9200 SKUs of the Cisco Catalyst 9200 Series Switches, the uplink interface remains in down state until the network module is recognized by the switch. The time taken for the switch to recognize the network module is longer in comparison to the time taken by the switch to recognize other interconnected devices.
  - If the 1-meter and 1.5-meter 10-GBase-CX1 cables, which are connected on the 10-G ports of the Catalyst 9200L switches, are connected to the 10-G peer ports of the Catalyst 9200L or Catalyst 9200 switches, the peer device might go into the error-disabled state because of link flapping if the local device is restarted. As a workaround, run the **shut** and **no shut** commands on the error-disabled peer interfaces.
- QoS restrictions
  - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - Policing and marking policy on sub interfaces is supported.
  - Marking policy on switched virtual interfaces (SVI) is supported.
  - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.
- Secure Shell (SSH)
  - Use SSH Version 2. SSH Version 1 is not supported.

- When the device is running SCP and SSH cryptographic operations, expect high CPU until the SCP read process is completed. SCP supports file transfers between hosts on a network and uses SSH for the transfer.

  Since SCP and SSH operations are currently not supported on the hardware crypto engine, running encryption and decryption process in software causes high CPU. The SCP and SSH processes can show as much as 40 or 50 percent CPU usage, but they do not cause the device to shutdown.

- Smart Licensing Using Policy: Starting with Cisco IOS XE Amsterdam 17.3.2a, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

  The licensing utilities and user interfaces that are affected by this limitation include only the following: Cisco Smart Software Manager (CSSM), Cisco Smart License Utility (CSLU), and Smart Software Manager On-Prem (SSM On-Prem).

  This limitation is removed from Cisco IOS XE Cupertino 17.9.1. If you configure a hostname and disable hostname privacy (**no license smart privacy hostname** global configuration command), hostname information is sent from the product instance and displayed on the applicable user interfaces (CSSM, CSLU, SSM On-Prem). For more information, see the command reference for this release.

- Stacking

  - Stacking is supported on Cisco Catalyst 9200 Series Switches. A switch stack supports up to eight stack members. However, you cannot stack C9200 SKUs with C9200L SKUs

    The supported stacking bandwidth on C9200L SKUs is up to 80Gbps; on C9200 SKUs, this is up to 160Gbps.

  - The C9200-24PB and C9200-48PB switch models can be stacked only with each other and not with other models of the Cisco Catalyst 9200 Series Switches.

  - Auto upgrade for a new member switch is supported only in the install mode.

- TACACS legacy command: Do not configure the legacy **tacacs-server host** command; this command is deprecated. If the software version running on your device is Cisco IOS XE Gibraltar 16.12.2 or a later release, using the legacy command can cause authentication failures. Use the **tacacs server** command in global configuration mode.

- USB Authentication—When you connect a Cisco USB drive to the switch, the switch tries to authenticate the drive against an existing encrypted preshared key. Since the USB drive does not send a key for authentication, the following message is displayed on the console when you enter **password encryption aes** command:

```
Device(config)# password encryption aes
Master key change notification called without new or old key
```

- Catatyst 9000 Series Switches support MACsec switch-to-switch connections. We do not recommend configuring MACsec switch-to-host connections in an overlay network. For assistance with an existing switch-to-host MACsec implementation or a design review, contact your Cisco Sales Representative or Channel Partner.

- VLAN Restriction—It is advisable to have well-defined segregation while defining data and voice domain during switch configuration and to maintain a data VLAN different from voice VLAN across the switch

stack. If the same VLAN is configured for data and voice domains on an interface, the resulting high CPU utilization might affect the device.

- YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.
- Embedded Event Manager—Identity event detector is not supported on Embedded Event Manager.
- Upgrading the software image from Cisco IOS XE Gibraltar 16.12.x to any of the later releases can result in a persistent database operation failure and after which the persistent database cannot be restored.

  To avoid the persistent database operation failure, use the **dir bootflash:.dbpersist** command to list all DB persist files and then use **delete bootflash:/.dbpersist/folder_name/file_name** and **bootflash:/.dbpersist/folder_name/file_name.meta** commands to delete individual database and meta files from each persistent database folder.
- The File System Check (fsck) utility is not supported in install mode.
- The DiagMemoryTest GOLD test is not supported on the Catalyst 9200 Series Switches.
- On Cisco Catalyst 9200CX Series Switches, zero touch provisioning and guest shell are supported but connecting to an external network from a guest shell does not work, as Management, AppGigabitEthernet, and VirtualPortGroup interfaces are not supported.
- The command **service-routing mdns-sd** is being deprecated. Use the **mdns-sd gateway** command instead.

Limitations and Restrictions