Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 12.3(1)

This document describes the features, bugs, and limitations for Cisco NX-OS software that runs on Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) switches. Use this document in combination with the *Cisco Application Policy Infrastructure Controller, Release 2.3(1), Release Notes*, which you can view at the following location:

https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Additional product documentation is listed in the "Related Documentation" section.

Release notes are sometimes updated with new information about restrictions and bugs. See the following website for the most recent version of the *Cisco NX-OS Release 12.3(1) Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches*:

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html

Table 1 shows the online change history for this document.

Table 1. Online History Change

Date	Description
July 6, 2021	In the Supported Hardware section, added the NXA-PAC-500W-PI and NXA-PAC-500W-PE PSUs.
June 24, 2021	Added open issue CSCvu07844.
January 19, 2021	In the Known Behaviors section, changed the following sentence: The Cisco Nexus 9508 ACI-mode switch supports warm (stateless) standby where the state is not synched between the active and the standby supervisor modules. To: The modular chassis Cisco ACI spine nodes, such as the Cisco Nexus 9508, support warm (stateless) standby where the state is not synched between the active and the standby supervisor modules.
March 13, 2020	12.3(1e): In the Resolved Bugs section, added bug CSCvr98827.
September 20, 2019	In the Usage Guidelines section, added the following bullet: ■ A 25G link that is using the IEEE-RS-FEC mode can communicate with a link that is using the CL16-RS-FEC mode. There will not be a FEC mismatch and the link will not be impacted.

Date	Description
September 11, 2019	In the Supported Hardware section, for the N9K-C93108TC-FX and N9K-C93180YC-FX switches, added the following note: Note: Incoming FCOE packets are redirected by the supervisor module. The data plane-forwarded packets are dropped and are counted as forward drops instead of as supervisor module drops.
August 14, 2019	12.3(1e): In the Open Bugs section, added bug CSCvp92269.
August 6, 2019	12.3(1e): In the Resolved Bugs section, added bug CSCvm96490.
July 31, 2019	In the Compatibility Information section, added the following bullet: ■ On Cisco ACI platforms, 25G copper optics do not honor auto-negotiation, and therefore auto-negotiation on the peer device (ESX or standalone) must be disabled to bring up the links.
January 30, 2019	12.3(1e): In the Open Bugs section, added bug CSCvn69340.
June 19, 2018	12.3(1p): Release 12.3(1p) became available. Added the resolved bugs for this release.
June 7, 2018	12.3(1e): In the Open Bugs section, added bug CSCvg35892.
April 24, 2018	12.3(1e): In the Open Bugs section, added bug CSCvi57920.
February 23, 2018	12.3(1o): Release 12.3(1o) became available. Added the resolved bugs for this release.
January 22, 2018	12.3(1l): Release 12.3(1l) became available. Added the resolved bugs for this release.
December 11, 2017	12.3(1e): Moved bug CSCvd80766 from the Open Bugs section to the Known Behaviors section.
December 6, 2017	12.3(1e): In the Know Behaviors section, added bug CSCvd63567.
November 3, 2017	12.3(1e): In the Open Bugs section, added bug CSCve65374.
October 20, 2017	12.3(1i): Release 12.3(1i) became available. Added the open and resolved bugs for this release.
July 9, 2017	12.3(1f): Release 12.3(1f) became available; there are no changes to this document for this release.
June 16, 2017	12.3(1e): Added bug CSCve82313 to Resolved Bugs.
June 14, 2017	12.3(1e): Release 12.3(1e) became available.

Contents

This document includes the following sections:

- Cisco Nexus 9000 Series ACI-Mode
- Supported Hardware
- Supported FEX Models
- New and Changed Information
- Installation Notes
- Compatibility Information
- Usage Guidelines
- Bugs
- Related Documentation

Cisco Nexus 9000 Series ACI-Mode

Cisco NX-OS Software for the Cisco Nexus 9000 Series is a data center, purpose-built, operating system designed with performance, resiliency, scalability, manageability, and programmability at its foundation. It provides a robust and comprehensive feature set that meets the requirements of virtualization and automation in data centers

Cisco NX-OS Release 12.3 works only on Cisco Nexus 9000 Series switches in ACI Mode.

See Table 2 for a list of modules that are supported on Cisco Nexus 9000 Series switches in ACI Mode.

Supported Hardware

Table 2 lists the hardware that the Cisco Nexus 9000 Series ACI Mode switches support.

Table 2. Cisco Nexus 9000 Series Hardware

Hardware Type	Product ID	Description
Chassis	N9K-C9504	Cisco Nexus 9504 chassis with 4 I/O slots
Chassis	N9K-C9508	Cisco Nexus 9508 chassis with 8 I/O slots
Chassis component	N9K-C9508-FAN	Fan tray
Chassis component	N9k-PAC-3000W-B	Cisco Nexus 9500 3000W AC power supply, port side intake
Pluggable module (GEM)	N9K-M12PQ	12-port or 8-port
Pluggable module (GEM)	N9K-M6PQ	6-port
Pluggable module (GEM)	N9K-M6PQ-E	6-port, 40 Gigabit Ethernet expansion module
Spine switch	N9K-C9336PQ	Cisco Nexus 9336PQ switch, 36-port 40 Gigabit Ethernet QSFP
Spine switch	N9K-C9508-B1	Cisco Nexus 9508 chassis bundle with 1 supervisor module, 3 power supplies, 2 system controllers, 3 fan trays, and 3 fabric modules
Spine switch	N9K-C9508-B2	Cisco Nexus 9508 chassis bundle with 1 supervisor module, 3 power supplies, 2 system controllers, 3 fan trays, and 6 fabric modules
Spine switch	N9K-C9516	Cisco Nexus 9516 switch with 16 line card slots

Hardware Type	Product ID	Description
Spine switch fan	N9K-C9300-FAN3	Port side intake fan
Spine switch fan	N9K-C9300-FAN3-B	Port side exhaust fan
Spine switch module	N9K-C9504-FM	Cisco Nexus 9504 fabric module supporting 40 Gigabit line cards
Spine switch module	N9K-C9504-FM-E	Cisco Nexus 9504 fabric module supporting 100 Gigabit line cards
Spine switch module	N9K-C9508-FM	Cisco Nexus 9508 fabric module supporting 40 Gigabit line cards
Spine switch module	N9K-C9508-FM-E	Cisco Nexus 9508 Fabric module supporting 100 Gigabit line cards
Spine switch module	N9K-X9732C-EX	Cisco Nexus 9500 32-port, 40/100 Gigabit Ethernet QSFP28 aggregation module
Spine switch module	N9K-X9736PQ	Cisco Nexus 9500 36-port, 40 Gigabit Ethernet QSFP aggregation module
Switch module	N9K-SC-A	Cisco Nexus 9500 Series system controller
Switch module	N9K-SUP-A	Cisco Nexus 9500 Series supervisor module
Switch module	N9K-SUP-A+	Cisco Nexus 9500 Series supervisor module
Switch module	N9K-SUP-B	Cisco Nexus 9500 Series supervisor module
Switch module	N9K-SUP-B+	Cisco Nexus 9500 Series supervisor module
Top-of-rack (ToR) leaf switch	N9K-C93108TC-EX	Cisco Nexus 9300 platform switch with 48 1/10GBASE-T (copper) front panel ports and 6 40/100-Gigabit QSFP28 spine facing ports.
Top-of-rack (ToR) leaf switch	N9K-C93108TC-FX	Cisco Nexus 9300 platform switch with 48 1/10GBASE-T (copper) front panel ports and 6 fixed 40/100-Gigabit Ethernet QSFP28 spine-facing ports. Note: Incoming FCOE packets are redirected by the supervisor module. The data plane-forwarded packets are dropped and are counted as forward drops instead of as supervisor module drops.
Top-of-rack (ToR) leaf switch	N9K-C93120TX	Cisco Nexus 9300 platform switch with 96 1/10GBASE-T (copper) front panel ports and 6-port 40-Gigabit Ethernet QSFP spine-facing ports

Hardware Type	Product ID	Description
Top-of-rack (ToR) leaf switch	N9K-C93128TX	Cisco Nexus 9300 platform switch with 96 1/10GBASE-T (copper) front panel ports and 6 or 8 40-Gigabit Ethernet QSFP spine-facing ports
Top-of-rack (ToR) leaf switch	N9K-C93180LC-EX	Cisco Nexus 9300 platform switch with 24 40-Gigabit front panel ports and 6 40/100-Gigabit QSFP28 spine-facing ports The switch can be used either 24 40G ports or 12 100G ports. If 100G is connected the Port1, Port 2 will be HW disabled. Note: This switch has the following limitations: • This release does not support 1 Gbps for QSA. • The top and bottom ports must use the same speed. If there is a speed mismatch, the top port takes precedence and bottom port will be error disabled. Both ports both must be used in either the 40 Gbps or 10 Gbps mode. • Ports 26 and 28 are hardware disabled. • This release supports 40 and 100 Gbps for the front panel ports. The uplink ports can be used at the 100 Gbps speed.
Top-of-rack (ToR) leaf switch	N9K-C93180YC-EX	Cisco Nexus 9300 platform switch with 48 1/10/25-Gigabit front panel ports and 6-port 40/100 Gigabit QSFP28 spine-facing ports
Top-of-rack (ToR) leaf switch	N9K-C93180YC-FX	Cisco Nexus 9300 platform switch with 48 1/10/25-Gigabit Ethernet SFP28 front panel ports and 6 fixed 40/100-Gigabit Ethernet QSFP28 spine-facing ports. The SFP28 ports support 1-, 10-, and 25-Gigabit Ethernet connections and 8-, 16-, and 32-Gigabit Fibre Channel connections. Note: Incoming FCOE packets are redirected by the supervisor module. The data plane-forwarded packets are dropped and are counted as forward drops instead of as supervisor module drops.
Top-of-rack (ToR) leaf switch	N9K-C9332PQ	Cisco Nexus 9332PQ Top-of-rack (ToR) Layer 3 switch with 26 APIC-facing ports and 6 fixed-Gigabit spine facing ports.

Hardware Type	Product ID	Description
Top-of-rack (ToR) leaf switch	N9K-C9372PX	Cisco Nexus 9372PX Top-of-rack (ToR) Layer 3 switch with 48 Port 1/10-Gigabit APIC-facing ports Ethernet SFP+ front panel ports and 6 40-Gbps Ethernet QSFP+ spine-facing ports Note: Only the downlink ports 1-16 and 33-48 are capable of supporting SFP1-10G-ZR SFP+.
Top-of-rack (ToR) leaf switch	N9K-C9372PX-E	Cisco Nexus 9372PX-E Top-of-rack (ToR) Layer 3 switch with 48 Port 1/10-Gigabit APIC-facing ports Ethernet SFP+ front panel ports and 6 40-Gbps Ethernet QSFP+ spine-facing ports Note: Only the downlink ports 1-16 and 33-48 are capable of supporting SFP1-10G-ZR SFP+.
Top-of-rack (ToR) leaf switch	N9K-C9372TX	Cisco Nexus 9372TX Top-of-rack (ToR) Layer 3 switch with 48 1/10GBASE-T (copper) front panel ports and 6 40-Gbps Ethernet QSFP spine-facing ports
Top-of-rack (ToR) leaf switch	N9K-C9372TX-E	Cisco Nexus 9372TX-E Top-of-rack (ToR) Layer 3 switch with 48 10GBASE-T (copper) front panel ports and 6 40-Gbps Ethernet QSFP+ spine-facing ports
Top-of-rack (ToR) leaf switch	N9K-C9396PX	Cisco Nexus 9300 platform switch with 48 1/10-Gigabit SFP+ front panel ports and 6 or 12 40-Gigabit Ethernet QSFP spine-facing ports
Top-of-rack (ToR) leaf switch	N9K-C9396TX	Cisco Nexus 9300 platform switch with 48 1/10GBASE-T (copper) front panel ports and 6 or 12 40-Gigabit Ethernet QSFP spine-facing ports
Top-of-rack (ToR) leaf switch fan	NXA-FAN-30CFM-B	Red port side intake fan
Top-of-rack (ToR) leaf switch fan	NXA-FAN-30CFM-F	Blue port side exhaust fan
Top-of-rack (ToR) leaf switch power supply unit	N9K-PAC-1200W	1200W AC Power supply, port side intake pluggable Note: This power supply is supported only by the Cisco Nexus 93120TX, 93128TX, and 9336PQ ACI-mode switches

Hardware Type	Product ID	Description
Top-of-rack (ToR) leaf switch power supply unit	N9K-PAC-1200W-B	1200W AC Power supply, port side exhaust pluggable Note: This power supply is supported only by the Cisco Nexus 93120TX, 93128TX, and 9336PQ ACI-mode switches
Top-of-rack (ToR) leaf switch power supply unit	N9K-PAC-650W	650W AC Power supply, port side intake pluggable
Top-of-rack (ToR) leaf switch power supply unit	N9K-PAC-650W-B	650W AC Power supply, port side exhaust pluggable
Top-of-rack (ToR) leaf switch power supply unit	N9K-PUV-1200W	1200W HVAC/HVDC dual-direction airflow power supply Note: This power supply is supported only by the Cisco Nexus 93120TX, 93128TX, and 9336PQ ACI-mode switches
Top-of-rack (ToR) leaf switch power supply unit	N9K-PUV-3000W-B	3000W AC Power supply, port side exhaust pluggable
Top-of-rack (ToR) leaf switch power supply unit	NXA-PAC-1200W-PE	1200W AC Power supply, port side exhaust pluggable, with higher fan speeds for NEBS compliance Note: This power supply is supported only by the Cisco Nexus 93120TX, 93128TX, and 9336PQ ACI-mode switches.
Top-of-rack (ToR) leaf switch power supply unit	NXA-PAC-1200W-PI	1200W AC Power supply, port side intake pluggable, with higher fan speeds for NEBS compliance Note: This power supply is supported only by the Cisco Nexus 93120TX, 93128TX, and 9336PQ ACI-mode switches.
Top-of-rack (ToR) leaf switch power supply unit	NXA-PAC-500W-PE	500W AC Power supply, port side exhaust pluggable
Top-of-rack (ToR) leaf switch power supply unit	NXA-PAC-500W-PI	500W AC Power supply, port side intake pluggable

Hardware Type	Product ID	Description
Top-of-rack (ToR) leaf switch power supply unit	UCSC-PSU-930WDC V01	Port side exhaust DC power supply compatible with all ToR leaf switches
Top-of-rack (ToR) leaf switch power supply unit	UCS-PSU-6332-DC	930W DC power supply, reversed airflow (port side exhaust)

Supported FEX Models

Table 3 lists the FEX models that the Cisco Nexus 9000 Series ACI Mode switches support. For more information on the FEX models, see the *Cisco Nexus 2000 Series Fabric Extenders Data Sheet* at the following location:

https://www.cisco.com/c/en/us/products/switches/nexus-2000-series-fabric-extenders/datasheet-listing.html

Table 3. Supported FEX Models

Product ID	Description
N2K-B22DELL-P	B22 FEX for Dell
N2K-B22HP-P	B22 FEX for HP
N2K-B22IBM-P	B22 FEX for IBM
N2K-C2248PQ-10GE	Cisco Nexus 2248PQ 10GE Fabric Extender, 2PS, 4 Fan Module, 48x1/10GE (req SFP/SFP+) + 4x40G QSFP+(req QSFP+), choice of airflow and power supply
N2K-C2248TP-1GE	Cisco Nexus 2248TP Series 1GE Fabric Extender, 2 AC PS, 1 Fan Module (Standard Airflow/port side exhaust), 48x100/1000Base-T + 4x10GE (req SFP+), same as N2K-C2248TP
N2K-C2248TP-E-1GE	Cisco Nexus 2248TP-E Series 1GE Fabric Extender, 2PS, 1 Fan Module, 48x100/1000Base-T + 4x10GE (req SFP+), 32MB buffer, choice of airflow and power supply
N2K-C2332TQ	Cisco Nexus 2332TQ 10G BASE T Fabric Extender, 2PS, 3 Fan Module, 48x100M/1/10GE + 4x40G QSFP+(req QSFP+), choice of airflow and power supply
N2K-C2348TQ	Cisco Nexus 2348TQ 10G BASE T Fabric Extender, 2PS, 3 Fan Module, 48x100M/1/10GE + 6x40G QSFP+(req QSFP+), choice of airflow and power supply
N2K-C2348UPQ	48 100M/1/10 Gigabit Ethernet and Unified Port host interfaces (SFP+) and up to 6 QSFP+ 10/40 Gigabit Ethernet fabric interfaces

Product ID	Description
N2K-C2232PP-10GE	Cisco Nexus 2232PP Series 10GE Fabric Extender, 2 AC PS, 1 Fan Module (Standard Airflow/port side exhaust), 32x1/10GE (req SFP/SFP+) + 8x10GE (req SFP+), same as N2K-C2232PP
N2K-C2232TM-E-10GE	Cisco Nexus 2232TM-E Series 10GBASE-T Fabric Extender, 2PS, 1 Fan Module, 32x1/10GBase-T + 8x10GE Module (req SFP+), choice of airflow and power supply

New and Changed Information

This section lists the new and changed features in this release.

- New Hardware Features
- New Software Features

New Hardware Features

This release supports the following new hardware features:

- Cisco Nexus N9K-SUP-A+, N9K-SUP-B+ are new supervisor modules based on Broadwell DE based Intel processor. These modules have backward compatibility with all existing line cards and fabric modules and seamlessly work with any existing Nexus 9000 modular chasses.
- The Cisco Nexus 93180LC-EX switch (N9K-C93180LC-EX) is a 1-RU, fixed-port ACI leaf switch for ACI deployments. This switch can be configured to work as 24 40- or 50-Gigabit server ports, and 6 100-Gigabit uplink ports. The switch can also support up to 12 100-Gigabit QSFP28 server ports and 6 100-Gigabit uplink ports. This switch has six fixed uplink QSFP28 ports that you can configure to work as 40- or 100-Gigabit ports.
- The following transceivers are now supported on all switch platforms:
  - QSFP-100G-AOC1M
  - QSFP-100G-AOC2M
  - QSFP-100G-AOC3M
  - QSFP-100G-AOC5M
  - QSFP-100G-AOC25M
  - QSFP-100G-AOC30M
  - QSFP-4X10G-AOC1M
  - QSFP-4X10G-AOC3M
  - QSFP-4X10G-AOC5M
  - QSFP-4X10G-AOC7M
  - QSFP-4X10G-AOC10M
  - QSFP-4SFP10G-CU1M
  - QSFP-4SFP10G-CU3M
  - QSFP-4SFP10G-CU5M
  - QSFP-4X10G-AC7M
  - QSFP-4X10G-AC10M
  - QSFP-H40G-AOC15M

- SFP-25G-AOC1M
- SFP-25G-AOC2M
- SFP-25G-AOC3M
- SFP-25G-AOC5M
- SFP-25G-AOC7M
- SFP-25G-AOC10M
- CWDM-SFP10G-1470
- CWDM-SFP10G-1490
- CWDM-SFP10G-1510
- CWDM-SFP10G-1530
- CWDM-SFP10G-1550
- CWDM-SFP10G-1570
- CWDM-SFP10G-1590
- CWDM-SFP10G-1610

New Software Features

For new software features, see the *Cisco APIC 2.3(1) Release Notes* at the following location:

https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Installation Notes

The following procedure installs a Gigabit Ethernet module (GEM) in a top-of-rack switch:

1. Clear the switch's current configuration by using the setup-clean-config command.
2. Power off the switch by disconnecting the power.
3. Replace the current GEM card with the new GEM card.
4. Power on the switch.

For other installation instructions, see the *Cisco ACI Fabric Hardware Installation Guide* at the following location:

https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Compatibility Information

- This release supports the hardware and software listed on the ACI Ecosystem Compatibility List, and supports the Cisco AVS, Release 5.2(1)SV3(2.14).
- Link level flow control is not supported on ACI-mode switches.
- To connect the N2348UPQ to ACI leaf switches, the following options are available:
  - Directly connect the 40G FEX ports on the N2348UPQ to the 40G switch ports on the ACI leaf switches
  - Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the 10G ports on all other ACI leaf switches

Note: A fabric uplink port cannot be used as a FEX fabric port.

- To connect the APIC (the controller cluster) to the ACI fabric, it is required to have a 10G interface on the ACI leaf. You cannot connect the APIC directly to the N9332PQ ACI leaf switch.
- We do not qualify third party optics in Cisco ACI. When using third party optics, the behavior across releases is not guaranteed, meaning that the optics might not work in some NX-OS releases. Use third party optics at your own risk. We recommend that you use Cisco SFPs, which have been fully tested in each release to ensure consistent behavior.
- On Cisco ACI platforms, 25G copper optics do not honor auto-negotiation, and therefore auto-negotiation on the peer device (ESX or standalone) must be disabled to bring up the links.

Usage Guidelines

- The current list of protocols that are allowed (and cannot be blocked through contracts) include the following. Some of the protocols have SrcPort/DstPort distinction.

  Note: See the APIC release notes for policy information: https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

  - UDP DestPort 161: SNMP. These cannot be blocked through contracts. Creating an SNMP ClientGroup with a list of Client-IP Addresses restricts SNMP access to only those configured Client-IP Addresses. If no Client-IP address is configured, SNMP packets are allowed from anywhere.
  - TCP SrcPort 179: BGP
  - TCP DstPort 179: BGP
  - OSPF
  - UDP DstPort 67: BOOTP/DHCP
  - UDP DstPort 68: BOOTP/DHCP
  - IGMP
  - PIM
  - UDP SrcPort 53: DNS replies
  - TCP SrcPort 25: SMTP replies
  - TCP DstPort 443: HTTPS
  - UDP SrcPort 123: NTP
  - UDP DstPort 123: NTP
- Leaf and spine switches from two different fabrics cannot be connected regardless of whether the links are administratively kept down.
- A 25G link that is using the IEEE-RS-FEC mode can communicate with a link that is using the CL16-RS-FEC mode. There will not be a FEC mismatch and the link will not be impacted.

Bugs

This section contains lists of open and resolved bugs and known behaviors.

- Known Limitations
- Open Bugs
- Resolved Bugs
- Known Behaviors

Known Limitations

The following list describes IpEpg (IpCkt) known limitations in this release:

- An IP/MAC Ckt endpoint configuration is not supported in combination with static endpoint configurations.
- An IP/MAC Ckt endpoint configuration is not supported with Layer 2-only bridge domains. Such a configuration will not be blocked, but the configuration will not take effect as there is no Layer 3 learning in these bridge domains.
- An IP/MAC Ckt endpoint configuration is not supported with external and Infra bridge domains because there is no Layer 3 learning in these bridge domains.
- An IP/MAC Ckt endpoint configuration is not supported with a shared services provider configuration. The same or overlapping prefix cannot be used for a shared services provider and IP Ckt endpoint. However, this configuration can be applied in bridge domains having shared services consumer endpoint groups.
- An IP/MAC Ckt endpoint configuration is not supported with dynamic endpoint groups. Only static endpoint groups are supported.
- No fault will be raised if the IP/MAC Ckt endpoint prefix configured is outside of the bridge domain subnet range. This is because a user can configure bridge domain subnet and IP/MAC Ckt endpoint in any order and so this is not error condition. If the final configuration is such that a configured IP/MAC Ckt endpoint prefix is outside all bridge domain subnets, the configuration has no impact and is not an error condition.
- Dynamic deployment of contracts based on instrImmedcy set to onDemand/lazy not supported; only immediate mode is supported.

The following list describes direct server return (DSR) known limitations in this release:

- When a server and load balancer are on the same endpoint group, make sure that the Server does not generate ARP/GARP/ND request/response/solicits. This will lead to learning of LB virtual IP (VIP) towards the Server and defeat the purpose of DSR support
- Load balancers and servers must be Layer 2 adjacent. Layer 3 direct server return is not supported. If a load balancer and servers are Layer 3 adjacent, then they have to be placed behind the Layer 3 out, which works without a specific direct server return virtual IP address configuration.
- Direct server return is not supported for shared services. Direct server return endpoints cannot be spread around different virtual routing and forwarding (VRF) contexts.
- Configurations for a virtual IP address can only be /32 or /128 prefix.

- Client to virtual IP address (load balancer) traffic always will go through proxy-spine because fabric data-path learning of a virtual IP address does not occur.
- GARP learning of a virtual IP address must be explicitly enabled. A load balancer can send GARP when it switches over from active-to-standby (MAC changes).
- Learning through GARP will work only in ARP Flood Mode.

Open Bugs

This section lists the open This section lists the open bugs. Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Exists In" column of the table specifies the 12.3(1) releases in which the bug exists. A bug might also exist in releases other than the 12.3(1) releases.

Table 4 Open Bugs in This Release

Bug ID	Description	Exists In
CSCvj50973	When the MTU settings for OSPF neighboring router interfaces do not match, the routers will be stuck in the Exstart/Exchange state. This behavior is expected. This bug is an enhancement to raise a fault to the APIC so that the routers' stuck state can be easily detected by the administrator.	12.3(1o) and later
CSCvc17015	Quick changes in the RPF interface trigger RPF lookups in MRIB and PIM for all of the routes, which results in a high convergence time.	12.3(1e) and later
CSCvd39719	Ping packets cannot be sent from spine1 (of pod1) to spine2 (of pod2) with MTU set to greater than 1350, irrespective of the control plane MTU value.	12.3(1e) and later
CSCvd63567	After upgrading a switch, Layer 2 multicast traffic flowing across PODs gets affected for some of the bridge domain Global IP Outsides.	12.3(1e) and later
CSCvd66411	When VPC and Bidirectional Forwarding Detection (BFD) are deployed on some ToR platforms, BFD might flap on an interface shut/no-shut of one leg of the VPC.	12.3(1e) and later
CSCve06334	MAC and IP endpoints are not learned on the local vPC pair.	12.3(1e) and later
CSCve65374	Traffic that flows toward some tunnel endpoints (TEPs) will be dropped. This issue occurs because the tunnel toward those TEPs is programmed with drop adjacency.	12.3(1e) and later
CSCve79295	The CoPP rate/burst might get set to the default values when the CoPP policy is changed.	12.3(1e) and later

Bug ID	Description	Exists In
CSCvf09313	In the 12.2(2i) release, the BPDU filter only prevents interfaces from sending BPDUs, but does not prevent interfaces from receiving BPDUs.	12.3(1e) and later
CSCvg35892	There is a delay in internal process communication of over a minute due to a timeout (timeout period is 60 seconds). This can manifest itself in different ways. In one way, the Policy Element sent a delete/create request for a VLAN to the VLAN manager, but the VLAN manager did not process the request until the initial request timed out. This resulted in an outage that lasted a little over a minute while changing a BD from Unknown Unicast Flood to Hardware Proxy.	12.3(1e) and later
CSCvi57920	A UCS 1225 vNIC goes down after changing the peer Cisco ACI leaf node name.	12.3(1e) and later
CSCvn69340	The BFD session does not get instantiated under some circumstances in one of the VPC legs for static routes.	12.3(1e) and later
CSCvp50075	A leaf switch experiences an unexpected reload due to a HAP reset.	12.3(1e) and later
CSCvp92269	Running a Qualys security scan results in the following message: CWE - 693 Protection Mechanism Failure - "HTTP Security Header Not Detected"	12.3(1e) and later
CSCvr98827	Some of the control plane packets are incorrectly classified as the user class and are reported as dropped in single chip spine switches. The statistics are incorrect because the packets are not actually dropped.	12.3(1e) and later

Bug ID	Description	Exists In
CSCvs18150	After a certain set of steps, it is observed that the deny-external-tag route-map used for transit routing loop prevention gets set back to the default tag 4294967295. Since routes arriving in Cisco ACI with this tag are denied from being installed in the routing table, if the VRF table that has the route-tag policy is providing transit for another VRF table in Cisco ACI (for instance and inside and outside VRF with a firewall connecting them) and the non-transit VRF table has the default route-tag policy, routes from the non-transit VRF table would not be installed in the transit VRF table. This bug is also particularly impactful in scenarios where transit routing is being used and OSPF or EIGRP is used on a vPC border leaf switch pair. vPC border leaf switches peer with each other, so if member A gets a transit route from BGP, redistributes into OSPF, and then advertises to member B (since they are peers)...without a loop prevention mechanism, member B would install the route through OSPF since it has a better admin distance and would then advertise back into BGP. This VRF tag is set on redistribution of BGP > OSPF and then as a table map in OSPF that blocks routes with the tag from getting installed in the routing table. When hitting this bug, the route-map used for redistributing into OSPF still sets the tag to the correct value. However, the table map no longer matches the correct tag. Rather, it matches the default tag. As a result, member A (could be B) would install the route through OSPF pointing to B. It would then redistribute it back into BGP with the med set to 1. The rest of the fabric (including member B) would install the BGP route pointing to member A since its med is better than the original route's med.	12.3(1e) and later
CSCvs76848	A switch SSD fails in less than two years and needs replacement. The /mnt/pss/ssd_log_amp.log file shows daily P/E cycles increasing by 10 or more each day, and fault "F3525: High SSD usage" is observed. Check the switch activity and contact Cisco Technical Support if the "High SSD usage" fault is raised on the switch.	12.3(1e) and later
CSCvt82388	A switch SSD fails in less than two years and needs replacement. The /mnt/pss/ssd_log_amp.log file shows daily P/E cycles increasing by 10 or more each day, and fault "F3525: High SSD usage" is observed. ARP/ICMPv6 adjacency updates can also contribute to many SSD writes.	12.3(1e) and later
CSCvu01639	There are faults for failed contract rules and prefixes on switches prior to the -EX switches. Furthermore, traffic that is destined to an L3Out gets dropped because the compute leaf switches do not have the external prefix programmed in ns shim GST-TCAM. You might also see that leaf switches prior to the -EX switches do not have all contracts programmed correctly in the hardware.	12.3(1e) and later
CSCvu07844	When a Cisco N9K-C93180LC-EX, N9K-93180YC-EX, or N9K-C93108TC-EX leaf switch receives control, data, or BUM traffic from the front panel ports with the storm policer configured for BUM traffic, the storm policer will not get enforced. As such, the switch will let all such traffic through the system.	12.3(1e) and later

Resolved Bugs

This section lists the resolved bugs. Click the bug ID to access the Bug Search tool and see additional information about the bug. The "Fixed In" column of the table specifies whether the bug was resolved in the base release or a patch release.

Table 5 Resolved Bugs in This Release

Bug ID	Description	Fixed In
CSCvc33025	When a Layer 2 domain is stretched through the ACI fabric across multiple sites using stretched fabric with N9K-93108TC-EX, N9K-93180YC-EX, or N9K-C93180LC-EX switches as the transit TORs and a tenant's configuration is deployed on them, this setup can lead to a longer convergence time for multi-destination packets in the event of network triggers. You should deploy N9K-93108TC-EX, N9K-93180YC-EX, or N9K-C93180LC-EX switches as pure transit if such a configuration cannot be avoided (spanning tree domain extended across sites).	12.3(1e)
CSCvc35197	Upon a stateless reload of the TOR, the VSAN on the NP port does not come up. This is because under heavy load, the FCF MAC programming takes longer than expected. In this case, FCF_MAC against the VSAN is programmed in the EPMC even though the VSAN is shown as "down" in the " show npv status" command.	12.3(1e)
CSCvc46611	If Layer 3 multicast is deployed in the fabric with more than two border leaf switches and a multicast traffic source is connected to fabric behind an L3Out, with fast convergence enabled for Layer 3 multicast, periodically there could be a multicast packet duplication for a few seconds in the fabric for a fraction of the groups.	12.3(1e)
CSCvc50422	When the transit ToR is an N9K-C93120TX, N9K-93128TX, N9K-C9332PQ, N9K-C9372PX, N9K-C9372PX-E, N9K-C9372TX, N9K-C9372TX-E, N9K-9396PX, N9K-9396TX, N9K-M6PQ GEM, or N9K-M6PQ-E GEM switch in a stretched fabric deployment, the .1Q tag of packets in unidirectional traffic—meaning that the destination endpoint is not known as an ingress ToR—is not preserved when it is switched within an 802.1Q tunneling bridge domain.	12.3(1e)
CSCvd34047	Many MTS messages are seen in the MTS buffer for SAP 213.	12.3(1e)
CSCvd51695	With more than 50,000 policy cam entries and depending on your configuration, upgrading from the 2.0(2) release to the 2.2(2) release can take several minutes longer to complete after the bootstrap is complete.	12.3(1e)
CSCve82313	Common Pervasive Gateway might not source Address Resolution Protocol (ARP) requests with Pseudo MAC (PMAC).	12.3(1e)
CSCvm96490	After a policy upgrade, fault "F1583 - BIOS version mismatch detected." is present for N9K-C93108TC-EX and N9K-C93180YC-EX switches.	12.3(1e)
CSCvf12659	Cisco ACI leaf switches will send DHCP ACK back to the DHCP client as a "BROADCAST" when the bootp flag is set to "UNICAST."	12.3(1i)
CSCvf67718	An EX linecard or E fabric module crashes and resets when it encounters the PCIe uncorrectable error. You can see that the card failed, powered off, and then got removed and reinserted by navigating to the following location in the Cisco APIC GUI and viewing the events: Fabric > Inventory > Pod *x* > Spine > History > Events	12.3(1i)
CSCvf73694	When using OpenStack to deploy a VM and the setup contains a FEX and N9K-C93180YC-EX switch, two NICs of one node go down. In addition, the Cisco OpFlex loses connection to the other nodes in the same FEX. As a result, the host loses infra VLAN connectivity to the fabric.	12.3(1i)
CSCvf80829	Traffic is not evenly load balanced onto all of the member links in a port channel.	12.3(1i)

Bug ID	Description	Fixed In
CSCvf81062	A linecard or fabric module cannot be initialized successfully due to the image failing to download from the supervisor engine. The linecard or fabric module remains in the "inserted" status even after being reset.	12.3(1i)
CSCvg04269	IP addresses do not get learned with GARP traffic when IP learning is disabled on the bridge domain.	12.3(1i)
CSCve40174	The IP address is missing in COOP after performing some fast IP address moves across a pod or site.	12.3(1l)
CSCvg05802	A leaf switch crashes after techsupport collection is triggered for that leaf switch.	12.3(1l)
CSCvh17376	This is an enhancement request to strengthen the implementation of vPC to avoid a split brain scenario in the case of the control plane becoming irresponsive while the data plane is still forwarding traffic.	12.3(1l)
CSCvc51529	Endpoints connected to a FEX vPC might move as traffic is load-balanced across vPC members. For example, if leaf1 and leaf2 are a vPC pair and have FEXes connected that have the vPC member ports, and if an endpoint that is learned on this vPC is communicating with an endpoint that is connected to some other leaf switch, that remote leaf will see a remote-to-remote endpoint move. This is because the source TEP being set by leaf 1 and leaf 2 is the physical leaf switch TEP rather than the vPC TEP that both own. Excessive endpoint moves could lead to other symptoms, such as learning getting disabled on a bridge domain.	12.3(1o)
CSCve60216	A Cisco ACI border leaf switch might not be able to ping the next hop router's IP address. Additionally, it will not be able to route traffic out of the fabric through the L3Out. When running the "show ip arp" command for the VRF instance, you might see something similar to the following entry (with negative age) for the next hop: Address Age MAC Address Interface 10.10.10.10 -00:00:00 0123.4567.8910 vlan10	12.3(1o)
CSCve80460	DTEP tunnels flap every 20 minutes.	12.3(1o)
CSCve88634	If a switch exhausts the terabytes written (TBW) threshold for an SSD, the drive might go into a read-only mode, which triggers the switch to crash and suffer subsequent boot failures, which requires the switch to be replaced. On console, the following log might be seen: /dev/hd-pss: ********** WARNING: Filesystem still has errors ********** e2fsck 1.42.1 (17-Feb-2012) /dev/hd-bootflash: recovering journal /sbin/e2fsck: unable to set superblock flags on /dev/hd-bootflash	12.3(1o)
CSCvf27593	The DHCP offer (relay packet) from the DHCP server gets dropped on the ToR that is connected to the server.	12.3(1o)

Bug ID	Description	Fixed In
CSCvf52033	A kernel crash is observed when an iping request is done with the -R option.	12.3(1o)
CSCvf59666	HAL crashes if the number of routes is beyond the scale limit and some routes are added and deleted quickly.	12.3(1o)
CSCvf65152	ipfib crashes if some routes are added and deleted quickly. This bug has a generic crash backtrace, which can happen due to multiple reasons. Check the FIB traces to determine the reason.	12.3(1o)
CSCvg16267	The dynamic tunnel that is needed for inter-pod traffic does not get setup when the stream that is sent is subjected to a policy-based redirect policy.	12.3(1o)
CSCvg18830	ipfib crashes if the number of routes is beyond the scale limit and some routes are added and deleted quickly.	12.3(1o)
CSCvg58924	ICMP traffic to between endpoints might get dropped, but other traffic, including TCP and UDP, are not impacted.	12.3(1o)
CSCvg65487	A ToR switch fails to join the fabric.	12.3(1o)
CSCvh51474	A leaf switch reloads while collecting tech support files, and there is a core file from the unicast Routing Information Base (RIB) process.	12.3(1o)
CSCvh53787	ipfib crashes if the number of routes is beyond the scale limit and some routes are added and deleted quickly.	12.3(1o)
CSCvh85309	Under certain situations, the log files for the forwarding traces are lost.	12.3(1o)
CSCvh89176	The loss of prefix list entries for a shared L3Out causes the leaf switch to stop advertising its subnets.	12.3(1o)
CSCvh91642	If VLAN scale limit is hit, the VLAN translation table will not be cleaned up even after removing overscale VLANs. This can introduce unexpected connectivity issues for those VLANs that do not have a translation entry.	12.3(1o)
CSCve75260	BGP and COOP are out of sync after endpoint flaps.	12.3(1p)
CSCve89025	A certain type of IP fragmented packet is always dropped by a Cisco N9K-C93180LC-EX, N9K-93180YC-EX, or N9K-C93108TC-EX leaf switch.	12.3(1p)
CSCvf65335	Fragmented packets with an IP fragment offset set to less than 0x14(20)=160 bytes are dropped on Cisco N9K-X9736C-EX, N9K-X97160YC-EX, and N9K-X9732C-EX leaf switches.	12.3(1p)

Bug ID	Description	Fixed In
CSCvg00085	After a Cisco N9K-C93180LC-EX leaf switch reload, the QSFP-40G-SR4 is not working; the Oper State of the port of the leaf switch is down. The only way to bring it up is to physically remove, then reinsert this QSFP. After the leaf switch reload, when QSFP-40G-SR4 does not work. The Oper State remains down even after performing the following actions: Disabling then enabling the port of the Leaf in the APIC GUI Changing the port configuration (link speed, ...) Unplugging and re-plugging the optical cable Disabling then enabling the port of the remote connected equipment	12.3(1p)
CSCvj76998	The ipfib service on a spine linecard experiences a HAP reset.	12.3(1p)

Known Behaviors

This section lists bugs that describe known behaviors. Click the Bug ID to access the Bug Search Tool and see additional information about the bug. The "Exists In" column of the table specifies the 12.3(1) releases in which the known behavior exists. A bug might also exist in releases other than the 12.3(1) releases.

Table 6 Known Behaviors in This Release

Bug ID	Description	Exists In
CSCuo37016	When configuring the output span on a FEX Hif interface, all the layer 3 switched packets going out of that FEX Hif interface are not spanned. Only layer 2 switched packets going out of that FEX Hif are spanned.	12.3(1e) and later
CSCuo50533	When output span is enabled on a port where the filter is VLAN, multicast traffic in the VLAN that goes out of that port is not spanned.	12.3(1e) and later
CSCup65586	The show interface command shows the tunnel's Rx/Tx counters as 0.	12.3(1e) and later
CSCup82908	The show vpc brief command displays the wire-encap VLAN Ids and the show interface .. trunk command displays the internal/hardware VLAN IDs. Both VLAN IDs are allocated and used differently, so there is no correlation between them.	12.3(1e) and later
CSCup92534	Continuous “threshold exceeded” messages are generated from the fabric.	12.3(1e) and later

Bug ID	Description	Exists In
CSCuq39829	Switch rescue user ("admin") can log into fabric switches even when TACACS is selected as the default login realm.	12.3(1e) and later
CSCuq46369	An extra 4 bytes is added to the untagged packet with Egress local and remote SPAN.	12.3(1e) and later
CSCuq77095	When the command show ip ospf vrf <vrf_name> is run from bash on the border leaf, the checksum field in the output always shows a zero value.	12.3(1e) and later
CSCuq83910	When an IP address moves from one MAC behind one ToR to another MAC behind another ToR, even though the VM sends a GARP packet, in ARP unicast mode, this GARP packet is not flooded. As a result, any other host with the original MAC to IP binding sending an L2 packet will send to the original ToR where the IP was in the beginning (based on MAC lookup), and the packet will be sent out on the old port (location). Without flooding the GARP packet in the network, all hosts will not update the MAC-to-IP binding.	12.3(1e) and later
CSCuq92447	When modifying the L2Unknown Unicast parameter on a Bridge Domain (BD), interfaces on externally connected devices may bounce. Additionally, the endpoint cache for the BD is flushed and all endpoints will have to be re-learned.	12.3(1e) and later
CSCuq93389	If an endpoint has multiple IPs, the endpoint will not be aged until all IPs go silent. If one of the IP addresses is reassigned to another server/host, the fabric detects it as an IP address move and forwarding will work as expected.	12.3(1e) and later
CSCur01336	The power supply will not be detected after performing a PSU online insertion and removal (OIR).	12.3(1e) and later
CSCur81822	The access-port operational status is always “trunk”.	12.3(1e) and later
CSCus18541	An MSTP topology change notification (TCN) on a flood domain (FD) VLAN may not flush endpoints learned as remote where the FD is not deployed.	12.3(1e) and later
CSCus29623	The transceiver type for some Cisco AOC (active optical) cables is displayed as ACU (active copper).	12.3(1e) and later
CSCus43167	Any TCAM that is full, or nearly full, will raise the usage threshold fault. Because the faults for all TCAMs on leaf switches are grouped together, the fault will appear even on those with low usage. Workaround: Review the leaf switch scale and reduce the TCAM usage. Contact TAC to isolate further which TCAM is full.	12.3(1e) and later

Bug ID	Description	Exists In
CSCus54135	The default route is not leaked by BGP when the scope is set to context. The scope should be set to Outside for default route leaking.	12.3(1e) and later
CSCus61748	If the TOR 1RU system is configured with the RED fan (the reverse airflow), the air will flow from front to back. The temperature sensor in the back will be defined as an inlet temperature sensor, and the temperature sensor in the front will be defined as an outlet temperature sensor. If the TOR 1RU system is configured with the BLUE fan (normal airflow), the air will flow from back to front. The temperature sensor in the front will be defined as an inlet temperature sensor, and the temperature sensor in the back will be defined as outlet temperature sensor. From the airflow perspective, the inlet sensor reading should always be less than the outlet sensor reading. However, in the TOR 1RU family, the front panel temperature sensor has some inaccurate readings due to the front panel utilization and configuration, which causes the inlet temperature sensor reading to be very close, equal, or even greater than the outlet temperature reading.	12.3(1e) and later
CSCut59020	If Backbone and NSSA areas are on the same leaf, and default route leak is enabled, Type-5 LSAs cannot be redistributed to the Backbone area.	12.3(1e) and later
CSCuu11347	Traffic from the orphan port to the vPC pair is not recorded against the tunnel stats. Traffic from the vPC pair to the orphan port is recorded against the tunnel stats.	12.3(1e) and later
CSCuu11351	Traffic from the orphan port to the vPC pair is only updated on the destination node, so the traffic count shows as excess.	12.3(1e) and later
CSCuu66310	If a bridge domain "Multi Destination Flood" mode is configured as "Drop", the ISIS PDU from the tenant space will get dropped in the fabric.	12.3(1e) and later
CSCuv57302	Atomic counters on the border leaf do not increment for traffic from an endpoint group going to the Layer 3 out interface.	12.3(1e) and later
CSCuv57315	Atomic counters on the border leaf do not increment for traffic from the Layer 3 out interface to an internal remote endpoint group.	12.3(1e) and later
CSCuv57316	TEP counters from the border leaf to remote leaf nodes do not increment.	12.3(1e) and later
CSCuw09389	For direct server return operations, if the client is behind the Layer 3 out, the server-to-client response will not be forwarded through the fabric.	12.3(1e) and later

Bug ID	Description	Exists In
CSCux97329	With the common pervasive gateway, only the packet destination to the virtual MAC is being properly Layer 3 forwarded. The packet destination to the bridge domain custom MAC fails to be forwarded. This is causing issues with certain appliances that rely on the incoming packets' source MAC to set the return packet destination MAC.	12.3(1e) and later
CSCuy00084	BCM does not have a stats option for yellow packets/bytes, and so BCM does not show in the switch or APIC GUI stats/observer.	12.3(1e) and later
CSCuy02543	Bidirectional Forwarding Detection (BFD) echo mode is not supported on IPv6 BFD sessions carrying link-local as the source and destination IP address. BFD echo mode also is not supported on IPv4 BFD sessions over multihop or VPC peer links.	12.3(1e) and later
CSCuy06749	Traffic is dropped between two isolated EPGs.	12.3(1e) and later
CSCuy22288	The iping command's replies get dropped by the QOS ingress policer.	12.3(1e) and later
CSCuy25780	An overlapping or duplicate prefix/subnet could cause the valid prefixes not to be installed because of batching behavior on a switch. This can happen during an upgrade to the 1.2(2) release.	12.3(1e) and later
CSCuy47634	EPG statistics only count total bytes and packets. The breakdown of statistics into multicast/unicast/broadcast is not available on new hardware.	12.3(1e) and later
CSCuy56975	You must configure different router MACs for SVI on each border leaf if L3out is deployed over port-channels/ports with STP and OSPF/OSPFv3/eBGP protocols are used. There is no need to configure different router MACs if you use VPC.	12.3(1e) and later
CSCuy61018	The default minimum bandwidth is used if the BW parameter is set to "0", and so traffic will still flow.	12.3(1e) and later
CSCuy96912	The debounce timer is not supported on 25G links.	12.3(1e) and later
CSCuz12913	An ACI leaf switch sends ARP to a device (such as a router or host) that belongs to directly connected subnets for an L3Out. After ARP is resolved, devices in directly connected subnets on two different L3Outs can talk each other without any contracts.	12.3(1e) and later
CSCuz13529	With the N9K-C93180YC-EX switch, drop packets, such as MTU or storm control drops, are not accounted for in the input rate calculation.	12.3(1e) and later

Bug ID	Description	Exists In
CSCuz13614	For traffic coming out of an L3out to an internal EPG, stats for the actrlRule will not increment.	12.3(1e) and later
CSCuz13810	When subnet check is enabled, a ToR does not learn IP addresses locally that are outside of the bridge domain subnets. However, the packet itself is not dropped and will be forwarded to the fabric. This will result in such IP addresses getting learned as remote endpoints on other ToRs.	12.3(1e) and later
CSCuz47058	SAN boot over a virtual Port Channel or traditional Port Channel does not work.	12.3(1e) and later
CSCuz65221	A policy-based redirect (PBR) policy to redirect IP traffic also redirects IPv6 neighbor solicitation and neighbor advertisement packets.	12.3(1e) and later
CSCva98767	The front port of the QSA and GLC-T 1G module has a 10 to 15-second delay as it comes up from the insertion process.	12.3(1e) and later
CSCvb36823	If you have only one spine switch that is part of the infra WAN and you reload that switch, there can be drops in traffic. You should deploy the infra WAN on more than one spine switch to avoid this issue.	12.3(1e) and later
CSCvb39965	Slow drain is not supported on FEX Host Interface (HIF) ports.	12.3(1e) and later
CSCvb49451	In the case of endpoints in two different TOR pairs across a spine switch that are trying to communicate, an endpoint does not get relearned after being deleted on the local TOR pair. However, the endpoint still has its entries on the remote TOR pair.	12.3(1e) and later
CSCvd11146	Bridge domain subnet routes advertised out of the Cisco ACI fabric through an OSPF L3Out can be relearned in another node belonging to another OSPF L3Out on a different area.	12.3(1e) and later
CSCvd63567	After upgrading a switch, Layer 2 multicast traffic flowing across PODs gets affected for some of the bridge domain Global IP Outsides.	12.3(1e) and later
CSCvd80766	When IGMP snooping is disabled on a bridge domain across the fabric, if a N9K-X9636 series switch is a transit leaf switch in the traffic path and the bridge domain is not deployed on the transit leaf switch, IGMP control packets will not be flooded and instead will be consumed by the switch.	12.3(1e) and later

- IPN should preserve the CoS and DSCP values of a packet that enters IPN from the ACI spine switches. If there is a default policy on these nodes that change the CoS value based on the DSCP value or by any other mechanism, you must apply a policy to prevent the CoS value from being changed. At the minimum, the

remarked CoS value should not be 4, 5, 6 or 7. If CoS is changed in the IPN, you must configure a multipod QoS policy in the ACI for the multipod that translates queuing class information of the packet into the DSCP value in the outer header of the iVXLAN packet.

- The following properties within a QoS class under "Global QoS Class policies," should not be changed from its default value and is only used for debugging purposes:
  - MTU (default – 9216 bytes)
  - Queue Control Method (default – Dynamic)
  - Queue Limit (default – 1522 bytes)
  - Minimum Buffers (default – 0)
- The modular chassis Cisco ACI spine nodes, such as the Cisco Nexus 9508, support warm (stateless) standby where the state is not synched between the active and the standby supervisor modules. For an online insertion and removal (OIR) or reload of the active supervisor module, the standby supervisor module becomes active, but all modules in the switch are reset because the switchover is stateless. In the output of the show system redundancy status command, warm standby indicates stateless mode.
- When a recommissioned APIC controller rejoins the cluster, GUI and CLI commands can time out while the cluster expands to include the recommissioned APIC controller.
- If connectivity to the APIC cluster is lost while a switch is being decommissioned, the decommissioned switch may not complete a clean reboot. In this case, the fabric administrator should manually complete a clean reboot of the decommissioned switch.
- Before expanding the APIC cluster with a recommissioned controller, remove any decommissioned switches from the fabric by powering down and disconnecting them. Doing so will ensure that the recommissioned APIC controller will not attempt to discover and recommission the switch.

IGMP Snooping Known Behaviors:

- Multicast router functionality is not supported when IGMP queries are received with VxLAN encapsulation.
- IGMP Querier election across multiple Endpoint Groups (EPGs) or Layer 2 outsides (External Bridged Network) in a given bridge domain is not supported. Only one EPG or Layer 2 outside for a given bridge domain should be extended to multiple multicast routers if any.
- The rate of the number of IGMP reports sent to a leaf switch should be limited to 1000 reports per second.
- Unknown IP multicast packets are flooded on ingress leaf switches and border leaf switches, unless "unknown multicast flooding" is set to "Optimized Flood" in a bridge domain. This knob can be set to "Optimized Flood" only for a maximum of 50 bridge domains per leaf.

  If "Optimized Flood" is enabled for more than the supported number of bridge domains on a leaf, follow these configuration steps to recover:
  - Set "unknown multicast flooding" to "Flood" for all bridge domains mapped to a leaf.
  - Set "unknown multicast flooding" to "Optimized Flood" on needed bridge domains.

Related Documentation

The Cisco Application Policy Infrastructure Controller (APIC) documentation can be accessed from the following website:

https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html