



Cisco Nexus 9000 ACI-Mode Switches

Release Notes, Release 12.0(2)

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 Notes, Release 2.0(2)*, 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 12.0(2) 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
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	12.0(2f): In the Resolved Bugs section, added bug CSCvr98827.
September 20, 2019	In the Usage Guidelines section, added the following bullet: <ul style="list-style-type: none">■ 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.
August 14, 2019	12.0(2l): In the Open Bugs section, added bug CSCvp92269.

Date	Description
July 31, 2019	In the Compatibility Information section, added the following bullet: <ul style="list-style-type: none"> ■ 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	12.0(2f): In the Open Bugs section, added bug CSCvn69340.
January 28, 2019	12.0(2f): In the Open Bugs section, added bug CSCvi76161.
February 19, 2018	12.0(2f): In the Open Bugs section, added bug CSCvc18574.
October 5, 2017	12.0(2o): Release 12.0(2o) became available; added CSCve26184 to resolved bugs.
March 23, 2017	12.0(2n): Release 12.0(2n) became available; added resolved bugs.
January 25, 2017	12.0(2m): Release 12.0(2m) became available. Added the resolved bugs for this release.
December 6, 2016	In the "Usage Guidelines" section, removed the bullet that began with, " GARP flooding is enabled by default for the Cisco Nexus 93180YC-EX switch..." GARP flooding is now disabled by default for 93180YC-EX switches.
November 21, 2016	12.0(2l): Release 12.0(2l) became available. Added the resolved bugs for this release.
October 28, 2016	In the Supported FEX Models section, added N2K-B22HP-P.
October 27, 2016	12.0(2g): Added the Cisco N9K-PUV-1200W power supply to the New Hardware Features section. Added open bug CSCvb84900.
October 13, 2016	12.0(2h): Release 12.0(2h) became available. Added the resolved bugs for this release.
September 21, 2016	12.0(2g): Added open bugs CSCvb38815 and CSCvb39177.
September 19, 2016	12.0(2g): Release 12.0(2g) became available. Added the resolved bugs for this release.
August 22, 2016	12.0(2f): Release 12.0(2f) 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 12.0 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-M6PQ	6-port
Pluggable module (GEM)	N9K-M6PQ-E	6-port, 40 Gigabit Ethernet expansion module
Pluggable module (GEM)	N9K-M12PQ	12-port or 8-port
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

Supported Hardware

Hardware Type	Product ID	Description
Spine switch	N9K-C9516	Cisco Nexus 9516 switch with 16 line card slots Note: This switch supports up to 10 line cards.
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-B	Cisco Nexus 9500 Series supervisor module
Top-of-rack (ToR) leaf switch	N9K-C93108TC-EX	Cisco Nexus 9300 with 48-port 1/10 Gigabit-T and 6-port 100 Gigabit Ethernet QSFP28 switch
Top-of-rack (ToR) leaf switch	N9K-C93120TX	Cisco Nexus 9300 with 96-port 1/10 Gigabit-T and 6-port 40 Gigabit Ethernet QSFP switch
Top-of-rack (ToR) leaf switch	N9K-C93128TX	Cisco Nexus 9300 96-port, 1-/10-Gbps BASE-T and 6-port or 8-port, 40 Gigabit Ethernet QSFP switch

Supported Hardware

Hardware Type	Product ID	Description
Top-of-rack (ToR) leaf switch	N9K-C93180YC-EX	Cisco Nexus 9300 Fixed with 48-port 10/25 Gigabit and 6-port 40/100 Gigabit QSFP28
Top-of-rack (ToR) leaf switch	N9K-C9332PQ	Cisco Nexus 9332PQ 32-port 40 Gigabit Ethernet QSFP+ Top-of-rack (ToR) Layer 3 switch
Top-of-rack (ToR) leaf switch	N9K-C9372PX	Cisco Nexus 9372PX 48-port, 10 Gigabit Ethernet SFP+ and 6-port 40 Gigabit Ethernet QSFP+ Top-of-rack (ToR) Layer 3 switch 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 48-port, 10 Gigabit Ethernet SFP+ and 6-port 40 Gigabit Ethernet QSFP+ Top-of-rack (ToR) Layer 3 switch 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 48-port, 1/10 Gbps Base-T and 6-port, 40 Gigabit Ethernet QSFP Top-of-rack (ToR) Layer 3 switch
Top-of-rack (ToR) leaf switch	N9K-C9372TX-E	Cisco Nexus 9372TX-E 48-port 1/10 Gbps Base-T and 6-port 40 Gbps Ethernet QSFP+ Top-of-rack (ToR) Layer 3 switch
Top-of-rack (ToR) leaf switch	N9K-C9396PX	Cisco Nexus 9300 48-port, 1/10 Gigabit Ethernet SFP+ and 6-port or 12-port, 40 Gigabit Ethernet QSFP switch
Top-of-rack (ToR) leaf switch	N9K-C9396TX	Cisco Nexus 9300 48-port, 1/10 Gbps Base-T and 6-port or 12-port, 40 Gigabit Ethernet QSFP switch
Top-of-rack (ToR) leaf switch power supply unit	N9K-PAC-650W-B	650W AC Power supply, port side exhaust pluggable

Supported Hardware

Hardware Type	Product ID	Description
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-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-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
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.

Supported FEX Models

Hardware Type	Product ID	Description
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 9336PO ACI-mode switches.
Top-of-rack (ToR) leaf switch power supply unit	UCS-PSU-6332-DC	930W DC power supply, reversed airflow (port side exhaust)
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 fan	NXA-FAN-30CFM-F	Port side exhaust fan
Top-of-rack (ToR) leaf switch fan	NXA-FAN-30CFM-B	Port side intake fan

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

New and Changed Information

Product ID	Description
N2K-C2248PO-10GE	Cisco Nexus 2248PO 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 6tQSFP+ 10/40 Gigabit Ethernet fabric interfaces
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

Cisco NX-OS release 12.0(2) supports the following new hardware features:

- The 12.0(2g) release adds support for the Cisco N9K-PUV-1200W power supply on the N9K-C9396PX and N9K-C9396TX switches. Due to open bug CSCvb84900, if you hot swap the PSU on a N9K-C9396TX or N9K-C9396PX switch in any of the 12.0 releases, you must perform a hard reset of the switch.

New Software Features

For new software features, see the *Cisco APIC 2.0(2) 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 the Cisco AVS, Release 5.2(1)SV3(2.1).
- Link level flow control is not supported on ACI-mode switches.
- The breakout of 40G ports to 4x10G on the N9332PQ switch is not supported in ACI-Mode.
- 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 N9396PX, N9372PX, or N9372PX-E switches
- 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.

Bugs

- 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: HTTPSS
- UDP SrcPort 123: NTP
- UDP DstPort 123: NTP

- Leafs and spines 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.

Bugs

- 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 instrlImmedcy 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 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 12.0(2) releases in which the bug exists. A bug might also exist in releases other than the 12.0(2) releases.

Table 4 Open Bugs in This Release

Bug ID	Description	Exists In
CSCvc86597	There is traffic loss on VxLAN endpoints for Layer 2 traffic between PODs.	12.0(2m) and later
CSCvp92269	Running a Qualys security scan results in the following message: CWE - 693 Protection Mechanism Failure - "HTTP Security Header Not Detected"	12.0(2l) and later

Bugs

Bug ID	Description	Exists In
CSCvb38815	An IPFIB core was dumped on a leaf switch after executing the VPC Leaf Stateful Reload Serial Order.	12.0(2g) and later
CSCvb39177	Traffic gets dropped after deleting or adding a context.	12.0(2g) and later
CSCvb84900	Auto-polling does not work on N9K-C9396TX and N9K-C9396PX switches after hot swapping the PSU.	12.0(2g) and later
CSCvc18574	Local endpoints are installed without a "Bounce" flag and point to a remote tunnel instead of a local interface.	12.0(2f) through 12.0(2l)
CSCun35596	FEX logs are missing in the output of the show fex detail command.	12.0(2f) and later
CSCun96495	The events and faults for interfaces are not updated under Ports in the GUI.	12.0(2f) and later
CSCup05629	The output of some CLI commands display very slowly.	12.0(2f) and later
CSCup86130	Because ibash is implemented on top of bash, when using ibash for the CLI, the bash behavior is inherited. For example, the sh mod command works in traditional Cisco switches. But when executed on N9K switches in ibash, because bash interprets sh differently, sh mod will not work. Similarly, if there is a clash in the next available options, the TAB key must be pressed twice to get the options rather than once as in other Cisco switches. In short, the CLI infra for ibash is not exactly the same as the CLI infra for the traditional Cisco switches because N9K ibash is built on top of bash.	12.0(2f) and later
CSCur32247	FEX-related diagnostic results are missing.	12.0(2f) and later
CSCva17432	If the PIM and multicast source is behind a Layer 3 out or is internal, receivers on the inside stop receiving multicast traffic. When vtep moves from one FI (FI-A) to the other FI (FI-B) VPC, multicast traffic stops.	12.0(2f) and later
CSCva27324	The virtual Fibre Channel (VFC) NP port enters the flogi-fail-retry state followed by the down state if there is a user-configured mismatch of the VSAN and VLAN mapping between the leaf switch and the Fibre Channel Forwarder (FCF). To recover the VFC NP port, delete the wrong VLAN-VSAN mapping on the leaf switch, delete and recreate the VLAN pool/encapsulation block if needed, and then create the correct VLAN-VSAN mapping.	12.0(2f) and later
CSCvi76161	A version mismatch between Cisco ACI leaf switches causes the EPM process to crash and a HAP reset to occur.	12.0(2f) and later
CSCvn69340	The BFD session does not get instantiated under some circumstances in one of the VPC legs for static routes.	12.0(2f) and later

Bugs

Bug ID	Description	Exists In
CSCvp50075	A leaf switch experiences an unexpected reload due to a HAP reset.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) 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
CSCva11574	When a port is applied with speed 100M and is configured with Autoneg-off, the link does not come up. For 100M speed, Autoneg-OFF is not supported.	12.0(2f)
CSCva92042	There is connectivity loss when a fabric has half N9K-93108TC-EX or N9K-93180YC-EX leaf switches and half N9K-93128TX, N9K-9396PX, or N9K-9396TX leaf switches leafs in VPC pairs. This occurs because the Multichassis EtherChannel module (MCECM) brings down the ports in the VPC when there is a domain mismatch between a N9K-93108TC-EX or N9K-93180YC-EX leaf switch and a N9K-93128TX, N9K-9396PX, or N9K-9396TX leaf switch.	12.0(2g)

Bugs

Bug ID	Description	Fixed In
CSCvb02613	A border leaf drops packets from a WAN router. This occurs when the L3out is shared with inter-VRF routing leaking, the L3out is shared in tenant Common, and the bridge domain is in a user tenant.	12.0(2g)
CSCvb03876	After the flapping of a physical interface (or port channel) on which an IGMP report is received through the VxLAN tunnel, such as Cisco AVS, that interface stops sending multicast traffic even though the IGMP report is still received on that interface after the flap.	12.0(2g)
CSCvb29717	There is traffic loss during VPC migration from an N9K-93128TX, N9K-9396PX, or N9K-9396TX switch to an N9K-93108TC-EX or N9K-93180YC-EX switch due to the multichassis EtherChannel trunk (MCT) being down.	12.0(2g)
CSCva75322	The snmpwalk command with the ifDescr keyword returns the value of ifAlias instead of the value of ifName.	12.0(2h)
CSCvb75573	LACP PDU's received with an 802.1 tagged might be dropped by a Cisco ACI leaf switch. As a result, LACP port channeling might fail, causing an interface to go into the suspended state or standalone/individual state.	12.0(2l)
CSCvb75623	FEXes on the same parent leaf switch reboot when a large amount of untagged traffic is injected into a FEX HIF that does not have a native/untag VLAN configured.	12.0(2l)
CSCvb77513	Traffic does not pass on VLANs that have more than 64 leaf switch to spine switch connections on a given spine switch.	12.0(2l)
CSCvb72043	IP endpoint programming fails. The epmc-trace.txt logs contains error messages similar to the following example: [2016 Oct 12 14:31:03.088915862:215149860:epmc_pd_bcm_batch_flush:1006:E] BCM_ERR: Failed TLV_TYPE_MY_L3_HOST_CREATE rv:-6 host_rv:0 egr_rv:-6 [2016 Oct 12 14:31:03.088916854:215149861:epmc_pd_bcm_ep_prog_fail:716:E] Programming failed for ep key: EPM EP IPV4 key :: VRF 2686976 IP:=10.58.12.22 [2016 Oct 12 14:31:03.088920707:215149863:epmc_pd_bcm_ep_prog_fail:728:E] BCM programming failed for EP, inserting ep to failed list	12.0(2l)
CSCvb61146	Spine and leaf switches cannot sync with the "Absolute Time Server" NTP server, but the APIC can.	12.0(2l)
CSCva60517	IPFIB crashes on a Cisco ACI leaf switch when there is a high number of IPv6 neighbor discoveries present on one or more Layer 2-only bridge domains.	12.0(2m)
CSCvc18574	Local endpoints are installed without a "Bounce" flag and point to a remote tunnel instead of a local interface.	12.0(2m)
CSCvc33849	AVS attached endpoints are not learned locally and the AVS tunnel is incorrectly pointing to the fabric instead of a local vPC interface.	12.0(2m)

Bugs

Bug ID	Description	Fixed In
CSCvc66860	The CPU queue fills up after pause frames are received at a high rate. The issue can manifest itself in various ways as CPU transmit frames are dropped in hardware: FEX might fail to come online if this queue is full because control plane process related to FEX discovery cannot send or receive all messages responsible for the bring-up. Endpoints connected to ACI leaf switches have intermittent connectivity, as ARP might fail to resolve on the host. Spine links to the affected leaf switch might be marked as "out-of-service" and LLDP adjacency will no longer be present.	12.0(2m)
CSCvd04264	Sclass is set to zero when a remote EP is logged through GARP. This might drop packets to the EP.	12.0(2n)
CSCvb44975	Issuing tech support local command on the leaf causes the crash and reload of the leaf.	12.0(2n)
CSCve26184	Cisco ACI leaf switch might automatically reboot as a result of an EPMC crash.	12.0(2o)

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 12.0(2) releases in which the known behavior exists. A bug might also exist in releases other than the 12.0(2) 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.	12.0(2f) 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.	12.0(2f) and later
CSCup65586	The show interface command shows the tunnel's Rx/Tx counters as 0.	12.0(2f) 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.	12.0(2f) and later
CSCup92534	Continuous "threshold exceeded" messages are generated from the fabric.	12.0(2f) and later

Bugs

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.	12.0(2f) and later
CSCuq46369	An extra 4 bytes is added to the untagged packet with Egress local and remote SPAN.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) and later
CSCur01336	The power supply will not be detected after performing a PSU online insertion and removal (OIR).	12.0(2f) and later
CSCur81822	The access-port operational status is always "trunk".	12.0(2f) 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.	12.0(2f) and later
CSCus29623	The transceiver type for some Cisco AOC (active optical) cables is displayed as ACU (active copper).	12.0(2f) 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.	12.0(2f) and later

Bugs

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.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) and later
CSCuv57316	TEP counters from the border leaf to remote leaf nodes do not increment.	12.0(2f) 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.	12.0(2f) and later

Bugs

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.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) and later
CSCuy06749	Traffic is dropped between two isolated EPGs.	12.0(2f) and later
CSCuy22288	The iping command's replies get dropped by the QOS ingress policer.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) 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.	12.0(2f) and later
CSCuy61018	The default minimum bandwidth is used if the BW parameter is set to "0", and so traffic will still flow.	12.0(2f) and later
CSCuy96912	The debounce timer is not supported on 25G links.	12.0(2f) 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.	12.0(2f) and later
CSCuz13614	For traffic coming out of an L3out to an internal EPG, stats for the actrlRule will not increment.	12.0(2f) and later

Bugs

Bug ID	Description	Exists In
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.	12.0(2f) and later
CSCuz47058	SAN boot over a virtual Port Channel or traditional Port Channel does not work.	12.0(2f) and later
CSCuz65221	A policy-based redirect (PBR) policy to redirect IP traffic also redirects IPv6 neighbor solicitation and neighbor advertisement packets.	12.0(2f) and later
CSCva21406	When nodes in the pod are running with mixed releases of the 12.0(x) release and pre-11.2(2) release, this can lead ISIS to core on the pre-11.2(2) release nodes.	12.0(2f) 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.

Related Documentation

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>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2016-2021 Cisco Systems, Inc. All rights reserved.