Cisco NX-OS Release 12.2(3) Release Notes for Cisco Nexus 9000 Series ACI-Mode Switches

This document describes the features, caveats, 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 2.2(3), 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 caveats. See the following website for the most recent version of the *Cisco NX-OS Release 12.2(3) 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
September 7, 2017	12.2(3j): Release 12.2(3j) became available.
November 13, 2017	12.2(3p): Release 12.2(3p) became available. Added the resolved caveats for this release.
December 2, 2017	12.2(3r): Release 12.2(3r) became available. Added the resolved caveats for this release.
December 6, 2017	12.2(3j): In the Know Behaviors section, added caveat CSCvd63567.
December 21, 2017	12.2(3s): Release 12.2(3s) became available. Added the resolved caveats for this release.
February 19, 2018	12.2(3t): Release 12.2(3t) became available. Added the resolved caveats for this release.
April 24, 2018	12.2(3j): In the Open Caveats section, added bug CSCvi57920.
June 7, 2018	12.2(3j): In the Open Caveats section, added bug CSCvg35892.
October 24, 2018	12.2(3j): In the Open Caveats section, added bug CSCvm66008.

Contents

Contents

This document includes the following sections:

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-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

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 platform switch with 48 1/10GBASE-T (copper) APIC-facing ports and 6 100-Gigabit Ethernet QSFP28 spine-facing ports
Top-of-rack (ToR) leaf switch	N9K-C93108TC-FX	Cisco Nexus 9300 platform switch with 48 1/10GBASE-T (copper) APIC-facing ports and 6 fixed 40/100-Gigabit Ethernet QSFP28 spine-facing ports

Hardware Type	Product ID	Description
Top-of-rack (ToR) leaf switch	N9K-C93120TX	Cisco Nexus 9300 platform switch with 96 1/10GBASE-T (copper) APIC-facing ports and 6-port 40-Gigabit Ethernet QSFP spine-facing ports
Top-of-rack (ToR) leaf switch	N9K-C93128TX	Cisco Nexus 9300 platform switch with 96 1/10GBASE-T (copper) APIC-facing 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 APIC-facing ports and 6 10/40/100-Gigabit QSFP28 spine-facing ports 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-C93108TC-FX	Cisco Nexus 9300 platform switch with 48 1/10GBASE-T (copper) APIC-facing ports and 6 fixed 40/100-Gigabit Ethernet QSFP28 spine-facing ports
Top-of-rack (ToR) leaf switch	N9K-C93180YC-EX	Cisco Nexus 9300 platform switch with 48 10/25-Gigabit APIC-facing ports and 6-port 40/100 Gigabit QSFP28 spine-facing ports

Hardware Type	Product ID	Description
Top-of-rack (ToR) leaf switch	N9K-C93180YC-FX	Cisco Nexus 9300 platform switch with 48 10/25-Gigabit Ethernet SFP28 APIC-facing 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.
Top-of-rack (ToR) leaf switch	N9K-C9332PQ	Cisco Nexus 9332PQ Top-of-rack (ToR) Layer 3 switch with 32 40-Gigabit Ethernet QSFP+ APIC-facing ports
Top-of-rack (ToR) leaf switch	N9K-C9372PX	Cisco Nexus 9372PX Top-of-rack (ToR) Layer 3 switch with 48 10GBASE-T (copper) Ethernet SFP+ APIC-facing 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 10GBASE-T (copper) Ethernet SFP+ APIC-facing 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) APIC-facing 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) APIC-facing 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 1/10GBASE-T (copper) SFP+ APIC-facing ports and 6 or 12 40-Gigabit Ethernet QSFP spine-facing ports

Hardware Type	Product ID	Description
Top-of-rack (ToR) leaf switch	N9K-C9396TX	Cisco Nexus 9300 platform switch with 48 1/10GBASE-T (copper) APIC-facing ports and 6 or 12 40-Gigabit Ethernet QSFP spine-facing ports
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-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.

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 9336PQ 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
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

Product ID	Description
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 100Mï1/10 Gigabit Ethernet and Unified Port host interfaces (SFP+) and up to 6ïQSFP+ 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 (required SFP/SFP+) + 8x10GE (required 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 (required 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

There are no new hardware features in this release.

New Software Features

For new software features, see the *Cisco APIC 2.2(3) 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

Compatibility Information

This release supports the hardware and software listed on the Cisco ACI Ecosystem Compatibility List, and supports the Cisco AVS, Release 5.2(1)SV3(2.14).

To connect the N2348UPQ to Cisco ACI leaf switches, the following options are available:

- Directly connect the 40G FEX ports on the N2348UPQ to the 40G switch ports on the Cisco ACI leaf switches

- Break out the 40G FEX ports on the N2348UPQ to 4x10G ports and connect to the 10G ports on all other Cisco 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 Cisco ACI fabric, it is required to have a 10G interface on the ACI leaf. You cannot connect the Cisco APIC directly to the N9332PQ Cisco ACI leaf switch.

Usage Guidelines

The following list shows the current protocols that are allowed and cannot be blocked through contracts. Some of the protocols have a SrcPort/DstPort distinction.

- 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 switches and spine switches from two different fabrics cannot be connected regardless of whether the links are administratively kept down.

Note: See the Cisco 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

Caveats

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

- Known Limitations
- Open Caveats
- Resolved Caveats

- 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 Caveats

This section lists the open caveats. Click the bug ID to access the Bug Search tool and see additional information about the bug. If a caveat is fixed in a patch of this release, the "Patch Fixed In" column of the tables specifies the release.

Open Caveats in the 12.2(3j) Release

The following table lists the open caveats in the 12.2(3j) release.

Table 4 Open Caveats in the 12.2(3j) Release

Bug ID	Description	Fixed In
CSCvf85014	Multicast traffic loss might occur during spine switch upgrade/reload when at least one fabric link port from spine switch to ToR is in "admin down" state.	
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.	
CSCvi57920	A UCS 1225 vNIC goes down after changing the peer Cisco ACI leaf node name.	
CSCvm66008	When you have two NSSA areas deployed on a vPC leaf switch pair that also see each other as OSPF peers and both L3Outs have the default route leak policy configured, then if you delete one of the L3Outs, the following things occur: • OSPF generates the default route without a tag • The peer installs that route in RIB • The peer redistributes the route into BGP • The peer advertises the route to rest of the leaf switches This issue blackholes all traffic that uses the default route.	

Open Caveats in the 12.2(3p) Release

There are no new open caveats in the 12.2(3p) release.

Open Caveats in the 12.2(3r) Release

There are no new open caveats in the 12.2(3r) release.

Open Caveats in the 12.2(3s) Release

There are no new open caveats in the 12.2(3s) release.

Open Caveats in the 12.2(3t) Release

There are no new open caveats in the 12.2(3t) release.

Resolved Caveats

This section lists the resolved caveats. Click the bug ID to access the Bug Search tool and see additional information about the bug.

Resolved Caveats in the 12.2(3j) Release

The following are resolved caveats in the 12.2(3j) release.

Table 5 Resolved Caveats in the 12.2(3j) Release

Bug ID	Description
CSCve05164	A leaf switch might send a DHCP request with an empty model or with a wrong pod model. This might break connectivity to the affected host.
CSCve26184	A Cisco Nexus 9000 Series ACI-Mode leaf switch might reboot if the endpoint manager client (EPMC) crashes.
CSCvd80459	The Broadcom “HiGig” link might go down for some links, causing traffic to those links to be destroyed or discarded without informing the sender or recipient of the traffic’s failed delivery.
CSCve25234	When the OpFlex traffic packet is in transit from the spine switch, the spine switch might be programming zero source MAC [What does this mean?] on the infra native transit packets, which might cause an OpFlex connection failure.
CSCve58800	Inband management might become unavailable after upgrading to one of the Cisco Nexus 9000 Series ACI-Mode Switch 12.2 releases.
CSCvb42675	The Endpoint Manager (EPM) process might leak memory when adding or removing an Attachable Access Entity Profile (AEP).
CSCvc21356	A N9K-C93108TC-EX switch might forward large packets (> 381 byte IP packets) as CRC errors if the switch receives the packets on a 100Mbp speed interface and transmits the packets to a 1 gigabit interface on the same leaf switch.
CSCvd87231	A fault F1321 might be raised and cleared periodically for all fan slots on a leaf switch.
CSCve04932	After an upgrading or downgrading a switch from the Cisco NX-OS Release 12.2(1o) or 12.2(1n), the Hot Standby Router Protocol (HSRP) virtual IP might be unreachable and the Address Resolution Protocol (ARP) table on external devices will show that the MAC for the virtual IP (VIP) is “Incomplete.” The external device ARP table might show that the MAC address for the VIP is the MAC address of the active IP interface and not the virtual MAC address. This might disable redundancy when the active leaf switch goes down.
CSCve30327	The Border Gateway Protocol (BGP) might be unable to form a neighbor connection across a Cisco ACI fabric where at least one leaf switch is an “EX” leaf.
CSCve40338	The fabric modules of a Cisco Nexus 9500 switch that is in ACI mode might enter the unrecoverable error status after the diagnostic level of the fabric modules get changed to full and the fabric modules are rebooted.

Bug ID	Description
CSCve56651	The connection between a local host/client and server might fail to form when using a contract filter that uses the "established" designation as a TCP session rule on older model Cisco Nexus 9000 Series ACI-mode "-EX" leaf switches.
CSCve79605	The HSRP virtual MAC address might attach from the virtual PortChannel (vPC) orphan port and might be announced with the vPC's virtual IP address instead of the physical IP address.
CSCvf01042	During an endpoint move between two leaf switches, a third leaf switch might maintain the old endpoint information.
CSCvd56870	In a multi-pod configuration with a single Layer 3 Out (L3out) distributed across four border leaf switches (two in pod 1 and two in pod 2), traffic might drop at the transit border leaf switch if the bounce bit is set.
CSCvf43074	Remote IP learning might be limited to a single bridge domain (BD) subnet.
CSCvd10246	If an ECMP route exists in the inband management VRF instance and is later deleted, there might be stale routes that cause forwarding issues.
CSCve39801	Simple Network Management Protocol (SNMP) process memory usage might increase because of continuous interface route flap.
CSCvd77155	An Open Shortest Path First (OSPF) session between border ToR switches using the stretched Switched Virtual Interface (SVI) might end and adjacency might point to an incorrect tunnel interface.

Resolved Caveats in the 12.2(3p) Release

The following are resolved caveats in the 12.2(3p) release.

Table 6 Resolved Caveats in the 12.2(3p) Release

Bug ID	Description
CSCve19668	The ACLQOS or Hardware Abstraction Layer (HAL) process might fail when there are multiple access SPAN sessions configured in both directions coupled with tenant SPAN.
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.
CSCvf32867	The EPM show commands do not work when the VRF instance name size is more than 32 characters.
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
CSCvg13666	A switch virtual interface (SVI) is down and does not come up.
CSCvg37153	Switches have a memory leak that can potentially lead to an out of memory reload, and the TAH_MEM_ENUM_tah_sug_fta_filtertcamdata table is seeing much greater memory allocation and usage than other nodes in the environment.

Resolved Caveats in the 12.2(3r) Release

The following are resolved caveats in the 12.2(3r) release.

Table 7 Resolved Caveats in the 12.2(3r) Release

Bug ID	Description
CSCve06787	Fault F2571 sometimes displays on leaf switches that are being used for Cisco Tetration Analytics integration.
CSCve08739	When using GOLF, a ping from outside or inside the Cisco ACI fabric to the GOLF router will not be successful.
CSCvf89664	An SNMP core is dumped when an SNMP context name is configured as null.
CSCvf99198	Bidirectional forwarding detection sessions between a Cisco ACI ToR and N7K keep flapping and never come up.
CSCvg58924	ICMP traffic to between endpoints might get dropped, but other traffic, including TCP and UDP, are not impacted.

Resolved Caveats in the 12.2(3s) Release

The following are resolved caveats in the 12.2(3s) release.

Table 8 Resolved Caveats in the 12.2(3s) Release

Bug ID	Description
CSCve19790	After a link is disabled between a policy element (PE) device and a GOLF N7000-series switch, the VxLAN tunnel between Cisco ACI leaf switches and the GOLF N7000-series switch is removed. Pings from endpoints in Cisco ACI to the PE device that is connected to GOLF devices begin to fail. Reenabling the link does not resolve the issue.
CSCve03012	When traffic flows from the internal leaf switch side to the external leaf switch side, from IntLeafs to ExtLeaf, the traffic is load-balanced well. However, from ExtLeaf to the external side, the traffic is not load-balanced; the traffic uses a single path only (it is polarized). After eliminating one of the two external leaf switches, the remained Ext_Leaf#1 switch sends traffic with both of the ECMP links. Additionally, when packets are generated through the other port of InternalLeaf#1 in the case of traffic that was injected through two ports from InternalLeaf#1, the traffic is transmitted through the other ECMP port of Ext_Leaf#1. In this case, both of links in Ext_Leaf#1 were used correctly.

Resolved Caveats in the 12.2(3t) Release

The following are resolved caveats in the 12.2(3t) release.

Table 9 Resolved Caveats in the 12.2(3t) Release

Bug ID	Description
CSCvh91642	If the VLAN scale limit is hit, the VLAN translation table will not be cleaned up even after removing the VLANs that exceed the scale limit. This can introduce unexpected connectivity issues for the VLANs that do not have a translation entry.
CSCvh64426	The RJ45 link does not come up when connecting to an N9K-C93108TC-EX switch at 100 Mbps.

Known Behaviors

This section lists caveats that describe known behaviors. Click the Bug ID to access the Bug Search Tool and see additional information about the bug.

Known Behaviors in the 12.2(3j) Release

The following table lists caveats that describe known behaviors in the 12.2(3j) release.

Table 10 Known Behaviors in the 12.2(3j) Release

Bug ID	Description
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.
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.
CSCup65586	The show interface command shows the tunnel's Rx/Tx counters as 0.
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.
CSCup92534	Continuous “threshold exceeded” messages are generated from the fabric.
CSCuq39829	Switch rescue user ("admin") can log into fabric switches even when TACACS is selected as the default login realm.
CSCuq46369	An extra 4 bytes is added to the untagged packet with Egress local and remote SPAN.
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.
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.

Bug ID	Description
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.
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.
CSCur01336	The power supply will not be detected after performing a PSU online insertion and removal (OIR).
CSCur81822	The access-port operational status is always “trunk”.
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.
CSCus29623	The transceiver type for some Cisco AOC (active optical) cables is displayed as ACU (active copper).
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.
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.
CSCus61748	If the TOR 1RU system is configured with the RED fan (the reverse airflow), the air will flow from back to front. 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 front to back. 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.
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.
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.
CSCuu11351	Traffic from the orphan port to the vPC pair is only updated on the destination node, so the traffic count shows as excess.
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.

Bug ID	Description
CSCuv57302	Atomic counters on the border leaf do not increment for traffic from an endpoint group going to the Layer 3 out interface.
CSCuv57315	Atomic counters on the border leaf do not increment for traffic from the Layer 3 out interface to an internal remote endpoint group.
CSCuv57316	TEP counters from the border leaf to remote leaf nodes do not increment.
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.
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.
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.
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.
CSCuy06749	Traffic is dropped between two isolated EPGs.
CSCuy22288	The iping command's replies get dropped by the QOS ingress policer.
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.
CSCuy47634	EPG statistics only count total bytes and packets. The breakdown of statistics into multicast/unicast/broadcast is not available on new hardware.
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.
CSCuy61018	The default minimum bandwidth is used if the BW parameter is set to "0", and so traffic will still flow.
CSCuy96912	The debounce timer is not supported on 25G links.
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.
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.
CSCuz13614	For traffic coming out of an L3out to an internal EPG, stats for the actrlRule will not increment.
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.

Bug ID	Description
CSCuz47058	SAN boot over a virtual Port Channel or traditional Port Channel does not work.
CSCuz65221	A policy-based redirect (PBR) policy to redirect IP traffic also redirects IPv6 neighbor solicitation and neighbor advertisement packets.
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.
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.
CSCvb39965	Slow drain is not supported on FEX Host Interface (HIF) ports.
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.
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.
CSCvd63567	After upgrading a switch, Layer 2 multicast traffic flowing across PODs gets affected for some of the bridge domain Global IP Outsides.

- 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 Cisco Nexus 9508 ACI-mode switch supports 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.

Known Behaviors in the 12.2(3p) Release

There are no new known behaviors in the 12.2(3p) release.

Known Behaviors in the 12.2(3r) Release

There are no new known behaviors in the 12.2(3r) release.

Known Behaviors in the 12.2(3s) Release

There are no new known behaviors in the 12.2(3s) release.

Known Behaviors in the 12.2(3t) Release

There are no new known behaviors in the 12.2(3t) release.

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