Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 13.1(2)

The Cisco NX-OS software for the Cisco Nexus 9000 series switches 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 13.1 works only on Cisco Nexus 9000 Series switches in ACI Mode.

This document describes the features, bugs, and limitations for the Cisco NX-OS software. Use this document in combination with the *Cisco Application Policy Infrastructure Controller, 3.1(2), 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 13.1(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
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 3, 2018	13.1(2m): Release 13.1(2m) became available.
April 24, 2018	13.1(2m): In the Open Bugs section, added bug CSCvi57920.
April 29, 2018	13.1(2o): Release 13.1(2o) became available. Added the resolved bugs for this release.

Date	Description
May 22, 2018	Changed: The dual rate BiDirectional (BiDi) transceiver QSFP-40/100-SRBD requires approximately 5 minutes for the link to come up... To: The dual rate BiDirectional (BiDi) transceiver QSFP-40/100-SRBD takes up to 90 seconds for the link to come up...
May 22, 2018	13.1(2p): Release 13.1(2p) became available. Added the resolved bugs for this release.
June 7, 2018	13.1(2q): Release 13.1(2q) became available. Added the resolved bugs for this release.
July 11, 2018	13.1(2q): In the Resolved Bugs section, added bug CSCvi51338.
November 14, 2018	13.1(2s): Release 13.1(2s) became available. Added the resolved bugs for this release.
January 7, 2019	13.1(2t): Release 13.1(2t) became available. Added the resolved bugs for this release.
January 30, 2019	13.1(2m): In the Open Bugs section, added bug CSCvn69340.
February 6, 2019	13.1(2m): In the Known Behaviors section, added bug CSCvo22890.
March 15, 2019	13.1(2u): Release 13.1(2u) became available. Added the resolved bugs for this release.
June 5, 2019	In the Supported Hardware section, for the N9K-C9364C switch, removed the following erroneous sentence: The last 16 of the QSFP28 ports are colored green to indicate that they support wire-rate MACsec encryption.
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.
August 8, 2019	13.1(2m): In the Open Bugs section, added bug CSCvi75421.
August 14, 2019	13.1(2v): Release 13.1(2v) became available. Added the resolved bugs for this release. 13.1(2m): In the Open Bugs section, added bugs CSCvp92269 and CSCvq43058.
September 11, 2019	In the Supported Hardware section, for the N9K-C9348GC-FXP, 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.

Date	Description
September 20, 2019	In the Usage Guidelines section, added the following bullet: ■ A 25G link that is using the lEEE-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.
March 13, 2020	13.1(2m): In the Resolved Bugs section, added bug CSCvr98827.

Contents

This document includes the following sections:

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

Hardware Type	Product ID	Description
Spine switch	N9K-C9364C	Cisco Nexus 9364C switch is a 2-rack unit (RU), fixed-port switch designed for spine-leaf-APIC deployment in data centers. This switch supports 64 40/100-Gigabit QSFP28 ports and two 1/10-Gigabit SFP+ ports. The following PSUs are supported for the N9K-C9364C: ■ NXA-PAC-1200W-PE ■ NXA-PAC-1200W-PI ■ N9K-PUV-1200W ■ NXA-PDC-930W-PE ■ NXA-PDC-930W-PI Note: Multipod is supported for the N9K-C9364C. Multipod and Cisco ACI Multi-Site together are currently not supported for N9K-C9364C. A 930W-DC PSU (NXA-PDC-930W-PE or NXA-PDC-930W-PI) is supported in redundancy mode if 3.5W QSFP+ modules or passive QSFP cables are used and the system is used in 40C ambient temperature or less; for other optics or a higher ambient temperature, a 930W-DC PSU is supported only with 2 PSUs in non-redundancy mode. 1-Gigabit QSA is not supported on ports 1/49-64.
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
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

Hardware Type	Product ID	Description
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-C9508-FM-E2	Cisco Nexus 9508 Fabric module supporting 100 Gigabit line cards
Spine switch module	N9K-C9516-FM	Cisco Nexus 9516 Fabric module supporting 100 Gigabit line cards
Spine switch module	N9K-C9516-FM-E2	Cisco Nexus 9516 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-X9736C-FX	Cisco Nexus 9500 36-port, 40/100 Gigabit Ethernet QSFP28 aggregation module Note: 1-Gigabit QSA is not supported on ports 1/29-36.
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
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.
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.

Hardware Type	Product ID	Description
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.
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.
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. ■ Port profiles and breakout ports are not supported on the same port.
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
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.

Hardware Type	Product ID	Description
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.
Leaf switch	N9K-C9336C-FX2	Cisco Nexus C9336C-FX2 Top-of-rack (ToR) switch with 36 fixed 40/100-Gigabit Ethernet QSFP28 spine-facing ports. Note: 1-Gigabit QSA is not supported on ports 1/1-6 and 1/33-36. The port profile feature does not support downlink conversion of ports 31 through 36.
Leaf switch	N9K-C9348GC-FXP	The Cisco Nexus 9348GC-FXP switch (N9K-C9348GC-FXP) is a 1-RU fixed-port, L2/L3 switch, designed for ACI deployments. This switch has 48 100/1000-Megabit 1GBASE-T downlink ports, 4 10-/25-Gigabit SFP28 downlink ports, and 2 40-/100-Gigabit QSFP28 uplink ports. This switch supports the following PSUs: ■ NXA-PAC-350W-PI ■ NXA-PAC-350W-PE 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. When a Cisco N9K-C9348GC-FXP switch has only one PSU inserted and connected, the PSU status for the empty PSU slot will be displayed as "shut" instead of "absent" due to a hardware limitation.
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+.
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+.

Hardware Type	Product ID	Description
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
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
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
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
Leaf switch fan	NXA-FAN-30CFM-B	Red port side intake fan
Leaf switch fan	NXA-FAN-30CFM-F	Blue port side exhaust fan
Leaf switch fan	NXA-FAN-65CFM-PE	Blue port side exhaust fan
Leaf switch fan	NXA-SFAN-65CFM-PE	Blue port side exhaust fan
Leaf switch fan	NXA-FAN-65CFM-PI	Burgundy port side intake fan
Leaf switch fan	NXA-SFAN-65CFM-PI	Burgundy port side intake fan
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
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
Leaf switch power supply unit	NXA-PAC-1100W-PE2	1100W AC power supply, port side exhaust pluggable
Leaf switch power supply unit	NXA-PAC-1100W-PI2	1100W AC power supply, port side intake pluggable
Leaf switch power supply unit	N9K-PAC-650W	650W AC Power supply, port side intake pluggable

Hardware Type	Product ID	Description
Leaf switch power supply unit	N9K-PAC-650W-B	650W AC Power supply, port side exhaust pluggable
Leaf switch power supply unit	NXA-PDC-1100W-PE	1100W AC power supply, port side exhaust pluggable
Leaf switch power supply unit	NXA-PDC-1100W-PI	1100W AC power supply, port side intake pluggable
Leaf switch power supply unit	NXA-PHV-1100W-PE	1100W HVAC/HVDC power supply, port-side exhaust
Leaf switch power supply unit	NXA-PHV-1100W-PI	1100W HVAC/HVDC power supply, port-side intake
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
Leaf switch power supply unit	N9K-PUV-3000W-B	3000W AC Power supply, port side exhaust pluggable
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.
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.
Leaf switch power supply unit	NXA-PAC-500W-PE	500W AC Power supply, port side exhaust pluggable

Hardware Type	Product ID	Description
Leaf switch power supply unit	NXA-PAC-500W-PI	500W AC Power supply, port side intake pluggable
Leaf switch power supply unit	NXA-PDC-440W-PI	440W DC power supply, port side intake pluggable, with higher fan speeds for NEBS compliance Note: This power supply is supported only by the Cisco Nexus 9348GC-FXP ACI-mode switch.
Leaf switch power supply unit	UCSC-PSU-930WDC V01	Port side exhaust DC power supply compatible with all ToR leaf switches
Leaf switch power supply unit	UCS-PSU-6332-DC	930W DC power supply, reversed airflow (port side exhaust)

Supported FEX Models

For tables of the FEX models that the Cisco Nexus 9000 Series ACI Mode switches support, see the following webpage:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/interoperability/fexmatrix/fextables.html

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

New and Changed Information

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

- New Hardware Features
- New Software Features

New Hardware Features

The following hardware features are now available:

- Cisco N9K-C9336C-FX2 Leaf switch
- Cisco N9K-C9516-FM-E2 fabric module
- Cisco NXA-PDC-440W-PI DC power supply

- The Cisco N9K-C9348GC-FXP ToR leaf switch now supports 1 Gigabit and 10 Gigabit speeds on the fabric ports (53 and 54).
- The N9K-C9336C-FX2 and N9K-C93180LC-EX switches in ACI mode now support 100G breakout. Before configuring a 100G port, connect it using a Cisco QSFP-4SFP25G-CuxM cable to four 25G SFP ports of a Cisco switch or server on the other end. The breakout feature is not supported on ports with port profiles or fast link failure profiles. For more information, see the "Dynamic Breakout Ports" section in the *Cisco APIC Layer 2 Networking Configuration Guide*.

New Software Features

For new software features, see the *Cisco APIC 3.1(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

Bugs

This section contains lists of open and resolved bugs and 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 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 13.1(2) releases in which the bug exists. A bug might also exist in releases other than the 13.1(2) releases.

Table 3 Open Bugs in This Release

Bug ID	Description	Exists in
CSCwd29346	An ACI switch's console may continuously output messages similar to: svc_ifc_eventmg (*****) Ran 7911 msecs in last 7924 msecs	13.1(2m) and later
CSCwb08081	A route profile that matches on community list and sets the local pref and community is not working post upgrade to 5.2.x release. route-map imp-l3out-L3OUT_WAN-peer-2359297, permit, sequence 4201 Match clauses: community (community-list filter): peer16389-2359297-exc-ext-in-L3OUT_WAN_COMMUNITY-rgcom Set clauses: local-preference 200 community xxxxx:101 xxxxx:500 xxxxx:601 xxxxy:4 additive The match clause works as expected, but the set clause is ignored.	13.1(2m) and later

Bug ID	Description	Exists in
CSCvu72416	Triggered by a physical layer issue, such as fiber or a bad transceiver, a link flap may happen every now and then. However, it is uncommon to have continuous flaps when the node is left unattended over an extended period, such as having 688,000 flaps over a year. Each time after the fabric link flaps, one dbgRemotePort managed object is added to the policyElement database. After a long time flapping like this, unexpected memory allocation and access can be triggered for the Nexus OS process, such as policy_mgr or ethpm. This defect is to enhance the object-store to reduce the impact for such scenarios.	13.1(2u) and later
CSCvu61024	Zoning-rules are not programmed in the hardware after reloading a switch.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) and later
CSCvt52620	There is a stale pervasive route after a DHCP relay label is deleted.	13.1(2m) 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.	13.1(2m) 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 fw 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.	13.1(2m) 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.	13.1(2m) and later
CSCvr79911	An LLDP/CDP MAC address entry gets stuck in the blade switch table on a leaf switch in a vPC. The entry can get stuck if the MAC address flaps and hits the move detection interval, which stops all learning for the address. Use the following command to verify if a switch has a stale MAC address entry: module-1# show system internal epmc bladeswitch_mac all	13.1(2m) and later
CSCvq43058	A spine switch fabric module or line card is reloaded unexpectedly due to a kernel panic. The stack trace includes the following statement: Kernel panic - not syncing: Out of memory: system-wide panic_on_oom is enabled	13.1(2m) and later
CSCvq25729	Traffic is dropped when it is destined to a pervasive route and when the endpoint is not learned. This issue can be also seen on a border leaf switch when "disable remote EP learning" is set.	13.1(2m) and later
CSCvp92269	Running a Qualys security scan results in the following message: CWE - 693 Protection Mechanism Failure - "HTTP Security Header Not Detected"	13.1(2m) and later
CSCvp91758	Fault F0449 gets raised and the ASIC vrm(5) status fails on the Cisco N9K-93108TC-EX or N9K-93180YC-EX switches.	13.1(2q) and later

Bug ID	Description	Exists in
CSCvp63213	While ACI switches are still initializing after an upgrade, TACACS requests are seen coming from the switch IP address, with the remote IP address set to 127.0.0.1 for the admin user.	13.1(2q) and later
CSCvp50075	A leaf switch experiences an unexpected reload due to a HAP reset.	13.1(2m) and later
CSCvp09949	Copy service traffic will fail to reach the TEP where the copy devices are connected. Traffic will not be seen on the spine switches.	13.1(2m) and later
CSCvn69340	The BFD session does not get instantiated under some circumstances in one of the VPC legs for static routes.	13.1(2m) and later
CSCvn17513	A memory leak of around 50 kb is seen when interfaces are created. There is approximately 1 kb of leak per interface created, depending on the VLAN configuration on the interface. This slow memory leak can eventually lead to a crash of the NFM process.	13.1(2s) and later
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.	13.1(2m) and later
CSCvi97670	Endpoints on an AVS host are intermittently or entirely unreachable. When running the "vemcmd show opflex" command on the AVS host, both Opflex tunnels are up/active. When running the "show endpoint ip X.X.X.X" command for the VTEP IP address of the AVS host on the leaf switches where the AVS host connects, no entries are seen. Running the same command for the endpoint IP addresses results in no entries.	13.1(2m) and 13.1(2o)
CSCvi75421	IGMP proxy-reports are not sent out from the ACI leaf switch to the external querier. As a result, the IGMP state will be broken on the external multicast router. The proxy-report shows up in an egress SPAN on the port and everything appears to be correct. However, the proxy-report is being set with a COS 6, which causes it to get punted back to the CPU and not actually be forwarded.	13.1(2m) and later
CSCvi57920	A UCS 1225 vNIC goes down after changing the peer Cisco ACI leaf node name.	13.1(2m) and later
CSCvi13378	The iping6 command might fail for intersite endpoints.	13.1(2m) and later
CSCvh97834	Atomic counters show faults or empty values.	13.1(2m) and later
CSCvh86144	SPAN on a breakout interface will not work after reloading the switch.	13.1(2m) and later
CSCvh25099	Unidirectional traffic from an on-premise leaf switch to a remote leaf switch going through a Cisco Nexus 93128TX, 9396PX, or 9396TX transit TOR switch will get dropped on the remote leaf switch in the ingress direction because of the "security group deny" error.	13.1(2m) and later

Bug ID	Description	Exists in
CSCvh18100	If Cisco ACI Virtual Edge or AVS is operating in VxLAN non-switching mode behind a FEX, the traffic across the intra-EPG endpoints will fail when the bridge domain has ARP flooding enabled.	13.1(2m) and later
CSCvh17285	When the global enforce subnet check option is enabled, the Cisco APIC will not learn MAC addresses from ARP packets arriving on Layer 2-only bridge domains, such as bridge domains that have routing disabled.	13.1(2m) through 13.1(2t)
CSCvh17221	8 to 10 seconds of traffic loss is seen after reloading one of the top-of-rack switches in vPC pair.	13.1(2m) and later
CSCvh16915	Cisco S-class modules for a bridge domain VLAN are incorrectly programmed on a TOR switch after the bridge domain is deleted and added, and traffic gets dropped due to the default deny rule.	13.1(2m) and later
CSCvh16226	A standby Supervisor Engine is left on the loader prompt, which can be loaded by the boot <image> command.	13.1(2m) and later
CSCvh14815	BGP EVPN has the tenant endpoint information, while COOP does not have the endpoint.	13.1(2m) and later
CSCvh11299	In COOP, the MAC IP address route has the wrong VNID, and endpoints are missing from the IP address DB of COOP.	13.1(2m) and later
CSCvg98431	While sending ping between 2 endpoints from a local leaf switch to a remote leaf switch, IPv6 XR gets learned on the remote leaf switch. IPv4 XR does not get learned. Remote leaf switches do not support vPC orphan ports.	13.1(2m) and later
CSCvg97944	The front panel ports do not go down when the sub-interface is shut down in inter-pod network (IPN).	13.1(2m) and later
CSCvg95192	Endpoint information is missing in the spine switches.	13.1(2m) and later
CSCvg85886	When an ARP request is generated from one endpoint to another endpoint in an isolated EPG, an ARP glean request is generated for the first endpoint.	13.1(2m) and later
CSCvg73592	Endpoint moves will be seen when a host is connected by an orphan port to a Cisco APIC leaf switch that has a vPC domain configuration. This generates a critical fault.	13.1(2m) and later
CSCvf09313	In the 12.2(2i) release, the BPDU filter only prevents interfaces from sending BPDUs, but does not prevent interfaces from receiving BPDUs.	13.1(2m) and later
CSCve06334	MAC and IP endpoints are not learned on the local vPC pair.	13.1(2m) 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 4 Resolved Bugs in This Release

Bug ID	Description	Fixed in
CSCvi75421	IGMP proxy-reports are not sent out from the ACI leaf switch to the external querier. As a result, the IGMP state will be broken on the external multicast router. The proxy-report shows up in an egress SPAN on the port and everything appears to be correct. However, the proxy-report is being set with a COS 6, which causes it to get punted back to the CPU and not actually be forwarded.	13.1(2v)
CSCvh17285	When the global Enforce Subnet Check option is enabled, the ACI leaf switch will not learn MAC addresses from ARP/GARP packets arriving on Layer 2-only bridge domains (Unicast Routing disabled).	13.1(2u)
CSCvi11291	XR IP learning occurs on border leaf switches even when 'disabled remote EP learn' is configured for the fabric. XR IP learns should only occur on border leaf switches for routed multicast packets with PIM enabled.	13.1(2u)
CSCvi22143	Multi-destination traffic is not sent out the leaf switch uplinks or downlinks to other devices. This can result in ARP resolution problems or issues with the spanning tree.	13.1(2u)
CSCvi83497	ARP/Broadcast traffic not leaving leaf port where BD port is programmed.Interface is not seen in the broadcast index of the BD.MFDM may core, but issues can be seen due to this defect without MFDM coring.	13.1(2u)
CSCvo16431	When negotiation is on, you see the following symptoms on remote devices: If the remote is running RedHat Server version 7.5, the link failure count is 1, when normally it is 0. If the remote is a standalone Nexus 9000 switch, the physical link flaps.	13.1(2u)
CSCvn76986	60 seconds of traffic loss for a Recursive Next Hop if the RNH loop detection mechanism detects a transient loop.	13.1(2t)
CSCvm48676	A Cisco N9K-C93180LC-EX switch reboots with the following reason: reset-triggered-due-to-ha-policy-of-reset	13.1(2s)
CSCvi51338	Several show commands do not work on a switch for a read-only admin user.	13.1(2q)
CSCvj76998	The ipfib service on a spine linecard experiences a HAP reset.	13.1(2q)
CSCvg13827	SPAN traffic coming into a Cisco N9K-X9736C-FX line card on the spine node will not be sent out. This includes SPAN traffic generated by N9K-X9736C-FX line card ports.	13.1(2p)

Bug ID	Description	Fixed in
CSCvi48943	The port tracking feature tracks uplink ports once per 60 seconds.	13.1(2p)
CSCvi96847	When the border leaf is reloaded in a POD. Traffic from other PODs to this border leaf might get dropped and might not recover.	13.1(2p)
CSCvi97670	Endpoints on an AVS host are intermittently or entirely unreachable. When running the "vemcmd show opflex" command on the AVS host, both Opflex tunnels are up/active. When running the "show endpoint ip X.X.X.X" command for the VTEP IP of the AVS host on the leaf switches where the AVS host connects, no entries are seen. Running the same command for the endpoint IP addresses results in no entries.	13.1(2p)
CSCvj15186	The DHCP Snoop (core) logs are flooded with the following messages: [ERR:proc-dhcp_snoop(tid: 11643)] Cannot allocate packet [ERR:proc-dhcp_snoop(tid: 11643)] set orig sisf_pak is null [ERR:proc-dhcp_snoop(tid: 11643)] pmsg set sisf_pak is null [DBG:proc-dhcp_snoop(tid: 11643)] SISF[ERR]:sisf_counters_inc_msg_rcvd(173) unkn sisf protocol 0 [DBG:proc-dhcp_snoop(tid: 11643)] SISF[ERR]:sisf_counters_inc_msg_sent(140) unkn sisf protocol 0 [DBG:proc-dhcp_snoop(tid: 11643)] SISF[ALL]:sisf_pak_rcv(873) ACIPAK RECEIVED In addition, the core file shows that the total virtual memory allocated is approaching the RLIMIT_AS (max) value.	13.1(2p)
CSCvg73430	The shared secondary IPv6 address state on an external SVI might become "DUP" (duplicate state) and become unusable as a result of the Duplicate Address Detection (DAD) process on the address provisioning. Use the "show ipv6 interface brief vrf <name>" command to check the state of the address on the external SVI to see if this issue is hit. The shared secondary address is the global IPv6 subnet that is shared across multiple border leaf switches to provide border leaf switch redundancy to externally connected Layer 3 devices in the L3Out policy.	13.1(2o)
CSCvi11810	The Cisco APIC and leaf switches have different configurations for the autonomous system number (ASN) prepend. The Cisco APIC prepends "1xASN." However, a border leaf switch prepends "4xASN."	13.1(2o)
CSCvi13133	All traffic between vPCs gets dropped because outer VxLAN traffic has a source MAC address and source IP address of "0" when coming to a spine switch.	13.1(2o)

Bug ID	Description	Fixed in
CSCvi47657	The Cisco N9K-C9348GC-FXP switch will freeze when used with the NXA-PDC-440W-PE PSU / NXA-FAN-30CFM-F fan due to fan/psu direction incompatibility.	13.1(2o)
CSCvi48242	Traffic is dropped due to the wrong filter priority for the IPv6 unspecified protocol setting.	13.1(2o)
CSCvi73383	A leaf switch reloads during techsupport collection. The reload reason is "Service on linecard had a hap-reset" and there is a core file generated for the ipfib process.	13.1(2o)
CSCvi73732	The shared secondary IPv6 address state on external SVI may go in DUP (Duplicate state) and become unusable as a result of the Duplicate Address Detection (DAD) process on the address provisioning. Use "show ipv6 interface brief vrf <name>" command to check the state of the address on the external SVI to see if this issue is hit. The shared secondary address is the global IPv6 subnet shared across multiple border leafs to provide border leaf redundancy to externally connected layer 3 device in the l3out policy.	13.1(2o)
CSCvi87993	There are multiple defunct ipmgr processes on the system.	13.1(2o)
CSCve48154	After deleting a hardware sensor form the Cisco Tetration Analytics GUI, is not possible to re-register the same sensor to the cluster.	13.1(2m)
CSCvf63418	No fault is raised on the PSU of a FEX if it is not connected.	13.1(2m)
CSCvg02010	In a multipod environment, a multicast receiver sends the proper IGMP packets, but one of the border leaf switches does not add the mroute. When this border leaf switch is also the stripe-winner of the group, multicast does not work.	13.1(2m)
CSCvg20627	With First Hop Security, when the endpoint with the uSEG EPG in VxLAN mode moves, the MAC DB does not get updated.	13.1(2m)
CSCvg23174	When using FEX model C2248PQ-10GEif you have a port channel that contains a host port in the range of 1/1 to 24 and another host port in the range of 1/24 to 48, the FEX might drop packets due to claiming that it has an incorrect vntag header when it tries to load balance.	13.1(2m)
CSCvg37153	There is a memory leak on a switch that can potentially lead to an out of memory reload issue, and the TAH_MEM_ENUM_tah_sug_fta_filtertcamdata table sees a much greater allocation and usage than other nodes in the environment.	13.1(2m)
CSCvg38918	The DHCP process crashes after a certain period of time.	13.1(2m)
CSCvg38922	There is a continuous memory leak in the aclqos process on fabric cards. This issue is observed on the fol-lowing spine switches: N9K-C92304QC, N9K-C9236C, N9K-C92300YC, N9K-C9272Q, and N9K-C9364C.	13.1(2m)
CSCvg58924	ICMP traffic to between endpoints might get dropped, but other traffic, including TCP and UDP, are not impacted.	13.1(2m)

Bug ID	Description	Fixed in
CSCvg66700	Communication through a shared L3Out is broken when an additional external network is added to the shared L3Out. This occurs because the prefix list that controls redistribution of the bridge domain static route into EIGRP is deleted. Communication to and from an EIGRP L3Out will be lost due to the route-map being deleted.	13.1(2m)
CSCvg71257	If the vPC is down, two faults will be raised. F0546 is raised on object topology/pod-1/node-101/sys/aggr-[po7]/aggrif, and F1296 is raised on topology/pod-1/node-101/sys/vpc/inst/dom-1/if-684. After you disable the port channel, fault F0546 will be cleared, but F1296 will remain on the Cisco APIC.	13.1(2m)
CSCvg71525	Traffic is dropped to 3 out of 64,000 endpoints that are learned on a leaf switch that is configured with a high-dual-stack profile.	13.1(2m)
CSCvg72327	Traffic loss is seen when there is unidirectional traffic from an AVS VM and there is a detach/attach operation done at the same time.	13.1(2m)
CSCvg76793	When a VM behind a DVS is used as an IP-based EPG (with the IP attribute), a policy-based redirect policy to redirect the traffic from the VM to a service node, such as a firewall, does not work.	13.1(2m)
CSCvg78439	Cisco ACI leaf switches continually download and upload the Cisco ACI catalog.	13.1(2m)
CSCvg80698	Unicast and multicast convergence can take up to 45 seconds when a line card or fabric module experiences a kernel crash.	13.1(2m)
CSCvg86136	A fault is raised for a bridge domain, which states that the operational state is down.	13.1(2m)
CSCvg87335	Traffic loss is seen for approximately 22 to 24 seconds after reloading a remote leaf switch.	13.1(2m)
CSCvg91161	In a GOLF setup, if there are multiple instP managed objects configured under a GOLF L3Out, deleting one of the instP managed objects clears the nexthop object (bgpPfxLeakCtrlP). This can also happen if there are multiple GOLF L3Outs for a given VRF instance (context) and one of the L3Outs is deleted. In a GOLF setup on Cisco ACI, when moving a regular L3Out from one GOLF VRF instance to anohter GOLF VRF instance, the bridge domain subnet might stop being advertised.	13.1(2m)
CSCvh03722	While doing decommission and recommission, the Spanning Tree Protocol (STP) enters the blocking state for an SVI vPC pair interface on a remote leaf switch.	13.1(2m)
CSCvh05960	When a vPC node goes down, multicast traffic loss is observed for 189ms. ACL create/delete operations are not batched, which take time to complete and affects convergence.	13.1(2m)
CSCvh11828	A spine switch does not join the fabric after a policy upgrade. The fabric discovery status is inactive.	13.1(2m)
CSCvh18253	When AVS is connected to the leaf switches through multiple paths (such as vPC with Cisco UCS Fabric Interconnects Topology), VM traffic loss might be observed. This happens when one path is disrupted, causing OpFlex control traffic to switch to the other path.	13.1(2m)

Bug ID	Description	Fixed in
CSCvh18399	In extremely rare circumstances, the maximum number of supported endpoint nexthops might be exhausted, resulting in hardware programming failures for endpoints learned after the endpoint nexthop limit was reached.	13.1(2m)
CSCvh20051	After reloading a leaf switch, there is a delay of 5-10 seconds between when the fabric uplinks are brought down and when the server-facing ports are brought down. This can cause a loss of traffic for devices that are connected to the leaf switch in question before their NICs failover to a redundant link.	13.1(2m)
CSCvh21652	A leaf switch reloads unexpectedly and generates a core file for the device_test process.	13.1(2m)
CSCvh25010	When the infraAccNodePGrp managed object is disassociated from a leaf switch, the uni/fabric/monfab-default policy replaced the customer configured fabric monitoring policy on the leaf switch.	13.1(2m)
CSCvh29461	BGP between spine switches in different pods in a multipod environment goes down and is unable to be re-established. After upgrading to a Cisco APIC 3.1 release, BGP between spine switches in different pods goes down if a QoS CoS translation policy is enabled.	13.1(2m)
CSCvh32225	An iBGP session goes down when iBGP breaks in stretched fabric when QoS Dot1p is enabled on switches whose product IDs end with "EX" or "FX."	13.1(2m)
CSCvh48223	A leaf switch reloads unexpectedly. The reset reason indicates a kernel panic and the "show processes log" command shows that nginx produced a stack trace.	13.1(2m)
CSCvh51474	A leaf switch reloads while collecting tech support files, and there is a core file from the unicast Routing Information Base (RIB) process.	13.1(2m)
CSCvh68033	Leaf switches will continuously see a crash due to the vleaf_elem process.	13.1(2m)
CSCvh68419	Layer 2 switched MPLS traffic is dropped in the Cisco ACI fabric.	13.1(2m)
CSCvh70146	Two routers are not able to form eBGP neighborship with ttl=1. The routers hit different sup-TCAM rules and flooded in the EPG.	13.1(2m)
CSCvh74146	A leaf switch resets due to an acllog process crash.	13.1(2m)
CSCvh79225	The vPC protection group gets removed when configuring and unconfiguring vPC through the Inventory tab.	13.1(2m)
CSCvh83687	There is a memory leak when a static route add is followed by a static route modify, because the same BFD entry gets installed multiple times for that BFD session.	13.1(2m)
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.	13.1(2m)
CSCvh92887	A memory leak in the stats_manager might result in the eventual exhaustion of memory. Exhaustion of memory might result in the Top of Rack (leaf) switch or spine switch reloading.	13.1(2m)

Bug ID	Description	Fixed in
CSCvh99171	The Policy-Mgr NXOS process dumps a core when too many management VRF instance prefixes are added and deleted.	13.1(2m)
CSCvi04324	The BFDC process might crash due to running out of memory.	13.1(2m)
CSCvj05990	For the interface enable/disable, IF-MIB (linkUp and linkDown) traps were not supported.	13.1(2m)

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 13.1(2) releases in which the known behavior exists. A bug might also exist in releases other than the 13.1(2) releases.

Table 5 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.	13.1(2m) 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.	13.1(2m) and later
CSCup65586	The show interface command shows the tunnel's Rx/Tx counters as 0.	13.1(2m) 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.	13.1(2m) and later
CSCup92534	Continuous "threshold exceeded" messages are generated from the fabric.	13.1(2m) and later
CSCuq39829	Switch rescue user ("admin") can log into fabric switches even when TACACS is selected as the default login realm.	13.1(2m) and later
CSCuq46369	An extra 4 bytes is added to the untagged packet with Egress local and remote SPAN.	13.1(2m) 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.	13.1(2m) and later

Bug ID	Description	Exists in
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.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) and later
CSCur01336	The power supply will not be detected after performing a PSU online insertion and removal (OIR).	13.1(2m) and later
CSCur81822	The access-port operational status is always "trunk".	13.1(2m) 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.	13.1(2m) and later
CSCus29623	The transceiver type for some Cisco AOC (active optical) cables is displayed as ACU (active copper).	13.1(2m) 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.	13.1(2m) and later
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.	13.1(2m) and later

Bug ID	Description	Exists in
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.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) and later
CSCuv57316	TEP counters from the border leaf to remote leaf nodes do not increment.	13.1(2m) 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.	13.1(2m) and later
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.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) and later

Bug ID	Description	Exists in
CSCuy06749	Traffic is dropped between two isolated EPGs.	13.1(2m) and later
CSCuy22288	The iping command's replies get dropped by the QOS ingress policer.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) and later
CSCuy61018	The default minimum bandwidth is used if the BW parameter is set to "0", and so traffic will still flow.	13.1(2m) and later
CSCuy96912	The debounce timer is not supported on 25G links.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) and later
CSCuz13614	For traffic coming out of an L3out to an internal EPG, stats for the actrlRule will not increment.	13.1(2m) 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.	13.1(2m) and later
CSCuz47058	SAN boot over a virtual Port Channel or traditional Port Channel does not work.	13.1(2m) and later
CSCuz65221	A policy-based redirect (PBR) policy to redirect IP traffic also redirects IPv6 neighbor solicitation and neighbor advertisement packets.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) and later

Bug ID	Description	Exists in
CSCvb39965	Slow drain is not supported on FEX Host Interface (HIF) ports.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) 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.	13.1(2m) and later
CSCvo22890	There is intermittent packet loss for some flows through FX2 leaf switches when the no-drop class is enabled.	13.1(2m) 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.
- Traffic destined to Static Route EP VIPs sourced from N9000 switches (switches with names that end in -EX) might not function properly because proxy route is not programmed.
- An iVXLAN header of 50 bytes is added for traffic ingressing into the fabric. A bandwidth allowance of (50/50 + ingress_packet_size) needs to be made to prevent oversubscription from happening. If the allowance is not made, oversubscription might happen resulting in buffer drops.

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

- For the supported optics per device, see the Cisco Optics-to-Device Compatibility Matrix.
- This release supports the hardware and software listed on the ACI Ecosystem Compatibility List, and supports the Cisco AVS, Release 5.2(1)SV3(3.10).
- 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
- The Cisco APIC GUI incorrectly reports more memory used than is actually used. To calculate the appropriate amount of memory used, run the "show system internal kernel meminfo | egrep "MemT|MemA"" command on

the desired switch. Divide MemAvailable by MemTotal, multiply that number by 100, then subtract that number from 100.

  - Example: 10680000 / 24499856 = 0.436 x 100 = 43.6% Free, 100% - 43.6% = 56.4% Used

- Leaf and spine switches from two different fabrics cannot be connected regardless of whether the links are administratively kept down.
- Only one instance of OSPF (or any multi-instance process using the managed object hierarchy for configurations) can have the write access to operate the database. Due to this, the operational database is limited to the default OSPF process alone and the multipodInternal instance does not store any operational data. To debug an OSPF instance ospf-multipodInternal, use the command in VSH prompt. Do not use ibash because some ibash commands depend on Operational data stored in the database.
- When you enable or disable Federal Information Processing Standards (FIPS) on a Cisco ACI fabric, you must reload each of the switches in the fabric for the change to take effect. The configured scale profile setting is lost when you issue the first reload after changing the FIPS configuration. The switch remains operational, but it uses the default port scale profile. This issue does not happen on subsequent reloads if the FIPS configuration has not changed.

  FIPS is supported on Cisco NX-OS release 13.1(2) or later. If you must downgrade the firmware from a release that supports FIPS to a release that does not support FIPS, you must first disable FIPS on the Cisco ACI fabric and reload all of the switches in the fabric.
- Link-level flow control is not supported on leaf switches that are running in ACI mode.
- The dual rate BiDirectional (BiDi) transceiver QSFP-40/100-SRBD takes up to 90 seconds for the link to come up after auto-negotiating the speed on both the local and remote end.
  - If both ends support the 40/100 combination, the link comes up quickly as 100G.
  - If one end is 40G and other end supports 40/100, then the link takes longer to negotiate to 40G.
- You cannot use the breakout feature on a port that has a port profile configured on a Cisco N9K-C93180LC-EX switch. With a port profile on an access port, the port is converted to an uplink, and breakout is not supported on an uplink. With a port profile on a fabric port, the port is converted to a downlink. Breakout is currently supported only on ports 1 through 24.
- On Cisco 93180LC-EX Switches, ports 25 and 27 are the native uplink ports. Using a port profile, if you convert ports 25 and 27 to downlink ports, ports 29, 30, 31, and 32 are still available as four native uplink ports. Because of the threshold on the number of ports (which is maximum of 12 ports) that can be converted, you can convert 8 more downlink ports to uplink ports. For example, ports 1, 3, 5, 7, 9, 13, 15, 17 are converted to uplink ports and ports 29, 30, 31 and 32 are the 4 native uplink ports, which is the maximum uplink port limit on Cisco 93180LC-EX switches.

  When the switch is in this state and if the port profile configuration is deleted on ports 25 and 27, ports 25 and 27 are converted back to uplink ports, but there are already 12 uplink ports on the switch in the example. To accommodate ports 25 and 27 as uplink ports, 2 random ports from the port range 1, 3, 5, 7, 9, 13, 15, 17 are denied the uplink conversion; the chosen ports cannot be controlled by the user. Therefore, it is mandatory to clear all the faults before reloading the leaf node to avoid any unexpected behavior regarding the port type. If a node is reloaded without clearing the port profile faults, especially when there is a fault related to limit-exceed, the ports might be in an unexpected mode.
- When using a 25G Mellanox cable that is connected to a Mellanox NIC, you can set the ACI leaf switch port to run at a speed of 25G or 10G.

- 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.

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