Cisco Nexus 9000 ACI-Mode Switches Release Notes, Release 15.0(1)

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.

This release works only on Cisco Nexus 9000 series switches in ACI mode.

This document describes the features, issues, and limitations for the Cisco Nexus 9000 switches in ACI mode. For the features, issues, and limitations for the Cisco Application Policy Infrastructure Controller (APIC), see the *Cisco Application Policy Infrastructure Controller Release Notes, Release 5.0(1)*.

For more information about this product, see Related Content.

Date	Description
April 27, 2023	Added the N9K-M12PQ, N9K-M6PQ, and N9K-M6PQ-E expansion modules to the No Longer Supported section.
October 31, 2022	In the Open Issues section, added bug CSCvv33100.
May 16, 2022	In the Open Issues section, added bug CSCwa47686.
March 16, 2022	In the Open Issues section, added bugs CSCwa95241 and CSCwb14844.
December 16, 2021	In the Open Issues section, added bug CSCvz95984.
December 7, 2021	In the Compatibility Information section, for the N9K-C9364C-GX switch, added: All 4 fans must be operational, otherwise the switch will power down due to a fan policy trigger.
August 18, 2021	In the Compatibility Information section, for the N9K-C9316D-GX, N9K-C93600CD-GX, and N9K-C9364C-GX switches, added: 1G and 100MB speeds are not supported.
July 6, 2021	In the Supported Hardware section, added the NXA-PAC-500W-PI and NXA-PAC-500W-PE PSUs.
June 21, 2021	In the Known Issues section, added bug CSCvu42069.
June 15, 2021	In the Open Issues section, added bug CSCvy43640.
March 23, 2021	In the Open Issues section, added bug CSCvx70611.

Date	Description
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.
June 25, 2020	Release 15.0(1l) became available. Added the resolved issues for this release.
May 14, 2020	Release 15.0(1k) became available.

Cisco Confidential

Contents

- **Supported Hardware**
- **No Longer Supported Hardware**
- **Supported FEX Models**
- **New Hardware Features**
- **Changes in Behavior**
- **Open Issues**
- **Resolved Issues**
- **Known Issues**
- **Compatibility Information**
- **Usage Guidelines**
- **Related Content**
- **Documentation Feedback**
- **Legal Information**

Cisco Confidential

Supported Hardware

The following sections list the supported hardware.

Table 1 Modular Spine Switches

Product ID	Description
N9K-C9504	Cisco Nexus 9504 switch chassis
N9K-C9508	Cisco Nexus 9508 switch chassis
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
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
N9K-C9516	Cisco Nexus 9516 switch chassis

Table 2 Modular Spine Switch Line Cards

Product ID	Description	Maximum Quantity		
		Cisco Nexus 9504	Cisco Nexus 9508	Cisco Nexus 9516
N9K-X9736C-FX	Cisco Nexus 9500 36-port 40/100 Gigabit Ethernet Cloud Scale line card	4	8	16
N9K-X9736Q-FX	Cisco Nexus 9500 36-port 40 Gigabit Ethernet Cloud Scale line card	4	8	16
N9K-X9732C-EX	Cisco Nexus 9500 32-port, 40/100 Gigabit Ethernet Cloud Scale line card Note: The N9K-X9732C-EX line card cannot be used when a fabric module is installed in FM slot 25.	4	8	16

Table 3 Modular Spine Switch Fabric Modules

Product ID	Description	Minimum	Maximum
N9K-C9508-FM-G	Cisco Nexus 9508 cloud scale fabric module (400G capable)	4	5
N9K-C9504-FM-E	Cisco Nexus 9504 cloud scale fabric module	4	5
N9K-C9508-FM-E	Cisco Nexus 9508 cloud scale fabric module	4	5
N9K-C9508-FM-E2	Cisco Nexus 9508 cloud scale fabric module	4	5
N9K-C9516-FM-E2	Cisco Nexus 9516 cloud scale fabric module	4	5

Cisco Confidential

Table 4 Modular Spine Switch Fans

Product ID	Description
N9K-C9508-FAN2	Fan tray that supports the Cisco N9K-C9508-FM-G fabric module
N9K-C9508-FAN-PWR	Blank fan power card that supports the N9K-C9508-FAN2 fan trays.
N9K-C9504-FAN	Fan tray for Cisco Nexus 9504 chassis
N9K-C9508-FAN	Fan tray for Cisco Nexus 9508 chassis
N9K-C9516-FAN	Fan tray for Cisco Nexus 9516 chassis

Table 5 Modular Spine Switch Supervisor and System Controller Modules

Product ID	Description
N9K-SUP-A+	Cisco Nexus 9500 Series supervisor module
N9K-SUP-B+	Cisco Nexus 9500 Series supervisor module
N9K-SUP-A	Cisco Nexus 9500 Series supervisor module
N9K-SUP-B	Cisco Nexus 9500 Series supervisor module
N9K-SC-A	Cisco Nexus 9500 Series system controller

Table 6 Fixed Spine Switches

Product ID	Description
N9K-C9316D-GX	Cisco Nexus 9300 platform switch with 16 10/40/100/400-Gigabit QSFP-DD ports (ports 1-16).
N9K-C9332C	Cisco Nexus 9300 platform switch with 32 40/100-Gigabit QSFP28 ports and 2 SFP ports. Ports 25-32 offer hardware support for MACsec encryption.
N9K-C9364C	Cisco Nexus 9300 platform switch with 64 40/100-Gigabit QSFP28 ports and two 1/10-Gigabit SFP+ ports. The last 16 of the QSFP28 ports are colored green to indicate that they support wire-rate MACsec encryption.

Table 7 Fixed Spine Switch Power Supply Units

Product ID	Description
N9K-PAC-1200W	1200W AC power supply, port side intake pluggable Note: This power supply is supported only by the Cisco Nexus 93120TX and 9336PQ ACI-mode switches
N9K-PAC-1200W-B	1200W AC power supply, port side exhaust pluggable Note: This power supply is supported only by the Cisco Nexus 93120TX and 9336PQ ACI-mode switches

Cisco Confidential

Product ID	Description
NXA-PAC-1200W-PE	1200W AC power supply, port side exhaust pluggable, with higher fan speeds for NEBS compliance
NXA-PAC-1200W-PI	1200W AC power supply, port side intake pluggable, with higher fan speeds for NEBS compliance
NXA-PAC-1100W-PE2	1100W AC power supply, port side exhaust pluggable
NXA-PAC-1100W-PI2	1100W AC power supply, port side intake pluggable
NXA-PAC-750W-PE	750W AC power supply, port side exhaust pluggable, with higher fan speeds for NEBS compliance Note: This power supply is supported only on release 14.2(1) and later.
NXA-PAC-750W-PI	750W AC power supply, port side intake pluggable, with higher fan speeds for NEBS compliance Note: This power supply is supported only on release 14.2(1) and later.
NXA-PDC-1100W-PE	1100W AC power supply, port side exhaust pluggable
NXA-PDC-1100W-PI	1100W AC power supply, port side intake pluggable
NXA-PDC-930W-PE	930W AC power supply, port side exhaust pluggable
NXA-PDC-930W-PI	930W AC power supply, port side intake pluggable
NXA-PHV-1100W-PE	1100W HVAC/HVDC power supply, port-side exhaust
NXA-PHV-1100W-PI	1100W HVAC/HVDC power supply, port-side intake
N9K-PUV-1200W	1200W HVAC/HVDC dual-direction airflow power supply

Table 8 Fixed Spine Switch Fans

Product ID	Description
N9K-C9300-FAN3	Burgundy port side intake fan
N9K-C9300-FAN3-B	Blue port side exhaust fan
NXA-FAN-160CFM-PE	Blue port side exhaust fan
NXA-FAN-160CFM-PI	Burgundy port side intake fan

Cisco Confidential

Product ID	Description
NXA-FAN-35CFM-PE	Blue port side exhaust fan
NXA-FAN-35CFM-PI	Burgundy port side intake fan

Table 9 Fixed Leaf Switches

Product ID	Description
N9K-C9364C-GX	Cisco Nexus 9300 platform switch with 64 100-Gigabit Ethernet QSFP28 ports, two management ports (one RJ-45 port and one SFP port), one console port (RS-232), and one USB port.
N9K-C93600CD-GX	Cisco Nexus 93600CD-GX switch with 28 10/40/100-Gigabit Ethernet QSFP28 ports (ports 1-28) and 8 10/40/100/400-Gigabit QSFP-DD ports (ports 29-36).
N9K-C93240YC-FX2	Cisco Nexus 9300 platform switch with 48 1/10/25-Gigabit Ethernet SFP28 ports and 12 40/100-Gigabit Ethernet QSFP28 ports. The N9K-C93240YC-FX2 is a 1.2-RU switch. Note: 10/25G-LR-S with QSA is not supported.
N9K-C93216TC-FX2	Cisco Nexus 9300 platform switch with 96 1/10GBASE-T (copper) front panel ports and 12 40 /100-Gigabit Ethernet QSFP28 spine-facing ports
N9K-C93360YC-FX2	Cisco Nexus 9300 platform switch with 96 1/10/25-Gigabit front panel ports and 12 40 /100-Gigabit Ethernet QSFP spine-facing ports. Note: The supported total number of fabric ports and port profile converted fabric links is 64.
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 supports downlink conversion of ports 31 through 34. Ports 35 and 36 can only be used as uplinks.
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.
N9K-C93108TC-FX-24	Cisco Nexus 9300 platform switch with 24 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.
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.

Cisco Confidential

Product ID	Description
N9K-C93180YC-FX-24	Cisco Nexus 9300 platform switch with 24 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.
N9K-C9348GC-FXP	Cisco Nexus 9348GC-FXP switch with 48 100/1000-Megabit 1GBASE-T downlink ports, 4 10-/25-Gigabit SFP28 downlink ports, and 2 40-/100-Gigabit QSFP28 uplink ports.
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.
N9K-C93108TC-EX-24	Cisco Nexus 9300 platform switch with 24 1/10GBASE-T (copper) front panel ports and 6 40/100-Gigabit QSFP28 spine facing ports.
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 as either a 24 40G port switch or a 12 100G port switch. If 100G is connected the Port1, Port 2 will be HW disabled.
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.
N9K-C93180YC-EX-24	Cisco Nexus 9300 platform switch with 24 1/10/25-Gigabit front panel ports and 6-port 40/100 Gigabit QSFP28 spine-facing ports.
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.

Table 10 Fixed Leaf Switch Power Supply Units

Product ID	Description
NXA-PAC-2KW-PE	Nexus 9000 2KW AC power supply, port-side exhaust Note: This power supply is supported only by the Cisco Nexus 9364C-GX ACI-mode switch.
NXA-PAC-2KW-PI	Nexus 9000 2KW AC power supply, port-side intake Note: This power supply is supported only by the Cisco Nexus 9364C-GX ACI-mode switch.
N9K-PAC-1200W	1200W AC power supply, port side intake pluggable Note: This power supply is supported only by the Cisco Nexus 93120TX and 9336PQ ACI-mode switches
N9K-PAC-1200W-B	1200W AC power supply, port side exhaust pluggable Note: This power supply is supported only by the Cisco Nexus 93120TX and 9336PQ ACI-mode switches

Cisco Confidential

Product ID	Description
N9k-PAC-3000W-B	3000W AC power supply, port side intake
N9K-PAC-650W	650W AC power supply, port side intake pluggable
N9K-PAC-650W-B	650W AC power supply, port side exhaust pluggable
NXA-PAC-1200W-PE	1200W AC power supply, port side exhaust pluggable, with higher fan speeds for NEBS compliance
NXA-PAC-1200W-PI	1200W AC power supply, port side intake pluggable, with higher fan speeds for NEBS compliance
NXA-PAC-1100W-PE2	1100W AC power supply, port side exhaust pluggable
NXA-PAC-1100W-PI2	1100W AC power supply, port side intake pluggable
NXA-PAC-750W-PE	750W AC power supply, port side exhaust pluggable, with higher fan speeds for NEBS compliance Note: This power supply is supported only on release 14.2(1) and later.
NXA-PAC-750W-PI	750W AC power supply, port side intake pluggable, with higher fan speeds for NEBS compliance Note: This power supply is supported only on release 14.2(1) and later.
NXA-PAC-650W-PE	650W AC power supply, port side exhaust pluggable
NXA-PAC-650W-PI	650W AC power supply, port side intake pluggable
NXA-PAC-500W-PE	500W AC Power supply, port side exhaust pluggable
NXA-PAC-500W-PI	500W AC Power supply, port side intake pluggable
NXA-PAC-350W-PE	350W AC power supply, port side exhaust pluggable
NXA-PAC-350W-PI	350W AC power supply, port side intake pluggable
NXA-PDC-2KW-PE	Nexus 9000 2KW DC power supply, port-side exhaust Note: This power supply is supported only by the Cisco Nexus 9364C-GX ACI-mode switch.
NXA-PDC-2KW-PI	Nexus 9000 2KW DC power supply, port-side intake Note: This power supply is supported only by the Cisco Nexus 9364C-GX ACI-mode switch.

Cisco Confidential

Product ID	Description
NXA-PDC-1100W-PE	1100W AC power supply, port side exhaust pluggable
NXA-PDC-1100W-PI	1100W AC power supply, port side intake pluggable
NXA-PDC-930W-PE	930W AC power supply, port side exhaust pluggable
NXA-PDC-930W-PI	930W AC power supply, port side intake pluggable
NXA-PDC-440W-PE	440W DC power supply, port side exhaust pluggable, with higher fan speeds for NEBS compliance Note: This power supply is supported only by the Cisco Nexus 9348GC-FXP ACI-mode switch.
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.
NXA-PHV-2KW-PE	Nexus 9000 2KW AC power supply, port-side exhaust Note: This power supply is supported only by the Cisco Nexus 9364C-GX ACI-mode switch.
NXA-PHV-2KW-PI	Nexus 9000 2KW AC power supply, port-side intake Note: This power supply is supported only by the Cisco Nexus 9364C-GX ACI-mode switch.
NXA-PHV-1100W-PE	1100W HVAC/HVDC power supply, port-side exhaust
NXA-PHV-1100W-PI	1100W HVAC/HVDC power supply, port-side intake
NXA-PHV-350W-PE	350W HVAC/HVDC power supply, port-side exhaust
NXA-PHV-350W-PI	350W HVAC/HVDC power supply, port-side intake
N9K-PUV-1200W	1200W HVAC/HVDC dual-direction airflow power supply
N9K-PUV-3000W-B	3000W AC power supply, port side exhaust pluggable
UCSC-PSU-930WDC V01	Port side exhaust DC power supply compatible with all ToR leaf switches
UCS-PSU-6332-DC	930W DC power supply, reversed airflow (port side exhaust)

Table 11 Fixed Leaf Switch Fans

Product ID	Description

Cisco Confidential

Product ID	Description
N9K-C9300-FAN2	Burgundy port side intake fan
N9K-C9300-FAN2-B	Blue port side exhaust fan
N9K-C9300-FAN3	Burgundy port side intake fan
N9K-C9300-FAN3-B	Blue port side exhaust fan
NXA-FAN-160CFM2-PE	Blue port side exhaust fan
NXA-FAN-160CFM2-PI	Burgundy port side intake fan
NXA-FAN-160CFM-PE	Blue port side exhaust fan
NXA-FAN-160CFM-PI	Burgundy port side intake fan
NXA-FAN-30CFM-B	Burgundy port side intake fan
NXA-FAN-30CFM-F	Blue port side exhaust fan
NXA-FAN-35CFM-PE	Blue port side exhaust fan
NXA-FAN-35CFM-PI	Burgundy port side intake fan
NXA-FAN-65CFM-PE	Blue port side exhaust fan
NXA-SFAN-65CFM-PE	Blue port side exhaust fan
NXA-FAN-65CFM-PI	Burgundy port side intake fan
NXA-SFAN-65CFM-PI	Burgundy port side intake fan

No Longer Supported Hardware

Starting in this release, the following hardware is no longer supported:

Hardware Type	Product ID
Spine switch	■ N9K-C9336PQ

Cisco Confidential

Hardware Type	Product ID
Modular spine switch line card	■ N9K-X9736PQ
Modular spine switch fabric module	■ N9K-C9504-FM ■ N9K-C9508-FM ■ N9K-C9516-FM
Leaf Switch	■ N9K-C9372PX-E ■ N9K-C9372TX-E ■ N9K-C9332PQ ■ N9K-C9372PX ■ N9K-C9372TX ■ N9K-C9396PX ■ N9K-C9396TX ■ N9K-C93128TX
Expansion Modules	■ N9K-M12PQ ■ N9K-M6PQ ■ N9K-M6PQ-E

Prior to upgrading your fabric to release 15.0(1) or later, replace these hardware elements in your fabric with other supported hardware. For modular spine switches, replace all unsupported modular line cards and fabric modules because these old generation line cards and fabric modules cannot be operated with newer line cards and fabric modules in the same chassis.

If you attempt to upgrade one of the unsupported hardware to the 15.0(1) or later release, the hardware will unsuccessfully attempt to boot three times, after which the switch will be reverted to the release that was previously installed on it. Therefore, the unsupported hardware will not upgrade to release 15.0(1) or later and the Cisco ACI fabric will operate with inconsistent firmware releases in each switch, which is why we recommend that you replace the unsupported hardware prior to performing the upgrade.

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 Hardware Features

- On the Cisco N9K-C9336C-FX2 switch, you can now apply a breakout configuration on ports 1 through 34, which can give up to 136 (34*4) server or downlink ports.
- The Cisco Nexus 9508-FM-G (N9K-C9508-FM-G) fabric module that supports the N9K-X9736C-FX and N9K-X9736Q-FX line cards.
- The Cisco Nexus 9508-FAN2 (N9K-C9508-FAN2) fan tray that supports the N9K-C9508-FM-G fabric modules.

Cisco Confidential

- The Cisco Nexus 9508-FAN-PWR (N9K-9508-FAN-PWR) blank fan power card that supports the N9K-C9508-FAN2 fan trays.

Changes in Behavior

For the changes in behavior, see the Cisco ACI Releases Changes in Behavior document.

Open Issues

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 15.0(1) releases in which the bug exists. A bug might also exist in releases other than the 15.0(1) releases.

Bug ID	Description	Exists In
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.	15.0(1k) and later
CSCvh18100	If Cisco ACI Virtual Edge or AVS is operating in VxLAN non-switching mode behind a FEX, the traffic between endpoints in the same EPG will fail when the bridge domain has ARP flooding enabled.	15.0(1k) 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.	15.0(1k) and later
CSCvs87190	The Cisco N9K-C93180YC-EX switch does not support auto-negotiation on 10/25/40/100G transceivers. Links will not come up if auto-negotiation enabled on Cisco N9K-C93180YC-EX ports.	15.0(1k) and later
CSCvt02504	The logs for a route table mismatch are not clear.	15.0(1k) and later
CSCvt55002	When MPLS config is enabled, a fault will be raised in APIC asking to reload the switch in order to enable MPLS statistics. Only after a reload is done, MPLS stats will start getting accounted.	15.0(1k) and later
CSCvt57460	There is slow convergence of traffic after a spine switch reload or ToR switch reload.	15.0(1k) and later
CSCvt87976	On a remote leaf switch, the sclass of a shared service endpoint can be incorrect due to overwriting of the sclass by the new share service prefix on a different EPG.Example:On the remote leaf switch, XR IP <IP1> is learned with sclass <S1>, which corresponds to the EPG sclass <sclass1> that is based on LPM (<prefix1>/24).If a more specific route leak subnet <prefix1/>29 is configured, then the XR endpoint is still learned with the EPG <sclass1> instead of the sclass coming from the <prefix1/>29 configuration.	15.0(1k) and later
CSCvu02013	Data/IFC traffic arriving from the IPN will be classified incorrectly to the CPU class (iclass/oclass = 8). This will cause issues such as a remote leaf switch going out of the fabric or traffic drops in the remote leaf switch.	15.0(1k) and later

Cisco Confidential

Bug ID	Description	Exists In
CSCvu22299	VRF communication between two EPGs is disrupted when the last endpoint security group (ESG) under this VRF table that is using a different contract (with a service graph) is removed and service-graph contract is un-deployed. One of the EPGs is in the main datacenter (that is, behind a local leaf switch) and other EPG is behind a remote location (that is, behind a remote leaf switch).	15.0(1k) and later
CSCvu23488	VRF VNID translation gets deleted on a spine switch after PIM is enabled and then disabled on a remote leaf switch, which leads to traffic loss.	15.0(1k) and later
CSCvu43278	BGP triggers the best path selection even without changes to the prefix.	15.0(1k)
CSCvu48401	IPv6 bidirectional forwarding detection (BFD) neighbors flap randomly.	15.0(1k)
CSCvu48703	Cisco ACI iNXOS switches running release 15.0(1k) suffer from PFM process crashing when the switches run for 40+ days.	15.0(1k)
CSCvu64219	There are 2 issues caused by this bug: 1. Dataplane learning is disabled, meaning learning is only occurs only from ARP and ND. This issue occurs on all platforms. 2. Hitbit does not get updated during learn disable, causing endpoints to age prematurely. This issue occurs with N9K-C9336C-FX2, N9K-C93240YC-FX2), N9K-C93240YC-FX2Z, and later switches.	15.0(1k)
CSCvv04251	A policy upgrade fails on the N9K-C9316D-GX and N9K-C93600CD-GX platforms that have the hw_changes_bit programmed as "0x03."	15.0(1k) and later
CSCvv33100	The IPS port is not down when an RX cable is removed on a Cisco ACI leaf switch 1G port. An ACI switch with 1G fiber would signal a peer IOS device, such as a Catalyst 6000 series switch, with flow control auto/desired to turn on the flow control.	15.0(1k) and later
CSCvx70611	ARP requests that should be flooded in encapsulation are instead flooded across encapsulations on the border leaf switches.	15.0(1k) and later
CSCvy43640	A leaf node crashes when PFC or LLFC is enabled on a stretched fabric or a Multi-tier fabric. PFC and LLFC is mainly used for FCoE and RoCE. For a stretched fabric, when a transit leaf node that has connectivity to spine nodes in both locations receives the traffic that matches the QoS class with No-Drop-Cos and PFC enabled, the transit leaf node crashes. For a Multi-tier fabric, when a tier-2 leaf node receives the traffic that matches the QoS class with No-Drop-Cos and PFC enabled, the tier-2 leaf node crashes.	15.0(1k) and later
CSCvz95984	The value of "Use count" in the "show flow monitor" command output is incorrect.	15.0(1k) and later
CSCwa12763	External route import for a VRF instance fails on a leaf switch after removing a shared services contract between two EPGs.	15.0(1k) and later

Cisco Confidential

Bug ID	Description	Exists In
CSCwa47686	For a Cisco ACI fabric with more than 128 leaf switches in a given pod, such as 210 leaf switches in a single pod deployment, after enabling PTP globally, only 128 leaf switches are able to enable PTP. The remaining 82 leaf switches fail to enable PTP due to the error F2728 latency-enable-failed.	15.0(1k) and later
CSCwa95241	An endpoint may fail to resolve an ARP request of another endpoint.	15.0(1k) 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.	15.0(1k) and later
CSCwb14844	There is a long delay when connecting a Cisco N9K-C9336C-FX2 switch to a Mellanox NIC/40G using QSFP-40G-SR4. The status of the port is down, not connected.	15.0(1k) and later
CSCwd29346	An ACI switch's console may continuously output messages similar to: svc_ifc_eventmg (*****) Ran 7911 msecs in last 7924 msecs	15.0(1k) and later
CSCwd36295	The BFD process crashes in Cisco ACI switches and the BFD process is listed in the output of the "show cores" command.	15.0(1k) and later
CSCwd44102	Fiber interfaces (QSA) show up as "Fcot Copper" in the USD port information. When a 10G Fiber optics with Copper QSA is inserted, the fcot gets updated as Copper only instead of Fiber.	15.0(1k) and later
CSCwd49996	A leaf switch may the bring front panel ports up before programming all policies, which causes traffic to get dropped. The issue is specific to a stateless reload or upgrade. The root cause is related to pushing the configuration from the Cisco APIC to the leaf switch, resolving all objects and programming hardware tables. In some corner cases, the bootstrap may be falsely claimed as completed and ports go up while the actual hardware tables are not fully ready. Another symptom may be a significant amount of time needed for bootstrap (possibly over an hour).	15.0(1k) and later
CSCwd75707	The parser drops IP-in-IP packets that are associated with IP traffic on ingress leaf switches.	15.0(1k) and later

Cisco Confidential

Bug ID	Description	Exists In
CSCwd83289	After reloading a leaf switch, HAL becomes unresponsive, other processes generate a core, and HAL continuously runs with ZMQ processing.	15.0(1k) and later
CSCwf04501	There are actrl.Rule programming failures followed by a policy-mgr HAP reset.	15.0(1k) and later
CSCwh71704	When one of the vPC peers reloads and comes up, the non-reloaded peer is seen to be suspending the vPC interfaces.	15.0(1k) and later
CSCwh72876	The EPM process crashed when there was no disk space was available at /var/sysmgr/tmp_logs/.	15.0(1k) and later
CSCwh73782	Traffic that is forwarded by a spine switch toward a leaf switch is dropped by one of the spine switch's fabric modules.On this fabric module where packets are dropped, the TEP of the destination leaf switch is not programmed in FIB and HAL.	15.0(1k) and later
CSCwh78987	Breakout ports configured as port channel members are no longer part of the port channel post clean reload.	15.0(1k) and later
CSCwi89535	A leaf switch crashes due to the following reason: Reason: Reset triggered due to HA policy of ResetService: sdkhal hap resetVersion : xxx	15.0(1k) and later

Resolved Issues

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.

Bug ID	Description	Fixed in
CSCvu43278	BGP triggers the best path selection even without changes to the prefix.	15.0(1l)
CSCvu48401	IPv6 bidirectional forwarding detection (BFD) neighbors flap randomly.	15.0(1l)
CSCvu48703	Cisco ACI iNXOS switches running release 15.0(1k) suffer from PFM process crashing when the switches run for 40+ days.	15.0(1l)
CSCvu64219	There are 2 issues caused by this bug: 1. Dataplane learning is disabled, meaning learning is only occurs only from ARP and ND. This issue occurs on all platforms. 2. Hitbit does not get updated during learn disable, causing endpoints to age prematurely. This issue occurs with N9K-C9336C-FX2, N9K-C93240YC-FX2), N9K-C93240YC-FX2Z, and later switches.	15.0(1l)

Cisco Confidential

Bug ID	Description	Fixed in
CSCva95547	When using the port-tracking feature, the front-panel leaf switch interfaces connected to a Cisco APIC are not brought down.	15.0(1k)
CSCvh11299	In COOP, the MAC IP address route has the wrong VNID, and endpoints are missing from the IP address DB of COOP.	15.0(1k)
CSCvn02710	A link is not err-disabled after continuous link flaps.	15.0(1k)
CSCvn53560	Packets are dropped on service ToR switch when returned from service device on the second path.	15.0(1k)
CSCvo43227	No fault is raised when the number of VMACs of a common perversive gateway is greater than the supported scale on a leaf switch. This is an enhancement to raise a fault in this situation.	15.0(1k)
CSCvp89526	On the Cisco N9K-9336C-FX2 switch, if breakout is configured on all 34 ports. each of the 34X4 subports are bundled into a port channel. This results in 16 subports in 1 port channel after configuring the port channel. When the switch is initialized, HAL crashes upon port bring up.	15.0(1k)
CSCvq00574	EPM on TOR or ETLMC on a spine switch may crash due to a race condition in libtrace logging.	15.0(1k)
CSCvq04973	During the upgrade process, if the Bidirectional Forwarding Detection (BFD) process goes down with the reason "Control Detection Time Expired," applications dependent on BFD, such as BGP, also go down. Immediately after that, the leaf switch brings the BGP up without BFD being up. On an L3Out, this may create traffic blackholing, as BGP might remain up on the leaf switch peer until it times out while the leaf switch reloads for the upgrade.	15.0(1k)
CSCvq57414	HSRP/VRRP packets failed to flood locally in a service leaf switch, which causes a dual active state.	15.0(1k)
CSCvq59201	FT packets are not exported from a line card that is reloaded or that has not completed its hardware programming.	15.0(1k)
CSCvr04782	BGP sessions between VRF tables on the same leaf switch is flapping or does not get established.	15.0(1k)
CSCvr08148	Under certain conditions, the system reset is not captured properly in NVRAM/OBFL. As a result, the reset-reason is shown as "Unknown."	15.0(1k)
CSCvr14699	The Cisco APIC raises fault F1925 for the switch's in-band IP address: lpCktEP provisioning failure for ip <IP_ADDRESS> on node with id <NODE_ID> with name <NODE_NAME> from pod <POD_ID> of fabric <FABRIC_NAME>.	15.0(1k)
CSCvr22599	Remote endpoints are learned behind the wrong ToR switch, which causes traffic to get forwarded and dropped at wrong the ToR switch.	15.0(1k)
CSCvr26165	This is an enhancement request and not a bug. The request is to remove the Layer 4 to Layer 7 services VIP feature from uSeg EPGs.	15.0(1k)

Cisco Confidential

Bug ID	Description	Fixed in
CSCvr35120	Traffic with a UDP destination port of 8472 is dropped on ingress by the Cisco ACI fabric.	15.0(1k)
CSCvr37040	The Cisco Nexus N9K-C9336C-FX2's 100G ports stay link-up even though the neighbor port is down. Even after unplugging the cable, the ports stay link-up.	15.0(1k)
CSCvr52832	There are no aggregated stats from Layer 3 interfaces to Layer 3 Outside logical objects.	15.0(1k)
CSCvr63689	The Cisco ACI N93360YC-FX2 leaf switch becomes inactive.	15.0(1k)
CSCvr71280	If the line card virtual shell (vsh_lc) crashes, the vsh_lc command must be rerun to get the CLI output. There is no other functional impact.	15.0(1k)
CSCvr76947	After upgrading leaf switches and after the switches come online on the target firmware version, reloading the chassis causes a failure to boot and a crash to the Loader> prompt with nothing left in the bootflash from which to boot.	15.0(1k)
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	15.0(1k)
CSCvr83337	A Cisco ACI leaf switch unexpectedly reloads and generates a core file.	15.0(1k)
CSCvr88542	When using 100G LR4 optics on a Cisco N9K-C9336C-FX2 switch, the link bring up time is more than 2 seconds. This bug is an enhancement request to optimize and bring the time to 2 seconds.	15.0(1k)
CSCvs02955	When running the "show system internal epm endpoint all summary" command on an FX leaf switch, the command output is cut short.	15.0(1k)
CSCvs05012	The IPv6 neighbor discovery protocol (NDP) is not triggered for a destination IPv6 address when the source is in one tenant's L3Out and the destination is in a different tenant's L3Out.	15.0(1k)
CSCvs05024	vPC interfaces enter the error-disabled state.	15.0(1k)
CSCvs06119	Multiple switches crash and generate a core file at same time when applying an NTP policy.	15.0(1k)
CSCvs06516	A multicast route does not get programmed in the hardware. This causes the multicast traffic to be dropped.	15.0(1k)
CSCvs14405	During a shared service scenario with an EPG and L3Out, if the same route is under both the EPG and L3Out, the route is leaked and the ctrl property of the route is set to pervasive. If the contract is later removed, the pervasive flag on the leaked route is not cleaned up.	15.0(1k)
CSCvs17688	Interfaces on a leaf switch show no input rate.	15.0(1k)
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	15.0(1k)

Cisco Confidential

Bug ID	Description	Fixed in
	table has the default route-tag policy, routes from the non-transit VRF table would not be installed in the transit VRF table.	
CSCvs18313	1. NTP appears to fail to sync to the server. This is not true; it is just a display issue. A fault is seen in Cisco APIC. 2. NTPD is not running on the leaf switches, which causes NTP to fail to sync to the server. A fault is seen in Cisco APIC. 3. NTP cores on applying new policies, which leads to a HAP reset.	15.0(1k)
CSCvs18318	1. NTP appears to fail to sync to the server. This is not true; it is just a display issue. A fault is seen in Cisco APIC. 2. NTPD is not running on the leaf switches, which causes NTP to fail to sync to the server. A fault is seen in Cisco APIC. 3. NTP cores on applying new policies, which leads to a HAP reset.	15.0(1k)
CSCvs21844	A data packet in a Layer 2-only VLAN dedicated for an FTD cluster communication link (CCL) has an invalid L4 checksum (expected). An N9K-C9364C switch seems to be stomping these packets when getting them from the IPN on interfaces 65-66. This results in an incorrect l2 frame checksum, and a data packet from FTD-A sent to FTD-B through Cisco ACI cannot be processed.	15.0(1k)
CSCvs27994	Ping to a bridge domain's IPv6 link local address may fail.	15.0(1k)
CSCvs28806	If initially only a few leaf switches were configured with the Netflow policy and then the leaf switch profile was changed to include all leaf switches, Netflow will fail on some of the leaf switches.	15.0(1k)
CSCvs31125	When using QSFP-100G-PSM4-S transceivers in an N9K-X9736C-FX linecard that is running ACI code, link flaps may be seen intermittently.	15.0(1k)
CSCvs43349	During 1st attempt to log in, the "#" character acts as a backspace and deletes the previous character. It is necessary to fail the first login attempt to be able to use the "#" character and complete the fallback login.	15.0(1k)
CSCvs45596	Cisco Nexus 9000 Series Fabric Switches includes a version of software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs: CVE-1999-0524 This bug was opened to address the potential impact on this product.	15.0(1k)
CSCvs49377	After a virtual machine is vMotioned, traffic begins to drop the source from that endpoint. When running "show logging ip access-list internal packet-log deny" on the leaf switch, you can see policy drops for the endpoint.	15.0(1k)
CSCvs50080	When fast-link failover hardware support is enabled with more than 32 fabric ports, the sdkhal process aborts.	15.0(1k)

Cisco Confidential

Bug ID	Description	Fixed in
CSCvs61270	A modular spine switch gets stuck during upgrade.	15.0(1k)
CSCvs66240	During leaf switch replacement, vPC ports (map-pinning mode) are flapped on existing switches in the vPC pair.	15.0(1k)
CSCvs75321	Broadcast Traffic/Unknown Unicast/multicast traversing the fabric can get blackholed on nodes that have inconsistent ISIS and MRIB states.	15.0(1k)
CSCvs83907	In the Cisco ACI fabric 14.x releases, when EPG labels or subject labels are used, the contract name may be missing inside the Name column of the "show zoning-rule" command output when executed on a leaf switch.	15.0(1k)
CSCvs96869	A leaf switch will crash with a vntag_mgr HAP reset and generate a core file.	15.0(1k)
CSCvs97901	A node resets with the following crash reason: Last reset at 0 usecs after Fri Jan 31 05:52:52 2020 CST Reason: reset-triggered-due-to-ha-policy-of-reset System version: 13.2(4d) Service: vntag_mgr hap reset	15.0(1k)
CSCvt03829	The interface rate counters freeze after pulling SFP.	15.0(1k)
CSCvt14727	When one DHCP relay label is deleted from the client bridge domain, the relay addresses (the helper addresses) that were programmed based on other labels and applied to the same bridge domain get deleted from the corresponding pervasive SVI as well.	15.0(1k)
CSCvt25313	Inter-pod traffic drops in ToR spine switches that have -EX, -FX, or later suffixes in the product ID. Packets destined to hosts in remote a pod reach the spine switch and are not forwarded despite having the routes present with the correct destination tunnels.	15.0(1k)
CSCvt25585	16 GB ToR switches that do not have -EX, -FX, or a later suffx in the product ID have a kernel panic without generating any core files. The dmesg output shows it was due to an out-of-memory issue.	15.0(1k)
CSCvt38188	After moving static bindings from EPG A to EPG B, static bindings are not deployed on the leaf switch. This is because the EPG is in lazy mode, which means the policy element needs the dynamic policy notification from EPM to download the policies. This condition is treated by the policy element as an add and delete of the EPG. This condition is treated as just an update from the EPM point of view.	15.0(1k)
CSCvt40739	The tunnel destination IP address is not leaned in EPM as a VTEP endpoint.	15.0(1k)
CSCvt41414	When a Layer 4 to Layer 7 vIP address move is triggered across PODs, the leaf switch does not update a local learn to a cached state.	15.0(1k)
CSCvt49916	A spine switch reloads with the following reason:	15.0(1k)

Cisco Confidential

Bug ID	Description	Fixed in
	reset-triggered-due-to-ha-policy-of-reset	
CSCvt49963	ARP requests between EPGs in the same bridge domain are being redirected by the service graph without using an Allow Any contract.	15.0(1k)
CSCvt57119	A Cisco ACI leaf switch sends traffic that is untagged for a particular VLAN even though it is configured as trunk (tagged).	15.0(1k)
CSCvt60814	A port-facing interpod network gets the "Uncalibrated" status, and PTP packets are not seen as received on the spine switch.	15.0(1k)
CSCvt63819	A border leaf switch reflects a certain number of EIGRP routes received from the external router. This issue is seen after a batch of routes are withdrawn downstream of the external router.	15.0(1k)
CSCvt64733	An ARP request from the endpoint behind the remote leaf switch is received on the ToR switch and is flooded to the spine switch as expected (ARP flooding enabled on bridge domain). This can be an issue in cases where the endpoint is behind something such as a Fabric Interconnects, in which it may be expected behavior to delete the MAC address if the endpoint receives the same MAC address back from the upstream leaf switches.	15.0(1k)
CSCvt72137	Traffic on the interface of leaf switch model N9K-C9348GC-FXP is being received at the rate of 125k pps and is not being dropped.	15.0(1k)
CSCvt80543	The Cisco N9K-C9316D-GX spine switches encounter a SDKHAL process crash if the route hardware scale limits are exceeded.	15.0(1k)
CSCvt94039	A leaf switch crashes and reloads due to "nfm hap reset".	15.0(1k)

Known Issues

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 15.0(1) releases in which the known behavior exists. A bug might also exist in releases other than the 15.0(1) releases.

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.	15.0(1k) 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.	15.0(1k) and later

Cisco Confidential

Bug ID	Description	Exists In
CSCup65586	The show interface command shows the tunnel's Rx/Tx counters as 0.	15.0(1k) 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.	15.0(1k) and later
CSCup92534	Continuous "threshold exceeded" messages are generated from the fabric.	15.0(1k) and later
CSCuq39829	Switch rescue user ("admin") can log into fabric switches even when TACACS is selected as the default login realm.	15.0(1k) and later
CSCuq46369	An extra 4 bytes is added to the untagged packet with Egress local and remote SPAN.	15.0(1k) 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.	15.0(1k) and later
CSCuq83910	When an IP address moves from one MAC behind one ToR to another MAC behind another ToR, even though the VM sends a GARP packet, in ARP unicast mode, this GARP packet is not flooded. As a result, any other host with the original MAC to IP binding sending an L2 packet will send to the original ToR where the IP was in the beginning (based on MAC lookup), and the packet will be sent out on the old port (location). Without flooding the GARP packet in the network, all hosts will not update the MAC-to-IP binding.	15.0(1k) 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.	15.0(1k) 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.	15.0(1k) and later
CSCur01336	The power supply will not be detected after performing a PSU online insertion and removal (OIR).	15.0(1k) and later
CSCur81822	The access-port operational status is always "trunk".	15.0(1k) and later

Cisco Confidential

Bug ID	Description	Exists In
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.	15.0(1k) and later
CSCus29623	The transceiver type for some Cisco AOC (active optical) cables is displayed as ACU (active copper).	15.0(1k) 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.	15.0(1k) 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.	15.0(1k) and later
CSCus61748	If the TOR 1RU system is configured with the RED fan (the reverse airflow), the air will flow from front to back. The temperature sensor in the back will be defined as an inlet temperature sensor, and the temperature sensor in the front will be defined as an outlet temperature sensor. If the TOR 1RU system is configured with the BLUE fan (normal airflow), the air will flow from back to front. The temperature sensor in the front will be defined as an inlet temperature sensor, and the temperature sensor in the back will be defined as outlet temperature sensor. From the airflow perspective, the inlet sensor reading should always be less than the outlet sensor reading. However, in the TOR 1RU family, the front panel temperature sensor has some inaccurate readings due to the front panel utilization and configuration, which causes the inlet temperature sensor reading to be very close, equal, or even greater than the outlet temperature reading.	15.0(1k) 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.	15.0(1k) 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.	15.0(1k) 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.	15.0(1k) 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.	15.0(1k) and later

Cisco Confidential

Bug ID	Description	Exists In
CSCuv57302	Atomic counters on the border leaf do not increment for traffic from an endpoint group going to the Layer 3 out interface.	15.0(1k) 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.	15.0(1k) and later
CSCuv57316	TEP counters from the border leaf to remote leaf nodes do not increment.	15.0(1k) 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.	15.0(1k) 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.	15.0(1k) 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.	15.0(1k) 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.	15.0(1k) and later
CSCuy06749	Traffic is dropped between two isolated EPGs.	15.0(1k) and later
CSCuy22288	The iping command's replies get dropped by the QOS ingress policer.	15.0(1k) 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.	15.0(1k) 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.	15.0(1k) 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.	15.0(1k) and later

Cisco Confidential

Bug ID	Description	Exists In
CSCuy61018	The default minimum bandwidth is used if the BW parameter is set to "0", and so traffic will still flow.	15.0(1k) and later
CSCuy96912	The debounce timer is not supported on 25G links.	15.0(1k) 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.	15.0(1k) and later
CSCuz13614	For traffic coming out of an L3out to an internal EPG, stats for the actrlRule will not increment.	15.0(1k) 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.	15.0(1k) and later
CSCuz47058	SAN boot over a virtual Port Channel or traditional Port Channel does not work.	15.0(1k) and later
CSCuz65221	A policy-based redirect (PBR) policy to redirect IP traffic also redirects IPv6 neighbor solicitation and neighbor advertisement packets.	15.0(1k) 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.	15.0(1k) 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.	15.0(1k) and later
CSCvb39965	Slow drain is not supported on FEX Host Interface (HIF) ports.	15.0(1k) 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.	15.0(1k) 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.	15.0(1k) and later

Cisco Confidential

Bug ID	Description	Exists In
CSCvd63567	After upgrading a switch, Layer 2 multicast traffic flowing across PODs gets affected for some of the bridge domain Global IP Outsides.	15.0(1k) and later
CSCvn94400	There is a traffic blackhole that lasts anywhere from a few seconds to a few mins after a border leaf switch is restored.	15.0(1k) and later
CSCvo39715	When downgrading a Cisco ACI fabric, the OSPF neighbors go down after downgrading the Cisco APICs from a 3.2 or later release to a pre-3.2 release. After the upgrade, the switches are still running a 13.2 or later release.	15.0(1k) and later
CSCvp04772	During an upgrade on a dual-SUP system, the standby SUP may go into a failed state.	15.0(1k) and later
CSCvq71034	There is a policy drop that occurs with L3Out transit cases.	15.0(1k) and later
CSCvr12912	A switch reloads due to a sysmgr heartbeat failure and sysmgr HAP reset.	15.0(1k) and later
CSCvr61096	In a port group that has ports of mixed speeds, the first port in the port group that has valid optics present and is not in the admin down state is processed. The ports that come up later are brought up if they are using the same speed; otherwise, they are put in the hw-disabled state. For example, if ports 14 and 15 are up and are using the 100G speed, then if ports 13 and 16 are using the 40G speed, these ports will be put in the hw-disabled state. After reloading or upgrading, you might not have the same interfaces in the port group in the UP state and in the hw-disabled state as you did before the reload or upgrade.	15.0(1k) and later
CSCvs75598	A link flap policy can be configured on Cisco switches that were released prior to the -EX switches. However, this feature does not work with such switches and no fault is raised in the Cisco APIC.	15.0(1k) and later
CSCvt61851	When MPLS VRF stats (egress) is compared with Layer 2 interface egress stats, we can find that the packet count matches for both while there could be a discrepancy with the bytes count.	15.0(1k) and later
CSCvu02371	The DEI value in a Layer 2 header of spanned Tx packets from an MPLS interface might not have the same value as the actual data path packet.	15.0(1k) and later
CSCvu42069	The event log shows VTEP tunnel down and up events. The down time and up time are the same, and there is no fault message.	15.0(1k) and later

Cisco Confidential

Bug ID	Description	Exists In
N/A	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.	15.0(1k) and later
N/A	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 DSCP-CoS translation policy in the APIC for the pod that translates queuing class information of the packet into the DSCP value in the outer header of the iVXLAN packet. You can also embed CoS by enabling CoS preservation. For more information, see the *Cisco APIC and QoS* KB article.	15.0(1k) and later
N/A	The following properties within a QoS class under "Global QoS Class policies" should not be changed from their 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)	15.0(1k) and later
N/A	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.	15.0(1k) and later
N/A	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.	15.0(1k) and later
N/A	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.	15.0(1k) and later
N/A	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.	15.0(1k) and later
N/A	Multicast router functionality is not supported when IGMP queries are received with VxLAN encapsulation.	15.0(1k) and later

Cisco Confidential

Bug ID	Description	Exists In
N/A	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.	15.0(1k) and later
N/A	The rate of the number of IGMP reports sent to a leaf switch should be limited to 1000 reports per second.	15.0(1k) and later
N/A	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 switch. 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 switch. ■ Set "unknown multicast flooding" to "Optimized Flood" on needed bridge domains.	15.0(1k) and later
N/A	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.	15.0(1k) and later
N/A	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.	15.0(1k) and later
N/A	An IP/MAC Ckt endpoint configuration is not supported in combination with static endpoint configurations.	15.0(1k) and later
N/A	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.	15.0(1k) and later
N/A	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.	15.0(1k) and later
N/A	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.	15.0(1k) and later
N/A	An IP/MAC Ckt endpoint configuration is not supported with dynamic endpoint groups. Only static endpoint groups are supported.	15.0(1k) and later

Cisco Confidential

Bug ID	Description	Exists In
N/A	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.	15.0(1k) and later
N/A	Dynamic deployment of contracts based on instrImmedcy set to onDemand/lazy not supported; only immediate mode is supported.	15.0(1k) and later
N/A	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.	15.0(1k) and later
N/A	Direct server return is not supported for shared services. Direct server return endpoints cannot be spread around different virtual routing and forwarding (VRF) contexts.	15.0(1k) and later
N/A	Configurations for a virtual IP address can only be /32 or /128 prefix.	15.0(1k) and later
N/A	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.	15.0(1k) and later
N/A	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).	15.0(1k) and later
N/A	Learning through GARP will work only in ARP Flood Mode.	15.0(1k) and later

Compatibility Information

- For the supported optics per device, see the Cisco Optics-to-Device Compatibility Matrix.
- QSFP-100G-LR4 and QSFP-40/100G-SRBD link up time between Cisco N9K-C9336C-FX2 (non-BV ports) to spine switch (non-BV ports, non-retimer ports) takes approximately 2 to 2.5seconds.
- QSFP-100G-LR4 and QSFP-40/100G-SRBD for all other links between all other switches takes approximately 3.5 to 6.5 seconds.
- 100mb optics, such as the GLC-TE, are supported in 100mb speed only on -EX, -FX, -FX2, and -FX3 switches, such as the N9K-C93180YC-EX and N9K-C93180YC-FX, and only on front panel ports 1/1-48. 100mb optics are not supported any other switches. 100mb optics cannot be used on EX or FX leaf switches on port profile converted downlink ports (1/49-52) using QSA.

Cisco Confidential

- 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).
- 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 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, you must have a 10G interface on the Cisco 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.
- Cisco NX-OS uses an SSL library called CiscoSSL, which is a customized version of the OpenSSL library to support CVE fixes and FIPS compliance. Cisco maintains an extended support contract with OpenSSL. CVE fixes from OpenSSL upstream is regularly incorporated in the older versions of CiscoSSL library as well.
- The following tables provide compatibility information for specific hardware:

Table 12 Modular Spine Switch Compatibility Information

Product ID	Compatibility Information
N9K-C9508	Downgrading a Cisco N9K-C9508 spine switch that has the Cisco N9K-C9508-FM-G fabric module to a pre-15.0(1) release is not supported.

Table 13 Modular Spine Switch Line Card Compatibility Information

Product ID	Compatibility Information
N9K-X9736C-FX	1-Gigabit QSA is not supported on ports 1/29-36. This line card supports the ability to add a fifth Fabric Module to the Cisco N9K-C9504 and N9K-C9508 switches. The fifth Fabric Module can only be inserted into slot 25.

Table 14 Modular Spine Switch Fabric Module Compatibility Information

Product ID	Compatibility Information
N9K-C9508-FM-G	The following information applies to this fabric module: ■ For maximum bandwidth, 5 fabric modules are required. ■ The -G fabric modules require the N9K-C9508-FAN2 fan trays for operation. ■ You must have all three fans running at all times. You must power off the chassis to change the fans and fabric modules.

Cisco Confidential

Table 15 Modular Spine Switch Line Card Compatibility Information

Product ID	Compatibility Information
N9K-C9348GC-FXP	This switch supports the following PSUs: ■ NXA-PAC-350W-PI ■ NXA-PAC-350W-PE ■ NXA-PAC-1100W-PI ■ NXA-PAC-1100W-PE The following information applies to this switch: ■ 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. ■ The PSU SPROM is not readable when the PSU is not connected. The model displays as "UNKNOWN" and status of the module displays as "shutdown."
N9K-C93180LC-EX	This switch has the following limitations: ■ 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.

Table 16 Fixed Spine Switch Compatibility Information

Product ID	Description

Cisco Confidential

Product ID	Description
N9K-C9364C	You can deploy multipod or Cisco ACI Multi-Site separately (but not together) on the Cisco N9K-9364C switch starting in the 3.1 release. You can deploy multipod and Cisco ACI Multi-Site together on the Cisco N9K-9364C switch starting in the 3.2 release. 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. This switch supports the following PSUs: ■ NXA-PAC-1200W-PE ■ NXA-PAC-1200W-PI ■ N9K-PUV-1200W ■ NXA-PDC-930W-PE ■ NXA-PDC-930W-PI
N9K-C9316D-GX	1G and 100MB speeds are not supported.

Table 17 Fixed Leaf Switch Compatibility Information

Product ID	Description
N9K-C93180YC-EX	The following information applies to this switch: ■ The following FEC modes are not supported on N9K-C93180YC-EX ports 1 through 48 when running in 25G speed: ○ cl91-rs-fec ○ cons16-rs-fec ○ ieee-rs-fec ■ Auto-negotiation is not supported if you convert port 51 or 52 to a downlink and you have 40/100G copper cables connected.
N9K-C93180YC-FX	Auto-negotiation is not supported if you convert port 51 or 52 to a downlink and you have 40/100G copper cables connected.

Cisco Confidential

Product ID	Description
N9K-C9336C-FX2	The following information applies to this switch: ■ On older N9K-C9336C-FX2 switches, auto-negotiation does not work on port eth1/4. You can check whether your switch is older by using the following command: ifav124-leaf5# cat /sys/kernel/cisco_board_info/hw_change_bits 0x0 Output of "0x0" indicates an older switch that has this limitation. ■ You can apply a breakout configuration on ports 1 through 34, which can give up to 136 (34*4) server or downlink ports. ■ Port profiles and breakouts are not supported on the same port. However, you can apply a port profile to convert a fabric port to a downlink, and then apply a breakout configuration. ■ If you apply a breakout configuration on 34 ports, you must configure a port profile on the ports first, which requires you to reboot the leaf switch. ■ If you apply a breakout configuration to a leaf switch for multiple ports at the same time, it can take up to 10 minutes for the hardware of 34 ports to be programmed. The ports remain down until the programming completes. The delay can occur for a new configuration, after a clean reboot, or during switch discovery. ■ Ports 7 through 32 have a link bring up time of less than 2 seconds with QSFP-100G-LR4 and QSFP-40/100G-SRBD optics. For all other ports, the link up time for these optics is between 5 to 14 seconds. In the following situations, the link bring up time will also be greater than 2 seconds: ■ After reloading the Top-of-Rack (ToR) switch ■ When using port optical insertion and removal (OIR) ■ When performing bulk flaps of ports on the ToR switch

Cisco Confidential

Product ID	Description
N9K-C93600CD-GX	This switch has the following limitations: ■ Auto-negotiation is not supported with 10G speed on ports 1 through 24. ■ For ports 1 through 24, every 4 ports (1-4, 5-8, 9-12, and so on, referred to as a "quad") will operate at a fixed speed. That is, all 4 ports will operate in 10G, or 40G, or 100G; you cannot mix the speeds. ■ Mixed speeds of 10G and 40G, or 10G and 100G, or 40G and 100G in a quad is not supported. Based on the port bring up sequence, the port in the quad where the speed mismatch is detected will be HW disabled. ■ If there is a speed mismatch in a quad even though the ports are configured in the disabled state, the working links in that quad might get into the HW disabled state upon upgrading or reloading, as the mixed speed is brought up first before admin down config is pushed. To avoid this issue, you must manually use the shut and no shut commands on the working ports to bring up the links. For more information, see bug CSCvr61096. ■ Ports 25-26 and ports 27-28 (port groups of 2 ports each) will operate in a fixed speed within the respective group, and you cannot mismatch the speed. ■ Uplink ports 29 to 36 do not have a mixed speed restriction; you can toggle the speed for the bidirectional ports. ■ For ports 1 to 28, even if you convert any ports to uplink with bidirectional optics, you cannot toggle the speed, as it will introduce mixed speeds and will disturb the neighboring ports. ■ For ports 1 to 28, if any of the ports are converted to uplink with bidirectional optics, the ports will stay in the not connected state if the peer is a 40G link. ■ 4X10 and 4X25 breakout is supported on ports 25-28 and 29-34 (port profile converted downlinks). ■ Ports 25-26 and 27-28 form respective port pairs, and each pair can operate with 4X10, 10G, or 4X25G speed. ■ This switch does not support 4X100 breakout in this release. ■ The Hardware Abstraction Layer (HAL) will spike and the console can hang if a port channel or vPC exists when overlying breakout ports are deleted. To avoid this issue, delete the PC or vPC before deleting the overlying breakout policy. ■ 1G and 100MB speeds are not supported.

Cisco Confidential

Product ID	Description
N9K-C9364C-GX	This switch has the following limitations: ■ Auto-negotiation is not supported with 10G speed on ports 1 through 64. ■ The switch will power down in 2 minutes after the first fan failure. The switch can be powered up only after replacing the failed fan. ■ For ports 1 through 64, every 4 ports (1-4, 5-8, 9-12, and so on, referred to as a "quad") will operate at a fixed speed. That is, all 4 ports will operate in 10G, or 40G, or 100G; you cannot mix the speeds. ■ Mixed speeds of 10G and 40G, or 10G and 100G, or 40G and 100G in a quad is not supported. Based on the port bring up sequence, the port in the quad where the speed mismatch is detected will be HW disabled. ■ If there is a speed mismatch in a quad even when the ports are configured in the disabled state, the working links in that quad might get into the HW disabled state upon upgrading and reloading because the mixed speed is brought up first before the admin down configuration is pushed. As a result, you must manually perform the shut and no shut commands on the ports to bring up the links. ■ Breakout of 4x25G or 4X10G ports is not supported. ■ There is a lane selector button on the hardware. The button is used for the breakout port LED status. Because breakout is not supported, this button does nothing. ■ 1G and 100MB speeds are not supported. ■ All 4 fans must be operational, otherwise the switch will power down due to a fan policy trigger.

Table 18 Fixed Spine Switch Fan Compatibility Information

Product ID	Description
N9K-C9508-FAN2	You must have either the N9K-C9508-FM-G or the C9508-FAN-PWR in every fabric slot. This is because each fan tray needs two power convertors (from 12V to 50V) to provide enough power.

- The following table provides MACsec and CloudSec compatibility information for specific hardware:

Table 19 MACsec and CloudSec Support

Product ID	Hardware Type	MACsec Support	CloudSec Support
N9K-C93108TC-FX	Switch	Yes	No
N9K-C93180YC-FX	Switch	Yes	No

Cisco Confidential

Product ID	Hardware Type	MACsec Support	CloudSec Support
N9K-c93216TC-FX2	Switch	Yes	No
N9K-C93240YC-FX2	Switch	Yes	No
N9K-C9332C	Switch	Yes	Yes, only on the last 8 ports
N9K-C93360YC-FX2	Switch	Yes	No
N9K-C9336C-FX2	Switch	Yes	No
N9K-C9348GC-FXP	Switch	Yes, only with 10G+	No
N9K-C9364C	Switch	Yes	Yes, only on the last 16 ports
N9K-X9736C-FX	Line Card	Yes	Yes, only on the last 8 ports

The following additional MACsec and CloudSec compatibility restrictions apply:

- MACsec is not supported with 1G speed on Cisco ACI leaf switch.
- MACsec is supported only on the leaf switch ports where an L3Out is enabled. For example, MACsec between a Cisco ACI leaf switch and any computer host is not supported. Only switch-to-switch mode is supported.
- When using copper ports, the copper cables must be connected directly the peer device (standalone N9k) in 10G mode.
- A 10G copper SFP module on the peer is not supported.
- CloudSec only works with spine switches in Cisco ACI and only works between sites managed by Cisco ACI Multi-Site.
- For CloudSec to work properly, all of the spine switch links that participate in Cisco ACI Multi-Site must have MACsec/CloudSec support.

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 *Cisco Application Policy Infrastructure Controller Release Notes, Release 5.0(1)* for policy information.

  - 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.

Cisco Confidential

- 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 typically have memory utilization of approximately 70% to 75%, even in a new deployment where no configuration has been pushed. This amount of memory utilization is due to the Cisco ACI-specific processes, which take up more memory compared to a standalone Nexus deployment. The memory utilization is not a problem unless it exceeds 90%. You can open a Cisco TAC case to troubleshoot proactively when memory utilization is more than 85%.
- 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 15.0(1) 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.
- 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

Cisco Confidential

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.
- You cannot enable auto-negotiation on the spine switch or leaf switch side with 40G or 100G CR4 optics. For 40G copper transceivers, you must disable auto-negotiation and set the speed to 40G. For 100G copper transceivers, you must disable auto-negotiation on the remote end and set the speed to 100G.
- You cannot enable auto-negotiation on an active QSFP to SFP/SFP+ Adapter (QSA) module. You can enable auto-negotiation only on a passive QSA module. The following example CLI command shows an active QSA module:

  ```
  module-1# show platform internal usd port info | grep -A 10 "Eth1/42"
  Port 107.0 (Eth1/42)  : Admin UP   Link DOWN Cfg_Fec Disabled Fec Disabled Fcot Copper retimer 0x116c0100
     AN_cfg Yes   AN_operSt No ln_debounce 0, Debounce-Time 100000 usecs SM sm qsa: Yes
  ```

  The following example CLI command shows a passive QSA module:

  ```
  module-1# show platform internal usd port info | grep -A 10 "Eth1/43"
  Port 109.0 (Eth1/43)  : Admin UP   Link UP   Cfg_Fec Disabled Fec Disabled Fcot Copper retimer 0x116c0100
     AN_cfg Yes   AN_operSt No ln_debounce 0, Debounce-Time 100000 usecs SM sm qsa: Passive
  ```

- You can enable auto-negotiation for 10G, 25G, 40G, or 100G on downlink ports on a Cisco ACI leaf switch. However, you cannot enable auto-negotiation on spine ports and uplink ports on a Cisco ACI leaf switch. Therefore, if the Inter-Pod Network (IPN) is connected to the spine ports using copper cables, you should disable auto-negotiation on the peer node that is the IPN port. Similarly, if a remote leaf switch is connected to the IPN using copper cables on the uplink port, you should disable auto-negotiation on the peer node that is the IPN port.
- 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.
- When the provider edge router is an IOS XR device, the router does not support route re-origination from one EVPN stitching site to another EVPN stitching site.

Related Content

See the Cisco Application Policy Infrastructure Controller (APIC) page for the Cisco APIC documentation.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to apic-docfeedback@cisco.com. We appreciate your feedback.

Legal Information

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

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

© 2020-2025 Cisco Systems, Inc. All rights reserved.