Cisco Nexus 3000 Series NX-OS Release Notes, Release 7.0(3)I7(9)

This document describes the features, issues, and exceptions of Cisco NX-OS Release 7.0(3)I7(9) software for use on Cisco Nexus 3000, 3100, 3200 and 3500 switches. For more information, see *Related Content*.

Note: The Cisco Nexus 3400-S and 3600 platform switches are not supported in Cisco NX-OS Release 7.0(3)I7(9). Starting with Cisco NX-OS Release 7.0(3)I2(1), the Cisco NX-OS image filename has changed to start with "nxos" instead of "n3000."

Table 1 Online History Change

Date	Description
Jan 18, 2021	Updated the Upgrade and Downgrade section for Compact NX-OS Image.
September 16, 2020	Added CSCvv31955 to resolved issues.
August 31, 2020	Cisco NX-OS Release 7.0(3)I7(9) became available.

Contents

New Software Features

Table 2: New Software Features

Feature	Description
Pre-compacted NX-OS Images	Cisco Nexus 3048, 3064, 3132 (except for the N3K-C3132Q-V), and 3172 platform switches with a model number that does not end in -XL must run a "compact" NX-OS software image due to limited bootflash space. This "compact" image can be created using the NX-OS Compact Image procedure; alternatively, a compact NX-OS software image can be downloaded directly from Cisco's Software Download website. This requirement does not apply to any other model of Cisco Nexus 3000 or 3100 series switch. This requirement does not apply to the Nexus 3132Q-V switch. For more information, see the following documents: • "Upgrade and Downgrade" section in this document. • Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x
DSCP Wildcard Mask	Added support for creating an ACL that matches or filters traffic based on a DSCP bit mask. For more information, see: Cisco Nexus 3000 Series NX-OS QoS Configuration Guide, Release 7.x
Model-Driven Telemetry	Added support added for Cisco Nexus 3500 platform switches. For more information, see: Cisco Nexus 3000 Series NX-OS Programmability Guide, Release 7.x
PTP ACL Redirect	Added support for PTP unicast forwarding by hardware ACL. For more information, see: Cisco Nexus 3548 Switch NX-OS System Management Configuration Guide, Release 7.x

New Hardware Features

Cisco NX-OS Release 7.0(3)I7(9) does not support any new hardware.

Open Issues

The following tables lists the Open Issues in Cisco Nexus 3000, 3100, 3200 and 3500 Series switches in Cisco NX-OS Release 7.0(3)I7(9). Click the Bug ID to search the Cisco Bug Search Tool for additional information about the bug.

- Open Issues in Cisco Nexus 3000, 3100 and 3200 Switches
- Open Issues in Cisco Nexus 3500 Switches

Table 3: Open Issues in Cisco Nexus 3000, 3100, 3200 Series Switches

Bug ID	Description
CSCvq96790	**Headline**: OSPF single hop BFD is not working on specific platforms **Symptom**: BFD sessions where peers are connected via intermediate hop Nanook switch may not come up. This is due to Nanook punting transit BFD packets to SUP instead of forwarding them. **Workaround**: No BFD should be configured on Nanook device when acting as intermediate hop switch. If BFD is required on intermediate hop switch due to other connectives/applications, no workaround exists.

Table 4: Open Issues in Cisco Nexus 3500 Series Switches

Bug ID	Description
CSCvq98238	**Headline**: Multicast UDP NAT support is not available on Cisco Nexus 3500 Switches **Symptom**: Multicast NAT UDP based translation won't happen. Only Multicast NAT based on source IP & destination IP is current supported but not based on UDP port. **Workaround**: Multicast NAT with only source IP or destination group must be used in translation.

Resolved Issues

The following tables list the Resolved Issues in Cisco Nexus 3000, 3100, 3200 and 3500 Series switches in Cisco NX-OS Release 7.0(3)I7(9). Click the Bug ID to search the Cisco Bug Search Tool for additional information about the bug.

- Resolved Issues in Cisco Nexus 3000, 3100 and 3200 Switches
- Resolved Issues in Cisco Nexus 3500 Switches

Table 5: Resolved Issues in Cisco Nexus 3000, 3100, 3200 Series Switches

Bug ID	Description

Bug ID	Description

CSCvu19105	**Headline**: LLDP packets with destination MAC of 01:80:c2:00:00:03 cause Cisco Nexus 3000 switches to learn the source mac address
	
	Symptom: One use-case where this can be an issue is when a server with an active/standby pair of NICs connects to a vPC pair and both active and standby NICs send LLDP packets using the same virtual Source MAC. Due to this defect, the switch learns the source MAC when it receives LLDP packets from the standby NIC, causing blackholing due to traffic being sent to the standby NIC instead.
	
	`F340.09.04-N3K-5# ethanalyzer local interface inband display-filter lldp limit-captured-frames 0`
	`Capturing on inband`
	`2020-05-09 08:18:08.142174 3c:51:0e:44:db:80 -> 01:80:c2:00:00:03 LLDP Chassis Id = 3c:51:0e:44:db:80 Port Id = Ethernet1/32 TTL = 120 System Name = N9336-2`
	`2020-05-09 08:18:13.142156 3c:51:0e:44:db:80 -> 01:80:c2:00:00:03 LLDP Chassis Id = 3c:51:0e:44:db:80 Port Id = Ethernet1/32 TTL = 120 System Name = N9336-2`
	`2020-05-09 08:18:14.322279 00:62:ec:40:4f:c8 -> 01:80:c2:00:00:0e LLDP Chassis Id = 00:62:ec:40:4f:c8 Port Id = Ethernet1/1 TTL = 120 System Name = F340.09.04-N3K-5`
	`F340.09.04-N3K-5# show lldp neighbors`
	`ERROR: No neighbour information`
	`F340.09.04-N3K-5# show mac address-table`
	`Legend:`
	`* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC`
	`age - seconds since last seen,+ - primary entry using vPC Peer-Link,`
	`(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan`
	`VLAN MAC Address Type age Secure NTFY Ports`
	`---------+-----------------+--------+---------+------+----+------------------`
	`* 921 3c51.0e44.db80 dynamic 0 F F Eth1/1 <<<<<<<<<<<<<<`
	Workaround: Disable LLDP on the device which generates this packet.

Bug ID	Description

CSCvv19549	**Headline**: Multiple ERSPAN Destination sessions not working as expected
	
	Symptom: When we configure two ERSPAN Destination session with two different ERSPAN ID, 2nd ERSPAN destination does not work. Traffic from both session is sent to destination port defined defined in 1st ERSPAN destination. In the example below ERSPAN Encapsulated traffic from both sessions will be send to E1/4
	`N3K-2(config-erspan-dst)# sh run monitor`
	`!Command: show running-config monitor`
	`!Running configuration last done at: Sun Mar 24 15:56:50 2002`
	`!Time: Sun Mar 24 16:06:00 2002`
	`version 9.3(3) Bios:version 5.3.1`
	`monitor session 1 type erspan-destination`
	`  erspan-id 1`
	`  source ip x.x.x.x`
	`  destination interface Ethernet1/4`
	`  no shut`
	`monitor session 3 type erspan-destination`
	`  erspan-id 2`
	`  source ip x.x.x.x`
	`  destination interface Ethernet1/5`
	`  no shut`
	`Note x.x.x.x is the same ip under both sessions above.`
	`N3K-2(config-erspan-dst)#`
	`Sesions will be show up`
	`N3K-2(config-erspan-dst)# sh monitor`
	`Session  State  Reason  Description`
	`-------  -----------  ----------  ----------`
	`1  up  The session is up`
	`3  up  The session is up`
	`N3K-2(config-erspan-dst)#`
	Workaround: None

CSCvt56401	**Headline**: ACL QoS crash when configure new QoS group in case of system QoS already apply
	Symptom: Rebooted the device and saw the following logs
	`2010 Feb 19 10:09:37 switch %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos" (PID 3201) hasn't caught signal 11 (core will be saved).`
	`2010 Feb 19 10:09:38 switch %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "aclqos" (PID 3915) hasn't caught signal 11 (core will be saved).`
	`2010 Feb 19 10:09:38 switch %SYSMGR-SLOT1-2-HAP_FAILURE_SUP_RESET: Service "aclqos" in vdc 1 has had a hap failure`
	`2010 Feb 19 10:09:38 switch %SYSMGR-SLOT1-2-LAST_CORE_BASIC_TRACE: fsm_action_become_offline: PID 17099 with message Could not turn off console logging on vdc 1 error: mts req-response with syslogd in vdc 1 failed (0xFFFFFFFF)`
	Workaround:
	1. Remove the "service-policy type qos input SET-QOS-Group" under "system qos".
	2. Add new group in this QoS.
	3. Re-apply the "service-policy type qos input SET-QOS-Group" to "system qos".

CSCvt81574	**Headline**: Cisco Nexus 3000 switches VxLAN - Multicast traffic forwarded back to source port in N3K mode **Symptom**: Multicast link-local traffic is being sent back to source-port configured to allow VLAN mapped to a vn-segment. **Workaround**: Remove vn-segment if not needed.
CSCvu82715	**Headline**: BCM-ATTACH optimization while BCM-SDK Initialization **Symptom**: This is a rare failure while upgrading image using Fast Reload. Upgrade takes 3 minutes more than expected time of 30 seconds of Data plane downtime. **Workaround**: None

Bug ID	Description
CSCvt65358	**Headline**: Cisco Nexus Switches reload due to service bcm_usd hap reset **Symptom**: Cisco Nexus 3000 and 3100 Series switches may reload due to in service "bcm_usd" crashes. **Workaround**: None
CSCvt72230	**Headline**: Openflow traffic loss when Eth1/32 is a member port in port-channel for egress traffic **Symptom**: Packet dropped when they are having Eth1/32 as a member in the egress port-channel. **Workaround**: None

CSCvu20773	**Headline**: Fast-reload upgrade goes to normal reload when it fails to extract initrd from compact image on Cisco Nexus 3064 Switches
	Symptom: When Fast-reload fails to extract image to be booted as below, fast-reload software should have mechanism to bail out.
	`INIT: version 2.88 booting`
	`Skipping ata_piix install for n3k.`
	`Unsquashing rootfs ...`
	`Removing libcrdcfgdata and linking libcrdcfgdata3nk`
	`Fastboot unexpected error: /bootflash//nxos.7.0.3.I7.7a-n3064-compact.bin not found`
	Workaround: None

CSCvu24785	**Headline**: switchport dot1q EhterType 0x88a8 but packets encapsulated in 0x8100
	Symptom:
	`Ethernet II, Src: 70:6d:15:41:6b:43 (70:6d:15:41:6b:43), Dst: e4:c7:22:dc:f8:01 (e4:c7:22:dc:f8:01)`
	`Destination: e4:c7:22:dc:f8:01 (e4:c7:22:dc:f8:01)`
	`Address: e4:c7:22:dc:f8:01 (e4:c7:22:dc:f8:01)`
	`.... ...0 .... .... .... .... = IG bit: Individual address (unicast)`
	`.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)`
	`Source: 70:6d:15:41:6b:43 (70:6d:15:41:6b:43)`
	`Address: 70:6d:15:41:6b:43 (70:6d:15:41:6b:43)`
	`.... ...0 .... .... .... .... = IG bit: Individual address (unicast)`
	`.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)`
	`Type: 802.1Q Virtual LAN (0x8100) <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< Remains 0x8100`
	`802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 82`
	`000. .... .... .... = Priority: 0`
	`...0 .... .... .... = CFI: 0`
	`.... 0000 0101 0010 = ID: 82`
	`Type: 802.1Q Virtual LAN (0x8100)`
	`802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 10`
	`000. .... .... .... = Priority: 0`
	`...0 .... .... .... = CFI: 0`
	`.... 0000 0000 1010 = ID: 10`
	`Type: IP (0x0800)`
	Workaround:
	1. Default the ethertype after port flap
	`no switchport dot1q ethertype`
	2. Re-apply the required ethertype
	`switchport dot1q ethertype`

Bug ID	Description

CSCvv18540	**Headline**: After fast reload upgrade Ipv6 RA message sent out with A bit set though configured for A bit clear
	Symptom: During nexus 3064 fast reload upgrade activity((6.0(2)U6(7) ------- > 7.0(3)I7(7a))) customer windows VM reportedly received IPv6 RA message from nexus 3064 with A bit set though configured for A bit clear on Vlan SVI interface. This caused VM to configure SLAAC Ipv6 address using RA message received. This caused VM to use SLAAC address over statis IPv6 address impacting VM reachablity.
	`interface Vlan702`
	`  ipv6 address 2603:10b0:90d:fcb2::1/64`
	`  ipv6 nd managed-config-flag`
	`  ipv6 nd prefix 2603:10b0:90d:fcb2::/64 infinite infinite no-autoconfig`
	Workaround: None

CSCvt76516	**Headline**: On Cisco Nexus 3000 switches, protocol multicast packets received over Layer 3 interface and flood to L2 BD **Symptom**: For Cisco Nexus 3000 switches, when protocol multicast packets received over Layer 3 interface will be flood to L2 BD consult **Workaround**: None
CSCvv31955	Headline: Multicast IP PIM register not sent and data packet got punt to CPU. Symptoms: S,G never built even though the data packet is hitting the L2 interface. IP PIM register is never generated by CPU due to data packet getting dropped inside CPU Workarounds: Flapping the corresponding SVI M will fix the issue or use static OIL Apply Static OIL makes it work. Even after static OIL removal, the working state still remains. The issue will trigger once again, after the sender stops sending packets for a while and the S,G timed out.

Table 6: Resolved Issues in Cisco Nexus 3500 Series Switches

Bug ID	Description
CSCvu59181	**Headline**: Layer 2 Multicast not working for PVLAN (same community VLAN) with IGMP snooping disabled **Symptom**: L2 Multicast not working for PVLAN (same community VLAN) with IGMP snooping disabled **Workaround**: None
CSCvu98485	**Headline**: %COPP-2-COPP_INVALID_POLICY_TEMPLATE: error observed with default COPP for copp-s-mpls **Symptom**: Nexus 3500 gives following error message even when 1. ***no COPP*** class is missing 2. Default COPP is applied 3. Setup command is ran to apply default copp-class `2020 Jul 13 13:52:18 switch %$ VDC-1 %$ %COPP-2-COPP_INVALID_POLICY_TEMPLATE: Current CoPP policy is missing system default class-maps. Please run "setup" command to configure missing class-maps.` **Workaround**: None
CSCvt39615	**Headline**: On Cisco Nexus 3500 switches, SPAN may stop creating copies and dropping packets with 40G intf as destination **Symptom**: No SPAN copies are received by attached host **Workaround**: Use 10G SPAN destination port.
CSCvu26463	**Headline**: Cisco Nexus 3500 switches may age out active tcp flow NAT translation unexpectedly **Symptom**: NAT TCP flow closed unexpectedly. **Workaround**: None
CSCvv23222	**Headline**: Transceiver is not recognized after configuring "no negotiate auto" **Symptom**: After configure "no negotiate auto", even configure "speed auto" and "negotiate auto" again, the transceiver is not recognized. **Workaround**: 7.0(3)I7(8): `F340.09.02-3500-1(config-if)# negotiate auto`

Bug ID	Description

	F340.09.02-3500-1(config-if)# speed 10000
	F340.09.02-3500-1(config-if)# no speed 40000
	F340.09.02-3500-1(config-if)# copy run startup-config
	[##] 100%
	F340.09.02-3500-1(config-if)# show run int ethernet 1/1 all | include nego|speed
	  speed auto
	  negotiate auto
	F340.09.02-3500-1(config-if)# reload
	This command will reboot the system. (y/n)? [n] y

CSCvn77945	**Headline**: MTC USD Core when executing "test hardware internal MTC-USD measure-eye front-port #" **Symptom**: When attempting to check the eye diagram/information for a Nexus 3524/3548 the switches crashes due to MTC USD when executing "test hardware internal MTC-USD measure-eye front-port <>" **Workaround**: Do not run the mentioned command on the affected released, upgrade to a fix version of NX-OS in order to get a fixed version of the command.
CSCvt09871	**Headline**: Interfaces connected with certain DAC cables may show as "not supported" **Symptom**: Certain DAC used on 3548 switches may show "transceiver is not supported" **Workaround**: Remove and reinsert the SFP
CSCvt25753	**Headline**: Nexus 3500 IGMPv3 leave from single host causes OIL flush until next query **Symptom**: When Nexus 3500 has downstream host using IGMPv3 and the host sends a leave for the multicast group the mroute OIL gets flushed and other hosts lose the multicast stream even though their interface is still populated in the IGMP snooping table. **Workaround**: Disable explicit host tracking under vlan configuration: configure terminal vlan configuration 10 no ip igmp snooping explicit-tracking
CSCvt55774	**Headline**: PPS exceed message not working on Cisco Nexus 3500 XL platform switches. **Symptom**: None **Workaround**: None

CSCvu04531	**Headline**: Nexus 3548-XL after upgrading to 7.0(3)I7(7), disabling mac learning is not working
	Symptom: With MAC learning disabled globally and on the interface level we still see MAC is being learnt:
	<pre>
	STLD1-630.02.02-N3K-RU35(config-if)# show run | i mac
	mac-learn disable
	  switchport mac-learn disable
	
	STLD1-630.02.02-N3K-RU35(config-if)# show mac address-table
	  VLAN MAC Address Type age Secure NTFY Ports
	---------+-----------------+--------+---------+------+----+-----------------
	* 1 e865.49ee.8101 dynamic 0 F F Eth1/10
	G - b4de.313e.c5fc static - F F sup-eth1(R)
	G 1 b4de.313e.c5fc static - F F sup-eth1(R)
	</pre>
	Workaround: Configure the interface seeing MAC learning in single interface Port-channel, for example: "channel-group mode x", where "x" is the port-channel number.

CSCvu54266	**Headline**: clearing ARP or MAC might break the ECMP hardware programming on Nexus 3500 switches **Symptom**: Latency/packet loss for data plane traffic Random packet loss for data plane flows Data plane is punted to the CPU (data plane flows reported on ethanalyzer captures) **Workaround**: Remove and re-configure ECMP (for example, modify the IGP cost in such a way that ECMP is removed and then revert the configuration). Any change to ECMP members which can cause reprogramming of the ECMP entry in hardware.
CSCvt31282	**Headline**: L3 connectivity issue due to hardware adjacency table mis-programming **Symptom**: Unknown unicast traffic is not gleaned. Nexus will not punt the traffic to CPU and ARP will not be forged which will cause connectivity issue once the ARP entry will time out. **Workaround**: Ping the host from the switch SVI to maintain the ARP entry

Bug ID	Description
CSCvt86775	**Headline**: N3548 'show ptp clock' displays incorrect PTP master offset in XML output **Symptom**: 'show ptp clock' displays incorrect offset-from-master value in xml format. **Workaround**: 'show ptp corrections | xml' displays correct values.
CSCvu39379	**Headline**: PTP packets not forwarded on interface with PVLAN configuration **Symptom**: PTP packets (Announce, Sync, Followup) are not forwarded / sent on interface with PVLAN configuration With below config : interface Ethernet1/1 ptp ptp vlan 2022 >>>>> switchport mode private-vlan host >>>>>> switchport private-vlan host-association 200 2022 >>>>>>> Below Output: show ptp counters interface e1/1 PTP Packet Counters of Interface Eth1/1: --- Packet Type TX RX --- Announce 0 0 Sync 0 0 FollowUp 0 0 Delay Request 0 0 Delay Response 0 0 PDelay Request 0 0 PDelay Response 0 0 PDelay Followup 0 0 --- **Workaround**: Downgrade to I7(7)
CSCvt34933	**Headline**: Cisco Nexus 3500 Switches reports high PTP correction in milli-seconds after reselecting original GM **Symptom**: N3500 reporting high PTP correction. **Workaround**: Reload the device.
CSCvu42328	**Headline**: N3500 NAT may create stale tcp translation entries with zero time-left **Symptom**: Stale NAT tcp translation entries left in NAT table. **Workaround**: None
CSCvr09523	**Headline**: N3500 incorrect LTL for L2 multicast **Symptom**: A Nexus 3548 with IGMP snooping enabled may drop L2 multicast packets for some groups. **Workaround**: Shut / no shut of outgoing interfaces may resolve the problem.
CSCvt50489	**Headline**: N3500 may stop sending PTP delay-response messages **Symptom**: PTP client reporting high PTP correction. **Workaround**: Flip-flop GPE16 interrupt from bash prompt: 1. echo disable > /sys/firmware/acpi/interrupts/gpe16 2. echo enable > /sys/firmware/acpi/interrupts/gpe16
CSCvv14062	**Headline**: Cisco Nexus 3548 Switch has IP unicast reachability from SUP to any direct connect end host **Symptom**: One of the Nexus across vPC is not reachable to direct connected device. All Control-plane generated IP unicast packet are impacted. Layer 2 forwarding is fine on data plane. TX counter never increased. **Workaround**: When you ping from the end host to the switch, everything for that specific port-channel starts working again. ERSPAN with source interface as the peer-link and apply and then delete the static mac entry with exit port as peer-link will also bring the device out of the broken state. After reloading the switch, it is back to the broken state again.
CSCvv05805	**Headline**: GMR5: MTC_USD crash seen while executing active buffer monitor show command **Symptom**: switch(config)# 2020 Jul 18 05:10:06 switch %$ VDC-1 %$ %SYSMGR-SLOT1-2-SERVICE_CRASHED: Service "mtc_usd" (PID 28711) hasn't caught signal 11 (core will be saved). switch %$ VDC-1 %$ %SYSMGR-SLOT1-2-HAP_FAILURE_SUP_RESET: Service "mtc_usd" in vdc 1 has had a hap failure

Bug ID	Description
	switch %$ VDC-1 %$ %SYSMGR-SLOT1-2-LAST_CORE_BASIC_TRACE: fsm_action_become_offline: PID 16896 with message Could not turn off console logging on vdc 1 error: mts req-response with syslogd in vdc 1 failed (0xFFFFFFFF) . switch %$ VDC-1 %$ %USER-2-SYSTEM_MSG: libsdk_tlv_dispatch:51: sse_call2 failed with rc=-1(Device Name:[0x3FF] Instance:[63] Error Type:[(null)] code:[255]) - iftmc switch %$ VDC-1 %$ %USER-2-SYSTEM_MSG: libsdk_tlv_fe_handler:216: TLV dispatch function failed, rc = -5(RPC error) - iftmc switch %$ VDC-1 %$ %USER-2-SYSTEM_MSG: libsdk_l3_route_stats_get:268: TLV front-end handler failed, rc = -5(RPC error) - iftmc switch %$ VDC-1 %$ %SYSMGR-SLOT1-2-LAST_CORE_BASIC_TRACE: core_client_main: PID 30213 with message filename = 0x102_mtc_usd_log.28711.tar.gz . switch %$ VDC-1 %$ %MODULE-2-MOD_DIAG_FAIL: Module 1 (Serial number: XXXXXXXXXX) reported failure due to Service on linecard had a hap-reset in device DEV_SYSMGR (device error 0x44a) **Workaround**: You must avoid executing below show commands: sh hardware profile buffer monitor buffer-block 1 detail sh hardware profile buffer monitor buffer-block 2 detail sh hardware profile buffer monitor buffer-block 3 detail

Known Issues

The following tables lists the known behaviors in Cisco Nexus 3000, 3100, 3200 and 3500 Series switches in Cisco NX-OS Release 7.0(3)I7(9). Click the bug ID to search the Cisco Bug Search Tool for details about the bug.

Table 7: Known Behaviors in Cisco Nexus 3000 and 3100 Series Switches

Bug ID	Description
CSCvj60944	ERSPAN packets punted to CPU on ERSPAN-destination when the destination interface is down.
CSCvb33981	Cisco Nexus 3172: IPV6 ND punted to CPU even with no ipv6 configured.
CSCvg21631	N3K PBR: 'set ip default next-hop' not preferred over default route
CSCvh27369	N3K: RACL applied to SVI interface blocks L2 traffic from vPC Peer-link.
CSCvi62638	The storm control feature does not affect on the Cisco Nexus 7.x releases.
CSCvr13118	If either the show tech-support all or show tech-support details is running on the same switch at the same time, the show tech-support <*component*> may not collect data

Large core files are split into 3 or more files. For example:

- 1405964207_0x101_iftmc_log.3679.tar.gzaa
- 1405964207_0x101_iftmc_log.3679.tar.gzab
- 1405964207_0x101_iftmc_log.3679.tar.gzac

To decode the multiple core files, first club the files to a single file:
$ cat 1405964207_0x101_iftmc_log.3679.tar.gz* > 1405964207_0x101_iftmc_log.3679.tar.gz

Device Hardware

The following tables list the Cisco Nexus 3000 Series hardware that Cisco NX-OS Release 7.0(3)I7(9) supports. For additional information about the supported hardware, see the Hardware Installation Guide for your Cisco Nexus 3000 Series devices.

Table 8: Cisco Nexus 3000 and 3100 Series Switches

Product ID	Description
N3K-C3048TP-1GE	Cisco Nexus 3048 switch
N3K-C3064PQ	Cisco Nexus 3064 switch
N3K-C3064PQ-10GE	Cisco Nexus 3064-E switch
N3K-C3064PQ-10GX	Cisco Nexus 3064-X switch
N3K-C3064TQ-10GT	Cisco Nexus 3064-TQ switch
N3K-C31108PC-V	Cisco Nexus 31108PC-V switch
N3K-C31108TC-V	Cisco Nexus 31108TC-V
N3K-C31128PQ-10GE	Nexus 31128PQ, 96 x 10 Gb-SFP+, 8 x 10-Gb QSFP+, 2-RU switch.
N3K-C3132C-Z	Cisco Nexus 3132C-Z switch
N3K-C3132Q-40GE	Cisco Nexus 3132Q switch
N3K-C3132Q-40GX	Cisco Nexus 3132Q-X switch
N3K-C3132Q-V	Cisco Nexus 3132Q-V switch
N3K-C3132Q-XL	Cisco Nexus C3132Q-XL switch
N3K-C3164Q-40GE	Cisco Nexus 3164Q, 64 x 40-Gb SFP+, 2-RU switch
N3K-C3172PQ-10GE	Cisco Nexus 3172PQ switch
N3K-C3172PQ-XL	Cisco Nexus C3172PQ-XL switch
N3K-C3172TQ-10GT	Cisco Nexus 3172TQ switch
N3K-C3172TQ-XL	Cisco Nexus C3172TQ-XL switch

Table 9: Cisco Nexus 3000 and 3100 Series Fans, Fan Trays and Power Supplies

Product ID	Description
N2200-PAC-400W	Cisco Nexus 2000 or Nexus 3000 400W AC power supply, forward airflow (port side exhaust)
N2200-PAC-400W-B	Cisco Nexus 2000 or 3000 400W AC power supply with reverse airflow (port-side intake).
N2200-PDC-400W	Cisco Nexus 2000 or Nexus 3000 400W DC power supply, forward airflow (port side exhaust)
N3K-C3048-FAN	Cisco Nexus 3048 fan module with forward airflow (port-side exhaust)
N3K-C3048-FAN-B	Cisco Nexus 3048 fan module with reverse airflow (port-side intake)
N3K-C3064-X-BA-L3	Cisco Nexus 3064-X reversed airflow (port-side intake) AC power supply

Product ID	Description
N3K-C3064-X-BD-L3	Cisco Nexus 3064-X forward airflow (port-side intake) DC power supply
N3K-C3064-X-FA-L3	Cisco Nexus 3064-X forward airflow (port-side exhaust) AC power supply
N3K-C3064-X-FD-L3	Cisco Nexus 3064-X forward airflow (port-side exhaust) DC power supply
N3K-PDC-350W-B	Cisco Nexus 2000 DC power supply with reverse airflow (port-side intake)
N3K-PDC-350W-B	Cisco Nexus 2000 or Nexus 3000 350W DC power supply, reversed airflow (port side intake)
NXA-FAN-30CFM-B	Cisco Nexus 2000 or Nexus 3000 individual fan, reversed airflow (port side intake)
NXA-FAN-30CFM-F	Cisco Nexus 2000 or Nexus 3000 individual fan, forward airflow (port side exhaust
NXA-PAC-500W	Cisco Nexus 3064-T 500W forward airflow (port-side exhaust) AC power supply
NXA-PAC-500W-B	Cisco Nexus 3064-T 500W reverse airflow (port-side intake) AC power supply

Table 10: Cisco Nexus 3200 Series Switches

Product ID	Description
C1-N3K-C3232C	Cisco Nexus 3232C switch.
N3K-C3264C-E	Cisco Nexus 3264C-E switch.
N3K-C3264Q	Cisco Nexus 3264Q switch.

Table 11: Cisco Nexus 3500 Series Switches

Product ID	Description
N3K-C3524P-10G	Cisco Nexus 3524 switch
N3K-C3524P-10GX	Cisco Nexus 3524 switch, 24 SFP+
N3K-C3524P-XL	Cisco Nexus 3524-XL switch
N3K-C3548P-10G	Cisco Nexus 3548 switch
N3K-C3548P-10GX	Cisco Nexus 3548x switch, 48 SFP+
N3K-C3548P-XL	Cisco Nexus 3548-XL switch

Table 12: Cisco Nexus 3500 Series Fans, Fan Trays and Power Supplies

Product ID	Description
N2200-PAC-400W	Cisco Nexus 2000 or Nexus 3000 400W AC power supply, forward airflow (port side exhaust)
N2200-PAC-400W-B	Cisco Nexus 2000 or Nexus 3000 400W AC power supply, reversed airflow (port side intake)
N2200-PDC-400W	Cisco Nexus 2000 or Nexus 3000 400W DC power supply, forward airflow (port side exhaust)
N3K-PDC-350W-B	Cisco Nexus 2000 or Nexus 3000 350W DC power supply, reversed airflow (port side intake)
NXA-FAN-30CFM-B	Cisco Nexus 2000 or Nexus 3000 individual fan, reversed airflow (port side intake)
NXA-FAN-30CFM-F	Cisco Nexus 2000 or Nexus 3000 individual fan, forward airflow (port side exhaust

Upgrade and Downgrade

Upgrading Cisco Nexus 3000 and 3100 Series Switches

To perform a software upgrade for Cisco Nexus 3000 and 3100 Series switches that run in N3K mode, follow the instructions in the Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x.

To perform a software upgrade for Cisco Nexus 3100 Series switches that run in N9K mode, follow the instructions in the Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x.

The upgrade process is triggered when you enter the install all command. This section describes the sequence of events that occur when you upgrade a single Cisco Nexus 3000 Series switch.

Note:

- If you have a release prior to Release 7.0(3)I2(1), upgrade to Cisco Nexus 3000 Release 6.0.2.U6(3a) first and then upgrade to Release 7.0(3)I2(1) or later releases.

Beginning with the 7.0(3)I2(1) release, kickstart and system images are no longer used to install the Cisco NX-OS software image on Cisco Nexus 3000 and 3100 Series switches. Instead, a single binary image is used (for example, nxos.7.0.3.I4.1.bin). To install the software, you would use the install all nxos bootflash:nxos.7.0.3.I4.1.bin command.

- Upgrade Path to Cisco NX-OS Release 7.0(3)I7(9)
- Upgrade Guidelines and Limitations

Upgrade Path to Cisco NX-OS Release 7.0(3)I7(9)

For the list of platforms and releases that support a non-disruptive In-Service Software Upgrade (ISSU) to Cisco NX-OS Release 7.0(3)I7(9), see the Cisco NX-OS ISSU Support Matrix.

The following disruptive upgrade paths are supported:

- For Cisco Nexus 3048 Switches:

  Cisco NX-OS Release 6.0(2)U5(1) > Cisco NX-OS Release 6.0(2)U6(10) > Cisco NX-OS Release 7.0(3)I7(9)

- For All Cisco Nexus 3000 Series switches (except Cisco Nexus 3048 Switches):

  Cisco NX-OS Release 6.0(2)U5(1) > Cisco NX-OS Release 6.0(2)U6(10) > Cisco NX-OS Release 7.0(3)I7(9)

Note: Starting with Cisco NX-OS Release 7.0(3)I7(5) Release, the fast reboot feature is not supported on Cisco Nexus 3000 and 3132 switches. It will be supported only for an upgrade to the next maintenance releases

The following table shows the upgrade paths for Cisco NX-OS Release 7.0(3)I7(9) from Cisco NX-OS Release 6.0(2)U5(1) and later.

Table 13: Upgrade Paths

From	To	Limitations	Recommended Procedure
7.0(3)I2(1) or later	7.0(3)I7(9)	None	install all is the recommended upgrade method supported.
6.0(2)U6(3a)[1] and later	7.0(3)I7(9)	None	install all is the only upgrade method supported because of a BIOS upgrade requirement. Warning: Make sure that you store the pre-Release, 6.0(2)U6(3)'s configuration file. For more information, see the *Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x*.

[1] *Cisco NX-OS Release 6.0(2)U6(3) is no longer available for a software download through www.cisco.com. This software release has been replaced by Cisco NX-OS Release 6.0(2)U6(3a).*

6.0(2)U6(2a)[2] or earlier	7.0(3)I7(9)	First, upgrade to Cisco NX-OS Release 6.0(2)U6(3a) or a later release. *A Cisco Nexus 3048 switch requires an additional step when you upgrade from a software version older than Cisco NX-OS 6.0(2)U6(2), otherwise the switch can fail to boot. You must first upgrade the switch to Cisco NX-OS Release 6.0(2)U6(2a), then to Cisco NX-OS Release 6.0(2)U6(3a), and finally to Cisco NX-OS Release 7.0(3)I7(9).*	install all is the only upgrade method supported because of a BIOS upgrade requirement. For more information, see the *Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide, Release 7.x*.

Upgrade Guidelines and Limitations

Follow these guidelines and limitations while upgrading to Cisco NX-OS Release 7.0(3)I7(9):

- Cisco Nexus 3048, 3064, 3132 (except for the N3K-C3132Q-V), and 3172 platform switches with a model number that does not end in -XL must run a "compact" NX-OS software image due to limited bootflash space. This "compact" image can be created using the NX-OS Compact Image procedure; alternatively, a compact NX-OS software image can be downloaded directly from Cisco's Software Download website. This requirement does not apply to any other model of Cisco Nexus 3000 or 3100 series switch. This requirement does not apply to the Nexus 3132Q-V switch.
- The MD5/SHA512 checksum published on Cisco's Software Download website for a compact NX-OS software image may not match the MD5/SHA512 checksum of a compact image created through the NX-OS Compact Image procedure.
- The only supported method of upgrading is install all from Release 6.0(2)U6(3a) or later due to the need to upgrade the BIOS. Without the Release 7.0(3)I7(9) BIOS, the 7.0(3)I7(9) image will not load.

[2] *Cisco NX-OS Release 6.0(2)U6(2) is no longer available for a software download through www.cisco.com. This software release has been replaced by Cisco NX-OS Release 6.0(2)U6(2a).*

- The no-save option is now required to downgrade from Release 7.x to Release 6.x. The bios-force is a hidden option that is only available on Cisco Nexus 3000 Series switches that are running 7.x releases.
- Cisco Nexus 3000 Series switches that use software versions older than Cisco NX-OS Release 5.0(3)U5(1) need to be updated to Cisco NX-OS Release 5.0(3)U5(1) before they are upgraded to Cisco NX-OS Release 6.0(2).
- Cisco NX-OS Release 5.0(3)U3(1) does not support a software upgrade from Cisco NX-OS Release 5.0(3)U2(2c). If you want to upgrade through this path, see CSCty75328 for details about how to work around this issue.

  Note: It is recommended that you upgrade to Cisco NX-OS Release 7.0(3)I7(9) by using Cisco NX-OS install procedures.
- In Cisco NX-OS Release 6.0(2)U2(2), the default interface name in LLDP MIB is in short form. To make it long form, you must set lldp portid-subtype to 1. In Cisco NX-OS Release 6.0(2)U2(3), this behavior was reversed. The default interface name in LLDP MIB is now in long form. To make it short form, you must set lldp portid-subtype to 0.
- If you have set lldp port-subtype to 1 and you are upgrading to Cisco NX-OS Release 6.0(2)U2(4), ensure that you set lldp port-subtype to 0.
- While performing a non-disruptive ISSU, VRRP and VRRPV3 will display the following messages:
  - If VRRPV3 is enabled:
    2015 Dec 29 20:41:44 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: Service "vrrpv3" has sent the following message: Feature vrrpv3 is configured. User can change vrrpv3 timers to 120 seconds or fine tune these timers based on upgrade time on all Vrrp Peers to avoid Vrrp State transitions. – sysmgr
  - If VRRP is enabled:
    2015 Dec 29 20:45:10 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: Service "vrrp-eng" has sent the following message: Feature vrrp is configured. User can change vrrp timers to 120 seconds or fine tune these timers based on upgrade time on all Vrrp Peers to avoid Vrrp State transitions. – sysmgr
- Packet loss may occur on Cisco Nexus 31108PC-V, 31108TC-V and 3132Q-V switches when they are in the default cut-through switching-mode and the default oversubscribed port mode. These packet losses are seen in hardware counters on the egress port as TERR and/or TFCS. One of the following workarounds can be implemented to address this issue without NX-OS upgrade. To view more details, see CSCvf87120.
- Change the port mode from oversubscribed to line-rate and then reload the switch:
  - On Nexus 31108PC-V and 31108TC-V switches, change from 48x10g+6x100g to 48x10g+4x100g+2x40g.
  - On Nexus 3132Q-V switches change from 32x40g or 26x40g to 24x40g.
- Change the switching-mode from cut-through to store-and-forward and then reload the switch.
- An error occurs when you try to perform an ISSU if you changed the reserved VLAN without entering the copy running-config save-config and reload commands.
- Subinterfaces cannot be used as network ports.

- Cisco Nexus 3000-XL platforms do not support breakout using speed 10000 CLI command. Use the interface breakout module 1 port <num> map 10g-4x CLI command instead.

- While installing the NXAPI https certificate that is present in the device, the following error message can appear if the user does not have the permission to install this certificate (See CSCup72219): Certificate file read error.Please re-check permissions.

- After configuring the NXAPI feature, the default http port (port 80) is still in the listening state even after we run the no nxapi http command. This results in the sandbox becoming accessible. Although the sandbox becomes accessible, HTTP requests from the sandbox to the device do not go through. Thus, the functionality is not affected. (See CSCup77051).

- Chunking is enabled while displaying XML output for any CLI, and html tags (& lt; and & gt;) are displayed instead of < and > both on the sandbox and while running the Python script (See CSCup84801).

  This is expected behavior. Each chunk should be in XML format for you to parse it and extract everything inside the <body> tag. This is done so that it can be later concatenated with similar output from all the chunks of the CLI XML output. After all the chunks are concatenated to get the complete XML output for the CLI, this complete XML output can be parsed for any parameter.

  The following workaround is recommended to address this issue:
  - Concatenate the <body> outputs from each chunk
  - Replace all the html tags (& lt; and & gt;) with < and >
  - Parse for any XML tag needed
- If you use the write erase command, you cannot view the output for the show startup *feature* command. To view the startup configuration, you must then use the show startup-config command. This limitation will remain until you run the copy running-config startup-config command. After that, the show startup-config feature command will display the feature-only configuration output as expected (See CSCuq15638).

- A Python traceback is seen while running the show xml command by using the Python shell. The exception type is httplib.IncompleteRead. This happens when you use Python scripts to leverage the NXAPI for retrieving switch data through XML or JSON. You should handle the exceptions in your Python scripts (See CSCuq19257).

- While upgrading to a new release, when you create a checkpoint without running the setup script, the checkpoint file does not contain the copp-s-mpls class. After you run the write erase command and reload the switch, the copp-s-mpls class is created when the default configuration is applied. When a rollback is done to this checkpoint file, it detects a change in the CoPP policy and tries to delete all class-maps. Because you cannot delete static class-maps, this operation fails and, in turn, the rollback also fails.

  This can also happen if you create a checkpoint, then create a new user-defined class and insert the new class before any other existing class (See CSCup56505).

  The following workarounds are recommended to address this issue:
  - Run setup after upgrading to a new release.
  - Always insert the new classes at the end before a rollback.

- When both the ip icmp-errors source and ip source *intf* icmp error commands are configured, then the command that is configured last takes effect.

  Thereafter, if the last configured command is removed, the switch does not get configured with the command that was configured first.

- Users who upgrade to 7.0(3)I7(9) need to run the set up script if they want to enable the MPLS static or the VRRpv3 feature.
- The following Cisco Nexus 9000 features are not supported on the Cisco Nexus 3100 Series switches in N3K or N9K mode:
  - FEX
  - Multicast PIM Bidir
  - Port VLAN (PV) switching and routing support for VXLAN
  - Auto-Config
  - Secure login enhancements:
    - Ability to block login attempts and enforce a quiet period
    - Ability to restrict the maximum login sessions per user
    - Ability to restrict the password length
    - Ability to prompt the user to enter a password after entering the username
    - Ability to hide the shared secret used for RADIUS or TACACS+ authentication or accounting
    - SHA256 hashing support for encrypted passwords
  - SHA256 algorithm to verify operating system integrity
  - Non-hierarchical routing mode
  - NX-API REST
- Link Level Flow Control (LLFC) is not supported on Cisco Nexus 3000 series and Cisco Nexus 3100 series switches.
- You can disable IGMP snooping either globally or for a specific VLAN.

You cannot disable IGMP snooping on a PIM enabled SVIs. The warning message displayed is: IGMP snooping cannot be disabled on a PIM enabled SVIs. There are one or more VLANs with PIM enabled

Upgrading Cisco Nexus 3500 Series Switches

Upgrade Path to Cisco NX-OS Release 7.0(3)I7(9)

Install All is the only option that supports upgrade and downgrade between releases. The following upgrade paths are supported:

- Cisco NX-OS Release 6.0(2)A8(7b) and later > Cisco NX-OS Release 7.0(3)I7(9)
- Cisco NX-OS Release 7.0(3)I7(2) and later > Cisco NX-OS Release 7.0(3)I7(9)

Upgrade Guidelines and Limitations

The following limitations are applicable when you upgrade from Releases 7.0(3)I7(2) or later to the NX-OS Release 7.0(3)I7(9):

- If a custom CoPP policy is applied after upgrading to Cisco NX-OS Release 7.0(3)I7(2) or later, and if the Nexus 3548 switch is downgraded to Cisco NX-OS Release 5.0, where changes to the CoPP policy are not permitted, the custom CoPP policy is retained and cannot be modified.
- copy r s and reload is not a supported method for an upgrade.
- You must run the setup script after you upgrade to Cisco NX-OS Release 7.0(3)I7(9).
- Cisco Nexus 3548 and 3548-X platform switches must run a “compact” NX-OS software image due to limited bootflash space. This “compact” image can be created using the NX-OS Compact Image procedure; alternatively, a compact NX-OS software image can be downloaded directly from Cisco's Software Download website. This requirement does not apply to the Cisco Nexus 3548-XL switch.
- The MD5/SHA512 checksum published on Cisco's Software Download website for a compact NX-OS software image may not match the MD5/SHA512 checksum of a compact image created through the NX-OS Compact Image procedure.

MIB Support

The Cisco Management Information Base (MIB) list includes Cisco proprietary MIBs and many other Internet Engineering Task Force (IETF) standard MIBs. These standard MIBs are defined in Requests for Comments (RFCs). To find specific MIB information, you must examine the Cisco proprietary MIB structure and related IETF-standard MIBs supported by the Cisco Nexus 3000 Series switch. The MIB Support List is available at the following FTP sites:

ftp://ftp.cisco.com/pub/mibs/supportlists/nexus3000/Nexus3000MIBSupportList.html

Exceptions

The following features are not supported for the Cisco Nexus 3232C and 3264Q switches:

- 3264Q and 3232C platforms do not support the PXE boot of the NX-OS image from the loader.
- Automatic negotiation support for 25-Gb and 50-Gb ports on the Cisco Nexus 3232C switch.
- Cisco Nexus 2000 Series Fabric Extenders (FEX)
- Cisco NX-OS to ACI conversion (The Cisco Nexus 3232C and 3264Q switches operate only in Cisco NX-OS mode.)
- DCBXP
- Designated router delay
- DHCP subnet broadcast is not supported
- Due to a Poodle vulnerability, SSLv3 is no longer supported
- FCoE NPV
- Intelligent Traffic Director (ITD)

- Enhanced ISSU. NOTE: Check the appropriate guide to determine which platforms support Enhanced ISSU.
- MLD
- NetFlow
- PIM6
- Policy-based routing (PBR)
- Port loopback tests
- Resilient hashing
- SPAN on CPU as destination
- Virtual port channel (vPC) peering between Cisco Nexus 3232C or 3264Q switches and Cisco Nexus 9300 platform switches or between Cisco Nexus 3232C or 3264Q switches and Cisco Nexus 3100 Series switches
- VXLAN IGMP snooping

Supported Optics

To determine which transceivers and cables are supported by Cisco Nexus 3000 Series switches, see the Transceiver Module (TMG) Compatibility Matrix.

To see the transceiver specifications and installation information, see https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-installation-guides-list.html.

Related Content

Cisco Nexus 3000 Series documentation: Cisco Nexus 3000 Series switch documentation

Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference: Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference

Licensing information:

Cisco NX-OS Licensing Guide

Cisco Nexus 9000 and 3000 Series NX-OS Switch License Navigator

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus3k-docfeedback@cisco.com. We appreciate your feedback.

Legal Information