



**Hewlett Packard
Enterprise**

**Onyx for HPE M-Series Ethernet Switch Release Notes
v3.10.4408 (LTS)**

Part Number: 882262-001

Published: Feb/15/2024

Edition: 1

Notices

© Copyright 2019-2024 Hewlett Packard Enterprise Development LP

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Mellanox®, Mellanox logo, ConnectX®, Mellanox Spectrum®, MLNX-OS®, SwitchX®, Virtual Protocol Interconnect®, are registered trademarks of Mellanox Technologies, Ltd. Mellanox Onyx is a trademark of Mellanox Technologies, Ltd.

All other trademarks are property of their respective owners.

For the most updated list of Mellanox trademarks, visit <http://www.mellanox.com/page/trademarks>

Table of Contents


1	Release Notes Update History	6
2	Overview	7
3	Switch General Support	8
3.1	Supported Switch Systems	8
3.1.1	End of Onyx Feature Development	8
3.1.2	Interoperable Switch Systems Supported by NVIDIA	8
3.2	Tested and Supported Firmware Versions	9
3.3	Software/Firmware Interoperability	9
3.4	Supported BIOS Version	9
3.5	Supported Software Licenses	9
3.6	Upgrade From Previous Releases	9
3.7	Supported Port Speeds	11
3.7.1	Spectrum-3 Supported Port Speeds	11
3.7.2	Spectrum-2 Supported Port Speeds	13
3.7.3	Spectrum Supported Port Speeds	14
3.8	Supported Scale	14
4	Changes and New Features	16
4.1	Customer Affecting Changes	16
5	Bug Fixes in This Version	17
6	Known Issues	18
6.1	General Known Issues	18
6.2	Ethernet Known Issues	21
6.3	IP Routing Issues	34
7	Changes and New Features History	40
7.1	Customer Affecting Changes History	49
8	Bug Fixes History	58
9	Support and Other Resources	66
9.1	Accessing Hewlett Packard Enterprise Support	66
9.1.1	Information to Collect	66
9.2	Accessing Updates	66
9.3	Customer Self Repair	66
9.4	Remote Support	67
9.4.1	Remote Support and Proactive Care Information	67
9.4.2	Proactive Care Customer Information	67
9.5	Warranty Information	67
9.5.1	Additional warranty information	67

9.6 Regulatory Information 68

9.6.1 Additional Regulatory Information 68

9.7 Documentation Feedback 68

9.8 Websites 68

 This is a long-term support (LTS) release. LTS is the practice of maintaining a software product for an extended period of time (up to three years) to help increase product stability. LTS releases include bug fixes and security patches.

1 Release Notes Update History

Version	Date	Description
3.10.4408	February 15, 2024	Initial release of this Release Notes version. This version introduces Bug Fixes in This Version .

2 Overview

This document is the Release Notes for switch software, a comprehensive management software solution that provides optimal performance for cluster computing, enterprise data centers, and cloud computing over various switch IC families.

The fabric management capabilities ensure the highest fabric performance while the chassis management ensures the longest switch up time.

The documentation package includes the following documents:

- User Manual which provides general information about the scope, organization, and command line interface, as well as basic configuration examples.
- Release Notes which provide information on the supported platforms, changes and new features, and reports on software known issues as well as bug fixes.

The NVIDIA Community also offers useful end-to-end and special How To guides at: <https://enterprise-support.nvidia.com/s/>.

3 Switch General Support

3.1 Supported Switch Systems

3.1.1 End of Onyx Feature Development

As of February 2023, long-term support (LTS) releases of this product will be provided. Long-term support (LTS) is the practice of maintaining a product for an extended period, typically three years, to help increase products' stability. LTS releases include updates that address bugs fixes and security patches.

Model Number	Description
SN4700	HPE SN4700M 400GbE 32QSFP-DD switch
SN4600cM	HPE SN4600cM 100GbE 64QSFP28 switch
SN3700M	HPE SN3700M 200GbE 32QSFP28 switch
SN3700cM	HPE SN3700cM 100GbE 32QSFP28 switch
SN2100M	HPE SN2100M 100GbE 16QSFP28 half width switch
SN2010M	HPE SN2010M 25GbE 18SFP+ 4QSFP28 switch
SN2410bM	HPE SN2410bM 10GbE 48SFP+ 8QSFP28 switch
SN2410M	HPE SN2410M 25GbE 48SFP28 8QSFP28 switch
SN2700M	HPE SN2700M 100GbE 32QSFP28 switch

3.1.2 Interoperable Switch Systems Supported by NVIDIA

Model Number	Description
SN2010	NVIDIA Spectrum 18-SFP port and 4-QSFP28 port 100GbE 1U Ethernet switch
SN2100	NVIDIA Spectrum 16-port QSFP28 100GbE 1U Ethernet switch
SN2410	NVIDIA Spectrum 8-Port QSFP28 100GbE 48-port SFP28 25GbE 1U Ethernet dual core switch
SN2700	NVIDIA Spectrum 32-port QSFP28 100GbE 1U Ethernet switch
SN3700	NVIDIA Spectrum-2 32-Port QSFP56 200GbE Ethernet switch

Model Number	Description
SN3700C	NVIDIA Spectrum-2 32-Port QSFP28 100GbE Ethernet switch
SN4600C	NVIDIA Spectrum-3 64-port QSFP28 100GbE 2U Ethernet Switch
SN4700	NVIDIA Spectrum-3 400GbE, 1U Open Ethernet switch, 32xQSFP-DD ports

3.2 Tested and Supported Firmware Versions

- Spectrum-3 firmware version 30.2010.4416
- Spectrum-2 firmware version 29.2010.4416
- Spectrum firmware version 13.2010.4416

3.3 Software/Firmware Interoperability


- ConnectX-4 Lx firmware version 14.32.1010
- ConnectX-5 firmware 16.35.2000
- ConnectX-6 firmware 20.35.2000
- ConnectX-7 firmware 28.35.2000
- BlueField®-2 firmware version 24.35.2000
- NVIDIA NEO™ version 2.7.1
- ONIE version 5.3.0008

3.4 Supported BIOS Version

- x86 ATOM 5.6.5—0ACIF007_02.02.x02

3.5 Supported Software Licenses

For the software licenses supported with Onyx software please refer to the “Licenses” section of the “Getting Started” chapter of the User Manual.

 When installing an HP license in the following format:
 aaaa bbbb cccc yyyy zzzz “Switch nx###GE upgrade SW License”
 The system will report the following error:
 “Malformed License: aaaa bbbb cccc ... yyyy”.
 To avoid this issue, please insert the license without the quoted description and make sure the date set on your system matches the date embedded in the supplied HP license.

3.6 Upgrade From Previous Releases

Older versions of the software may require upgrading to one or more intermediate versions prior to upgrading to the latest. Missing an intermediate step may lead to errors. Please refer to table below to identify the correct upgrade order.

Table 1: Supported Software Upgrades

Target Version	Verified Versions From Which to Upgrade
3.10.4xxx	3.10.3xxx, 3.10.2xxx
3.10.3xxx	3.10.2xxx, 3.10.1xxx
3.10.2xxx	3.10.1xxx, 3.10.0xxx, 3.9.3xxx
3.10.1xxx	3.10.0xxx, 3.9.3xxx, 3.9.2xxx
3.9.3xxx	3.9.2xxx, 3.9.1xxx
3.9.2xxx	3.9.1xxx, 3.9.0xxx
3.9.1xxx	3.9.0xxx, 3.8.2xxx
3.9.0xxx	3.8.2xxx, 3.8.1xxx
3.8.2xxx	3.8.1xxx, 3.7.1xxx
3.8.1xxx	3.8.1xxx, 3.7.1xxx
3.7.1xxx	3.7.0xxx, 3.6.8xxx, 3.6.6xxx
3.6.8xxx	3.6.6xxx, 3.6.5xxx
3.6.6xxx	3.6.5xxx, 3.6.4xxx
3.6.5xxx	3.6.4xxx, 3.6.3xxx
3.6.4xxx	3.6.3xxx, 3.6.2xxx
3.6.3xxx	3.6.2xxx, 3.6.1xxx
3.6.2xxx	3.6.1xxx, 3.5.1xxx
3.6.1xxx	3.5.1xxx, 3.5.0xxx, 3.4.3xxx
3.5.1xxx	3.5.0xxx, 3.4.3xxx
3.5.0xxx	3.4.3xxx, 3.4.2xxx
3.4.3xxx	3.4.2xxx, 3.4.1xxx

Target Version	Verified Versions From Which to Upgrade
3.4.2xxx	3.4.1xxx,3.4.0xxx
3.4.1xxx	3.4.0xxx, 3.3.5006
3.4.0xxx	3.3.5006

For upgrade instructions, refer to the section “Upgrading Operating System Software” in the User Manual.

3.7 Supported Port Speeds

- When configuring force mode, configure the same Speed and FEC on both sides.
- In Spectrum-2 and above, the link between the Local and Peer ports must be raised only in the same mode (i.e., Force ↔ Force or Auto-Negotiation ↔ Auto-Negotiation modes)

3.7.1 Spectrum-3 Supported Port Speeds

- When DR4 is connected between 2 400G_R8 switches, split is not supported, only 400G_R8.

Table 2: SN4700 Supported Port Speeds

Speed [GbE]	AutoNeg	Force			Cable / Modules	Cable Length [m]
		RS FEC	FC FEC	NO FEC		
50G PAM4*: 400 (split to 8) 200 (split to 4) 100 (split to 2) 50 (no split)	✓	✓	✗	✗	Optics	Up to 50
					Copper	Up to 2.5
50G PAM4*: 200 (split to 4) 100 (split to 2) 50 (no split)	✓	✓	✗	✗	Optics	Up to 100
					Copper	Up to 2.5
100 (NRZ)	✓	✓	✗	✓	Optic	Up to 100
					Copper	Up to 5
25/50 (NRZ)	✓	✓	✓	✓	Optic	Up to 100
					Copper	Up to 5

Speed [GbE]	AutoNeg	Force			Cable / Modules	Cable Length [m]
		RS FEC	FC FEC	NO FEC		
10/40	✓	✗	✗	✓	Optic	Up to 100
					Copper	Up to 5
1	✓	✗	✗	✓	Optic/Copper	Up to 5

*PAM4 is the system's default.

When Connecting NVIDIA-to-NVIDIA in PAM4, Auto-Neg should always be enabled.

Table 3: SN4600C Supported Port Speeds

Speed [GbE]	AutoNeg	Force			Cable / Modules	Cable Length [m]
		RS FEC	FC FEC	NO FEC		
50G PAM4*: 200 (split to 4) 100 (split to 2) 50 (no split)	✓	✓	✗	✗	Optic	Up to 100
					Copper	Up to 2.5
100 (NRZ)	✓	✓	✗	✓	Optic	Up to 100
					Copper	Up to 3
25/50 (NRZ)	✓	✓	✓	✓	Optic	Up to 100
					Copper	Up to 5
10/40	✓	✗	✗	✓	Optic	Up to 100
					Copper	Up to 5
1	✓	✗	✗	✓	Optic/Copper	Up to 5

3.7.2 Spectrum-2 Supported Port Speeds

Table 4: SN3700/SN3700C/SN3420 Supported Port Speeds

Speed [GbE]	AutoNeg	Force			Cable/ Modules	Cable Length [m]
		RS FEC	FC FEC	NO FEC		
50G PAM4*: 200 (split to 4) 100 (split to 2) 50 (no split)	✓	✓	✗	✗	Optic	Up to 30
					Active Optic Module	Up to 100
					Copper	Up to 2.5
100 (NRZ)	✓	✓	✗	✓	Optic	Up to 100
					Active Optic Module	Up to 80km
					Copper	Up to 5**
25/50 (NRZ)	✓	✓	✓	✓	Optic	Up to 100
					Active Optic Module	Up to 10km
					Copper	Up to 5**
10/40	✓	✗	✗	✓	Optic	Up to 100
					Active Optic Module	Up to 10km
					Copper	Up to 5**
1	✓	✗	✗	✓	Optic	Up to 100
					Copper	Up to 5**

*PAM4 is only supported on SN3700 system and is the system's default

**On SN3420 system, copper cables are supported up to 3m

When Connecting NVIDIA-to-NVIDIA in PAM4, Auto-Neg should always be enabled


3.7.3 Spectrum Supported Port Speeds

Speed [GbE]	AutoNeg	Force			Cable/ Modules	Cable Length [m]
		RS FEC	FC FEC	NO FEC		
100	✓	✓	✗	✓	Optic	Up to 100
					Active Optic Module	Up to 80km
					Copper	Up to 5
25/50	✓	✓	✓	✓	Optic	Up to 100
					Active Optic Module	Up to 10km
					Copper	Up to 5
10/40	✓	✗	✓	✓	Optic	Up to 100
					Active Optic Module	Up to 80km
					Copper	Up to 5
1	✓	✗	✗	✓	Optic	Up to 100
					Copper	Up to 5

3.8 Supported Scale

Category	Spectrum	Spectrum-2 and Spectrum-3
IPv4 (UC)	100K	100K
IPv6 short prefix (UC)	50K	50K
IPv6 long prefix (UC)	50K	20K
MAC (FDB)	100K	100K
ACL (18B key)	5K	5K
ACL (36B key)	5K	5K

Category	Spectrum	Spectrum-2 and Spectrum-3
ACL (54B key)	4K	4K
Host Routes IPv4 (local)	100K	100K
Host Routes IPv6 short prefix (local)	50K	50K
Host Routes IPv6 long prefix (local)	50K	50K
RIF	999	999
IPv4 (UC)	100K	100K
IPv6 short prefix (UC)	50K	50K
IPv6 long prefix (UC)	50K	20K
MAC (FDB)	100K	100K
ACL (18B key)	5K	5K
ACL (36B key)	5K	5K
ACL (54B key)	4K	4K
Host Routes IPv4 (local)	100K	100K
Host Routes IPv6 short prefix (local)	50K	50K
Host Routes IPv6 long prefix (local)	50K	50K
RIF	999	999

 To reach the maximal numbers, use each category separately.

4 Changes and New Features

Category	Description
General	Bug fixes

4.1 Customer Affecting Changes

There are no new Customer Affecting Changes in this version. For a list of Customer Affecting Changes from previous versions, see [Customer Affecting Changes History](#) section.


5 Bug Fixes in This Version

The following table lists the bug fixes in this software release. For bug fixes from previous versions, see [Bug Fixes History](#) section.

Internal Ref.	Category	Description
3.10.4408		
3748676	Third-Party Modules	Some third-party modules are causing false-alarmed interrupts during SERDES tuning, which overload the ASIC and causing delay in its response.
3737801	CLI Interface	Running the "show interface status" CLI command may result in an error when the interface description contains special characters.
3.10.4404		
3527932	VLAN	After removing the VLAN interface using the IPL configuration and rebooting the switch, errors are seen in the log.
3571204	LACP	When combining LACP fast rate and LACP slow rate on different devices, the LACP link flapping occurs.
3510518	Cables	Tx bias current shows N/A on some cables.
3700976	LDAP	Fixed the "group-attribute/group-dn" LDAP configurations. If the "group-dn" is set, a user must be a member of this group or the user will not be authorized to log in as the membership of group is set by the group-attribute.
3565862	IGMP	IGMP snooping sends Source and Group Specific queries as a response to the received IGMPv3 Current-State-Record Membership report.

6 Known Issues

The following sections describe Onyx® known issues in this software release and possible workarounds.

 For hardware issues, refer to the switch support product page.

6.1 General Known Issues

Internal Ref.	Category	Description	Workaround
366005	CLI	Command output filtering does not support the commands "show log", "show ib sm log", and "show configuration text files <file>".	N/A
806900	Cables	40GbE passive copper cable of 5m length might experience link rise issues when connected to some 3rd party 40GbE interfaces.	Replace copper cable with fiber cable.
806878	Chassis Management	Duplicate notification is sent upon high temperature alerts, both specific module alerts and general "too high" alerts.	N/A
2137269	Configuration Management	Merging two binary configuration files using the command "configuration merge" is not supported.	Use "configuration text file apply" instead.
806802	Configuration Management	Binary configuration files saved from releases older than 3.6.1000 cannot be fetched to the switch and fail with a decryption error. It is recommended to create a new copy of the bin configuration file after upgrade in case configuration backup is needed.	Save configurations as text files before upgrading to this version.
806791	Configuration Management	Applying a configuration file of one system profile to another is not supported from one system type to another.	N/A

Internal Ref.	Category	Description	Workaround
1298137	Docker	If two docker images are installed, both from same distribution and both chosen as “latest”, the command “show docker images” may display image name and image version as “none”.	Delete older latest image or download while specifying a version.
3115850	Force Mode, FEC, Speed	When configuring force mode, configure the same speed and FEC on both sides.	
1966186	JSON	Sending JSON commands that exceed 50K lines, the JSON job gets stuck in the background or gets timed out.	Divide the 50K lines into multiple JSON requests.
1796691	JSON	The command "show whoami" is not supported through JSON HTTP request.	Run the command through the CLI.
1085293	Linux Dockers, Configuration Management	When running “configuration text apply” (with “docker no shutdown”), a container that is configured as init, may run immediately (instead of waiting for next boot).	Run the init configuration from the CLI session.
777720	Logging	The warning “[pm.WARNING]: snapshots and sysdumps are on separate partitions; space constraints not thoroughly enforced on sysdumps” may appear if operating with an encrypted file system. This warning can be safely ignored.	N/A
2615903	Management Interface, Docker	It is not possible to call a container name "ns" and it is not possible to create a username called “ns”.	Call the container and/or username by a name other than "ns".
806744	Management Interfaces	Switch systems may have an expired HTTPS certification.	Generate a new certificate by changing the hostname.
807310	Modules	When using 5m splitter cable (P/N MC2609125-005), wrong data is displayed under transceiver information.	N/A

Internal Ref.	Category	Description	Workaround
806875	SNMP	Request timeout should be set to at least 20 seconds since initial table calculation requires time.	N/A
806874	SNMP	The tables dot1dTpFdbTable and dot1qTpFdbTable support up to 10,000 entries.	N/A
806899	System Management	If a faulty cable is used, rise time of other interfaces in the system may be delayed.	N/A
957353	Telemetry	Splitting a port with telemetry configuration makes telemetry non-functional and may cause errors in log.	Telemetry histograms may be applied after a port is split (unsplitting may only be done if no telemetry configuration is present).
3464879	Upgrade	Upgrading LTS version to last GA version does not work well.	N/A
2066713	Upgrade/Downgrade	Downgrading back to 3.8.2204 after upgrading to 3.8.2306 will save configuration modifications from 3.8.2306.	N/A
3064354	Username	A new username cannot be called "*".	Set username as something other than "*".
1434387	WebUI	Interactive CLI commands cannot be executed via WebUI.	N/A
806834	WebUI	The following commands cannot be executed from "Execute CLI commands" section on WebUI. – interface ethernet <interface> module-type – dcb priority-flow-control enable	Run these commands through the CLI instead.
806832	WebUI	Enabling/disabling HTTPS while connected via HTTP to the WebUI may result in temporary loss of connection to the webpage.	Refresh the page or navigate back using the browser's back button.
806829	WebUI	Reversing the time clock can result in WebUI graphs' corrupted data.	Clear the graphs data after setting the clock.

Internal Ref.	Category	Description	Workaround
461989	WebUI	Importing a configuration text file with commands that only get enabled after running other commands is not possible through the WebUI. For example: the command “mlag-vip” is only available after running “protocol mlag”.	Import the configuration text file through the CLI.

6.2 Ethernet Known Issues

Internal Ref.	Category	Description	Workaround
807348	802.1x	PAE may send unneeded EAP-START messages when authentication starts.	N/A
2173600	ACL	The Maximum supported ACL scale numbers are 5k for mac-acl, 5k for ipv4-acl, and 4k for ipv6-acl. Using existing configurations with a higher scale, will prevent login via SSH.	N/A
2103960	ACL	Configuring 6k ACL role on the switch leads to out-of-memory errors when performing ‘reset-factory’ action, during which the switch is inaccessible.	N/A
2335472	ACL, CLI	Execution of "show running-config" right after deleting large number of ACLs may cause CLI to become unavailable.	Wait a few minutes between ACL deletion and "show running-config" execution.
1289271	ACLs	A single ACL table is limited to up to 2K rules.	N/A
807307	ACLs	Packets dropped by the switch due to congestion or ACL rules are added to the bad type counter of the matching VLAN interface.	N/A

Internal Ref.	Category	Description	Workaround
2298500	BGP	When there are multiple BGP IPv4 or IPv6 sessions in different VRFs running on switches and the sessions have overlapped IPv4 or IPv6 peer addresses, only one password will be taken if different passwords are configured. That is, only one of the sessions will be negotiated with its correct password; the others may not reach the established state.	If there are multiple BGP sessions in multiple VRFs with overlapped IPv4 or IPv6 peer addresses, use the same password or do not use a password for the sessions.
2284442	CRC	Replacing CRC field with timestamp is currently not supported on Spectrum-based systems.	N/A
1933579	Cables	100GbE optical cables may not raise a link against ConnectX-5 devices after many link toggles.	N/A
2873125	Cables, FEC, Force Mode	When connecting a Spectrum-2 or Spectrum-3 systems that is Force mode and in FC FEC and connecting it to a Spectrum system, the link will not rise.	Set auto-negotiation protocol and/or do not override FEC with FC.
807345	DCBX	DCBX auto-select type (IEEE/CEE) is not supported.	DCBX type should be selected manually.
807344	DCBX	When moving from DCBX CEE to DCBX IEEE, TLVs may be sent improperly.	After mode change, the TLVs to be sent must be reset.
807342	DCBX	Enabling LLDP triggers a faulty notation of PFC oper-state. This status may be ignored.	N/A
807304	ECN	Configuration of minimum-absolute value smaller than 3K might cause constant ECN tagging.	N/A
2300727	EVPN Centralized Gateway	EVPN Centralized Gateway is not supported on Spectrum-based A0 systems. Use "show inventory" command to see ASIC revision.	N/A

Internal Ref.	Category	Description	Workaround
2256231	EVPN, IPv6 Neighbor	When Neighbor Suppression (NS) is enabled, all incoming IPv6 NS packets are handled by the switch and are not transmitted via the Tunnel. Even though these packets are not entering the Tunnel, they are still counted as encapsulated on the tunnel and will be shown when using "show interface NVE" or specific vni counters.	N/A
2255178	EVPN, IPv6 Neighbor suppression	When Neighbor Suppression (NS) is enabled, all incoming IPv6 NS packets are handled by the switch and are not transmitted via the Tunnel. Even though these packets are not entering the Tunnel, they are still counted as encapsulated on the tunnel and will be shown when using "show interface NVE" or specific vni counters.	N/A
2284676	Ethernet Interface	Not all discarded packets are visible in "show interface ethernet 1/17 counters" command.	N/A
806743	Ethernet Interfaces	The "no" negation prefix is not supported prefix in the CLI commands "interface ethernet <s/p> ipv4 port access-group nodhcprelay".	Use the "no" keyword as an infix (e.g., "interface port-channel <num> no switchport").
2722500	Firmware Crash	If the firmware crashes and the NOS continues to send commands, the firmware dump will not take place and there will be no debug information available.	N/A
1167153	HLL	Changing the HLL duration configuration while the port is in stall state takes effect after a few seconds of random delay. The next time stall state is entered, it may take a little less time (next HLL) or up to 60 seconds.	No action is needed because once it exits stall state, expected system behavior resumes.
1602721	Historical Statistics	JSON output for the command "show stats sample interface-port-channel data max-samples" supports up to 800 max-samples.	N/A

Internal Ref.	Category	Description	Workaround
1572264	IGMP Snooping	Fast leave always works on v3 reports even when “fast-leave” is disabled.	N/A
807291	IGMP Snooping	IGMP snooping is limited to a single MC IP per MC MAC.	N/A
807282	IGMP Snooping	If the IP address of the IGMP querier is not specified explicitly and no IP address is configured on the VLAN interface, the default IGMP querier address is 0.0.0.0.	Configure IGMP querier IP address explicitly or setup an IP address on the required VLAN.
807280	IGMP Snooping	There is no possibility to have more than one MRouter port on a single VLAN if IGMP snooping is disabled for that VLAN.	After enabling IGMP snooping on that VLAN, the user needs to re-add the MRouter ports on that VLAN.
2246698	IGMP Snooping, VXLAN	IGMP Snooping over VXLAN is not supported on Spectrum-based A0 systems. Use “show inventory” command to see ASIC revision.	N/A
2176230	IGMP snooping, MSTP, STP	IGMP Snooping does not work on a VLAN which is added to an MSTP instance if STP is disabled and is then changed to MSTP mode.	Run the "spanning-tree" command via the CLI in config mode.
1891323	LAG	Spanning tree configuration performed on a LAG is not retained by ports when they are removed from the LAG. Adding back ports to a LAG that has spanning tree configuration will fail due to mismatch.	Configure the same values on the port before insertion to the LAG.
1239514	LLDP	The command “show lldp statistics” displays incremented “TLVs Unrecognized” inaccurately.	N/A
807303	LLDP	LLDP ifIndexes do not match the ones published in the ifTable in IEEE 802.1.	Use the ifDescr and fields.

Internal Ref.	Category	Description	Workaround
2116921	MLAG	During manual reconfiguration MLAG Port-channel (disabling and then enabling ports in the MLAG port-channel), small traffic loss may be observed.	N/A
1838571	MLAG	MLAG does not work when configuring IPL with IPv6 address.	Work with IPv4 source address.
1590944	MLAG	Redundant links between the MLAG peers do not converge properly.	Remove the redundant links between peers (just like a standard configuration of an MLAG cluster) to only enable the IPL between peers.
982276	MLAG	Changing MLAG port configuration on master MLAG switch (higher IP over the IPL) before software upgrade is finished might cause traffic flood (BC and MC).	N/A
806932	MLAG	Changing STP mode affects traffic and may cause MLAG to stop working for an interval of 21 seconds until the new STP topology is built.	User should disable MLAG prior to changing the STP mode.
669345	MLAG	Fast LACP cannot be used on the link partner when working with over 40 MLAG port-channels and over 650 VLANs.	Cannot use fast LACP on the link partner when working with over 40 MLAG port-channels and over 650 VLANs.
1917838	MLAG EVPN	In specific cases, traffic loss occurs on MLAG peers when using MLAG EVPN configuration.	When using MLAG EVPN configuration, enable boot delay of 240 on each on the MPO member ports on both MLAG peers in order to eliminate traffic loss upon reload.
2204896	MLAG, EVPN	IPL flapping on MLAG cluster (Which also has EVPN configuration) while traffic is running may lead to a situation where the Slave switch has one or more non-ageable entries in FDB that do not appear on the master switch.	Perform "clear mac-address-table dynamic" to clean out all dynamic entries from FDB table and re-learn.

Internal Ref.	Category	Description	Workaround
1969656	MLAG, STP	Spanning tree domains do not converge correctly on the rare occasion that an MLAG peer running MSTP is connected to a different region and needs to act as a border switch for no MPOs ports.	Disable the relevant ports before adding VLANs to MST instances.
2485435	Modules	When using DR4 modules with an old firmware version below 18.0.0, some links get stuck.	When using DR4 modules, use firmware above version 18.0.0.
2244527	Monitor Session	Monitor session commands entered in rapid succession (i.e., pasting a script at once), may cause errors.	Allow one second or more between monitor session commands.
2116433	Monitor Session	Changing the port type from local analyzer to remote analyzer or regular port (not a monitor session destination) deletes some user configuration such as admin state and speed.	Reapply the deleted configuration after the port type change.
2306849	OpenFlow	When setting flows with the same match keys, only the last flow will be considered. If the last flow is deleted, other flows configured with the same match key will also be deleted.	N/A
2287799	OpenFlow	When clearing the maximum number of flows added by the controller, the switch may get stuck.	Reboot the switch.
2256140	OpenFlow	"no protocol openflow" fails if all supported tables are used.	Use no more than 40 tables for OpenFlow.
936880	OpenFlow 1.3	Using "TRAP" in FDB floods the packets to all ports.	N/A

Internal Ref.	Category	Description	Workaround
2467778	OpenFlow, MLAG	Forwarding control traffic from one MPO interface to another one is currently not supported. It may lead to the scenario when LACP packets will be delivered on the wrong destination port when the OpenFlow rule which forwards traffic from one MPO interface to another one is installed.	Use a separate OpenFlow rule with a higher priority and destination MAC for the LACP packets in order to forward such packets in the proper direction. Example: openflow add-flows 1 table=0, priority=200, dl_dst=01:80:c2:00:00:02, actions=NORMAL openflow add-flows 1 table=0, priority=100, in_port=Mpo1, actions=output:Mpo2
2455767	OpenFlow, MLAG, Group SELECT	There is no possibility to add LAG (MPO) into group SELECT (FG LAG).	Do not add LAG/MLAG into OpenFlow group SELECT.
2125230	OpenFlow, OVS	Configuring an OVS server port which is already in use, causes errors in the log.	Change OVS server port configuration to an unused port.
2265107	OpenFlow, OvS	The count of rules is based on the key size. Minimum key size is 18 on Spectrum and 9 on Spectrum-2 and Spectrum-3. The algorithm always uses 18 as a minimum key size, therefore on Spectrum-2 and Spectrum-3 systems, the maximum number of rules will not match the real value for a 1 small key.	N/A
2345563	PAM4, Auto-Negotiation	When connecting a NVIDIA-to-NVIDIA in PAM4, auto-negotiation should always be enabled.	N/A
2366241	PTP	On very rare occasion, link down when PTP is enabled may lead to the following error message in the log: "[ptp4l.ERR]: [.....] port 1 []: bad message". This error can be safely ignored.	N/A
2336394	PTP	On occasion, when disabling protocol PTP the following error message may appear in the log: "[phc2sys.ERR]: [...] poll failed". This error can be safely ignored.	N/A

Internal Ref.	Category	Description	Workaround
2829515	PTP, OpenFlow	When PTP is configured on a switchport which is also in OpenFlow hybrid mode, PTP stops working.	Configure a DROP rule for PTP packets intended to be terminated on the switch for all switchports in OpenFlow hybrid mode. PTP will still receive the packet with the even with the DROP rule.
2306061	PTP, Port Channel	Adding L2 interface to port channel after PTP was enabled for this L2 interface will lead to fault on PTP.	Enable PTP on L2 interface only after adding the L2 interface to port channel.
807325	Port Mirroring	When port mirroring congestion is configured to “drop-excessive-frames” (best effort), while using the same analyzer port for more than a single mirroring session, that port could drops packets from all flows not according to their configured priorities.	N/A
838743	QinQ	QinQ is not supported over VXLAN.	N/A
2876506	RIF MTU Configuration	When IP tunnels, VxLAN tunnels, or MPLS RIF is configured to reach optimal end-to-end latency, the RIF MTU sizes of all RIFs should accommodate a max non-encapsulated supported packet size with possible max encapsulation. IP tunnels—48 byte VxLAN tunnel—56 byte MPLS—24 byte	
2691958	Resource Manager	On Spectrum devices, when a minimum reservation is made for the IPv6 UC route resource type, the reservation is made only for short IPv6 prefixes. There is no reservation guarantee for long prefix types. On Spectrum-2 devices and above, the reservation is done assuming that all IPv6 UC routes are long routes.	Do not use a reservation for IPv6 UC routes.

Internal Ref.	Category	Description	Workaround
807314	SNMP	LLDP MIB OID lldpRemPortDesc is not supported.	N/A
2133817	SNMP, VTEP Certification	On power cycle, part of the hardware gateway test from the VTEP certification test suit, the system appears up, but does not respond to SNMP uptime requests.	N/A
1511230	Spanning Tree	Setting spanning tree port type to “network” (interfaces ethernet <if> spanning-tree port type network) does not work.	N/A
1509251	Spanning Tree	Moving from one STP mode to another while the system is functional may lead to error in the log which can be ignore.	N/A
807264	Spanning Tree	BPDU's are sent from both the superior and the inferior switches.	N/A
1447052	Spanning Tree, RPVST	RPVST is not interoperable with RPVST+ on Cisco's Nexus system when using TAG VLAN.	N/A
2934873	Spectrum, Cables, Link Up	On a rare occasion, when using 5m copper cables, the link up time may take up to 9 seconds.	N/A
2545727	Spectrum, FDB MAC, CRC	FDB MACs are learned even if packets have CRC Errors and/or are dropped by the CRC.	
2952790	Spectrum, Force Mode, Link Up	When setting link to quick link up with force mode, link up time may take longer than 5 seconds.	N/A
2934867	Spectrum, Optical Cables, Link Up	On rare occasions, when quick link up is required, link up time on optical media can be higher than 5 seconds.	
2848664	Spectrum, SN2700, Optical Modules	When connecting Spectrum systems with FTLX1471D3BCL or MMA2L20-AR Optical modules and performing PMAOS on all ports link might not raise.	Toggle the port.

Internal Ref.	Category	Description	Workaround
2403400	Spectrum, Spectrum-2, Loopback	At times, after disabling loopback mode, there is no link-up.	N/A
2750456	Spectrum-2, CRC Timestamp	CRC Timestamp for mirror packets is only FRC (Free Running Counter) and not UTC. When an outgoing packet is a mirror packet (meaning an analyzer port is used), the hardware does not modify the timestamp from FRC to UTC.	There is no workaround, but ACL can be used instead of mirroring.
1834738	Spectrum-2, Cables, Speed	At 200GbE speed, traffic drop occurs between SN3700 and IXIA K400.	N/A
1726900	Spectrum-2, Cables, Speed	Currently, raising the link at 10GbE link speed is not supported when using 200GbE optical cables.	N/A
1778526	Spectrum-2, EVPN	Tunnel encapsulated counters is not increased when ARP packets are forwarded to tunnel.	N/A
2395745	Spectrum-2, Modules, COLORZ	COLORZ module link up time increased to 85 seconds.	N/A
2502625	Spectrum-2, PFC	On Spectrum-3 systems, slow reaction time to Rx pause packets on 40GbE ports may lead to buffer overflow on servers.	N/A
2781548	Spectrum-2, Port Split/ Unsplit, Traffic	Due to a hardware limitation in Spectrum-2 switch systems, when splitting/unsplitting the ports, traffic might drop on the other port members on the same 8x group in case of FWS traffic.	N/A
2214897	Spectrum-2, SN3420, Cables	SN3420 system supports copper cables up to 3m in length.	N/A
2284447	Spectrum-2, SN3700, Cables, Speeds, Testing, Ixia	Testing SN3700 200GbE with Ixia AresONE requires additional steps. Contact our technical support for specific settings.	N/A

Internal Ref.	Category	Description	Workaround
2235645	Spectrum-2, SN3700, Port Split	On SN3700 and SN3700C systems, when splitting ports, the following error may appear: "[issd.ERR]: getIssindexFromIindex can't find in port_indexes_ht the entry for ifindex 134238448" This error can be safely ignored.	N/A
2137424	Spectrum-2, SN3700C	On SN3700C systems, the maximum allowed power class for QSFP ports is 4.5W for ports 1-2 and 21-31 and 3.5W for all other ports.	N/A
2053350	Spectrum-2, SN3800, Link	In SN3800 system, when the link goes down on the remote side, the "link down counter" increases by two.	N/A
3129617	Spectrum-2, Spectrum-3, PTP	On SN3700C and SN4600C, using PTP at 100GbE caused inaccuracies. As a result, PTP accuracy is improved by the calibration test.	
2284444	Spectrum-3	The following capabilities are currently not supported on Spectrum-3-based systems: -MPLS -Auto-Negotiation Link Training in PAM4	N/A
2137445	Spectrum-3, Boot	In Spectrum-3 devices, boot can take up to 75 seconds.	N/A
2589614	Spectrum-3, Cables	On rare occasion, reading original Cisco cables may produce an information mismatch, causing log of unexpected speed.	
2284449	Spectrum-3, Cables, Speeds, Testing, Ixia, SN4700	Testing SN4700 200GbE and 400GbE with Ixia AresONE requires additional settings. Contact our technical support for specific settings.	N/A

Internal Ref.	Category	Description	Workaround
2413409	Spectrum-3, DAC	BER may be experienced when using 5m DAC cables between SN4700 and SN2700 in 100GbE speed.	N/A
2699968	Spectrum-3, DR1, Boot	When connecting a Spectrum-3 device using DR1 (MMS1V70-CM) modules, the boot time can take up to 75 seconds.	N/A
2272238	Spectrum-3, Link	Connecting DR4 to DR1 using 100GbE may cause link flap.	N/A
2175541	Spectrum-3, MTU, 400GbE	When using 400GbE speed in Spectrum-3 systems, xon value should be less than 2 MTUs.	N/A
1469002	Spectrum-3, Port Mirroring	For egress mirroring on a 400GbE port the monitor session congestion mode should be set to "drop-excessive-frames" as the "pause-excessive-frames" mode does not work in this case.	N/A
2231118	Spectrum-3, Port Toggle	On rare occasion, when connecting DR4 to Spectrum-3 systems on both sides, toggling from both sides may cause the link to not rise.	N/A
2316849	Spectrum-3, Reboot	On Spectrum-3 devices, when rebooting the switch manually, on rare occasions, "show reboot cause" displays incorrect reboot reason.	N/A
2752473	Spectrum-3, SN4600C, Cables	When using SN4600C with Base-T cable (OPN MC3208411-T) using 1GbE speed, errors on traffic may be observed.	
2245426	Spectrum-3, SN4600C, Cables	In the SN4600C system, the link does not rise when using LUX42604CO module at 40GbE after toggle.	N/A
2137437	Spectrum-3, SN4700	Active Copper Cable does not raise link on SN4700.	N/A

Internal Ref.	Category	Description	Workaround
2329924	Spectrum-3, SN4700, Link, 400GbE	When connecting SN4700 with Cisco 3432C using 400GbE with copper DAC cables, link does not rise in the corner port when using auto-negotiation.	Use force mode on the ports.
2697324	Spectrum-3, SN4700, NRZ, Splitter Copper Cables	When connecting SN4700 to SN4700 back to back in 50GbE NRZ with splitter copper cable, Fast link up is not operational.	N/A
2729276	Spectrum-3, SN4700, PSU	Insertion of power supply to SN4700 or plugging-in power to secondary PSU may cause traffic disruption of few milliseconds.	To avoid interim packet loss, connect PSU in the maintenance window.
2368615	Spectrum-3, Split	On Spectrum-3 systems, links are not stable on split interfaces that were split using qsfpsplit-4 or qsfpsplit-2 command.	N/A
2284453	Speeds, Cables, Testing, Spirent	Default configuration of "Spirent dX3 400G" may result in errors. Contact our technical support if interested in testing with Spirent.	N/A
2284452	Speeds, Cables, Testing, Spirent	Using "Spirent dX3 400G" to test SN3700 systems while using PAM4 may, on some occasions, result in traffic loss.	N/A
2259364	Traffic, Port	While there is traffic to a port, when either running "no shutdown" or reloading a port that has incoming traffic, the counters of the discard packets will be counted for 3 seconds.	N/A
2284445	Unsupported Protocols	The following are currently unsupported: -SSH server -TCACAS	N/A

Internal Ref.	Category	Description	Workaround
2245329	WJH	WJH "t trap_probability" is the probability to extract a packet from the stream of packets that were dropped by HW. If the packet drop rate is low (small number of packets) then WJH events are not triggered.	N/A
2293954	sFlow	There is an invalid agent-ip in first exported sFlow packet. All other packets are sent properly.	N/A
807331	sFlow	Errors are seen when defining sFlow session from two WebUI or CLI sessions simultaneously.	N/A
807329	sFlow	Discard counters are not reported to the collector.	N/A
807328	sFlow	The discarded packets counter in sFlow samples may not be accurate and may expose a skew of one second.	N/A

6.3 IP Routing Issues

Internal Ref.	Category	Description	Workaround
1399010	BFD	User cannot clear BFD counters.	N/A
1114699	BFD	A BFD session is not signaled as removed on a static route which is set to admin down.	N/A
1267569	BGP	If there are multiple IP addresses configured on an IP interface, when update-resource is configured on a peer group, there is no guarantee that the primary IP address gets used as the source IP address to establish peer relationship.	Do not use "peer-group", enable "update-source" per individual peer.
1021951	BGP	IGP metric does not influence route selection where routes are learned from different IGP.	N/A

Internal Ref.	Category	Description	Workaround
953776	BGP	A peer does not inherit the update-source parameter from its group configuration.	Run “shutdown” then “no shutdown” on the peer.
807464	BGP	The command “no neighbor <ip-address> local-as” is not functional.	Delete the neighbor with “no neighbor {<ip-address>} remote-as” and restore the neighbor without the command “neighbor local-as”.
807461	BGP	When running both BGP and OSPF, changing the configuration of the command “router bgp <AS> <external distance> <internal distance> <local distance>” requires running “clear ip bgp all” afterwards.	N/A
807459	BGP	AS-path request/set are limited to 128. When more are received, TCP FIN is sent and connection to the peer is lost.	N/A
807458	BGP	The command “bgp aggregate-address summary-only” does not silence aggregate-route re-advertisements.	N/A
807457	BGP	Using the command “clear ip bgp <ip> soft in” mandates enabling route-fresh on the peer.	If route-refresh is not supported on the peer device, use the command “clear ip bgp <ip> in” instead.
807456	BGP	Aggregate overlapping is not supported.	N/A
807455	BGP	Route aggregation configuration cannot be modified.	Delete route aggregation and create a new configuration.
2089263	BGP Unnumbered	When 1 VRF loopback interface alias is set, it will copy addresses from the target loopback, which is a duplicated address. The following warning log will appear: Jan 8 13:38:46 mtbc-onyx-01-2410 snmpd8543: [snmpd.WARNING]: Duplicate IPv4 address detected, some interfaces may not be visible in IP-MIB	N/A

Internal Ref.	Category	Description	Workaround
2065498	BGP Unnumbered	When there are parallel multiple BGP unnumbered sessions running between two Onyx switches, only one password will be taken if different passwords are configured. That is, only one of the sessions will be negotiated with its correct password, the others may not reach the established state. The limitation also applies to sessions belonging to one or more peer groups with passwords.	Use the same password on parallel multiple BGP unnumbered sessions.
2121257	BGP, IPv6 Routing	When enabling or disabling IPv6 routing, BGP sessions of the related VRF will be restarted.	N/A
2262991	Bidirectional PIM	The switch forwards all multicast traffic for a group even though only a particular source is requested via IGMPv3. The "show ip mroute" command will show that only a particular source was requested.	N/A
2337361	Bidirectional PIM, Load Balance	Changing Load Balance mode from LB to Non-LB will not clear the routes that are no longer required. Those routes will remain as long as there is traffic on those routes.	Use "clear ip mroute" command to clear the desired routes or stop traffic before changing load balance mode.
807373	Counters	In IP Routing mode, multicast or broadcast packets (such as ARP) may be counted as "RX discard" in case only one interface is a member of the VLAN. Such packets reach the CPU for processing. The progressing counter can be ignored.	N/A
1070613	DHCP	DHCP-client is not functional.	Use static IP instead.
2170574	EVPN Central Gateway	<ul style="list-style-type: none"> • In Spectrum systems, packets that come from ports (IPL in our example) that are isolated from VXLAN tunnel are discarded and COUNTED as ENCAPSULATED • In Spectrum-2 and up, packets that come from ports (IPL...) that are isolated from VXLAN tunnel are discarded and NOT COUNTED as ENCAPSULATED 	N/A

Internal Ref.	Category	Description	Workaround
984275	IGMP Querier	Running the command “show ip igmp groups” does not print “source” and “expires” parameters in its output.	N/A
2166167	IGMP Snooping, CLI	When there is 10k STATIC groups exist, "show ip igmp snooping groups" may take up to 80 seconds.	N/A
2137488	IP Routing	When TFTP source IP is enabled, ICMP redirects are not sent.	N/A
2137483	IP Routing	IPv4 link local addresses (169.254.0.0/16) are not supported. Addresses should be changed before upgrade, if not changed, they will be removed from the interface.	N/A
1472151	IP Routing	It is required for neighbor entries on an IP interface to be fewer than 25K.	N/A
807349	Interfaces	ICMP echo packets are not counted as part of the VLAN interface counters.	ICMP packets are counted in the interface L2 counters.
807366	LLDP	A port connected to a router-port receives from it an LLDP packet containing IPv4 and IPv6 management addresses. However, the IPv6 address is not included in the LLDP MIB as a remote management address. Only the IPv4 remote management address is published.	N/A
2137378	Multicast	Multicast packets sent over VLAN with enabled EVPN/VNI and IGMP snooping at the same time are not sent over VXLAN network and are only sent to local receivers.	Disable either EVPN/VNI or IGMP snooping for that VLAN.
2284454	Multicast, VLAN, IGMP	In Spectrum-based systems, multicast packets sent over VLAN with enabled EVPN/VNI and IGMP snooping are flooded to all VTEPs and flooded to VLAN after VxLAN decap to all VLAN members.	N/A

Internal Ref.	Category	Description	Workaround
807393	OSPF	Reverse packet filtering is not supported. When misconfigured, traffic may pass on an unintended subnet.	N/A
807386	OSPF	Removing a static ID using the command “no router-id” requires at list one VLAN interface to be configured.	N/A
2382385	PIM	In the rare cases where more than 100 PIM neighbors are learned, some PIM "show" commands (e.g., "show ip pim neighbors") may take approximately 40 seconds.	N/A
1756541	PIM	PIM-SM MRoute is not created when incoming multicast data traffic is not mapped to RP, or when RP is not reachable.	N/A
1703693	PIM	In PIM-SM, the non-DR router displays interfaces with received IGMP reports under “outgoing interface list”. Traffic is forwarded from DR router.	N/A
1512261	PIM	Next-hop multi-path: Multicast traffic continues being forwarded for 2-3 minutes after deleting PIM configuration from an interface which is part of port distribution.	N/A
1266347	PIM	When a static IP route is configured after an IP MRoute (with the same prefix), the static route has higher priority.	Configure static MRoute after configuring static route.
1182847	PIM	MRoute entries learned via PIM remains when the interface is shut down until the timer expires.	N/A
807364	Router Port	A trunk port which is configured as router port does not receive traffic to the host interface.	Configure the port to access mode (CLI command “switchport mode access”) before making it a router port.

Internal Ref.	Category	Description	Workaround
807361	Router Port	Setting 802.1Q mode on a router port does not function properly.	N/A
807359	Router Port	ICMP redirect is not supported over router port.	N/A
2563357	SNMP, IGMP Snooping	Configuring a large scale of IGMP snooping configuration (i.e., enabling IGMP snooping on a large number of VLANs), leads to SNMP query timeout when querying igmpInterfaceTable.	The default timeout between retries for 'snmpcmd' is 1 second. Increase the SNMP query timeout to fetch igmpInterfaceTable for big-scale configuration.
2321421	SNMP, MIB, IGMP Snooping	SNMP static multicast MIB dot1qStaticMulticastAddress is not supported.	N/A
2635933	Subnet	There is no routing between primary IP subnet to secondary IP subnet on the same RIF.	Send GARP from the host, to enable traffic to pass.
807468	VRF	Any VRF can be monitored with sFlow, but a collector can be on the management VRF only.	N/A
807399	VRRP	Using the same Virtual IP (VIP) as the VLAN interface is not supported.	N/A

7 Changes and New Features History

Category	Description
3.10.4202	
General	Bug fixes
3.10.4100	
General	Bug fixes
3.10.4006	
10GBASE-T Transceiver	Added support for 10GBASE-T SFP copper transceiver (Methode DM7053).
SN3700, Module	On SN3700 system, added support for 200GbE AOC VPI module MFS1S00-HxxxV.
SN4600C, DR1 Transceiver	On SN4600C system, added support for DR1 transceiver.
SN4700, Transceiver	On SN4700 system, added support for 400GbE LR4 optical transceiver.
General	Bug fixes
3.10.3100	
Cables, QSFP-DD	Added support for split to 8 on QSFP-DD for PAM4 rates on Spectrum-3 systems.
General	Bug fixes
3.10.3004	
System management	Enabled IP Filter feature by default and applied default firewall rules. If any of the rules is changed (delete/modify/moved), the full rule list for this chain will appear in the "show running-config" command. To review the default firewall rules refer to section the "Control Plane Policing (CoPP)" in the user manual.

TX Timestamp	Added support for the following parameters to be saved after reset: -pi_proportional_const, pi_integral_const -fault_reset_interval -tx_timestamp_timeout
General	Bug fixes
3.10.2202	
LDAP Nested Groups	Added support for authenticating from LDAP Nested Group. For more information, see LDAP. For more information, see "User Management and Security Commands" section in the user manual.
PTP Global Counters	Added support for new PTP global counters. For more information, see "PTP Commands" section in the user manual.
Cables	Added support for KS-100GAOC-DQ-10 (Hisense and WTD) 100G DQ AOC cable on Spectrum-3 systems when connecting to ConnectX-6 systems.
Modules	Added support for ColorZ modules on SN4700 and SN4600C systems.
Modules, DR4	Added support for Finisar DR4 (FTCD4523E2PCM) on Spectrum-2 and Spectrum-3 systems.
Systems SN4600C	Added support for SN4600C A1 Spectrum-2 systems.
General	Bug fixes
3.9.3302	
WebUI	Rebranding WebUI to NVIDIA design.
General	Bug fixes
3.9.3202	
System Dump	System dump (related CLI command is "debug generate dump") was extended with interface link diagnostic information.
ACL	Added support for new mirroring action in ACL. For more information see "monitor session" command and the "ACL" section in the user manual.

Gratuitous ARP (GARP)	<p>Added GA-level support for gratuitous ARP in EVPN on IPv4, also when ARP Suppression is enabled.</p> <p>The feature allows generating GARP packets on the egress VTEP only when neighbor-suppression is enabled on both VTEPs in the chain (ingress and egress).</p> <p>Added GA-level support for Unsolicited Neighbor Advertisement in EVPN on IPv6, also when Neighbor Suppression is enabled.</p> <p>The feature allows forwarding the Unsolicited NA packets through the tunnel despite the Neighbor Suppression.</p> <p>The suppression should be enabled on interface NVE or on a particular VLAN of the VTEP.</p>
Learning Unsolicited Neighbors	<p>Added support for learning unsolicited neighbors per interface. For more information see "Management Interface Commands" in the user manual.</p>
PTP	<p>Added beta-level support for PTP on Spectrum-3 systems.</p>
SN3700, Module	<p>Added support for new module MMS1W50-HM (2km transceiver FR4) for 200GbE.</p>
SN4600C, Fastboot	<p>Added beta-level support for Fastboot in NRZ on SN4600C system.</p>
Systems, SN4700	<p>Added support for Spectrum-3-based SN4700 system.</p>
OSS Compliance	<p>Added support for uploading the Open Source Licenses files. For more information see "file open-source-licenses upload" command in the "Configuration Management Commands" section of the user manual.</p>
Security, IPsec	<p>Updated IPsec to improve security and added support for IKEv2 and new ciphers. For more information, see "crypto ipsec peer local" command in Cryptographic (X.509, IPsec) and Encryption section of the user manual.</p>
3.9.3124	
General	<p>Bug fixes</p>
3.9.2500	
Gratuitous ARP (GARP)	<p>The feature allows forwarding the Unsolicited NA packets through the tunnel despite the Neighbour Suppression.</p> <p>Added GA-level support for gratuitous ARP in EVPN on IPv4, also when ARP Suppression is enabled.</p> <p>The feature allows generating GARP packets on the egress VTEP only when neighbor-suppression is enabled on both VTEPs in the chain (ingress and egress).</p> <p>Added GA-level support for Unsolicited Neighbor Advertisement in EVPN on IPv6, also when Neighbour Suppression is enabled.</p> <p>The suppression should be enabled on interface NVE or on a particular VLAN of the VTEP.</p>

General	Bug fixes
3.9.2400	
Gratuitous ARP (GARP)	Added beta-level support for gratuitous ARP in EVPN on IPv4, also when ARP Suppression is enabled. The feature allows generating GARP packets on the egress VTEP only when neighbor-suppression is enabled on both VTEPs in the chain (ingress and egress). The suppression should be enabled on interface NVE or on a particular VLAN of the VTEP.
MLAG	Added support for MLAG interface in OpenFlow. For more information, see "Support of MLAG Interface in OpenFlow" section and "openflow mode hybrid" command in the user manual.
Cables	Added support for cable MMS1W50-HM 2km NVIDIA transceiver, IB HDR, up to 200Gb/s, QSFP56, MPO, 1310nm, FR4 on MQM8700-HS2R.
3.9.2302	
PTP	Added possibility to ignore the management messages on the port in a forced master mode in order to improve the security and avoid storm which can cause the management messages
SN3420, Cables and Modules	Added support for Finisar 1G 10km module (FTLF1318P3BTL) on SN3420 system.
SN3420, Cables and Modules	Added support for Finisar 1GBase-T 1G 100m module (FCLF8522P2BTL) on SN3420 system.
SN3700, Cables and Modules	Added support for 200GBASE-SR4 QSFP56 module (R5Z83A) in SN3700 system.
SN3700, SN4700, Cables and Modules	Added support for the following HDR OPNs on SN3700, SN4700 systems at rates of 200GbE: MCP1650-HxxxEyy (copper cable up to 2m) MCP7H50-HxxxRyy (copper splitter cable up to 2m) MMA1T00-HS (transceiver) MFS1S00-HxxxE (AOC) MFS1S50-HxxxE (AOC splitter cable)
SN4600C, Ports	Added support for up to 5W on ports 49 to 64 on SN4600C system.
General	Bug fixes
3.9.2110	
Systems	Added GA-level support for SN4700 A0 system.

IGMP Snooping	Added support for IGMP snooping report profile filtering and max-group limit. For more information, see "IGMP Snooping Commands" and "Debugging" sections in the user manual.
General	Bug fixes
3.9.2006	
CRC	Added beta-level support for replacing CRC field with PTP timestamp on Spectrum-2 and Spectrum-3 systems. For more information see "System Synchronization" section in the user manual.
Deprecation	In the next GA release, version 3.9.3114, the commands "ip l3", "no ip l3" and "no ip l3 force" will be deprecated. Upon system upgrade, "ip l3" mode will be enabled automatically.
Management VRF	Added support for Management VRF. For more information, see "Management Interfaces" section in the user manual.
Modules	Added support for 40GbE SWDM4 modules on SN2700 system.
Modules	Added support for 100GbE CWDM4 transceiver MMA1L30-CM.
OpenFlow	Added ability to add router ports into OpenFlow bridge.
Password	Added support for password hardening. For more information see "Getting Started" section in the user manual.
PBR	Added support for Policy Based Routing (PBR). For more information, see "IP Routing Overview" and "General IP Routing Commands" section in the user manual.
PIM BiDir	Added GA-level support for Bidirectional PIM. For more information, see "IGMP and PIM" section in the user manual.
PTP	Added GA-level support for PTP on Spectrum-2 systems.
PTP	Added beta-level support for PTP on Spectrum-3 systems.
PTP TTL	Added ability to set the TTL value of the PTP messages. For more information, see "PTP Commands" section in the user manual.
Systems	Added support for SwitchIB-2 SB7880 system as an IB Router.
WJH	Added support for WHAT JUST HAPPENED event suppression by the severity for each drop group. For more information, see "Configure What Just Happened (WJH) Using CLI" in the user manual.

WJH SNMP	Added support for WHAT JUST HAPPENED SNMP. For more information, see "Configure What Just Happened (WJH) Using CLI" section in the user manual.
WJH, Buffer	Added Buffer Occupancy filed in WJH buffer event. For more information, see "Configure What Just Happened (WJH) Using CLI" section in the user manual.
3.9.1900	
Bidirectional PIM	Added beta-level support for Bidirectional PIM. For more information see "Multicast" section in the user manual.
General	Bug fixes
PTP	Added beta-level support for PTP on Spectrum-2 systems.
3.9.1604	
Docker Login	Added ability to securely login and logout through the CLI to various server repositories and pull docker images from these servers. See the commands "docker login", "docker logout", and "show docker login" in the Virtualization section of the user manual.
General	Bug fixes
OpenFlow	Added support for using a maximum number of ports per ASIC in an OpenFlow group.
3.9.1304	
EVPN	Added GA-level EVPN centralized gateway functionality.
3.9.1014	
10GBASE-T modules	Added support for 10GBASE-T modules on SN3700 and SN3700C systems.
Counters	Added the ability to use a range of ports in "show interfaces ethernet counters" commands. For more information see the following sections in the user manual: "Ethernet Interfaces Commands," "QoS Commands," "Link Aggregation Group (LAG)," and "MLAG Commands."
CRC	Added support for replacing CRC field with timestamp on Spectrum-2 and Spectrum-3 systems. For more information see "System Synchronozation" section in the user manual.

Ethernet Interfaces	Improved the performance of "show running config" & "show configuration running" commands. When running the above commands for the first time after configuring the switch, the configuration is saved in internal cache and the execution time of these commands will be as in previous releases. Each following execution of these commands will retrieve the running configuration from internal cache and will display the output immediately. In case configuration on switch is changed again, the internal cache will be re-build and the output of these commands will be as in previous releases.
Link, Auto-Negotiation, SN4600C	Added GA-level support for link auto-negotiation on SN4600C systems.
Link, Auto-Negotiation, SN4700	Added beta-level support for link auto-negotiation on SN4700 systems.
PAM4, SN4700	Extended interface speed configuration with additional speeds for PAM4.
Ports, Reset Port	Added support for resetting an interface to its default settings. For information see "default interface ethernet" command under "Ethernet Interface Commands" section in the user manual.
Systems	Added beta-level support for SN4700 system.
Systems	Added GA-level support for SN3700 system.
Systems	Added GA-support for SN3420.
Telemetry, Spectrum-3	Added beta-level support for Telemetry Threshold Spectrum-3 systems.
VRRP	Added support for IPv6 in VRRP and MAGP.
VXLAN, IPv6	Added support for IPv6 Neighbor Suppression. For more information see "nve neigh-suppression" in the VXLAN Commands section of the user manual.
Web UI	Added support for BGP feature in the Web UI.
Web UI	Added support for VRF feature in the Web UI.
3.9.0920	
General	Bug fixes
3.9.0914	
Cables	Enabled KP4RS FEC on Active Fiber cable up to 30m (OPN: MFS1S00-V0xxE).

General	Bug fixes
IP Address	Added command "switchmode exceptions sip-equals-dip" to disable the packet drops for packets with a source IP address that equals to the destination IP address. For more information, see "Configure What Just Happened (WJH) Using CLI" section in the user manual.
Link, Auto-Negotiation	Added GA-level support for link auto-negotiation on Spectrum-2 systems.
Link, Auto-Negotiation	Added ES-level support for link auto-negotiation on Spectrum-3 systems.
MAC	Added support for MAC masking in log messages. For more information, see "Logging" section in the user manual.
SHARP	Added support for legacy SHARP port and performance counters.
SN4700, QSFP-DD	Added split capabilities to QSFP-DD cables on SN4700 system. For more information, see "Ethernet Interfaces" section in the user manual.
UFM	Added support for IPv6 in UFM Agent.
WJH	Added support for WJH auto-export file generation. For more information, see "Logging" section in the user manual.
WJH	Extended WHAT JUST HAPPENED ACL display to show the user ACL rule information of dropped packets. For more information, see "show WHAT JUST HAPPENED" command in the user manual. *Not including ACL rules added using OpenFlow. This will be supported in future releases.
3.9.0612	
General	Bug fixes
3.9.0608	
BGP Unnumbered	Added GA-level support for BGP unnumbered interfaces.
Configuration Management	Added support for automated configuration file backup.
EVPN	Added beta-level EVPN centralized gateway functionality.
General	Bug fixes

QSFP-DD, Cables	Added support for QSFP-DD Ethernet cables.
Recirculation Port	Added GA-level support for port recirculation feature for Spectrum-based systems, which supports display of buffer dropped packets by circulating them into the CPU using a reserved port. For more information see "Ethernet Interfaces" section in the user manual.
SN3420	Added ES-level support for SN3420 system.
SN3700	Added GA-level support for 200GbE NVIDIA↔NVIDIA in Force mode.
SN4600C	Added ES-level support for SN4600C system.
SN4700	Added ES-level support for breakout cables on Spectrum-3 systems.
SN4700	Added ES-level support for 200GbE NVIDIA↔NVIDIA in Force mode.
SN4700	Added ES-level support for 200GbE and 400GbE speeds on SN4700 system with optic and copper cables.
Spectrum-2	Added software GA-level support for DC power supply SN3700 system.
Telemetry, Spectrum-2	Added beta-level support for Telemetry Threshold on Spectrum-2-based systems.
Telemetry, Spectrum-2	Added support for Telemetry Sampling on Spectrum-2-based systems.
WJH	Added support for WJH concurrent operation of raw and aggregated channels on the same level.
WJH	Added support for Forwarding and ACL drop groups in WJH aggregation.
WJH	Added support for WJH Layer-1 raw and aggregation data.
3.9.0450	
Configuration Management	Added support for automated configuration file backup.
3.9.0300	
Cables	Added support for the following OPNs: MMA1L30-CM MMA1T00-HS MCA1J00-H003E/4E MCA7J50-H00XX

DCQCN	Added support for DCQCN Congestion Control.
SHARP	SHARP (SAT) is at GA level. *SAT: Streaming Aggregation Tree
Ports, Speed	Added beta-level support for 200Gb/s NVIDIA↔NVIDIA Force.
Recirculation Port	Added beta-level support for port recirculation feature for Spectrum-based systems, which supports display of buffer dropped packets by circulating them into the CPU using a reserved port. For more information see "Ethernet Interfaces" section in the user manual.
RoCE	Enhanced the "show roce" command to display a list of exceptions from the default profile on RoCE.
Security	SSH Login Notification now displays the following information after authentication: -Last successful and unsuccessful login date/time -Number of unsuccessful logins since last successful login -Changes to user's account since last login (password, capability) -Location of last successful and unsuccessful login (terminal or IP) -Number of total successful logins since last X days
Security	Upgraded OpenSSH version to 8.0p1.
Split	Added ability to CS8500 systems to configure split-ready profile and split ports using CLI.
WJH	Added support for Layer-1 aggregation data.
General	Bug fixes

7.1 Customer Affecting Changes History

Category	Description
3.10.4302	
IPv6 Address, Auto-Configuration	IPv6 address auto config is enabled by default for all management interfaces. The change will be applied for new switches and for switches that upgrade from older OS versions. To disable this, run "no interface mgmt0/1 ipv6 address autoconfig"
PTP (Spectrum-2 / Spectrum-3)	As of this release, when PTP forced-master is set, it allows the interface to block both ingress and egress PTP management messages from/to other PTP peers. In previous releases, only ingress PTP management messages were blocked on the forced-master interface.
Category	Description

3.10.4100	
Deprecation, SNMPv3 Privacy Mode	SNMPv3 privacy mode 3des is no longer supported in secure mode. If secure mode is enabled during image install, SNMPv3 privacy mode 3des will be changed to aes-128 by default.
SSH, RSA/DSA Keys	When generating new SSH host keys in secure mode, only RSA keys will be generated. The generation of DSA keys is no longer supported in secure mode (still available in non-secure mode).
3.10.4006	
Deprecation, Virtual Machine	Virtual Machine is no longer supported. As of this release, the following CLI commands are deprecated and will not be available: -virtual-machine enable -virtual-machine host -virtual-machine vnet -virtual-machine volume -show virtual-machine configured -show virtual-machine host
Authentication	OpenSSL version was upgraded to version 1.1.1g. It is compatible for clients with OpenSSL 1.1.1 and above.
Authentication	Due to OpenSSL upgrade in the latest version, some ciphers have become deprecated and therefore not supported by default. Due to this upgrade, configuring the LDAP to use ssl ciphers may not work. To bypass this, add the following string on customer LDAP server "ldaps:///" to the SLAPD_SERVICES in the LDAP config file.
Deprecation, SSLv3 Ciphers	From version 3.10.4000, the SSLv3 ciphers are deprecated, and will not be supported for any web connection.
Deprecation, Puppet Agent	All Puppet tools are no longer supported. As of this release, the following commands are deprecated and will not be available: -puppet-agent -puppet-agent [vrf <vrf-name>] enable [force] -(config puppet-agent) # master-hostname <hostname> -(config puppet-agent) # enable -(config puppet-agent) # run-interval <time> -(config puppet-agent) # restart -show puppet-agent -show puppet-agent log [[not] [matching continuous] <string> files [[not] matching] <string>]
Chassis Management	SN4600C, SN3700C, SN2700, SN2410 systems, AC/DC voltage sensors were removed and are no longer displayed in the UI.
Authentication	OpenSSL version was upgraded to version 1.1.1g. It is compatible for clients with OpenSSL 1.1.1 and above.

3.10.3004	
Deprecation	As of this software version, the command "show interfaces ethernet transceiver counters details" is deprecated. Use the command "show interfaces ethernet transceiver counters" instead.
Deprecation	All Puppet tools will be deprecated in the next release. For more information, see "Puppet Agent" section in the user manual.
Security	As of 3.10.3004, the IP Filter feature is now enabled by default with a set of given rules. When this configuration is disabled, the "no ip filter enable" command will appear in the running config after the upgrade. After upgrade: In case the feature is enabled, but has different rules than the default, the running config will display the relevant rules that are different than the new default. For more information, see "Control Plane Policing (CoPP)" section in the user manual.
3.10.1000	
Event Logging	The log output of port state change event has changed. Old output: Oct 14 07:51:53 (switch) portd[11477]: Interface IB 1/19 changed state to UP New output: Oct 14 07:51:53 (switch) portd[11477]: [portd.NOTICE]: Interface IB 1/19 changed state to UP
show cpld	Changed output of "show cpld" command. For more information, see "Chassis Management Commands" section in the user manual.
3.9.3220	
Ansible	3.9.3220 is the final version to support Ansible.
3.9.3206	
Virtual Machine	From the next release, 3.10.20xx, Virtual Machine will not be supported. The following CLI commands will not be available: -virtual-machine enable -virtual-machine host -virtual-machine vnet -virtual-machine volume -show virtual-machine configured -show virtual-machine host For more details, see the "Virtual Machine" chapter in the User Manual.
3.9.3202	
Deprecation	As of 3.9.3200 SSH cipher diffie-hellman-group14-sha1 is deprecated and was removed from strict SSH ciphers to non-strict ciphers.

3.9.3124	
Deprecation	As of 3.9.3124, the commands "ip l3", "no ip l3", and "no ip l3 force" are deprecated. Upon system upgrade, "ip l3" mode will be enabled automatically.
MAC	Changed the show command outputs to be lowercase MAC address.
Security, IPsec	<ul style="list-style-type: none"> • crypto ipsec peer <ip> local <ip> keying ike negotiation ikev1/ikev2 Configure if ikev1 or ikev2 will be used. • crypto ipsec peer <ip> local <ip> keying ike auth * Null and hmac-md5 are no longer supported. • crypto ipsec peer <ip> local <ip> keying ike encrypt * null is no longer supported. aes-gcm will be supported with ikev2 only. • crypto ipsec peer <ip> local <ip> keying ike dh-group * 1, 2, 5, 22, 23, 24 are no longer supported. 19, 20, 21 will be supported with ikev2 only. • crypto ipsec peer <ip> local <ip> keying ike pfs-group * 1, 2, 5, 22, 23, 24 are no longer supported. 19, 20, 21 will be supported with ikev2 only. • crypto ipsec peer <ip> local <ip> keying ike transform-set ah-and-esp-ah are no longer supported. <p>If deprecated options are used, the file will be moved to its default value. For more information, see "crypto ipsec peer local" command in Cryptographic (X.509, IPsec) and Encryption section of the user manual.</p>
Terminal sysrq	As of 3.9.3124, the SysRq over the serial connection (RS232 or Console port) is disabled by default. When this configuration is enabled, "terminal sysrq enable" will appear in the running config after upgrade. See "UI Commands" section in the user manual.
3.9.2302	
VXLAN, EVPN, ECMP Containers	In Spectrum-2 and Spectrum-3 systems, additional 256 KVD entries are reserved for ECMP NVE containers.
VXLAN, EVPN, ECMP Containers	In Spectrum-2 and Spectrum-3 systems, the limitation of 32K VXLAN multicast and flood destinations is removed. Now the number of VXLAN multicast and flood destinations is limited by KVD occupation.
3.9.2110	
Spectrum-3, SN4700, Speed	The default speed for the SN4700 has been changed to 400GbE.
3.9.2006	

MTU	<p>MTU default value of L2 and L3 interfaces was changed from 1500 to 9216. The new behavior depends on how the versions are installed.</p> <p>1. Switches that perform an upgrade to the new version will experience the following:</p> <ul style="list-style-type: none"> -MTU value of interfaces included in MLAG IPL will get the default value (9216). -MTU value of all existing interfaces will not be changed (will be 1500 or any other value configured by user). -Show running config will now show the configuration. -For newly created L2/L3 interfaces, MTU value will be 9216. <p>2. Switches that will perform a manufacture restart to the new version will experience the following:</p> <ul style="list-style-type: none"> -All L2 interfaces will be created with MTU value of 9216. -Newly created L2/L3 interfaces will have MTU value of 9216.
Spectrum-2, Spectrum-3, SNMP	<p>On Spectrum-2 and Spectrum-3 systems, entPhysicalIndex calculation for port module and port module sensor will change and a new value will be displayed in the following SNMP tables: Entity MIB—entPhysicalTable and Entity Sensor MIB—entPhySensorTable.</p>
SSH	<p>SSH connections will no longer support the diffie-hellman-group14-sha1 cipher under key exchange algorithms and will be moved to non-secure ciphers.</p>
3.9.1900	
Static IP	<p>In cases where a management interface has both static IP and DHCP configured, DHCP will not tun and static IP will be the assigned IP.</p>
3.9.1304	
JSON	<p>Changed the JSON output of command "show ip bgp neighbors".</p>
Logging Monitor Event	<p>The behavior of "logging monitor event" was changed and the prompt line will now be printed for each event that arrives. As a result, multiple events can no longer be seen printed as a group; each event is treated separately.</p>
WJH	<p>The following changes have been made when another application takes control of WJH. show what-just-happened status:Before change: WJH groups appeared with "Operational status" as Enabled. After change: If another application (e.g. NEO) takes control of WJH, the "Operational status" will be Disabled. show what-just-happened <drop-reason-group> will no longer try to take control of WJH. Running the show command while another application controls WJH will now provide no output.If the OS needs to take control of WJH, the command must be disabled the flow must be enabled again.</p>
3.9.1014	
Certificate Configuration	<p>If a certificate is provided without the CA flag, the switch will parse this certificate as though the flag was set to false. All CA certificates should have the CA flag set to true.</p>

<p>Default Port Speed, Spectrum-2, SN3700</p>	<p>The default port speed for SN3700 system has been changed from 100GbE to 200GbE. As such, while splitting to 2, the default speed is now 100GbE and, which splitting to 4, the default speed is 50GbE. The speeds that have been configured, will remain unchanged. Note: This change does not relate to the SN3700C system.</p>
<p>Ethernet Interfaces, Counters</p>	<p>Due to new counter display enhancement, the JSON output has been modified.</p>
<p>QoS, Congestion-Control</p>	<p>show interface congestion-control output was modified to increase readability and fix JSON form.</p>
<p>RoCE</p>	<p>The behavior in the following scenario has been changed: The system starts in non-RoCE mode. Parameter 'v1' has value 'x' which is the default in non-RoCE mode. The user manually configures parameter 'v1' to 'y'. The user switches to RoCE mode. Parameter 'v1' still has the value 'y'. 'y' also happens to be the default in RoCE mode. The user switches back to non-RoCE mode. We now check the value of parameter 'v1'. The old behavior: Parameter 'v1' now has value 'y'. The new behavior: Parameter 'v1' now has value 'x'.</p>
<p>VRRP</p>	<p>The ping response to VIP is now with the interface VLAN MAC of the Master and not with the VMAC.</p>

Deprecation	<p>The following previously-unsupported commands are officially deprecated as of 3.9.1000:</p> <pre> ipv6 multicast-routing ipv6 multicast-routing vrf * no ipv6 multicast-routing no ipv6 multicast-routing vrf * show ipv6 mld interface show ipv6 mld interface * brief show ipv6 mld * groups interface * show ipv6 mld * groups interface * detail clear ipv6 mld * groups interface * protocol mld no protocol mld [no] interface <type> <id> { ipv6 mld ipv6 mld immediate-leave ipv6 mld robustness-variable ipv6 mld robustness-variable * ipv6 mld query-max-response-time ipv6 mld query-max-response-time * ipv6 mld query-interval ipv6 mld query-interval * ipv6 mld last-member-query-response-time ipv6 mld last-member-query-response-time * ipv6 mld version ipv6 mld version * ipv6 mld join-group ipv6 mld static-oif ipv6 mld static-oif * ipv6 mld static-oif * source-ip ipv6 mld static-oif * source-ip * ipv6 mld last-member-query-count ipv6 mld last-member-query-count * ipv6 mld startup-query-interval } </pre>
3.9.0914	
MAC	<p>From this release on, the first two bytes of the MAC address in the log will be marked with asterisks for security purposes. This may be disabled using the no form of the “logging mac masking” command. See “Logging” section in the user manual for more information.</p>
PAM4 Link Speeds when Using 400GbE/200GbE	<p>The following are the minimal software/firmware versions that support PAM4 link speeds when connected using NVIDIA-to-NVIDIA and NVIDIA-to-3rd party devices:</p> <p>Spectrum-3: 30.2007.1142 Spectrum-2: 29.2007.1142 NVIDIA Onyx: 3.9.0830 SONiC/SAI: 201911- fffee7e33a1e9ccf564407966003ac45305fe64e ConnectX-6/ConnectX-6 Dx: 20/22.27.2008*</p> <p>*Note: NICs with this firmware version, and above, support NVIDIA-to-NVIDIA connectivity with PAM4 link speeds</p>
Split	<p>For split commands, the syntax “module-type qsf” was replaced with “no module-type”. For more information, see “Ethernet Interfaces” section in the user manual.</p>
WJH, Logging	<p>For the logging commands, the “interfaces” option/syntax was replaced with “what-just-happened-packets”. For more information, see “Logging” section in the user manual.</p>

3.9.0608

Autonegotiation	The "no auto-neg" command is no longer available. Autonegotiation configuration can be achieved by the 'auto' option.
WJH	no-pcap' attribute will be removed, and no pcap file will be generated with execution of the basic flavor of the command. To create pcap files on command execution, use the following form: switch (config) # show what-just-happened * [export [<file-name>]] [no-metadata]

3.9.0300

WJH	WJH pcap file names beginning with a dot are now prohibited, since such files cannot be uploaded or deleted.
WJH	Modified "show what-just-happened" table output.
BGP [deprecation]	BGP command "no-route-map" is deprecated and been replaced with the disable form of the BGP route-map command. For more information see "BGP Commands" section in the User Manual.
Counters [deprecation]	Currently, not all discarded packets are counted in "show interface counters" command 'discard packets' counter. The name of the counter will be changed to 'no buffer discards' in upcoming releases.
VRF [deprecation]	"show interfaces <IP Interface>" (for example, router-port or VLAN interface) will be deprecated in a future release. Use "show ip interface . . ." command that has VRF support, for example "show ip interface vrf all brief".

3.8.2204

EVPN	<p>Existing configuration CLI was changed from "router bgp 100 address-family l2vpn-evpn auto-create" to "router bgp 100 address-family l2vpn-evpn vni auto-create"</p> <p>When enabling address-family l2vpn-evpn vni auto-create mode then RT value will be generated as following: (a) In case of 2bytes AS, AN is VNI (b) In case of 4bytes AS, AN is VLAN.</p> <p>There is no interoperability with old EVPN releases when running VNI auto-create VS. VNI auto-create mode. A workaround to interoperate with old EVPN VNI auto-create is to switch to manual VNI mode by using the following commands: (1) Disable VNI auto-create mode: (config) # no router bgp * address-family l2vpn-evpn vni auto-create (2) Configure manual VNI: (config) # router bgp * address-family l2vpn-evpn vni * (3) Configure VNI RD: (config) # router bgp * address-family l2vpn-evpn vni * rd * (4) Configure manual VNI RT: (config) # router bgp * address-family l2vpn-evpn vni * route-target both *</p>
------	--

3.8.2102

RoCE, Port Channel, LAG	The default value of port-channel load-balance has been changed from "source-destination-mac" to "source-destination-mac, source-destination-ip, source-destination-port, l3-protocol, l2-protocol, flow-label". This occurs only upon fresh installations or after "reset factory". Upgrading users will retain the old load balancing value and show running-config will indicate this.
3.8.2008	
Security Enhancements	As of version 3.8.20xx, California law SB-327 will be enforced so that Admin and Monitor passwords must be typed upon initial configuration. Default passwords will no longer be created automatically. Nevertheless, the user will be allowed to manually write in the default user name and password (admin/admin or monitor/monitor). The changes are implemented in a manner that minimizes the impact on the automation processes so that Zero Touch Provisioning (ZTP) will continue to work as usual and will not be affected by the new regulation.
XPL API Deprecation	As of the September release of software version 3.8.2000, the XML user accounts will no longer be supported and the XML gateway will be closed. Access through XML will no longer be available. Interfaces will only be available through SNMP and JSON.
Web UI	Re-designed interface to enhance user experience.
IGMP	The default IGMP version was changed from v2 to v3. This occurs only upon fresh installations or after "reset factory". Upgrading users that are running with IGMP v2 will not be affected and show running configure will indicate this.
LLDP	LLDP is now enabled by default. This occurs only upon fresh installations or after "reset factory". Upgrading users that have LLDP disabled will leave LLDP disabled and show running configure will indicate this.

8 Bug Fixes History

⚠ This section includes bug fixes history of three major releases back. For older releases history, please refer to the relevant versions.

Internal Ref.	Category	Description
3.10.4302		
3410587	AAA, ARP	When a host entry in the ARP table ages out, an ARP request for the host will not be generated by the switch from gleaned DNS traffic. This may result in DNS services intermittently failing until non-DNS traffic to the host is received by the switch to generate an ARP request for the destination IP.
3389513	AAA, MLAG	After removing the MLAG-vip configuration, the system does not reset the MLAG system-mac and system-id, which will lead to misalignment in MLAG setup, when one of MLAG-peers rebooted.
3510518	Cables	Tx bias current shows N/A on some cables.
3500373	JSON	After overflowing the system with JSON requests (more than 1 million requests), system may not respond to other JSON queries.
3205792	LACP	SDK dump generation with configured fast-rate LACP causes IPL link flapping.
3440835/ 3434543	LDAP SSL	LDAP SSL option (ldap ssl mode ssl) is missing from the CLI. For more information see ldap sll command in "User Management and Security Commands" section in the user manual.
3475217	MLAG, IPv6 Neighbor Discovery Router Advertisement	IPv6 neighbor discovery router advertisement packets looped on VNI interfaces.
3464662	PTP Management Messages	PTP management messages are forwarded though forced MASTER ports.
3528970	SLAAC	SLAAC does not work well with ZTP. As part of the fix, SLAAC will be enabled by default for management interfaces and will also be also enabled after upgrade.
3502330	WJH, SNMP Traps	When WJH with SNMP traps is configured, a possible daemon may hang, causing the system to go into an error state.

Internal Ref.	Category	Description
3.10.4202		
3366133	IGMP Snooping	IGMP snooping failed to process any IGMP packet if packet size is greater than 2048 bytes.
3167994	MAGP	In the event of a network loop, traffic with MAGP source vMAC may be forwarded back to the switch port.
3315167	NTP, Logging	When NTP is configured, the following print may appear to the log every minute: <pre>ntpd5510: bind(23) AF_INET6 ::1#123 flags 0x5 failed: Cannot assign requested address</pre>
3338504	NTP, VRF	When enabling VRF management on NTP, the NTP servers are not displayed.
3362827	OpenFlow	When OpenFlow flow is modified with a group that contains more than 50 actions, the switch crashes.
3284730	PTP, Sysdump, Output	Output of show PTP commands was missing in sysdump.
Internal Ref.	Category	Description
3.10.4100 LTS		
3236568	Cables, CMIS	The CMIS cables lengths were rounded. Improved accuracy of CMIS cables length to display exact cable length.
3233054	Debug Dump	When there are both IPv4 and IPv6 routes configured, once the IPv4 and IPv6 SHSPM trees are turned into left-bound trees due to lack of resources, a following SDK debug dump generation may cause SDK process to crash.
3284414	EULA	On WebUI and CLI, the EULA document did not appear properly.
3267893	MAC Address	At times a remote route is received for a MAC address for which a local route exists that has been marked as sticky. Once in this state, a second remote route received for this same MAC can lead to an assertion and L3 stack to restart, resulting in switch reboot.
3283539	Power Supply, Fan	When power supply cable is removed and inserted again, the fan speed sometimes did not set properly on the power supply fan.

3269345	Spectrum, Optical Cables, Close State	On SN2010 system, when using optical cables, the system may get stuck when the port is in close state.
3.10.4006		
3197376	BaseT Modules	When using BaseT modules and running "show interfaces ethernet 1/<port>" or "show interfaces ethernet", an internal error appears. This can be safely ignored.
3268999	Ethernet Interfaces, Optical Transceiver	Using the command "show interface <interface name> transceiver diagnostics" with a CMIS-based (QSFP-DD/OSFP) optical transceiver might displays wrong power values for per lane.
3220796	LACP Policer	Configuration for trap-group LACP policer cannot be applied.
3209606	LLDP, Traffic Class	Remote information about supported traffic class is not displayed.
3173334	Management Interfaces	On systems that include two management interfaces, when connecting mgmt1, ping may not be available for mgmt0.
3172492	PTP	PTP module does not log negative mean path delay values.
3143414	Shared Buffer, On-The-Fly Configuration	When many ports are active (e.g., 70 ports up), and the configuration of shared buffer is applied on the fly, occasionally, the firmware might get stuck.
3213254	Spectrum-2, SN3420	On SN3420 system, SDK returns error when FEC mode is set on twisted pair.
3149861	Spectrum-2, SN3700C, 1GbE, PTP	PTP Mean Path Delay (MPD) calculation gets improved in 1G Anaconda.
3.10.3100		
3172779	ACL, IPv6	The ACLD may crash when ACL with log action captures an IPv6 frame with a very large number of nested headers (total header length larger then 512B). Unexpected system behavior may occur due to the crash.
3172851	JSON API Authentication	In version 3.10.300x, JSON API authentication fails when posting to /admin/launch?script=rh&template=json-request&action=json-login.

3123387	Spectrum, PTP	On Spectrum systems, there is a 3 ns deviation in the offset of the standby clock with IPv6 PTP.
3077667	Spectrum-2, Spectrum-3, ECN Marking, Split	On the Spectrum-2 and Spectrum-3 switch, if you enable ECN marking and the port is in split mode, traffic sent to the port under congestion (for example, when connecting two ports with a total speed of 50GbE to a single 25GbE port) is not marked.
3158861	Spectrum-2, Spectrum-3, PTP	On Spectrum-2 and Spectrum-3 systems, part of the PTP packets were sent from CPU as 'control' packets, while others were sent as 'data'. They are now all sent as 'data'.
3205701	Spectrum-3, PCI Calibration	In Spectrum-3 systems SN4700 and SN4600C PCI calibration is modified from a static to a dynamic mechanism. As such the use of software versions older than 3.10.310x in these platforms is not permitted.
3205700	Spectrum-3, PCI Calibration	In Spectrum-3 systems SN4700 and SN4600C PCI calibration is modified from a static to a dynamic mechanism. As such the use of software versions older than 3.10.310x in these platforms is not permitted.
3162664	Spectrum-3, PCI Calibration	In Spectrum-3 systems SN4700 and SN4600C PCI calibration is modified from a static to a dynamic mechanism. As such the use of software versions older than 3.10.310x in these platforms is not permitted.
3123584	Split to 8	In split-to-8 mode, if an even port is split, the lower odd is port gets disabled and if the odd port is split, the upper even port is gets disabled.
3135787	Sysdump	On rare occasions, during the snapshot creation, sysdump was not automatically generated.
3.10.3004		
3090001	ECMP, Resilient	After editing an ECMP, the resilient ECMP next-hop counter may not count correctly.
3111472	EVPN, VRF	In an MLAG-EVPN setup with ARP suppression, configuring VRRP/MAGP over any VRF other than the default results in the MAC-IP of the VRRP/MAGP interface not showing up on any of the EVPN tables.
3085287	Password Hardening	On some occasions, after setting a password for new user, an internal error in password hardening may appear.
3072365	SDK Dump	SLL configuration is missing in SDK dump.
3055490	SDK Dump	SDK Dump missing column headers in some GC tables may result in difficulty understanding the dump.

3106297	Spectrum, Counters	SDK debug dump shows "Unknown" Counter in the PPCNT Traffic Class Counter Group.
3106262	Spectrum, Counters	SDK debug dump shows "Unknown" Counter in RFC3635 Counter Group.
3066165	Spectrum, IGMP Querier Guard	On Spectrum systems, when IGMP querier guard is enabled on any port of the system (even if it is not participating in the VLAN of the external query and is not on its port), the switch sends the IGMP query from the external device to all ports in the VLAN with a double tag.
3070681	Spectrum, Link Up	On Spectrum systems, sometimes during link failure, not all previous firmware indications cleared properly, potentially affecting the next link up attempt.
3066050	Spectrum, PTP	When using Spectrum systems at 100GE, the PTP parameters were not tuned properly resulting in a mean path delay value that is too low.
3055177	Spectrum-2, LAG, VXLAN	Deleting a port from a LAG that has port isolation configured with a VXLAN tunnel may result in errors.
3129809	WebUI	The default certificates (rather than customer-loaded certificates) were used upon conducting a reload.
3.10.2202		
3021773	CLI	CLI command "show interfaces" may take up to 30 seconds.
3055594	Cable Burning	100GbE FCI DAC (10137628-4050LF/HPE PN: 845408-B21) was recognized by mistake as supporting "cable burning" which caused the switch firmware to read page 0x9f (which unsupported in the cable) and to report this cable as having "bad eeprom".
3010092	NEO, Driver	When NEO agent fails, it may, upon reload, attempt to reload the driver resulting in unexpected behavior.
3044236	Timestamp	Timestamp over CRC is not supported in ONYX v3.10.2002.
3077375	Upgrade, IP Filter	When upgrading to 3.10.20xx with existing IP filter configuration, the upgrade will fail and there will be a rollback to the older software version.
3038797	VXLAN, UDP	For the tunnel VXLAN UDP packets source port is always "0".
3003011	Memory	A memory leak in the master module caused it to stall, causing the standby module to take over and become master.

3011244	OpenFlow, OVS	When trying to modify the OpenFlow group with the number of actions that is not supported in OpenFlow, the switch crashes.
2999383	VRF	When VRF mgmt is configured, switching to non VRF mgmt configuration file via Web UI is not possible.
3.10.2002		
2901444	Spectrum, Router. FDB, Tunnel	On rare occasions, removing an entry from the KVD on Spectrum systems, may cause the firmware to get stuck upon the next insertion.
2950888	Certification	When whitespaces appeared in the "flag" certificate, caused certificate parsing failure.
2818461	ECMP, VLAN, Next Hop	When ECMP has high amount of next-hops based on VLAN interfaces, in some rare cases, packets will get a wrong VLAN tag and will be dropped.
2947760	EVPN, VRRP	EVPN tunnel drops VRRP packets.
2963304	Email Notifications	White spaces in the "flag" certificate caused certificate parsing failure.
2866195	FDB	On rare occasion, when the self-own interface was learned in FDB as dynamic entry, L3 traffic cannot reach L3 VLAN interface, causing a loss of router functionality.
2723981	IPv6	The command "interface * * ipv6 nd ra suppress" did not set the value.
2732840	MAC	Under very heavy load of both APIs and capacity that utilizes a very high number of bridges may lead to the disabling of MAC learning.
2963599	MLAG	On the MLAG setup, saving configuration on the master switch causes the configuration to be saved on the standby switch. On rare occasions, during reboot flow on the standby switch, the saved configuration can be requested from the master switch (e.g., running "configuration write"), causing possible configuration damage.
2749107	OpenFlow, ARP	When using OpenFlow flow for key=arp with action=normal does not trap ARP to CPU, causing ARP not to work.
2369065	PTP	PTP over port-channel is not supported on Spectrum-2 and Spectrum-3 systems.
3004309	SSH	Applying "ssh server listen interface [interface name]" caused improper SSHD configuration, preventing the establishment of a new SSH session. Sessions established before mentioned configuration remained.

2855928	Spectrum, Firmware	In rare cases, the system got stuck when a peer port went down.
2902365	Spectrum, PTP	On Spectrum systems, a timing issue causes the firmware to get stuck on port flap while PTP is enabled.
2868244	Spectrum, Tx	Changing the SerDes Tx parameters on Spectrum devices was not supported.
2814703	Spectrum-2, Ports, Speeds	On rare occasions, when working with port rates of 1GbE or 10GbE and congestion occurs, packets may get stuck in the chip and may cause switch to hang.
2884838	Spectrum-2, Spectrum-3, IP Routing	SDK crashed on Spectrum-2 and Spectrum-3 systems when the background process tried to switch both the IPv4 and IPv6 routing trees.
2669055	Spectrum-2, Spectrum-3, Marvell PHY, Auto-Negotiation	In Spectrum-2 and Spectrum-3 systems, link did not work in auto-negotiation when connected to Marvell PHY. KR mechanism has been enhanced to integrate with Marvell PHY.
2786687	Spectrum-3, ConnectX-6, Link	On some occasions, connecting Spectrum-3 to ConnectX-6 may cause link to go down.
2887350	Spectrum-3, Counters, MTU	On Spectrum-3 systems, when sending traffic from 1GbE to higher speeds and packet size it close to ingress port MTU, packets can be dropped on FCS errors.
2642414	Spectrum-3, SN4600C, Cables	While using SN4600C system with Finisar FTLC1157RGPL 100GbE CWDM4 modules, intermittent link flaps across multiple ports may be observed.
2610967	Spectrum-3, SN4600C, Cables	Using SN4600C with copper or optics, link may raise in long link up times (up to 70 seconds).
2664336	Spectrum-3, SN4600C, Fastboot, Auto Negotiation	In SN4600C system, when the peer is in auto-negotiation, link up time may take up to 8 seconds.
2780348	Spectrum-3, SN4600C, Link Up	When connecting SN4600C, 100GbE port with CWDM4 module (Gen 3.0), link up time is 30 seconds.
2837462	Stamping	Under various circumstances, in Spectrum systems, Ethernet ports falsely showed that InfiniBand cables were connected.

2808172	VXLAN, VRF	Non default VRF interfaces do not advertise mac-ip pair.
2785511	MLAG	When MPO interface on the MLAG-master is down, the MLAG-standby takes ownership of the STP and sends BPDUs from the corresponding MPO interface. Instead of sending BPDUs only with the Master source mac address, the MLAG-standby sends two BPDUs (one with MLAG-master and one with MLAG-standby source MAC address).
2833052	Password	Changing the user password and then proceeding SSH login with the new password affects configurations. When running "show configuration files", the "unsaved changes" field is reflected as "yes" (instead of "no").
2803887	Logging	Updated format of port state change event print to log to include severity.
2695327	Spectrum-3, PTP, L3	On L3 interfaces on Spectrum-3 devices, PTP configuration was applied in all interfaces of a 2x or 4x port.

9 Support and Other Resources

9.1 Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

<http://www.hpe.com/assistance>

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:


<http://www.hpe.com/support/hpesc>

9.1.1 Information to Collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

9.2 Accessing Updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:
Hewlett Packard Enterprise Support Center
www.hpe.com/support/hpesc
Hewlett Packard Enterprise Support Center: Software downloads
www.hpe.com/support/downloads
Software Depot
www.hpe.com/support/softwaredepot
- To subscribe to eNewsletters and alerts:
www.hpe.com/support/e-updates
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:
www.hpe.com/support/AccessToSupportMaterials

 **Important:** Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

9.3 Customer Self Repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

<http://www.hpe.com/support/selfrepair>

9.4 Remote Support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

9.4.1 Remote Support and Proactive Care Information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

9.4.2 Proactive Care Customer Information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

9.5 Warranty Information

To view the warranty for your product or to view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products reference document, go to the Enterprise Safety and Compliance website:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

9.5.1 Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

9.6 Regulatory Information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

9.6.1 Additional Regulatory Information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

9.7 Documentation Feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

9.8 Websites

General Websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

www.hpe.com/storage/spock

Storage white papers and analyst reports

www.hpe.com/storage/whitepapers

For additional websites, see Support and other resources.