April 2024

Extreme SLX-OS 20.6.1a

Release Notes

Supporting ExtremeRouting and ExtremeSwitching SLX 9740, SLX 9640, SLX 9540, SLX 9250, SLX 9150, Extreme 8720, Extreme 8520, and Extreme 8820

Part Number 9038914-00 Rev AB

Contents

Document History

Version	Summary of changes	Publication date
1.0	Initial version for 20.6.1a	April 2024
1.1	In the section Release Overview, updated the Smartoptics support information	April 2024

Preface

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- Extreme Portal: Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.
- The Hub: A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees but is not intended to replace specific guidance from GTAC.
- Call GTAC: For immediate support, call (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form. All fields are required.
3. Select the products for which you want to receive notifications.
   Note: You can change your product selections or unsubscribe at any time.
4. Select **Submit**.

Extreme Resources

Visit the Extreme website to locate related documentation for your product and additional Extreme resources.

White papers, data sheets, and the most recent versions of Extreme software and hardware manuals are available at https://www.extremenetworks.com/. Product documentation for all

supported releases is available to registered users at https://www.extremenetworks.com/support/documentation/.

Document Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information
- Improvements that would help you find relevant information in the document
- Broken links or usability issues

You can provide feedback in the following ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at http://www.extremenetworks.com/documentation-feedback-pdf.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Release Overview

Release SLX-OS 20.6.1a provides the following features:

- Critical defects were addressed.
- No new features were added.

Release SLX-OS 20.6.1 provides the following features:

- Integrating BMC firmware upgrade to SLX-OS image upgrade methods
- SLX-OS Debugging enhancements
- MCT Improvements (Cluster Implementation Robustness) - HW Failure case
- IPv6 routes next hop conversion in MP-BGP (transporting IPv6 routes over IPv4 peer)
- Notification for Password expiration for SLX-OS user
- Extending QoS support on SLX 9540 and SLX 9640
- Enhancing display info and availability of Power supply attributes
- EVPN interoperable Interface-less support as per RFC 9136
- Lookup destination for routed packets in sFlow
- REST API on SLX-OS to fetch the switch details from an SLX platform
- Smartoptics qualification on SLX-OS. Only one type of SFP is qualified for this release.
  - SO-QSFP28-D46 (IN-Q2AY2-46)

Behavior Changes

The following behavioral changes for SLX-OS 20.6.1a

- No behavioral changes were added in this release.

The following is the behavioral change for SLX-OS 20.6.1

- When performing SLX-OS upgrade, in case it is identified that BMC firmware upgrade is also required, the upgrade process will require an additional 4 to 7 minutes to complete.

Software Features

The following key software features are added in the SLX-OS 20.6.1 release:

Feature Name	Supported SLX Platforms	Description
Integrating BMC firmware upgrade to SLX-OS image upgrade methods	Extreme 8520, Extreme 8720, Extreme 8820, SLX 9740	Introduced to keep the BMC supported devices updated with latest BMC firmware automatically on the field. BMC firmware upgrade will automatically happen along with SLX-OS image upgrade on the BMC-supported platforms
SLX-OS Debugging enhancements	ALL	SFP absent and corruption cases Enhancing SDK logs with additional parameters
MCT Improvements – HW Failure case	Extreme 8520, Extreme 8720, Extreme 8820, SLX 9740, SLX 9150 and SLX 9250	Improving Multi-chassis Trunking (MCT) failover time. The solution currently works with 40 and 100G fiber optics and breakout combinations.
IPv6 routes next hop conversion in MP-BGP (transporting IPv6 routes over IPv4 peer)	ALL	Allow user to configure outbound route map policy to modify the next hop of IPv6 prefixes sent over IPv4 eBGP sessions. This is an alternative to earlier provided option of IPv4-mapped-v6 address
Notification for Password expiration for SLX-OS user	ALL	User passwords on SLX-OS are monitored for expiry and notified via RASlog for an early warning for password expiry.
Extending QoS support on SLX 9540 and SLX 9640	SLX 9540, SLX 9640	QoS support on SLX 9540 and SLX 9640 is added to Virtual Ethernet (VE) and Port channel interface types
Enhancing display info and availability of Power supply attributes	ALL	The SLX-OS show command show environment power is enhanced to display more power related attributes

Feature Name	Supported SLX Platforms	Description
EVPN interoperable Interface-less support as per RFC 9136	ALL	Provides only interoperable support for interface-less IRB model defined in RFC 9136
Lookup destination for routed packets in sFlow	ALL	Support updating of destination MAC address in sFlow samples for Routed traffic. Prior to SLX-OS 20.6.1, destination mac address carries the sampled interface MAC, instead of MAC address of the next hop device
REST API on SLX-OS to fetch the switch details from an SLX platform	ALL	REST API to fetch the chassis and inventory related details of a switch
Smartoptics qualification on SLX-OS	ALL	Smartoptics brand of optics are qualified on SLX-OS

CLI Commands

The following commands were added, modified, or deprecated for the 20.6.1a release:

- No commands were added, modified, or deprecated for this release.

New commands for 20.6.1a

- No commands were added in this release.

Modified commands for 20.6.1a

- No commands were modified in this release.

Deprecated commands for 20.6.1a

- No commands were deprecated in this release.

The following commands were added, modified, or deprecated for the 20.6.1 release:

New commands for 20.6.1

- sflow update-destination-mac
- password-attributes expiry-alert-level

Modified commands for 20.6.1

- firmware download
- show chassis
- show environment power

- show sflow
- show running-config sflow

Deprecated commands for 20.6.1

- chassis

Hardware Support

Supported devices and software licenses

Supported devices	Description
SLX9740-40C	Extreme SLX 9740-40C Router. Base unit with 40x100GE/40GE capable QSFP28 ports, 2 unpopulated power supply slots, 6 unpopulated fan slots
SLX9740-40C-AC-F	Extreme SLX 9740-40C-AC-F Router. Base unit with 40x100GE/40GE capable QSFP28 ports, 2 AC power supplies, 6 fan modules
SLX9740-80C	Extreme SLX 9740-80C Router. Base unit with 80x100GE/40GE capable QSFP28 ports, 4 unpopulated power supply slots, 4 unpopulated fan slots
SLX9740-80C-AC-F	Extreme SLX 9740-80C-AC-F Router. Base unit with 80x100GE/40GE capable QSFP28 ports, 4AC power supplies, 4 fan modules
SLX9740-ADV-LIC-P	Advanced Feature License for MPLS, BGP-EVPN and Integrated Application Hosting for Extreme SLX 9740
SLX9150-48Y-8C	Extreme SLX 9150-48Y Switch with two empty power supply slots, six empty fan slots. Supports 48x25GE/10GE/1GE + 8x100GE/40GE.
SLX9150-48Y-8C-AC-F	Extreme SLX 9150-48Y Switch AC with Front to Back Airflow. Supports 48x25GE/10GE/1GE + 8x100GE/40GE with dual power supplies, six fans.
SLX9150-48Y-8C-AC-R	Extreme SLX 9150-48Y Switch AC with Back to Front Airflow. Supports 48x25GE/10GE/1GE + 8x100GE/40GE with dual power supplies, six fans.
SLX9150-48XT-6C	Extreme SLX 9150-48XT 10GBaseT Switch with two empty power supply slots, six empty fan slots, Supports 48x10GE/1GE + 6x100GE/40GE.
SLX9150-48XT-6C-AC-F	Extreme SLX 9150-48XT 10GBaseT Switch AC with Front to Back Airflow, Supports 48x10GE/1GE + 6x100GE/40GE with dual power supplies, six fans.
SLX9150-48XT-6C-AC-R	Extreme SLX 9150-48XT 10GBaseT Switch AC with Back to Front Airflow, Supports 48x10GE/1GE + 6x100GE/40GE with dual power supplies, six fans.
SLX9150-ADV-LIC-P	SLX 9150 Advanced Feature License for GuestVM, Analytics Path, PTP, BGP-EVPN.

Supported devices	Description
SLX9250-32C	SLX 9250-32C Switch with two empty power supply slots, six empty fan slots. Supports 32x100/40GE.
SLX9250-32C-AC-F	SLX 9250-32C Switch AC with Front to Back Airflow. Supports 32x100GE/40GE with dual power supplies, six fans.
SLX9250-32C-AC-R	SLX 9250-32C Switch AC with Back to Front Airflow. Supports 32x100GE/40GE with dual power supplies, six fans.
SLX9250-ADV-LIC-P	SLX 9250 Advanced Feature License for GuestVM, Analytics Path, BGP-EVPN.
BR-SLX-9540-48S-AC-R	SLX 9540-48S Switch AC with Back to Front airflow (Non-port Side to port side airflow). Supports 48x10GE/1GE + 6x100GE/40GE. (1+1) redundant power supplies and (4+1) redundant fans included.
BR-SLX-9540-48S-AC-F	SLX 9540-48S Switch AC with Front to Back airflow (Port-side to non-port side airflow). Supports 48x10GE/1GE + 6x100GE/40GE. (1+1) redundant power supplies and (4+1) redundant fans included.
BR-SLX-9540-24S-DC-R	SLX 9540-24S Switch DC with Back to Front airflow (Non-port Side to port side airflow). Supports 24x10GE/1GE + 24x1GE ports.
BR-SLX-9540-24S-DC-F	SLX 9540-24S Switch DC with Front to Back airflow (Port-side to non-port side airflow). Supports 24x10GE/1GE + 24x1GE ports.
BR-SLX-9540-24S-AC-R	SLX 9540-24S Switch AC with Back to Front airflow (Non-port Side to port side airflow). Supports 24x10GE/1GE + 24x1GE ports.
BR-SLX-9540-24S-AC-F	SLX 9540-24S Switch AC with Front to Back airflow (Port-side to non-port side airflow). Supports 24x10GE/1GE + 24x1GE ports.
BR-SLX-9540-48S-DC-R	SLX 9540-48S Switch DC with Back to Front airflow (Non-port Side to port side airflow). Supports 48x10GE/1GE + 6x100GE/40GE. (1+1) redundant power supplies and (4+1) redundant fans included.
BR-SLX-9540-48S-DC-F	SLX 9540-48S Switch DC with Front to Back airflow (Port-side to non-port side airflow). Supports 48x10GE/1GE + 6x100GE/40GE. (1+1) redundant power supplies and (4+1) redundant fans included.
BR-SLX-9540-24S-COD-P	Upgrade 24x1GE to 24x10GE/1GE for SLX 9540
BR-SLX-9540-ADV-LIC-P	Advanced Feature License for SLX 9540
EN-SLX-9640-24S	Extreme SLX 9640-24S Router. Supports 24x10GE/1GE + 4x100GE/40GE. (24S+4C sku no Power supplies or Fans)
EN-SLX-9640-24S-12C	Extreme SLX 9640-24S Router. Supports 24x10GE/1GE + 12x100GE/40GE. (All ports 24S+12C sku with no Power supplies or Fans)
EN-SLX-9640-24S-AC-F	Extreme SLX 9640-24S Router AC with Front to Back airflow. Supports 24x10GE/1GE + 4x100GE/40GE.(1 Power supply 6 Fans)

Supported devices	Description
EN-SLX-9640-24S-12C-AC-F	Extreme SLX 9640-24S Router AC with Front to Back airflow. Supports 24x10GE/1GE + 12x100GE/40GE.(1 Power supply 6 Fans)
EN-SLX-9640-4C-POD-P	Extreme SLX 9640 Ports on Demand License for 4 ports of 100GE/40GE Uplinks
EN-SLX-9640-ADV-LIC-P	Extreme SLX 9640 Advanced Feature License
8720-32C	Extreme 8720-32C Switch with two empty power supply slots, six empty fan slots and a 4-post rack mount kit, Supports 32x100/40GE
8720-32C-AC-F	Extreme 8720-32C Switch with front to back airflow, Supports 32x100/40G with two AC power supplies, six fans and a 4-post rack mount kit
8720-32C-AC-R	Extreme 8720-32C Switch with back to front airflow, Supports 32x100/40G with dual AC power supplies, six fans and a 4-post rack mount kit
8720-32C-DC-F	Extreme 8720-32C Switch with front to back airflow, Supports 32x100/40G with dual DC power supplies, six fans and a 4-post rack mount kit
8720-32C-DC-R	Extreme 8720-32C Switch with back to front airflow, Supports 32x100/40G with dual DC power supplies, six fans and a 4-post rack mount kit
8520-48Y-8C	Extreme 8520-48Y Switch with two empty power supply slots, six empty fan slots; Ships with one 4-post rack mount kit; Supports 48x25/10/1G and 8x100/40G ports
8520-48Y-8C-AC-F	Extreme 8520-48Y Switch with front-back airflow; Ships with two AC power supplies, six fans, one 4-post rack mount kit; Supports 48x25/10/1G and 8x100/40G ports
8520-48Y-8C-AC-R	Extreme 8520-48Y Switch with back-front airflow; Ships with two AC power supplies, six fans, one 4-post rack mount kit; Supports 48x25/10/1G and 8x100/40G ports
8520-48Y-8C-DC-F	Extreme 8520-48Y Switch with front-back airflow; Ships with two DC power supplies, six fans, one 4-post rack mount kit; Supports 48x25/10/1G and 8x100/40G ports
8520-48Y-8C-DC-R	Extreme 8520-48Y Switch with back-front airflow; Ships with two DC power supplies, six fans, one 4-post rack mount kit; Supports 48x25/10/1G and 8x100/40G ports
8520-48XT-6C	Extreme 8520-48XT Switch with two empty power supply slots, six empty fan slots; Ships with one 4-post rack mount kit; Supports 48x10/1G copper ports and 6x100/40G fiber ports

Supported devices	Description
8520-48XT-6C-AC-F	Extreme 8520-48XT Switch with front-back airflow; Ships with two AC power supplies, six fans, one 4-post rack mount kit; Supports 48x10/1G copper ports and 6x100/40G fiber ports
8520-48XT-6C-AC-R	Extreme 8520-48XT Switch with back-front airflow; Ships with two AC power supplies, six fans, one 4-post rack mount kit; Supports 48x10/1G copper ports and 6x100/40G fiber ports
8520-48XT-6C-DC-F	Extreme 8520-48XT Switch with front-back airflow; Ships with two DC power supplies, six fans, one 4-post rack mount kit; Supports 48x10/1G copper ports and 6x100/40G fiber ports
8520-48XT-6C-DC-R	Extreme 8520-48XT Switch with back-front airflow; Ships with two DC power supplies, six fans, one 4-post rack mount kit; Supports 48x10/1G copper ports and 6x100/40G fiber ports
8000-PRMR-LIC-P	Extreme 8000 Premier Feature License (includes Integrated Application Hosting)
8820-40C	Extreme 8820-40C base unit with 40x100GE/40GE QSFP28 ports with 2 unpopulated power supply slots, 6 unpopulated fan slots and a 4-post rack mount kit
8820-40C-AC-F	Extreme 8820-40C with Front-Back airflow. Base unit with 40x100GE/40GE QSFP28 ports with 2 AC power supplies, 6 fan modules and a 4-post rack mount kit
8820-40C-AC-R	Extreme 8820-40C with Back-Front airflow. Base unit with 40x100GE/40GE QSFP28 ports with 2 AC power supplies, 6 fan modules and a 4-post rack mount kit
8820-40C-DC-F	Extreme 8820-40C with Front-Back airflow. Base unit with 40x100GE/40GE QSFP28 ports with 2 DC power supplies, 6 fan modules and a 4-post rack mount kit
8820-40C-DC-R	Extreme 8820-40C with Back-Front airflow. Base unit with 40x100GE/40GE QSFP28 ports with 2 DC power supplies, 6 fan modules and a 4-post rack mount kit
8820-80C	Extreme 8820-80C. Base unit with 80x100GE/40GE QSFP28 ports with 4 unpopulated power supply slots, 4 unpopulated fan slots and a 4-post rack mount kit
8820-80C-AC-F	Extreme 8820-80C with Front-Back airflow. Base unit with 80x100GE/40GE QSFP28 ports with 4 AC power supplies, 4 fan modules and a 4-post rack mount kit
8820-80C-AC-R	Extreme 8820-80C with Back-Front airflow. Base unit with 80x100GE/40GE QSFP28 ports with 4 AC power supplies, 4 fan modules and a 4-post rack mount kit

Supported devices	Description
8820-80C-DC-F	Extreme 8820-80C with Front-Back airflow. Base unit with 80x100GE/40GE QSFP28 ports with 4 DC power supplies, 4 fan modules and a 4-post rack mount kit
8820-80C-DC-R	Extreme 8820-80C with Back-Front airflow. Base unit with 80x100GE/40GE QSFP28 ports with 4 DC power supplies, 4 fan modules and a 4-post rack mount kit

Supported power supplies, fans, and rack mount kits

XN-ACPWR-1600W-F	SLX 9740 Fixed AC 1600W Power Supply Front to Back. Power cords not included Extreme 8820 Fixed AC 1600W Power Supply Front to Back. Power cords not included
XN-ACPWR-1600W-R	SLX 9740 Fixed AC 1600W Power Supply Back to Front. Power cords not included. Extreme 8820 Fixed AC 1600W Power Supply Back to Front. Power cords not included
XN-DCPWR-1600W-F	SLX 9740 Fixed DC 1600W Power Supply Front to Back. Power cords not included Extreme 8820 Fixed DC 1600W Power Supply Front to Back. Power cords not included
XN-DCPWR-1600W-R	Extreme 8820 Fixed DC 1600W Power Supply Back to Front. Power cords not included.
XN-FAN-003-F	SLX 9740 FAN Front to Back airflow for SLX9740-40C Extreme 8820 FAN Front to Back airflow for 8820-40C
XN-FAN-003-R	SLX 9740 FAN Back to Front airflow for SLX9740-40C Extreme 8820 FAN Back to Front airflow for 8820-40C
XN-FAN-004-F	SLX 9740 FAN Front to Back airflow for SLX9740-80C Extreme 8820 FAN Front to Back airflow for 8820-80C
XN-FAN-004-R	SLX 9740 FAN Back to Front airflow for SLX9740-80C Extreme 8820 FAN Back to Front airflow for 8820-80C
XN-4P-RKMT299	2-Post Rail Kit for SLX 9740-40C
XN-2P-RKMT300	2-Post Rail Kit for SLX 9740-80C
XN-4P-RKMT301	4-Post Rail Kit for SLX 9740-80C
XN-4P-RKMT302	4-Post Rail Kit for SLX 9740-40C
XN-ACPWR-750W-F	AC 750W PSU, Front to Back Airflow supported on VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520

XN-ACPWR-750W-R	AC 750W PSU, Back to Front Airflow supported on VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520
XN-DCPWR-750W-F	DC 750W PSU, Front to Back Airflow supported on VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520
XN-DCPWR-750W-R	DC 750W PSU, Back to Front Airflow supported on VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520
XN-FAN-001-F	Front to back Fan for use in VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520
XN-FAN-001-R	Back to Front Fan for use in VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520
XN-4P-RKMT298	Four post rack mount rail kit supported on VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520
XN-2P-RKMT299	Two post rack mount rail kit supported on VSP 7400, SLX 9150, SLX 9250, X695, Extreme 8720, Extreme 8520, Extreme 8820
XN-2P-RKMT300	2-Post Rail Kit for Extreme 8820-80C
XN-4P-RKMT301	4-Post Rail Kit for Extreme 8820-80C
XN-4P-RKMT302	4-Post Rail Kit for Extreme 8820-40C

Supported Optics and Cables

For a complete list of all supported optics, see **Extreme Optics** at https://optics.extremenetworks.com/.

Supported FEC modes

SLX 9250 and Extreme 8720

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
100G	Passive DAC	RS-FEC	RS-FEC Disabled
100G	SR4	RS-FEC	RS-FEC Disabled
100G	LR4	Disabled	RS-FEC Disabled
25G	Breakout DAC SR	Auto-Neg	RS-FEC FC-FEC Auto-Neg Disabled
25G	Breakout SR4	FC-FEC	RS-FEC FC-FEC Disabled
25G	Breakout LR	RS-FEC	RS-FEC FC-FEC Disabled

SLX 9740 and Extreme 8820

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
100G	Passive DAC	RS-FEC	RS-FEC Disabled
100G	SR4	RS-FEC	RS-FEC Disabled
100G	LR4	Disabled	RS-FEC Disabled
25G	Breakout DAC SR	FC-FEC	FC-FEC RS-FEC Disabled
25G	Breakout SR4	FC-FEC	FC-FEC RS-FEC Disabled

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
25G	Breakout LR	RS-FEC	RS-FEC FC-FEC Disabled

SLX 9150 and Extreme 8520

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
100G	Passive DAC	RS-FEC	RS-FEC Disabled
100G	SR4	RS-FEC	RS-FEC Disabled
100G	LR4	Disabled	RS-FEC Disabled
25G(Native)	DAC	Auto-Neg	RS-FEC FC-FEC Auto-Neg Disabled
25G(Native)	SFP	FC-FEC	RS-FEC FC-FEC Disabled
25G(Native)	LR	RS-FEC	RS-FEC FC-FEC Disabled

SLX 9540 and SLX 9640

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
100G	Passive DAC	RS-FEC	RS-FEC Disabled
100G	SR4	RS-FEC	RS-FEC Disabled
100G	LR4	Disabled	RS-FEC Disabled
25G	Breakout LR	RS-FEC	RS-FEC FC-FEC Disabled

Software Download and Upgrade

For more information about the various methods of upgrading to SLX-OS 20.6.1 see the *Extreme SLX-OS Software Upgrade Guide.*

Image files

Download the following images from www.extremenetworks.com.

Image file name	Description
SLX-OS_20.6.1a.tar.gz	SLX-OS 20. 6.1a software
SLX-OS_20. 6.1a_mibs.tar.gz	SLX-OS 20. 6.1a MIBS
SLX-OS_20. 6.1a.md5	SLX-OS 20. 6.1a md5 checksum
SLX-OS_20. 6.1a-digests.tar.gz	SLX-OS 20. 6.1a sha checksum
SLX-OS_20. 6.1a-releasenotes.pdf	Release Notes

Baseboard Management Controller (BMC) firmware upgrade

- With SLX-OS 20.6.1 onwards, BMC firmware update will be performed along with SLX-OS update on BMC supported platforms. This upgrade will happen only if the installed BMC firmware version is older than the version bundled along with the SLX-OS firmware. Supported SLX platforms are Extreme 8520, Extreme 8720, Extreme 8820 and SLX 9740.
- No new SLX-OS CLI is introduced for BMC firmware upgrade, as this being an implicit BMC firmware update.
- With this new feature, BMC firmware image is bundled as part of SLX-OS image. When the user updates the OS, and, if BMC firmware version on the device is found to be older than the BMC image bundled with SLX-OS image, the BMC image bundled with SLX shall be updated on BMC along with SLX-OS update.
- By design, only BMC firmware upgrade is supported – downgrade is not supported.
- BMC firmware upgrade will occur with all supported SLX-OS upgrade methods – incremental, full install and net install
- In case the BMC upgrade fails, “firmware download” of SLX-OS will continue without any disruption.
- During BMC upgrade, IPMI/BMC connectivity will be impacted. Hence intermittent RASLOGS (e.g. FW-1404 and EM-1050, HIL-1404 etc) from environmental monitoring daemon may be observed. These intermittent RASLOG messages will disappear only after the device is reloaded.
- Existing BMC configuration will be preserved even after the BMC is updated.
- Limitations -
  - There is a small increase in SLX-OS installation time (around 4 to 7 minutes), if BMC firmware is also upgraded.
  - Intermittent RASLOGS or FFDC messages are generated due to interruption at BMC/IPMI channel.

Extreme 8820

To / From	20.4.3/a/b	20.5.1/a	20.5.2a	20.6.1	20.6.1a
20.4.3 (Factory Image)	For upgrade: normal firmware download / coldboot				
20.5.1/a					
20.5.2a					
20.6.1					
20.6.1a					

Extreme 8720

To / From	20.3.2/a-h	20.3.4/a-c	20.4.1x, 20.4.2x	20.4.3/a/b	20.5.1/a	20.5.2a	20.6.1	20.6.1a
20.3.2/a-h	For upgrade: normal firmware download / coldboot For downgrade: full install							
20.3.4/a-c	For upgrade and downgrade: normal firmware download / coldboot							
20.4.1x, 20.4.2x								
20.4.3/a/b								
20.5.1/a								
20.5.2a								
20.6.1								
20.6.1a								

Extreme 8520

To / From	20.3.3	20.3.4/a -c	20.4.1x, 20.4.2x	20.4.3/a /b	20.5.1/a	20.5.2a	20.6.1	20.6.1a
20.3.3	For upgrade and downgrade: normal firmware download / coldboot							
20.3.4/a -c								
20.4.1x, 20.4.2x								
20.4.3/a /b								
20.5.1/a								
20.5.2a								
20.6.1								
20.6.1a								

SLX 9740

To / From	20.3.2/a -h	20.3.4/a -c	20.4.1x, 20.4.2x	20.4.3/a /b	20.5.1/a	20.5.2a	20.6.1	20.6.1a
20.3.2/a -h	For upgrade: normal firmware download / coldboot For downgrade: full install							
20.3.4/a -c	For upgrade and downgrade: normal firmware download / coldboot							
20.4.1x, 20.4.2x								
20.4.3/a /b								
20.5.1/a								
20.5.2a								
20.6.1								
20.6.1a								

Note:

For SLX 9740, downgrade to any 20.2.2x version needs to be done in two steps, with an intermediate step for downgrading to 20.2.2c and then to 20.2.x from 20.2.3x or higher. This restriction is not applicable for upgrade/downgrade between 20.2.3x and 20.3.x releases.

SLX 9540 and SLX 9640

<table>
<tr><th>To
From</th><th>20.3.2/a-h</th><th>20.3.4/a-c</th><th>20.4.1x, 20.4.2x</th><th>20.4.3/a/b</th><th>20.5.1/a</th><th>20.5.2a</th><th>20.6.1</th><th>20.6.1a</th></tr>
<tr><td>20.3.2/a-h</td><td colspan="8">For upgrade: normal firmware download / coldboot
For downgrade: full install</td></tr>
<tr><td>20.3.4/a-c</td><td colspan="8" rowspan="6">For upgrade and downgrade: normal firmware download / coldboot</td></tr>
<tr><td>20.4.1x, 20.4.2x</td></tr>
<tr><td>20.4.3/a/b</td></tr>
<tr><td>20.5.1/a</td></tr>
<tr><td>20.5.2a</td></tr>
<tr><td>20.6.1</td></tr>
<tr><td>20.6.1a</td></tr>
</table>

Notes:

- Upgrade to 20.3.x from earlier releases requires “fullinstall” due to change in glibc.
- Downgrading from 20.3.x/20.2.2x/20.2.3x to 20.1.1 requires ‘fullinstall’ option for all platforms due to a change in glibc

SLX 9150 and SLX 9250

<table>
<tr><th>To
From</th><th>20.3.2/a-h</th><th>20.3.4/a-c</th><th>20.4.1x, 20.4.2x</th><th>20.4.3/a/b</th><th>20.5.1/a</th><th>20.5.2a</th><th>20.6.1</th><th>20.6.1a</th></tr>
<tr><td>20.3.2/a-h</td><td colspan="8">For upgrade: normal firmware download / coldboot
For downgrade: full install</td></tr>
<tr><td>20.3.4/a-c</td><td colspan="8" rowspan="7">For upgrade and downgrade: normal firmware download / coldboot</td></tr>
<tr><td>20.4.1x, 20.4.2x</td></tr>
<tr><td>20.4.3/a/b</td></tr>
<tr><td>20.5.1/a</td></tr>
<tr><td>20.5.2a</td></tr>
<tr><td>20.6.1</td></tr>
<tr><td>20.6.1a</td></tr>
</table>

Upgrade and Downgrade considerations for Threshold Monitor configuration:

Downgrade Considerations:

1. If configured value for Cpu "limit" exceeds valid range in older release [0-80] then downgrade will be blocked with error. User can reconfigure Cpu “limit” in the range [0-80] and downgrade.
2. If configured value for Memory "high-limit" exceeds valid range in older release [0-80] or if it is less than the default value of "limit" in older release [60], then downgrade will be blocked with error. User can reconfigure Memory “high-limit” in the range [60-80] and downgrade.
3. If the startup file has “actions” configured as “snmp” or “all”, then config replay process triggered in firmware full-install downgrade, will lead all the corresponding threshold-monitor CLI parameters, such as poll, retry, to reset to respective default values.

Upgrade Considerations:

1. If the startup file has “Memory limit and /or low-limit” configured, then config replay process triggered in firmware full-install downgrade, will lead all the corresponding threshold-monitor CLI parameters, such as poll, retry, to reset to respective default values.

SLX TPVM Support Matrix

SLX Build	SLX 9150/9250	Extreme 8520	Extreme 8720
20.4.2/a-b	TPVM 4.1.1 and later	TPVM 4.4.0 and later	TPVM 4.2.2 and later
20.4.3/a	TPVM 4.2.x and later	TPVM 4.4.0 and later	TPVM 4.2.2 and later
20.5.1/a	TPVM 4.2.5 and later	TPVM 4.4.0 and later	TPVM 4.2.5 and later
20.5.2a	TPVM 4.4.0 and later	TPVM 4.4.0 and later	TPVM 4.4.0 and later
20.5.3/a	TPVM 4.5.0 and later	TPVM 4.5.0 and later	TPVM 4.5.0 and later
20.6.1	TPVM 4.5.4 and later	TPVM 4.5.4 and later	TPVM 4.5.4 and later
20.6.1a	TPVM 4.5.4 and later	TPVM 4.5.4 and later	TPVM 4.5.4 and later

Upgrading the TPVM without configuration persistence (Legacy upgrade method)

Upgrading TPVM from 4.0.x or 4.1.x to 4.2.x, 4.3.x, 4.4.x, 4.5.x

Consider the following when upgrading TPVM from 20.1.2x , 20.2.2/x to 20.2.3x, 20.3.1 to 20.3.2x, 20.3.3, 20.3.4x, 20.4.x, 20.5.x

- SLX-OS 20.3.x, 20.2.3/x has TPVM 4.2.x. SLX-OS 20.1.2x variants have TPVM 4.0.x, which is based on Ubuntu18.
- To upgrade from TPVM 4.0 to latest, do the following:
  - Upgrade to SLX-OS 20.3.x, 20.2.3/x, 20.4.x while the existing TPVM installation continues to run
  - Remove the existing TPVM using the **tpvm stop** and **tpvm uninstall** commands.
  - Copy the new tpvm-4.x.x-0.amd64.deb to /tftpboot/SWBD2900 on the SLX device.
  - Install TPVM 4.x.x using the **tpvm install** or **tpvm deploy** command.
    Note that any additional TPVM disks, including vdb (implicitly created by TPVM 4.0.x or 4.1.x), are preserved with data during the previous steps.
  - If you need to remove the disks and start clean, then use the **tpvm uninstall force** command in place of **tpvm uninstall** in these steps. Alternatively, you can use **tpvm disk remove name <disk name>** to remove each additional disk manually. For example, tpvm disk remove name vdb.
  - To perform patch upgrade from TPVM 4.5.x to latest, do the following:
    - Upgrade to SLX-OS 20.5.x while the existing TPVM 4.5.x installation continues to run
    - Copy the new tpvm_inc_upg-4.5.X-X.amd64.deb to /tftpboot/SWBD2900 directory on the SLX device.
    - Install latest TPVM 4.5.x using **tpvm upgrade incremental** command

Notes:

- TPVM 4.5.x can be incrementally upgraded from TPVM 4.4.0 and beyond.
- TPVM 4.5.x supports full install upgrade/downgrade from TPVM 4.4.0.

Consider the following when you upgrade TPVM from releases earlier than SLX-OS 20.2.1 to SLX-OS 20.2.x:

- During startup, the latest TPVM creates an additional TPVM disk (named vdb) and creates an ext4 partition inside it (named vdb1).
- This additional disk partition is mounted at `/apps` inside TPVM.
- The disk uses all the free space available and reserved for TPVM (platform specific) TPVM disk quota.
- If you are running an older TPVM and have the additional TPVM disks already created, it is recommended and as a best practice to make a backup and then delete the old disks. Use the **tpvm disk remove name <disk name>** command to remove the disk, which requires TPVM to be started if not already running.
- Uninstall the older TPVM using the **tpvm stop** and **tpvm uninstall** command.
- Install the new TPVM package using the **tpvm install** or **tvpm deploy** command.

Alternatively, after SLX has been upgraded, you can use one command, **tpvm uninstall force**, to uninstall the TPVM and delete all the disks in the TPVM disk pool.

After tpvm uninstall force, it is recommended to perform “no deploy” from tpvm config.

Important: The **tpvm uninstall force** process is destructive and irreversible, causing all TPVM data to be lost. The process works only if the TPVM is installed on the system.

Entire TPVM Data is automatically backed up in SLX while doing "**tpvm stop**" and restored during the next "**tpvm start**". However, all the TPVM partitions data will be preserved. The data is preserved during "tpvm stop, uninstall" & "tpvm install". User installed applications in TPVM are not preserved. During TPVM upgrade, it is advised to take EFA data backup from TPVM using "**efa system backup**" and transfer the backup file outside TPVM to be completely safe. EFA release note document has a section for TPVM upgrade scenario and entire steps are mentioned in that document.

"**When EFA is installed on TPVM, "tpvm stop" followed by "uninstall" or "no deploy" tpvm config command, automatically takes only EFA database backup and not a backup of EFA installation."**

Notes:

Security updates are added to the TPVM image and also to the separate Debian file used for incremental TPVM update. Main TPVM image size is ~2.0 GB and the TPVM incremental update Debian file size is ~0.5 GB. You must have at least 1GB of free space on the switch before proceeding with the tpvm upgrade incremental command. The latest TPVM 4.5.14 has security updates till July 21st, 2023.

Ubuntu Linux distribution on TPVM is upgraded to 20.04 LTS from TPVM version 4.6.0 onwards.
As Ubuntu Linux distribution on TPVM is upgraded to 20.04 LTS incremental upgrade is not supported, upgrading TPVM from 4.5.x to 4.6.x needs a full upgrade.
Please refer to the respective TPVM 4.6.x Release notes for more information
The latest TPVM 4.6.9 has security updates till 1st March, 2024.
Main TPVM image size of 4.6.9 is ~2.0 GB and the TPVM incremental update Debian file size is ~0.8 GB.

VDB disk size for EFA has changed to 40 GB to accommodate storage for snapshot and the remaining space is considered as reserved space, for the new TPVM installation.

Upgrading the TPVM with configuration persistence – Recommended method

Consider the following when upgrading TPVM from 20.1.2x, 20.2.2/x, 20.3.x to 20.3.2x, 20.3.3, 20.3.4x, 20.4.x

1. SLX-OS old version with tpvm instance installed/deployed and few related config may be set.

2. SLX-OS upgrade done vide firmware download CLI command.
3. Across SLX-OS reboots, old TPVM too shall reboot if auto-boot config was there, else shall be there in installed state.
   a. tpvm stop
   b. tpvm uninstall
   c. (or) tpvm uninstall force – if you plan to delete disk vdb (i.e. the TPVM /apps partition).

Note:

1. New mode like old mode, create disk vdb (/apps) by default upon first install/deploy or reuse previously existing partition.
2. Currently the new mode does not support new disk creation. The **tpvm disk add** command can be used.

4. As simple example for new mode of deploying TPVM:
   a. Copy new TPVM debian Image under /tftpboot/SWBD2900. Only one file should be there and no subfolder should be present/created within this folder.
   b. Deploy TPVM in Config Mode:

```
SLX # config terminal
SLX (config)# tpvm TPVM
SLX (config-tpvm-TPVM) # deploy
SLX (config-tpvm-TPVM) # end
```

   Above will install and start any TPVM image kept under /tftpboot/SWBD2900.
   c. Deploy TPVM with some configuration and later update any runtime configuration:

```
SLX # config terminal
SLX (config)# tpvm TPVM
SLX (config-tpvm-TPVM) # password newpassword
SLX (config-tpvm-TPVM) # interface management ip 10.25.24.21/24
SLX (config-tpvm-TPVM) # auto-boot
SLX (config-tpvm-TPVM) # hostname newhostname
SLX (config-tpvm-TPVM) # timezone Europe/Stockholm
SLX (config-tpvm-TPVM) # deploy
SLX (config-tpvm-TPVM) # end
SLX # config terminal
SLX (config)# tpvm TPVM
SLX (config-tpvm-TPVM) # hostname oldhostname
SLX (config-tpvm-TPVM) # no timezone
SLX (config-tpvm-TPVM) # exit
```

Note:

a. Now, say, if the **tpvm config hostname xyz** command is used. It will still work and apply on TPVM instance. But this configuration shall not be persisted in SLX Database and will become inconsistent. Same is true for any other configuration done in old way.

b. As in above example, password, management configuration should always be set before deploy. If required later, refer User Guide and use tpvm stop, start for such update/maintenance reason.
c. If **tpvm unstall force** command is used, then you will need to perform a **no deploy** and **deploy** in the new mode.

For more information on configuring TPVM Configuration Persistence, refer the 'Management Configuration Guide' for this version.

TPVM Migration

Upgrading the SLXOS to 20.3.2x, 20.3.3, 20.3.4x, 20.4.x, 20.5.x results in the creation of TPVM entries in SLX running-config implicitly (This happens when upgrading TPVM from SLXOS 20.1.2x, SLXOS 20.2.2/x, SLXOS 20.3.x to SLXOS 20.3.2x, 20.3.3, 20.3.4x)

Consider the following when upgrading TPVM from SLXOS 20.1.2x, SLXOS 20.2.2/x, SLXOS 20.3.x to SLXOS 20.3.2x, 20.3.3, 20.3.4x, 20.4.x, 20.5.x

a. SLX-OS old version with tpvm instance installed/deployed and few related config may be set in legacy exec CLI method
b. SLX-OS upgrade done with “firmware download” CLI command.
c. Across SLX-OS reboot, TPVM entries are created in SLX running-config implicitly as part of the TPVM migration feature
d. Check the configuration are persisted in TPVM using the CLI “show running configuration tpvm”
e. For TPVM upgrade to the latest version use command “tpvm upgrade … “
f. For TPVM upgrade incremental to the latest patch use command “ tpvm upgrade incremental …”

Limitations and Restrictions

Copy flash to startup and reload with TPVM

setNTPServer and setLDAPServer statuses are reported as failed in the output of the show tpvm status-history. After reload, TPVM is expected to be running when the above configurations are re-applied. When the TPVM is not running and the NTP and LDAP configurations are applied, these errors are seen. This is a limitation as reapplying NTP and LDAP configurations are not supported.

You need to have minimum 1GB free space on TPVM when you try to perform the security patch upgrade using the command tpvm upgrade incremental …

TPVM upgrade incremental command and file support is available only from 4.5 if we try to perform the incremental upgrade from 4.4.0 to latest, the upgrade fails and ask to perform the tpvm upgrade.

TPVM upgrade incremental command will not be supported when you try TPVM deploy in config mode and TPVM upgrade incremental command will not support with snapshot option.

Do not use the **tpvm upgrade incremental** command to upgrade the patches with *tpvm-4.X.X-X.amd64.deb*. Use the *tpvm_inc_upg-4.X.X-X.amd64.deb* image file to perform incremental upgrades.

Similarly, do not use the *tpvm_inc_upg-4.X.X-X.amd64.deb* image file to perform full upgrade. Do not use this file to perform **tpvm deploy** in *config mode* and *option*.

TPVM Migration

The following table lists the various TPVM configurations and their migration status.

Configuration	Migration State	Notes
tpvm auto-boot	Migrated	
tpvm disk	Not Migrated	Disk configuration is not supported in the configuration mode, and therefore, not migrated.
tpvm password	Migrated	Only the old password is migrated. This is due to the password being encrypted and stored and it is not possible to know if the password was changed during the migration.
tpvm config ntp	Migrated	
tpvm config dns	Migrated	
tpvm config ldap	Migrated	Secure LDAP require certificates. It is assumed that certificates are already downloaded and installed. Certificates are not validated during this migration. A notification will be sent to the user to reconfigure LDAP certificate settings.
tpvm config hostname	Migrated	

Configuration	Migration State	Notes
tpvm config timezone	Migrated	
tpvm deploy <interface> allow-pwless	Not Migrated	This is the new default configuration and is not migrated.
tpvm deploy mgmt [dhcp | static]	Migrated	
tpvm deploy insight	Not Migrated	Insight interface configuration is not supported when configuring using the Privilege Execution Mode commands.
tpvm config ldap ca-cert	Not Migrated	Configuring the TPVM LDAP ca certificate
tpvm config trusted-peer	Not Migrated	All trusted-peer configurations are not migrated.

Additional information on TPVM Commands

Following list of TPVM commands under exec mode may not be supported (Not recommended to use from 4.2.x and later) in the future releases. The equivalent commands will continue to be available under config mode. Please refer to latest CLI documentation.

- `tpvm config dns`
- `tpvm config hostname`
- `tpvm config ldap`
- `tpvm config ntp`
- `tpvm config timezone`
- `tpvm config trusted-peer`
- `tpvm auto-boot`
- `tpvm deploy`
- `tpvm password`

Port macro restrictions on breakout port configuration on SLX 9740

A port macro (PM) is a port group. Each PM has 4 ports, which are contiguous. PM0 has ports 0/1-0/4, PM1 has ports 0/5-0/8, PM2 has ports 0/9-0/12, and so on.

There are 9 PMs in the SLX 9740-40C and 18 PMs in the SLX 9740-80C. Only the odd ports can be split to 4x10G or 4x25G using the breakout cables: 0/1, 0/3, 0/9, 0/11, 0/13, 0/15, 0/17, 0/19, 0/21, 0/23, 0/25, 0/27, 0/29, 0/31, 0/33, 0/35, 0/37, 0/39, 0/41, 0/43, 0/49,

0/51, 0/53, 0/55, 0/57, 0/59, 0/61, 0/63, 0/65, 0/67, 0/69, 0/71, 0/73, 0/75, 0/77, and 0/79. Breaking out these ports using the breakout cables results in 72 interfaces for the SLX 9740-40 and 144 interfaces for the SLX 9740-80C.

- Ports 5-8 and 45-48 cannot be broken up and are supported only in 100G.
- For any PM, 40G and 10G ports cannot coexist with 25G ports. The following configurations are not supported:

PM Configuration	Examples
If any port is configured as 40G or 4x10G breakout, no 4x25G breakout is allowed unless the 40G ports will be removed as part of the breakout operation.	• If 0/3 or 0/4 is 40G, you cannot configure 0/1 as 4x25G breakout. • If 0/1 is 4x10G breakout, you cannot configure 0/3 as 4x25G breakout. • If 0/3 is 4x10G breakout, you cannot configure 0/1 as 4x25G breakout. • If 0/1 or 0/2 is 40G, you can configure 0/1 as 4x25G breakout because 0/1 and 0/2 will be removed. • If 0/3 or 0/4 is 40G, you can configure 0/3 as 4x25G breakout because 0/3 and 0/4 will be removed.
If 4x25G breakout is configured, no 40G or 4x10G.	• If 0/1 is configured as 4x25G breakout, you cannot configure 0/3 or 0/4 as 40G. • If 0/1 is configured as 4x25G breakout, you cannot configure 0/3 as 4x10G breakout. • If 0/3 is configured as 4x25G breakout, you cannot configure 0/1 or 0/2 as 40G. • If 0/3 is configured as 4x25G breakout, you cannot configure 0/1 as 4x10G breakout.

QoS

- PCP remarking is not supported for SLX 9740 and Extreme 8820.
- Egress rate limiting in a Bridge Domain configuration is not supported for SLX 9740 and Extreme 8820.
- DSCP-COS map is not supported for SLX 9740 and Extreme 8820.

Others

- sflow sampling does not work for VLL when BUM rate limiting is applied on interface in SLX 9740

- sflow sample traffic to CPU is rate limited. You can use the **qos cpu slot** command to change the rate.
- When Resilient Hashing CLI is enabled or disabled, or the *max-path* value is changed, it may cause **BFD sessions** in **related VRFs** to go down. However, **BFD sessions in unrelated VRFs will not be affected.**
- Resilient Hashing feature is supported only on SLX 9150, SLX 9250, SLX 9740, Extreme 8720 and Extreme 8520. Other platforms are not supported.
- Resilient Hashing supports 32K flowset entries for Extreme 8720 and Extreme 8520.

Open Config Telemetry Support

- User authentication not supported.
- gNMI calls through inband interfaces not supported.
- Usage of wild cards is not supported.
- gNMI SET is not supported.
- gNMI ON CHANGE subscription is not supported.

SNMP

- Not all counters related to UDP, and TCP MIBs are supported.
- Configuring an in-band port into a Management VRF requires SNMP agent reload.

Maximum Logical Interfaces or LIFs scale

Maximum Logical Interface (LIF) (Port-VLAN/Port-Bridge Domain (BD)) associations supported on SLX 9150, SLX 9250, Extreme 8520, Extreme 8720 is 14200. Since VLAN and BD resources share the same hardware table memory space, the max scale of one has a trade-off with the scale of the other. That is, for example, the maximum Port-BD associations cannot be scaled to 14200 when the combined scale of VLAN and BDs exceeds 8096.

IPv6 Manageability support on TPVM

- The TPVM management interface can be configured with a single IPv6 address. You can configure an IPv4 address in addition to the IPv6 address. Configuring IPv4 address is optional.
- tpvm stop and tpvm start commands must be issued to configure the TPVM management interface's IPv4 and IPv6 address.

Removal of DF towards IP Fabric (Local Bias support for LVTEP)

- Single-homed LVTEP client (spine uplink DOWN in one of the MCT nodes) is not supported.
- Need to have backup routing over ICL to reach the spines in case of uplink failure.

ICMP and ICMPv6 redirect

Enable/disable ICMP and ICMPv6 redirect are only available on SLX 9540 and SLX 9640. On these platforms, these are only supported on physical ports.

Transporting IPv6 traffic over GRE IPv4 Tunnel

- If GRE feature is enabled, IPv6 ACL filters to drop OSPFv3 packets will not work for SLX 9740 and Extreme 8820 platforms.
- Multicast traffic is not supported over IPv6 GRE overlay. Multicast packets will be dropped.
- IPv6 ACL is not supported on GRE tunnel.
- IPv4 and IPv6 control packets over the GRE Tunnel are not accounted for in the GRE tunnel statistics.
- DSCP value from the inner IPv6 packet is not copied to outer GRE header on SLX 9540 and SLX 9640 platforms.

Flow Based Mirroring

(Applicable to SLX 9150, SLX 9250, Extreme 8720 and Extreme 8520 platforms)

- Flow based ingress mirroring does not support port-channel port as a mirroring source port.
- Flow based ingress mirroring supports VLAN as a mirroring source port, but VLAN range is not supported.

Open Defects

The following software defects are open in SLX-OS 20.6.1a as of April 2024:

Parent Defect ID:	SLXOS-64409	**Issue ID:**	SLXOS-64606
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4a
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	TPVM configuration is lost when the device reloads with default configuration during firmware update.		
Condition:	Issue happens when "default-config" option is provided in "firmware download" command.		
Workaround:	Execute following commands - "copy default-config startup-config" and then "firmware download" command without "default-config" option.		

Parent Defect ID:	SLXOS-65249	**Issue ID:**	SLXOS-65249
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	-	**Technology:**	-
Symptom:	In SLX 9740, Traffic Convergence takes ~3 seconds.		
Condition:	Nexthop change takes place in ECMP prefixes.		

Parent Defect ID:	SLXOS-66144	**Issue ID:**	SLXOS-66144
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	-	**Technology:**	-
Symptom:	Traffic takes more than 900 msec in the N-S direction when a port channel between the Gateway and Border Leaf fails. Minimum link is configured over this port channel and the trigger is the shutdown of one interface belonging to the port channel.		
Condition:	Minimum-link is configured between border leaf and gateway. When a port channel member between them is shutdown in the BL side, the PO is expected to fail. The GW should redirect the traffic to the other border leaf. This was seen to take more than 900 ms. The GW is a SLX 9640.		

Parent Defect ID:	SLXOS-66738	**Issue ID:**	SLXOS-66738

Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	-	**Technology:**	-
Symptom:	In port mirroring configuration if destination interface is a port-channel and source interface is either a port-channel or member of a port-channel then destination port-channel interface goes down.		
Condition:	Issue is seen if in port mirroring configuration destination interface is configured as a port-channel.		

Parent Defect ID:	SLXOS-68095	**Issue ID:**	SLXOS-68095
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2
Technology Group:	-	**Technology:**	-
Symptom:	Convergence of L3VNI Asymmetric traffic takes 30 seconds.		
Condition:	Reloading one of the Multi-homed peer.		

Parent Defect ID:	SLXOS-70172	**Issue ID:**	SLXOS-70172
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Unexpected reload of device.		
Condition:	Device reloaded unexpectedly on execution of execution of "clear ip route all vrf" with "prefix-independent-convergence-static" already configured.		

Parent Defect ID:	SLXOS-70592	**Issue ID:**	SLXOS-70592
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD sessions flap while rebooting a leaf node		
Condition:	In an MCT pair, BFD sessions flap while rebooting a leaf node with SRIOV clients		

Parent Defect ID:	SLXOS-71412	**Issue ID:**	SLXOS-71901
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2b_CVR
Technology Group:	MPLS	**Technology:**	MPLS Traffic Engineering
Symptom:	Unexpected reload is seen due to MPLSD module reset.		
Condition:	MPLSD module reset due to the message queue becoming full on MPLS.		

Parent Defect ID:	SLXOS-73347	**Issue ID:**	SLXOS-73347
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	In VPLS environments, sometimes MAC is not learned on AC ports resulting in flooding of L2 traffic destined for the missed MAC.		
Condition:	In VPLS environments, MAC is not learned on AC ports because of Ingress Vlan Editing table full which could happen under the following conditions: - More than one tag-type is configured on the system. - Many different types of Vlan editing configured on the system. - Issue is seen on 9740/8820 only		
Workaround:	Changes in the configuration could resolve the issue. Different tag-types need more Vlan editing resources. Reducing the number of different tag-types and reconfiguring the port could resolve the issue.		

Parent Defect ID:	SLXOS-74036	**Issue ID:**	SLXOS-74036
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4b
Technology Group:	IP Multicast	**Technology:**	IGMP - Internet Group Management Protocol
Symptom:	mc_hms daemon reload.		
Condition:	On reception of IGMP packet (AF_IGMP_SNOOP,0x34) with non-multicast destination MAC.		

Parent Defect ID:	SLXOS-74529	**Issue ID:**	SLXOS-74529

Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3ja
Technology Group:	MPLS	**Technology:**	MPLS VLL - Virtual Leased Line
Symptom:	IGMP traffic via VPLS VLL is getting dropped in hardware		
Condition:	IGMP traffic passed via VPLS VLL is getting dropped in SLX-9740 and Extreme-8820 platforms		

Parent Defect ID:	SLXOS-75012	**Issue ID:**	SLXOS-75012
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3
Technology Group:	Traffic Management	**Technology:**	Traffic Queueing and Scheduling
Symptom:	QoS user map TC-to-COS is not allowed to configure on interface (Physical/Logical).		
Condition:	When we apply the service policy first on the interface (physical/Logical) before QoS Map		

The following software defects are open in SLX-OS 20.6.1 as of March 2024:

Parent Defect ID:	SLXOS-64409	**Issue ID:**	SLXOS-64606
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.3.4a
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	TPVM configuration is lost when the device reloads with default configuration during firmware update.		
Condition:	Issue happens when "default-config" option is provided in "firmware download" command.		
Workaround:	Execute following commands - "copy default-config startup-config" and then "firmware download" command without "default-config" option.		

Parent Defect ID:	SLXOS-65249	**Issue ID:**	SLXOS-65249
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1
Technology Group:	-	**Technology:**	-
Symptom:	In SLX 9740, Traffic Convergence takes ~3 seconds.		

Condition:	Nexthop change takes place in ECMP prefixes.

Parent Defect ID:	SLXOS-66144	**Issue ID:**	SLXOS-66144
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1
Technology Group:	-	**Technology:**	-
Symptom:	Traffic takes more than 900 msec in the N-S direction when a port channel between the Gateway and Border Leaf fails. Minimum link is configured over this port channel and the trigger is the shutdown of one interface belonging to the port channel.		
Condition:	Minimum-link is configured between border leaf and gateway. When a port channel member between them is shutdown in the BL side, the PO is expected to fail. The GW should redirect the traffic to the other border leaf. This was seen to take more than 900 ms. The GW is a SLX 9640.		

Parent Defect ID:	SLXOS-65379	**Issue ID:**	SLXOS-66289
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.3j
Technology Group:	MPLS	**Technology:**	MPLS VPLS - Virtual Private LAN Services
Symptom:	MPLS encapsulated 'Unicast ICMP with destination MAC starts on 4' traffic fails to forward from 9740(PHP/P) to 9850(PE).		
Condition:	a) Establish VPLS session between 9850 & MLX with adding 9740 as Transit Node. b) Initiate traffic with destination MAC starts with 4 from CE to CE.		

Parent Defect ID:	SLXOS-66738	**Issue ID:**	SLXOS-66738
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1
Technology Group:	-	**Technology:**	-
Symptom:	In port mirroring configuration if destination interface is a port-channel and source interface is either a port-channel or member of a port-channel then destination port-channel interface goes down.		

Condition:	Issue is seen if in port mirroring configuration destination interface is configured as a port-channel.

Parent Defect ID:	SLXOS-68095	**Issue ID:**	SLXOS-68095
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.2
Technology Group:	-	**Technology:**	-
Symptom:	Convergence of L3VNI Asymmetric traffic takes 30 seconds.		
Condition:	Reloading one of the Multi-homed peer.		

Parent Defect ID:	SLXOS-70172	**Issue ID:**	SLXOS-70172
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Unexpected reload of device.		
Condition:	Device reloaded unexpectedly on execution of execution of "clear ip route all vrf" with "prefix-independent-convergence-static" already configured.		

Parent Defect ID:	SLXOS-70592	**Issue ID:**	SLXOS-70592
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD sessions flap while rebooting a leaf node		
Condition:	In an MCT pair, BFD sessions flap while rebooting a leaf node with SRIOV clients		

Parent Defect ID:	SLXOS-71412	**Issue ID:**	SLXOS-71901
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.2b_CVR
Technology Group:	MPLS	**Technology:**	MPLS Traffic Engineering

Symptom:	Unexpected reload is seen due to MPLSD module reset.
Condition:	MPLSD module reset due to the message queue becoming full on MPLS.

Parent Defect ID:	SLXOS-73347	**Issue ID:**	SLXOS-73347
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.2
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	In VPLS environments, sometimes MAC is not learned on AC ports resulting in flooding of L2 traffic destined for the missed MAC.		
Condition:	In VPLS environments, MAC is not learned on AC ports because of Ingress Vlan Editing table full which could happen under the following conditions: - More than one tag-type is configured on the system. - Many different types of Vlan editing configured on the system. - Issue is seen on 9740/8820 only		
Workaround:	Changes in the configuration could resolve the issue. Different tag-types need more Vlan editing resources. Reducing the number of different tag-types and reconfiguring the port could resolve the issue.		

Parent Defect ID:	SLXOS-74529	**Issue ID:**	SLXOS-74529
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.3ja
Technology Group:	MPLS	**Technology:**	MPLS VLL - Virtual Leased Line
Symptom:	IGMP traffic via VPLS VLL is getting dropped in hardware		
Condition:	IGMP traffic passed via VPLS VLL is getting dropped in SLX-9740 and Extreme-8820 platforms		

Parent Defect ID:	SLXOS-75012	**Issue ID:**	SLXOS-75012
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.3
Technology Group:	Traffic Management	**Technology:**	Traffic Queueing and Scheduling
Symptom:	QoS user map TC-to-COS is not allowed to configure on interface (Physical/Logical).		

Condition:	When we apply the service policy first on the interface (physical/Logical) before QoS Map

Defects Closed with Code Changes

The following software defects were closed in SLX-OS 20.6.1a with code changes as of April 2024.

Parent Defect ID:	SLXOS-73961	**Issue ID:**	SLXOS-73961
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	1. Additional SNMP Link Down Trap being sent as part of 'Protocol Down' state transition of Port-channel member interface 2. When Port-channel is Operationally Down, toggling member interface(s) was not sending SNMP Traps		
Condition:	1. During member addition to a LACP port-channel 2. When a Port-channel is Operationally Down, and any of its member interface is toggled		
Workaround:	NA		
Recovery:	NA		

Parent Defect ID:	SLXOS-75084	**Issue ID:**	SLXOS-75084
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	SAG IP is not reachable after reload.		
Condition:	Scale SAG config and reload.		
Workaround:	NA		
Recovery:	NA		

Parent Defect ID:	SLXOS-75714	**Issue ID:**	SLXOS-75714
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3

Technology Group:	Network Automation and Orchestration	**Technology:**	NETCONF - Network Configuration Protocol
Symptom:	NETCONF RPC error 'Wave Management Interface Client Is Not Available' is observed while changing the SLX configuration though EFA		
Condition:	When changing the SLX configuration though EFA		
Workaround:	NA		
Recovery:	NA		

Parent Defect ID:	SLXOS-75811	**Issue ID:**	SLXOS-75811
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.6.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	BGP daemon crashes with memory corruption.		
Condition:	When the overlay gateway is configured with VNI range beyond 8K.		
Workaround:	NA		
Recovery:	NA		

Parent Defect ID:	SLXOS-76002	**Issue ID:**	SLXOS-76002
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.6.1
Technology Group:	Monitoring	**Technology:**	Hardware Monitoring
Symptom:	The below 4 SNMP attributes related to the TxPower and RxPower, instead of displaying the aggregate values of all lane values of the port were wrongly displaying only the values of the first lane of the port. bcsiOptMonInfoTxPower (1.3.6.1.4.1.1588.3.1.8.1.2.1.3) bcsiOptMonInfoTxPowerVal (1.3.6.1.4.1.1588.3.1.8.1.2.1.4) bcsiOptMonInfoRxPower (1.3.6.1.4.1.1588.3.1.8.1.2.1.6) bcsiOptMonInfoRxPowerVal (1.3.6.1.4.1.1588.3.1.8.1.2.1.7)		
Condition:	The issue was happening when querying the TxPower and RxPower values of the ports through SNMP MIB OIDs. The issue		

	has now been fixed to display the aggregate of all the lane values of the port.

The following software defects were closed in SLX-OS 20.6.1 with code changes as of March 2024:

Parent Defect ID:	SLXOS-68208	**Issue ID:**	SLXOS-68208
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.3.2f
Technology Group:	Monitoring	**Technology:**	OAM - Operations, Admin & Maintenance
Symptom:	Failed to fetch the utilization-watermark stats on the "show interface stats utilization-watermark interface ethernet <x/x>".		
Condition:	In SLX 9540 device configured with "system interface utilization-watermark".		

Parent Defect ID:	SLXOS-69621	**Issue ID:**	SLXOS-70060
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.3.2g
Technology Group:	Layer 2 Switching	**Technology:**	LAG - Link Aggregation Group
Symptom:	Fail to add port to Link Aggregation Group		
Condition:	On removing a port from LACP LAG and add it again to same LAG, port fails to be part of LAG and will throw "[LACP-1005]" RAS log		
Workaround:	Remove all member ports of LAG and add them again.		

Parent Defect ID:	SLXOS-71342	**Issue ID:**	SLXOS-71538
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1d
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Complete traffic loss when hslagtd daemon crashes in primary MCT node		
Condition:	Cluster keep-alive is not disconnected, right after the daemon crash, triggering split-brain scenario which results in client ports also being shut in the secondary MCT node		

Recovery:	It will recover on its own when the primary MCT node is reloaded

Parent Defect ID:	SLXOS-71395	**Issue ID:**	SLXOS-71655
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.3
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP MIB(1.3.6.1.4.1.1588.3.1.12.1.1.1.3.1.60 and 1.3.6.1.4.1.1588.3.1.13.1.1.1.4.1) reporting very large value/zero CPU and memory utilization randomly.		
Condition:	While doing the snmpwalk for OID (1.3.6.1.4.1.1588.3.1.12.1.1.1.3.1.60 and 1.3.6.1.4.1.1588.3.1.13.1.1.1.4.1), it is displaying very large value/sometime Zero CPU and memory utilization in SNMP response randomly.		

Parent Defect ID:	SLXOS-73017	**Issue ID:**	SLXOS-73017
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.3j
Technology Group:	MPLS	**Technology:**	LDP - Label Distribution Protocol
Symptom:	Targeted LDP peering doesn't come up		
Condition:	After targeted LDP configuration is applied and then the device is rebooted, corresponding sessions won't come up.		

Parent Defect ID:	SLXOS-73769	**Issue ID:**	SLXOS-73769
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.2
Technology Group:	Other	**Technology:**	Other
Symptom:	The port LED is off on the port with SP7053-EXT optic in it.		
Condition:	When 4x1G breakout is done with SP7053-EXT (via QSA adpater) in QSFP28 ports of SLX-9250 device.		

Parent Defect ID:	SLXOS-73781	**Issue ID:**	SLXOS-73781
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	GRE - Generic Routing Encapsulation
Symptom:	Status of the VE interface binded to the GRE Tunnel is set to 'Down'		
Condition:	Tunnel VE interface status is 'Down' when the VE interface is created post the GRE Tunnel		
Workaround:	First create the VE, then the GRE Tunnel and bind the VE to Tunnel		

Parent Defect ID:	SLXOS-73891	**Issue ID:**	SLXOS-73891
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.3.2j
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	VRRPv3 - Virtual Router Redundancy Protocol Version 3
Symptom:	Error is seen while re-configuring VRRP-E under VE interface.		
Condition:	Issue is seen only while applying the same VRRPE group to the VE interface which was deleted and added again. DUT(config-if-Ve-503)# vrrp-extended-group 1 %% Error: VRRPE session with same modulo-VRID under an interface is not allowed DUT(config-if-Ve-503)#		

Parent Defect ID:	SLXOS-74075	**Issue ID:**	SLXOS-74075
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.1
Technology Group:	Other	**Technology:**	Other
Symptom:	Unexpected error is seen while configuring the RADV.		
Condition:	When configuring logging message suppression, an error maybe seen when configuring the 4th entry: DUT(config)# logging raslog message RADV-1006 suppress Configuration Change is saved in the database but failed to apply to Syslog server:		

	N O T A K N O W N R e s o u r c e I d DUT(config)#

Parent Defect ID:	SLXOS-74737	**Issue ID:**	SLXOS-74737
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.2a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	IPHELP Daemon detect termination with dumping core file.		
Condition:	In case of SLX(DHCPv6-RELAY) device processing DHCPv6-PD Relay-Reply[13] message which received from DHCPv6 Server,		

Parent Defect ID:	SLXOS-74802	**Issue ID:**	SLXOS-74802
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD multihop IPv6 sessions flap		
Condition:	When BFD multihop session is configured on the SLX 9740-40c device.		

Parent Defect ID:	SLXOS-74893	**Issue ID:**	SLXOS-74893
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.1a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	EVPN AD route is advertised for disabled ethernet segment.		
Condition:	Route refresh happens during configuration changes.		

Parent Defect ID:	SLXOS-74984	**Issue ID:**	SLXOS-74984
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.3
Technology Group:	Management	**Technology:**	Other

Symptom:	HTTP server down
Condition:	Sometimes web server goes down when HTTP server is enabled in an user-vrf.
Recovery:	Remove http server config for user-vrf and reboot the device couple of times.

Parent Defect ID:	SLXOS-75006	**Issue ID:**	SLXOS-75006
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.3
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	Dscp value will not be remarked according to dscp-mutation map applied on the interface (Phy/Logical).		
Condition:	1.First configure "qos dscp-mutation" map then configure IP address on the interface (physical/Logical) OR 2.If you remove the IP address and re-configure IP address, while keeping the QoS map.		
Workaround:	Remove the QoS maps configuration before removal of the IP-address.		
Recovery:	Remove and Re-configure the QoS map configuration on the interface (physical/Logical).		

Parent Defect ID:	SLXOS-75091	**Issue ID:**	SLXOS-75091
Severity:	S1 - Critical		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.2c
Technology Group:	Traffic Management	**Technology:**	Traffic Queueing and Scheduling
Symptom:	DHCP packets received at a higher rate builds up the CPU Queues		
Condition:	When DHCP packets are received at a higher rate, it builds up the CPU Queues and may impact other control protocols in SLX-9540, SLX-9640, SLX-9740 and Extreme-8820 platforms.		

Parent Defect ID:	SLXOS-75183	**Issue ID:**	SLXOS-75183
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.1a

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	MAC entry pointing to multi-homed peer tunnels is not updated with correct egress tunnel in MAC table.		
Condition:	Receiving EVPN MAC withdraw route from one of the multi-homed peer.		

Parent Defect ID:	SLXOS-75267	**Issue ID:**	SLXOS-75267
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.2b
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	In an MCT environment, following a reload of an MCT peer device, routed traffic from subnets other than the connected subnets on certain VEs may not function correctly.		
Condition:	In an MCT environment, after an MCT peer device is reloaded, certain dual-homed hosts may start receiving untagged traffic, despite the CCEP port being configured as a switchport trunk. This can lead to the hosts dropping incoming untagged traffic. - The problem is limited to routed traffic - Traffic within the same subnet is not affected by this issue		
Workaround:	Shutting down the CCEP port on the recently reloaded MCT peer device can serve as a workaround, but it will impact traffic performance because the host will then be single-homed.		
Recovery:	While some hosts recover during a CCEP port flap, all hosts recover only with a VE flap.		

Parent Defect ID:	SLXOS-75278	**Issue ID:**	SLXOS-75278
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Static Routing (IPv4)
Symptom:	Static route configuration with 'null 0' as the nexthop fails.		
Condition:	If Resilient Hashing feature is enabled under the corresponding VRF.		

Parent Defect ID:	SLXOS-75290	**Issue ID:**	SLXOS-75290

Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.2b
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	The dynamic-CCL MAC addresses are not aging out even after the specified aging interval. Consequently, the stale MAC address causes the traffic to loop back on the same CCEP interface when both the source MAC address (SMAC) and destination MAC address (DMAC) are learned from the same interface.		
Condition:	In MCT environment, the non-active dynamic-CCL MAC addresses are not aging out even after the specified aging interval. The issue is applicable to SLX-9540/SLX-9640 platforms.		
Workaround:	Clearing the dynamic MAC using the "clear mac-address-table dynamic address" command should resolve the situation.		

Parent Defect ID:	SLXOS-75306	**Issue ID:**	SLXOS-75306
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.3ac
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	When GTP packets are received with high rate to CPU, BFD protocol sessions maybe impacted due to ARP learning issue on SLX 9740 devices.		
Condition:	When GTP control packets are received with high rate to CPU		

Parent Defect ID:	SLXOS-75313	**Issue ID:**	SLXOS-75313
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.3a
Technology Group:	Layer 2 Switching	**Technology:**	xSTP - Spanning Tree Protocols
Symptom:	STP interface is being set to errDisable		
Condition:	If there is MAC move with PVST configuration		

Parent Defect ID:	SLXOS-75321	**Issue ID:**	SLXOS-75321
Severity:	S2 - Major		

Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.3a
Technology Group:	Other	**Technology:**	Other
Symptom:	With speed 100M configuration on one particular port (say eth 0/1), the other ports (say eth0/2, eth0/3, eth0/4 in port macro) links go down and not come up.		
Condition:	On 9540 or 9640 platform that have 10G/1G ports. Issue occurs when there are 1G optics in consecutive ports (port macro) and are UP.		

Parent Defect ID:	SLXOS-75341	**Issue ID:**	SLXOS-75341
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.2b
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	The acceptable frame type of the CCEP port was reset to the default untagged mode when deleting a bound Bridge Domain. This caused incoming tagged traffic to be discarded on the CCEP.		
Condition:	In MCT environments, if the CCEP has Logical Interfaces (LIFs) bound to Bridge Domains (BD) and a user attempts to remove a Bridge Domain without properly unbinding the Logical Interfaces from the Bridge Domain, this situation may occur. Issue is not seen on VLAN delete cases.		
Workaround:	The desired sequence of operations to avoid this situation is to unbind the Logical Interface (LIF) followed by deleting the Bridge Domain (BD).		

Parent Defect ID:	SLXOS-75357	**Issue ID:**	SLXOS-75357
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	DHCP request packet will carry wrong IP address under option 82.		
Condition:	When multiple IP addresses are configured under the interface in addition to the DHCP gateway address.		

Parent Defect ID:	SLXOS-75361	**Issue ID:**	SLXOS-75361
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.3a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	Internal OSPF debug messages will be seen on the terminal, if 'terminal monitoring' is enabled.		
Condition:	OSPF is configured on the switch.		

Parent Defect ID:	SLXOS-75403	**Issue ID:**	SLXOS-75403
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	A limited number of BFD sessions (IPv4/IPv6) may fail to establish.		
Condition:	After a switch reboot due to a crash, a limited number of BFD sessions (IPv4/IPv6) may fail to establish.		

Parent Defect ID:	SLXOS-75452	**Issue ID:**	SLXOS-75452
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.6.1
Technology Group:	Security	**Technology:**	HTTP/HTTPS
Symptom:	OAuth2 certificate will not be imported in SLX switch		
Condition:	This issue happens upon upgrade to this firmware and perform a certificate import via EFA.		
Workaround:	None.		

Parent Defect ID:	SLXOS-75473	**Issue ID:**	SLXOS-75473
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.1a
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	Output of "show ip interface ve", "show ip interface ethernet" always displays "ICMP unreachables are always sent"		

	irrespective of whether "ip icmp unreachable" is configured or not.
Condition:	Issue is seen when "ip icmp unreachable" is not configured on the interface
Workaround:	None.

Parent Defect ID:	SLXOS-75521	**Issue ID:**	SLXOS-75521
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.3
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	'show qos maps' output does not display few ports		
Condition:	When QoS maps are applied on both regular and breakout interfaces 'show qos maps' output does not display few ports		

Parent Defect ID:	SLXOS-75629	**Issue ID:**	SLXOS-75629
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.3a
Technology Group:	Security	**Technology:**	SSH - Secure Shell
Symptom:	Unable to login via SSH using the user accounts with a public key.		
Condition:	After upgrade to SLXOS20.5.3a from 20.5.1a		

Defects Closed without Code Changes

The following software defect was closed without code changes in SLX-OS 20.6.1a as of April 2024:

Parent Defect ID:	SLXOS-65379	**Issue ID:**	SLXOS-66289
Reason Code:	Third Party Issue	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3j
Technology Group:	MPLS	**Technology:**	MPLS VPLS - Virtual Private LAN Services
Symptom:	MPLS encapsulated 'Unicast ICMP with destination MAC starts on 4' traffic fails to forward from 9740(PHP/P) to 9850(PE).		
Condition:	a) Establish VPLS session between 9850 & MLX with adding 9740 as Transit Node. b) Initiate traffic with destination MAC starts with 4 from CE to CE.		

The following software defects were closed in SLX-OS 20.6.1 without code changes as of March 2024:

Parent Defect ID:	SLXOS-55266	**Issue ID:**	SLXOS-55266
Reason Code:	Will Not Fix	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.2
Technology Group:	-	**Technology:**	-
Symptom:	On SLX 9740, ARP is not resolved and Source mac is not learned when the incoming IP packets are Priority Tagged (Vlan-0 with PCP bit set).		
Condition:	The connected device to the switch is configured to send Priority tagged packets on an untagged port. The source MACs are not learnt from IP packets on the switch.		
Workaround:	Use DSCP instead of using Priority tagging for QoS.		

Parent Defect ID:	SLXOS-56740	**Issue ID:**	SLXOS-57454
Reason Code:	Will Not Fix	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol

Symptom:	Convergence times > 500 msec are seen for South - North traffic when a port from Border Leaf to L3 gateway is shut
Condition:	This is a test for convergence numbers. The port between a Border Leaf and an L3 gateway is shut which forces the BL to reprogram the next hop for the South - North traffic to go over the ICL. The convergence times vary and there are occasional spikes between 800 to 1000 msec.

Parent Defect ID:	SLXOS-58198	**Issue ID:**	SLXOS-58198
Reason Code:	Not Reproducible	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.3c
Technology Group:	Other	**Technology:**	Other
Symptom:	ICL interface is not coming up.		
Condition:	After the BGP process is killed.		

Parent Defect ID:	SLXOS-61347	**Issue ID:**	SLXOS-61598
Reason Code:	Will Not Fix	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.3.2c
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	In Multi-homed environment, shutdown of an LACP ES Port-channel may cause traffic flooding to other ES interfaces if the client/host device is not able to detect link flap and continue to send the traffic. Whenever LACP port-channel is shut, member ports will be disaggregated and laser will be down for few msec(around 100ms) to allow peer device to detect link event. After that link comes up and member port will be transitioned to disaggregated individual port. Some old devices may not be able to detect link flap and continue to send traffic for some more time till LACP timeout.		
Condition:	Some old hosts may not be able to detect link flap when the link goes down for short period of time. SLX 9150/9250 keep the link down for 100msec before bring up the link as lacp individual. If the dual homed host is not able to detect the link flap on LACP ESI shut, the host continues to send the traffic till LACP timeout. SLX device may flood the traffic (in vlan) during that period.		
Workaround:	Shutting the individual member ports along with ES port-channel avoids flooding in this scenario.		

Recovery:	This situation will be recovered automatically after LACP timeout. Client device detects LACP timeout after 3sec (in case of short lacp interval), and stops traffic.

Parent Defect ID:	SLXOS-62671	**Issue ID:**	SLXOS-62995
Reason Code:	Not Reproducible	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	Latency of around 250ms to 1second is observed on SLX device.		
Condition:	SLX node has experienced the CPU congestion		

Parent Defect ID:	SLXOS-54373	**Issue ID:**	SLXOS-67650
Reason Code:	Not Reproducible	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.1
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	Interface MTU value not set		
Condition:	Sometimes a reload will not set MTU value		
Workaround:	Re-configure MTU value		

Parent Defect ID:	SLXOS-68264	**Issue ID:**	SLXOS-68264
Reason Code:	Not Applicable	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1b
Technology Group:	Other	**Technology:**	Other
Symptom:	Link not coming up after reload. And if it comes up, after certain time (in secs) pld algorithm kicks in and link goes down after which it comes up again based on the configured time. This happens in loop.		
Condition:	When port link dampening CLI is configured. link-error-disable 2 120 300		

Parent Defect ID:	SLXOS-72546	**Issue ID:**	SLXOS-72546
Reason Code:	Not Reproducible	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.3ad

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	IP address of a VE interface in NSSA area not getting installed as summary route in backbone area.		
Condition:	One of the VE interface IP from NSSA area is not getting installed as summary route in backbone area.		

Parent Defect ID:	SLXOS-72629	**Issue ID:**	SLXOS-72629
Reason Code:	Not Reproducible	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.2b
Technology Group:	Monitoring	**Technology:**	Telemetry
Symptom:	System will reload.		
Condition:	After enable/disable of app-telemetry multiple times.		

Parent Defect ID:	SLXOS-72212	**Issue ID:**	SLXOS-72696
Reason Code:	Will Not Fix	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1cb
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Extra whitespace seen after 80 chars in AS PATH display.		
Condition:	While checking the output for "show ip bgp route detail " for a certain ip prefix whose AS PATH has more than 80 characters, an extra white space appears after that.		

Parent Defect ID:	SLXOS-73702	**Issue ID:**	SLXOS-73702
Reason Code:	Insufficient Information	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.2a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	IP Addressing
Symptom:	Traffic loss observed in forwarding IP traffic		
Condition:	In case of SLX forwarding invalid 0xffff IP header checksum packet (UDP) without recalculating them.		

Parent Defect ID:	SLXOS-73722	**Issue ID:**	SLXOS-73722
Reason Code:	Already Implemented	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.3a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	Generic Network Virtualization Encapsulated (Geneve) packets may get corrupted during IPv4 routing.		
Condition:	Geneve packets may get corrupted during IPv4 routing if Geneve header uses Variable-length Option Data. Option Data will be truncated by 4-bytes after routing. Since the Geneve header contents are truncated, the receiving Vmware may drop the incoming packets. Additional info: packets with GRE/UDPoIP tunnels that exceed 40B IP layer size when collapsed at parsing, causing the packet to be wrongly rebuilt at the Egress, all bytes above 40 are removed from the packet. The packet truncation issue can be seen with GRE/UDPoIP tunnel traffic which exceeds 40bytes of IP layer size (Outer IP header + UDP header + tunnel Encapsulation header). Geneve has variable length (TLV type) header options, and the IP layer size can go beyond 40B upon using the optional fields. As a result, the issue is more prominent in Geneve encapsulation. Furthermore, VxLAN traffic is not affected by the issue since its header size is fixed at 36 bytes, which is below 40 bytes.		

Parent Defect ID:	SLXOS-74014	**Issue ID:**	SLXOS-74014
Reason Code:	Insufficient Information	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.3.2d
Technology Group:	IP Multicast	**Technology:**	IPv4 Multicast Routing
Symptom:	(S,G) creation is delayed on FHR after traffic is started.		
Condition:	In a two node setup, with multiple VLANs and (*,G) groups already existing - only one node is the FHR, RP and LHR - when traffic is started for a few groups and then followed by traffic		

	for a single group, the (S,G) entry creation for the latter is delayed.
Workaround:	Configure ACL to drop the looped traffic.

Parent Defect ID:	SLXOS-74074	**Issue ID:**	SLXOS-74074
Reason Code:	Not Reproducible	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.1a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGPd process reload maybe seen.		
Condition:	1. BGP neighborship is established between BGP peers which are running in the BGP-EVPN scenario, and both these devices are likely connected on a LAG port. 2. ARP route is already learnt from the peer and it's sitting in the BGP DB 3. Flap the LAG, probably using the command, "configure conf-if-eth-x/xx no channel-group"		

Parent Defect ID:	SLXOS-74943	**Issue ID:**	SLXOS-74943
Reason Code:	Not Reproducible	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.1a
Technology Group:	MPLS	**Technology:**	IP over MPLS
Symptom:	CPU initiated packets at Provider Edge (PE) node might get dropped and fail in the Transit nodes.		
Condition:	CPU initiated packets at Provider Edge (PE) node might get dropped at Transit nodes due to improper label imposition. Transit data traffic will not have any impact.		

Parent Defect ID:	SLXOS-74985	**Issue ID:**	SLXOS-74985
Reason Code:	Already Reported	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	The error message "Hardware resource allocation failed for ECMP table" appears on the console. There may be traffic drop following this.		

Condition:	This happens when there are too many nexthops in the switch. In the test case, 600 20-path ECMP nexthops were converted to 19-path ECMP. Because the 19-path ECMP is created before the older nexthops are deleted, temporarily too much resources were consumed.
Workaround:	Lower the scale. In this test case, there were 300 VRFs with 20-path ECMP nexthops that became 19-path. When the scale was reduced to 240 VRFs, the issue is not seen.

Parent Defect ID:	SLXOS-75087	**Issue ID:**	SLXOS-75087
Reason Code:	Third Party Issue	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	DHCP lease time is not renewed.		
Condition:	Acknowledgement not received for DHCP Renew message from DHCP client to DHCP server, when option-82 is enabled on SLX device which is acting as Relay Agent.		
Workaround:	Initiate DHCP Rebind message		
Recovery:	Initiate DHCP Rebind message.		

Parent Defect ID:	SLXOS-75262	**Issue ID:**	SLXOS-75268
Reason Code:	Not Reproducible	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.3
Technology Group:	MPLS	**Technology:**	BGP/MPLS VPN
Symptom:	CPU initiated packets at Provider Edge (PE) node might get dropped and fail in the transit nodes.		
Condition:	CPU initiated packets at Provider Edge (PE) node might get dropped at Transit nodes due to improper label imposition. Transit data traffic will not have any impact.		