May 2025

Extreme SLX-OS 20.5.3d

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 9037971-04 Rev AA

Contents

Document History

Version	Summary of changes	Publication date
AA	Initial version for 20.5.3d. Removed version earlier than 20.5.3b	May 2025

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 20.5.3d provides the following features:

- Critical defect fixes

Release SLX-OS 20.5.3c provides the following features:

- Critical defect fixes
- Resolves regreSSHion Vulnerability in OpenSSH Server (CVE-2024-6387)

Release SLX-0S 20.5.3b provides the following features:

- Critical defect fixes

Behavior Changes

The following are the behavioral changes for SLX-OS 20.5.3d

No behavioral changes were introduced in this release.

The following are the behavioral changes for SLX-OS 20.5.3c

No behavioral changes were introduced in this release.

The following are the behavioral changes for SLX-OS 20.5.3b

No behavioral changes were introduced in this release.

Software Features

The following key software features are added in the SLX-OS 20.5.3d release:

No new features were added in this release.

The following key software features are added in the SLX-OS 20.5.3c release:

No new features were added in this release.

The following key software features are added in the SLX-OS 20.5.3b release:

No new features were added in this release.

CLI Commands

The following commands were added, modified, or deprecated for the 20.5.3d program.

New commands for 20.5.3d

No commands were added in this release.

Modified commands for 20.5.3d

No commands were modified in this release.

Deprecated commands for 20.5.3d

No commands were deprecated in this release.

The following commands were added, modified, or deprecated for the 20.5.3c program.

New commands for 20.5.3c

No commands were added in this release.

Modified commands for 20.5.3c

No commands were modified in this release.

Deprecated commands for 20.5.3c

No commands were deprecated in this release.

The following commands were added, modified, or deprecated for the 20.5.3b program.

New commands for 20.5.3b

No commands were added in this release.

Modified commands for 20.5.3b

No commands were modified in this release.

Deprecated commands for 20.5.3b

No commands were deprecated in this release.

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.
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.

Supported devices	Description
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)
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

Supported devices	Description
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
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

Supported devices	Description
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
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/PSM4	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/PSM4	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
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/PSM4	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

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
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/PSM4	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 20.5.3d see the *Extreme SLX-OS Software Upgrade Guide.*

Image files

Download the following images from www.extremenetworks.com.

Image file name	Description
SLX-OS_20.5.3d.tar.gz	SLX-OS 20.5.3d software
SLX-OS_20.5.3d_mibs.tar.gz	SLX-OS 20.5.3d MIBS
SLX-OS_20.5.3d.md5	SLX-OS 20.5.3d md5 checksum
SLX-OS_20.5.3d-digests.tar.gz	SLX-OS 20.5.3d sha checksum
SLX-OS_20.5.3d-releasenotes.pdf	Release Notes

Notes:

Upgrade to 20.3.x from earlier releases requires “fullinstall” due to change in glibc for all platforms.

Extreme 8820

<table>
<tr><th>To
From</th><th>20.4.3/a/b</th><th>20.5.1/a</th><th>20.5.2a</th><th>20.5.3/a/b/c</th><th>20.5.3d</th></tr>
<tr><td>20.4.3 (Factory Image)</td><td colspan="3" rowspan="3">For upgrade: normal firmware download / coldboot</td><td colspan="2" rowspan="3">For upgrade and downgrade: full install</td></tr>
<tr><td>20.5.1/a</td></tr>
<tr><td>20.5.2a</td></tr>
<tr><td>20.5.3/a/b/c</td><td colspan="3" rowspan="2">For upgrade and downgrade: full install</td><td colspan="2" rowspan="2">For upgrade and downgrade: normal firmware download / coldboot</td></tr>
<tr><td>20.5.3d</td></tr>
</table>

Note : Upgrade to 20.5.3/a/b/c/d from 20.5.2a and earlier releases require “fullinstall”. Downgrade from 20.5.3 to 20.5.2a and earlier releases require “fullinstall”.

Upgrade/Downgrade from 20.5.2b to 20.5.3a and above releases supported by normal firmware download / coldboot

Extreme 8720

<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>20.5.3/a/b/c</th><th>20.5.3d</th></tr>
<tr><td>20.3.2/a-h</td><td colspan="7">For upgrade: normal firmware download / coldboot
For downgrade: full install</td></tr>
<tr><td>20.3.4/a-c</td><td colspan="7" rowspan="8">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>20.5.3/a/b/c</td></tr>
<tr><td>20.5.3d</td></tr>
</table>

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	20.5.3/a/b /c	20.5.3d
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								
20.5.3/a /b/c								
20.5.3d								

SLX 9740

To / From	20.3.1 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	20.5.3/a/b /c	20.5.3d
20.3.1 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								
20.5.3/a /b/c								
20.5.3d								

SLX 9540 and SLX 9640

To / From	20.3.1 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	20.5.3/a/b /c	20.5.3d
20.3.1 20.3.2/a -h	For upgrade: normal firmware download / coldboot For downgrade: full install							

To / From	20.3.1 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	20.5.3/a/b /c	20.5.3d
20.3.4/a -c 20.4.1x, 20.4.2x 20.4.3/a /b 20.5.1/a 20.5.2a	For upgrade and downgrade: normal firmware download / coldboot							
20.5.3/a /b/c								
20.5.3d								

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
- Downgrading from 20.3.x/20.2.2x/20.2.3x to 20.1.1 may not require a 2-step procedure.

SLX 9150 and SLX 9250

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	20.5.3/a/b /c	20.5.3d
20.3.1 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								
20.5.3/a /b/c								
20.5.3d								

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 the 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/b	TPVM 4.5.0 and later	TPVM 4.5.0 and later	TPVM 4.5.0 and later
20.5.3c	TPVM 4.5.9 and later	TPVM 4.5.9 and later	TPVM 4.5.9 and later
20.5.3d	TPVM 4.6.4 and later	TPVM 4.6.4 and later	TPVM 4.6.4 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, 4.6.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 4.5.0 and beyond.
- TPVM 4.6.x supports only full install upgrade/downgrade from TPVM 4.5.0.

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:

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 version of TPVM 4.6.x branch, TPVM 4.6.22, has security updates till 30th April, 2025.
Main TPVM image size of 4.6.22 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`

      `tpvm uninstall` (or) `tpvm uninstall force` – if you plan to delete disk vdb (i.e. the TPVM /apps partition).

      Note:

      i. New mode like old mode, create disk vdb (/apps) by default upon first install/deploy or reuse previously existing partition.
      ii. 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:

i. 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.

ii. 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.

iii. 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

Configuration	Migration State	Notes
		user to reconfigure LDAP certificate settings.
tpvm config hostname	Migrated	
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

- 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.
- Service policy and TC-CoS user map are mutually exclusive and cannot be applied together.
- For SLX 9740 and Extreme 8820:
    a. TC-COS maps is not supported by underlying HW ASIC, so CoS mutation map is added on the Egress side.
    b. Egress QoS maps are only supported on BD VLAN.
    c. DSCP remark on L2 switchport is not supported.

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 ECMP IPv6 control packets over the GRE Tunnel are not accounted 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.

BGP/EVPN

- A maximum of 3000 VLANs or 3000 Bridge Domains can be added per Ethernet Segment.

OSPF

- For OSPF-LSP shortcuts, OSPF virtual link is not yet supported.

MPLS

- '`show mpls statistics tunnel`' at ingress LER does not account for all the LSPs (in ECMP case), post the device reload. Recommended workaround is to either use the transit LSR statistics or remove/reconfigure ingress tunnel accounting at ingress LER.

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

NOTE: No software defects are open in SLX-OS 20.5.3d as of May 2025.

NOTE: No software defects are open in SLX-OS 20.5.3c as of September 2024.

The following software defects are open in SLX-OS 20.5.3b as of May 2024:

Parent Defect ID:	SLXOS-75343	**Issue ID:**	SLXOS-75889
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3j
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	IPv6 Addressing
Symptom:	IPv6 ND packets with duplication potentially leading to protocol flaps.		
Condition:	Ipv6 ND packets are duplicated more during route loop conditions.		

Parent Defect ID:	SLXOS-75357	**Issue ID:**	SLXOS-75856
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-75842	**Issue ID:**	SLXOS-75842
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3a
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	From the perspective of a dual-homed client, there is a small window of time when one port is up and the second port is coming up, during which BUM (Broadcast, Unknown unicast, and Multicast) traffic could be inadvertently looped back to the client.		
Condition:	During the CCEP port-channel link up, BUM traffic received on the newly activated port is briefly flooded back to the client via the MCT peer until the MCT control plane converges. The BUM flooding was observed for approximately 20msec on 8820/9740 platforms.		
Workaround:	No known workarounds		

Defects Closed with Code Changes

The following software defects were closed in 20.5.3d with code changes as of May 2025.

Parent Defect ID:	SLXOS-77798	**Issue ID:**	SLXOS-77877
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3c
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP requests are not processed.		
Condition:	When we do SNMP walk for default-vrf after upgrade.		
Workaround:	Restart the SNMP service.		

Parent Defect ID:	SLXOS-77320	**Issue ID:**	SLXOS-77878
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3c
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	IGP cost is not considered for bgp l3vpn route best path calculation, which results in non-optimal path selection for routes.		
Condition:	When 'nexthop-mpls follow-igp-metric' is configured under bgp address family.		
Workaround:	NA		
Recovery:	NA		

Parent Defect ID:	SLXOS-77690	**Issue ID:**	SLXOS-77879
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3c
Technology Group:	Platform	**Technology:**	Support Save
Symptom:	HSLagt daemon is terminated leading to a reboot of the node		
Condition:	When collecting the Support Save on SLX 9540 and SLX 9640		

Parent Defect ID:	SLXOS-77343	**Issue ID:**	SLXOS-77880
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3c
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Broadcast DHCP packets received on a CCEP interface were incorrectly looping between MCT peers over the ICL, leading to excessive DHCP packet punting to the CPU. Since DHCP and VRRP packets share the same CPU queue, some VRRP control packets were dropped, resulting in VRRP failures.		

Condition:	When a DHCP relay agent is configured on any VE, the handling of broadcast DHCP packet flooding is managed by the software. Upon receiving a broadcast DHCP packet on a CCEP/CEP port, the MCT forwards the packet to the software, which then floods it across the L2 domain. This process includes duplicating the packet to local client ports and transmitting it to the peer MCT node over the ICL. Upon receiving this packet over the ICL, the peer MCT node was expected to flood it only to local CEP/CCEP ports. However, due to the local client port-channel being down, the packet was incorrectly flooded back to the ICL with the intention of reaching the client via the peer MCT node. This caused the same packet to return to the originator MCT node, triggering another round of flooding. The problem becomes worse if the client port-channel is down on both MCT nodes, as the packet continuously loops between the MCT nodes over the ICL.
Workaround:	The loop can be resolved by globally disabling DHCP relay flooding using the CLI command "ip dhcp relay disable-flooding". However, there is no per-VE CLI option to restrict flooding for specific VLANs or BDs. As a result, this global setting may inadvertently block some clients from reaching DHCP servers.

Parent Defect ID:	SLXOS-77206	**Issue ID:**	SLXOS-77881
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	System reload is observed		
Condition:	Adding and removing bgp rpki server configs multiple times triggers the crash		

Parent Defect ID:	SLXOS-77132	**Issue ID:**	SLXOS-77882
Severity:	S1 - Critical		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3a
Technology Group:	Layer 2 Switching	**Technology:**	VXLAN - Virtual Extensible LAN
Symptom:	VxLAN Tunnel does not come back up after reloading the device		
Condition:	When Insight port is configured and SNMP walk is issued, the SNMP-GET for the Insight port can go into an infinite loop causing the system to be non-responsive.		
Workaround:	Un-configure the Insight port		
Recovery:	Un-configure the Insight port and reload		

Parent Defect ID:	SLXOS-77505	**Issue ID:**	SLXOS-77883

Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3
Technology Group:	Platform	**Technology:**	Port Optics & FEC
Symptom:	"Identification data corruption detected" is thrown on the console.		
Condition:	During optic removal and insertion or during reload on some breakout ports randomly.		
Workaround:	No workaround.		

Parent Defect ID:	SLXOS-77696	**Issue ID:**	SLXOS-77884
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	SLX node is reporting a BGP Keepalive TTL exceeded Timeout error		
Condition:	It is applicable for Extreme 8520, Extreme 8720, SLX 9150 and SLX 9250 platforms only, when the node is acting as a transit Layer 2 device between BGP peers		

Parent Defect ID:	SLXOS-76808	**Issue ID:**	SLXOS-77885
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3
Technology Group:	Monitoring	**Technology:**	sFlow
Symptom:	It is possible to configure 'sflow enable' on a Port-channel interface using REST API, even though the same is blocked while using the CLI		
Condition:	Configure 'sflow enable' using REST API (curl command) on a disallowed platform		

Parent Defect ID:	SLXOS-76095	**Issue ID:**	SLXOS-77886
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	DHCP server is not processing DHCP requests from client		
Condition:	When the padding value is non-zero in the DHCP packets		

Parent Defect ID:	SLXOS-77569	**Issue ID:**	SLXOS-77887
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3c
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection

Symptom:	BFD sessions are flaps with VSP routers.
Condition:	When peer is VSP routers.
Workaround:	NA
Recovery:	NA

Parent Defect ID:	SLXOS-77618	**Issue ID:**	SLXOS-77888
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3c_CVR
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	L3 routing table pointing to the previous best path		
Condition:	With BGP PIC enabled, during path change, the route table may continue to point to the old best path		

Parent Defect ID:	SLXOS-77115	**Issue ID:**	SLXOS-77889
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3d
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	One of the SLX processes runs out of memory and the device may unexpectedly reboot		
Condition:	This issue is seen only with BGP PIC feature enabled and the device is exposed to Internet Feed level route scale.		

Parent Defect ID:	SLXOS-77913	**Issue ID:**	SLXOS-78026
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.6.3ab
Technology Group:	Platform	**Technology:**	Support Save
Symptom:	Unexpected reload of SLX device		
Condition:	System had configured more than 255 anycast IP's under VE interface and interface to be online. perform any interface commands like - show ip interface brief - show interface status		

The following software defects were closed in 20.5.3c with code changes as of September 2024:

Parent Defect ID:	SLXOS-75343	**Issue ID:**	SLXOS-75889
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3j

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	IPv6 Addressing
Symptom:	IPv6 ND packets with duplication potentially leading to protocol flaps.		
Condition:	Ipv6 ND packets are duplicated more during route loop conditions.		

Parent Defect ID:	SLXOS-76734	**Issue ID:**	SLXOS-76680
Severity:	S1 - Critical		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.6.2
Technology Group:	Security	**Technology:**	SSH – Secure Shell
Symptom:	The symptoms are detailed in the below CVE link https://nvd.nist.gov/vuln/detail/CVE-2024-6387		
Condition:	The symptoms are detailed in the below CVE link https://nvd.nist.gov/vuln/detail/CVE-2024-6387		

Parent Defect ID:	SLXOS-76002	**Issue ID:**	SLXOS-76730
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.		

Parent Defect ID:	SLXOS-75290	**Issue ID:**	SLXOS-76731
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-75848	**Issue ID:**	SLXOS-76732
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP is advertising a stale route to its peers. And any traffic directed to that route is getting blackholed.		
Condition:	In a rare situation of where a 3rd party BGP nexthop is also redistributed as a local route via RTM.		

Parent Defect ID:	SLXOS-76453	**Issue ID:**	SLXOS-76733
Severity:	S1 - Critical		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3c
Technology Group:	IP Multicast	**Technology:**	IGMP - Internet Group Management Protocol
Symptom:	SLX 9640 device experienced unexpected reload		
Condition:	IGMP gets message from HSL using recvfrom socket system call (igmp_sock_read_from_hsl). In this function to read the data we are allocating memory of size RCV_BUFSIZ. RCV_BUFSIZ is defined as 9000 in our code. #define RCV_BUFSIZ 9000 In issue case igmp received a fragmented packet with packet length grater than 9000bytes size (tot_len = 14552) and we are trying to copy that using memcpy causing crash.		

Parent Defect ID:	SLXOS-76457	**Issue ID:**	SLXOS-76747
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	IP Addressing
Symptom:	Ping and traffic forwarding fails on a Layer 3 Port-channel		
Condition:	After repeated interface flaps, ping and traffic forwarding fails on the Layer 3 Port-channel interface		
Workaround:	Delete the Port-channel and create a new Port-channel interface with the same member ports		

Parent Defect ID:	SLXOS-76398	**Issue ID:**	SLXOS-76748
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4b
Technology Group:	Other	**Technology:**	Other
Symptom:	The threshold monitor show CLI on AFBR-710ASMZ-EX2 optic is shown as 10G ER optic when it actually is a 10 SR optic.		
Condition:	When AFBR-710ASMZ-EX2 is used and show threshold monitor CLI is executed on it.		

Parent Defect ID:	SLXOS-76436	**Issue ID:**	SLXOS-76757
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.6.1a
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP requests are not processed.		
Condition:	When no VE interface is up and running in the device.		

Parent Defect ID:	SLXOS-76469	**Issue ID:**	SLXOS-76758
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2d
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	Disruption in traffic after reload		
Condition:	When an ip access-list attached to an interface has more than one rule with vlan configuration		
Workaround:	Delete and reconfigure the access-list configuration		

Parent Defect ID:	SLXOS-76159	**Issue ID:**	SLXOS-76760
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.6.1
Technology Group:	Management	**Technology:**	Software Installation & Upgrade
Symptom:	SLX-OS image download will be in-complete or firmware download will not be successful, and device will go for a reboot.		
Condition:	When the network is slow, and the firmware download takes more time, this condition happens.		
Workaround:	None		
Recovery:	None		

Parent Defect ID:	SLXOS-76305	**Issue ID:**	SLXOS-76761
Severity:	S3 - Moderate		

Product:	SLX-OS	**Reported in Release:**	SLXOS 20.6.1a
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	Unexpected reload of the device		
Condition:	The device has 2 scripts running in parallel. First one to create and then delete the port-channel; and a second script to fetch the port-channel interface counters		

Parent Defect ID:	SLXOS-76134	**Issue ID:**	SLXOS-76763
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3
Technology Group:	Other	**Technology:**	Other
Symptom:	show media CLI on the 40G ports was always reporting high alarm for TxPower.		
Condition:	Issue was in reading the correct threshold values for the TxPower which was wrongly read, which caused this issue to report high alarms for any TxPower value		
Workaround:	None		
Recovery:	None		

Parent Defect ID:	SLXOS-76007	**Issue ID:**	SLXOS-76764
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2b
Technology Group:	Management	**Technology:**	Software Installation & Upgrade
Symptom:	BMC firmware update through the exec mode CLI will not be successful.		
Condition:	This happens when the BMC firmware update CLI is used the 'VRF' option.		
Workaround:	None		
Recovery:	None		

Parent Defect ID:	SLXOS-75842	**Issue ID:**	SLXOS-76765
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3a
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	From the perspective of a dual-homed client, there is a small window of time when one port is up and the second port is coming up, during which BUM (Broadcast, Unknown unicast, and Multicast) traffic could be inadvertently looped back to the client.		

Condition:	During the CCEP port-channel link up, BUM traffic received on the newly activated port is briefly flooded back to the client via the MCT peer until the MCT control plane converges. The BUM flooding was observed for approximately 20msec on 8820/9740 platforms.
Workaround:	No known workarounds

Parent Defect ID:	SLXOS-75714	**Issue ID:**	SLXOS-76766
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:	.		
Recovery:	.		

Parent Defect ID:	SLXOS-75401	**Issue ID:**	SLXOS-76768
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	SLX crash		
Condition:	Can lead to SLX crash on receiving FCoE/FIP control frames, trapped and handled in the CPU.		

Parent Defect ID:	SLXOS-74982	**Issue ID:**	SLXOS-76769
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	DNS - Domain Name System
Symptom:	Incorrect error returned mentioning DNS resolution failed, when the DNS server resolves to an unreachable IP.		
Condition:	DNS server configured on a default vrf DNS server returning an unreachable IP		
Workaround:	None		
Recovery:	None		

Parent Defect ID:	SLXOS-76700	**Issue ID:**	SLXOS-76805
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3

Technology Group:	Security	**Technology:**	SSH - Secure Shell
Symptom:	Unable to login via SSH with user configure port number.		
Condition:	After upgrade to SLXOS20.5.3 from 20.4.3		
Workaround:	Remove and re-configure "ssh server port xxxx".		

Parent Defect ID:	SLXOS-76408	**Issue ID:**	SLXOS-76832
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	Control protocol flaps due to packet buffer exhaustion and may lead to traffic loss		
Condition:	Flaps due to the packet buffer exhaustion is seen only with DHCP Relay configuration		
Recovery:	Remove the DHCP Relay configuration on the node and then reload		

Parent Defect ID:	SLXOS-76723	**Issue ID:**	SLXOS-76834
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1b
Technology Group:	Security	**Technology:**	PBR - Policy-Based Routing
Symptom:	PBR is not updating the new route to reach configured next-hop when the previously selected route is unreachable.		
Condition:	"next-hop-recursion" configuration is enabled for PBR. PBR next hop is configured with non directly connected IP.		

Parent Defect ID:	SLXOS-76724	**Issue ID:**	SLXOS-76836
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1b
Technology Group:	Security	**Technology:**	PBR - Policy-Based Routing
Symptom:	VRRP-E peers are stuck with Master/Master state due to split brain issue after applying PBR		
Condition:	1. Configure the PBR ACL with permit rule to redirect all packets to configured PBR next-hop. 2. Configure the PBR ACL with deny rule for VRRP-E multicast destination to skip PBR action. seq 10 permit ip any any count seq 20 deny ip any host 224.0.0.2 count		

Parent Defect ID:	SLXOS-76640	**Issue ID:**	SLXOS-76846

Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP daemon gets crashed, while route-reflector-client config gets remove and re-add.		
Condition:	Issue noticed while remove and re-add the config of route-reflector-client neighbor.		

The following software defects were closed in 20.5.3b with code changes as of May 2024:

Parent Defect ID:	SLXOS-73017	**Issue ID:**	SLXOS-75509
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-75453	**Issue ID:**	SLXOS-75512
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Not able to delete individual stanza from an IP prefix list configuration, if the same is referenced in BGP configuration		
Condition:	All the time.		
Workaround:	- Remove the usage: Delete the existing IP prefix from the BGP configuration. - Edit the configuration: Modify the desired attributes of the IP prefix (e.g., network mask, next hop). - Reapply the configuration: Add the updated IP prefix back to the BGP configuration.		

Parent Defect ID:	SLXOS-74529	**Issue ID:**	SLXOS-75598
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-75091	**Issue ID:**	SLXOS-75599
Severity:	S1 - Critical		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-75361	**Issue ID:**	SLXOS-75600
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-74075	**Issue ID:**	SLXOS-75699
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-75313	**Issue ID:**	SLXOS-75743
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-75306	**Issue ID:**	SLXOS-75758
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-75403	**Issue ID:**	SLXOS-75793
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-75629	**Issue ID:**	SLXOS-75795
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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		

Parent Defect ID:	SLXOS-73891	**Issue ID:**	SLXOS-75825
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-75922	**Issue ID:**	SLXOS-75922

Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.3a
Technology Group:	Security	**Technology:**	PBR - Policy-Based Routing
Symptom:	Traffic is not falling back to normal routing path when PBR next-hop is not available		
Condition:	PBR next-hop becomes unreachable		
Workaround:	Rebind the PBR configuration		

Parent Defect ID:	SLXOS-75325	**Issue ID:**	SLXOS-75953
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	Switch experiences a crash on the srm daemon.		
Condition:	Applying a list of static BFD sessions with an unresolved next-hop.		

Parent Defect ID:	SLXOS-75278	**Issue ID:**	SLXOS-76170
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-75620	**Issue ID:**	SLXOS-76174
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3c
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	SLX device may get inadvertently rebooted due to out of memory crash of RIB manager process.		
Condition:	BGP PIC feature enabled.		

Defects Closed without Code Changes

NOTE: No defects were closed without code changes in SLX-OS 20.5.3d as of May 2025.

NOTE: No defects were closed without code changes in SLX-OS 20.5.3c as of September 2024.

NOTE: No defects were closed without code changes in SLX-OS 20.5.3b as of May 2024.