September 2024

Extreme SLX-OS 20.5.3c

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 9037971-03 Rev AA

Contents

Preface 5
Release Overview 7
Behavior Changes 7
Software Features 9
CLI Commands 10
Hardware Support 13
Supported FEC modes 19
Software Download and Upgrade 22
Limitations and Restrictions 30
Open Defects 35
Defects Closed with Code Changes 60
Defects Closed without Code Changes 92

Document History

Version	Summary of changes	Publication date
1.0	Initial version for 20.5.3c	September 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 20.5.3c 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

Release SLX-OS 20.5.3a provides the following features:

- Critical defect fixes

Release SLX-OS 20.5.3 provides the following features:

- LSP-OSPF shortcuts
- Fabric QoS – QoS Egress maps and Out LIF support
- Apache OSS Upgrade
- EVPN Multihoming support on SLX 9740 and Extreme 8820 as a leaf
- Monitoring and SNMP Notification Event - Layer 3 HW Resources
- EVPN-MH: RFC 8584 to add the DF-per-AC election attribute
- DHCPv4 relay packet processing over VxLAN tunnel
- Qualify new BRCM and DDR5 parts on SLX 9640 platform
- Add IPv6 update-source option for BGP Peer-group
- Temperature sensor enhancements on SLX-OS
- Optics Qualification
- Added a global-level BGP option to enable or disable the ability to transport IPv6 prefixes over IPv4 peer connections for BGP peer groups.

Behavior Changes

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.

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

No behavioral changes were introduced in this release.

The following are the behavioral changes for SLX-OS 20.5.3

- Threshold monitoring configuration for BFD, LIF, VxLAN tunnel and MAC table is changed. Rate limiting parameters "`count`" and "`interval`" are not configurable per resource. A new separate CLI, common to all HW resources, is made available to configure "`count`" and "`interval`" globally.
- Following MIB objects are deprecated:
  - extremeThreshMonNotif
  - extremeThreshMonResourceId
  - extremeThreshMonNotifType

- extremeThreshMonResourceLimit

SNMP notification `extremeThreshMonNotif` , which was for status change of an individual resource, is replaced by `extremeHWResourceUsageAlert` notification, which will give the comprehensive status of all resources in a bitmap `extremeHWResourceOverallUsage`.

- IP prefix-list usage in the default-vrf in BGP
  - When assigning an IP prefix-list to BGP peers/peer-groups, now only an existing IP prefix-list will be accepted.

  During software upgrade from a prior release, if the configuration is applied from a startup config file and existing configuration contains a BGP peer with an undefined prefix-list, the configuration will be lost. Previously usage of an undefined prefix-list in BGP would deny all prefixes.

Software Features

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.

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

No new features were added in this release.

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

Feature Name	Supported SLX Platforms	Description
LSP-OSPF shortcuts	SLX 9540, SLX 9640, SLX 9740, Extreme 8820	Allows OSPF to use MPLS LSPs as shortcut next hops
Fabric QoS	SLX 9740 and Extreme 8820	QoS egress maps and OutLIF support are added
Apache OSS Upgrade	All	Upgraded Apache module to a higher version
Support for EVPN Multihoming	SLX 9740 and Extreme 8820	Extended EVPN Multihoming support to include SLX 9740 and Extreme 8820 as a leaf in an IP Fabric deployment
Threshold monitoring for Layer 3 hardware resources	SLX 9150, SLX 9250, Extreme 8520, Extreme 8720, SLX 9740, Extreme 8820	L3 hardware tables are monitored, and notifications are generated as user-defined thresholds are exceeded
EVPN-MH: RFC 8584 to add the DF-per-AC election attribute	SLX 9150, SLX 9250, Extreme 8520, Extreme 8720, SLX 9740, Extreme 8820	Support added to elect Designated Forwarder (DF) per AC as per RFC 8584
Support for DHCPv4 relay over VxLAN	All	DHCPv4 relay packet processing over VxLAN tunnel. A knob is added to prevent flooding of DHCPv4 Broadcast packets in IP-Fabric
Qualify new component parts	SLX 9640	New BRCM and DDR5 parts are qualified
Add IPv6 update-source option for BGP Peer-group	All	Missing IPv6 address for update-source option under BGP Peer-group is added.
Temperature sensor enhancements on SLX-OS	All	Show output for temperature sensors is enhanced
Optics Qualification	All	100G-PSM4-QSFP10KM

Feature Name	Supported SLX Platforms	Description
		(without Pigtail) 25G/10G LR –SFP10KM
BGP command is added - “peer-group ipv6prefix-over-ipv4peer"	All	Global-level BGP knob (CLI, NETCONF and REST) to enable and disable exchanging of IPv6 routes over IPv4 BGP peer-group peers.

CLI Commands

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.

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

New commands for 20.5.3a

No commands were added in this release.

Modified commands for 20.5.3a

No commands were modified in this release.

Deprecated commands for 20.5.3a

No commands were deprecated in this release.

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

New commands for 20.5.3

- advertise capabilities ac-influenced-df-election
- debug ip ospf shortcuts
- map cos to cos
- shortcuts ospf
- show debug ip ospf all
- show debug ip ospf internal lsp-shortcuts
- show ip ospf lsp-shortcuts
- show threshold monitor ecmp
- show threshold monitor host
- show threshold monitor nexthop
- show threshold monitor route
- show qos maps
- show qos maps cos-mutation
- threshold-monitor ecmp
- threshold-monitor hardware-resources
- threshold-monitor host
- threshold-monitor nexthop
- threshold-monitor route
- qos map cos-mutation (SLX 9740 and Extreme 8820)
- qos cos-mutation all-zero-map

Modified commands for 20.5.3

- ip dhcp relay
- neighbor update-source
- show bgp evpn ethernet-segment
- show bgp evpn routes type
- show debug all
- show debug ip ospf all
- show environment temp
- show ip dhcp relay address
- show ip ospf border-routers
- show ip ospf routes
- show ipv6 bgp neighbors
- show ipv6 bgp summary
- show mpls lsp
- show mpls statistics
- show qos interface ethernet
- show qos maps
- show qos maps traffic-class-cos

- threshold-monitor bfd-session
- threshold-monitor lif
- threshold-monitor mac-table
- threshold-monitor vxlan-tunnel

Deprecated commands for 20.5.3

- qos map traffic-class-cos (deprecated in SLX 9740 and Extreme 8820)
- qos traffic-class-cos (deprecated in SLX 9740 and Extreme 8820)

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	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
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

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	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 20.5.3c see the *Extreme SLX-OS Software Upgrade Guide.*

Image files

Download the following images from www.extremenetworks.com.

Image file name	Description
SLX-OS_20.5.3c.tar.gz	SLX-OS 20.5.3c software
SLX-OS_20.5.3c_mibs.tar.gz	SLX-OS 20.5.3c MIBS
SLX-OS_20.5.3c.md5	SLX-OS 20.5.3c md5 checksum
SLX-OS_20.5.3c-digests.tar.gz	SLX-OS 20.5.3c sha checksum
SLX-OS_20.5.3c-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

To / From	20.4.3/a/b	20.5.1/a	20.5.2a	20.5.3/a/b	20.5.3c
20.4.3 (Factory Image)	For upgrade: normal firmware download / coldboot			For upgrade and downgrade: full install	
20.5.1/a					
20.5.2a					
20.5.3/a/b	For upgrade and downgrade: full install			For upgrade and downgrade: normal firmware download / coldboot	
20.5.3c					

Note : Upgrade to 20.5.3/a/b from 20.5.2a and earlier releases requires full install. Downgrade from 20.5.3 to 20.5.2a and earlier releases require full install.

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

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	20.5.3/a/b	20.5.3c
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								
20.5.3c								

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	20.5.3c
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								
20.5.3c								

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	20.5.3c
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								
20.5.3c								

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	20.5.3c
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	20.5.3c
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								
20.5.3c								

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	20.5.3c
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								
20.5.3c								

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/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

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:

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 version of TPVM 4.6.x branch, TPVM 4.6.15, has security updates till September 1st, 2024.
Main TPVM image size of 4.6.13 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 20.5.3c.

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		

The following software defects are open in SLX-OS 20.5.3a as of December 2023:

Parent Defect ID:	SLXOS-68264	**Issue ID:**	SLXOS-68264
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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

The following software defects are open in SLX-OS 20.5.3 as of November 2023:

Parent Defect ID:	SLXOS-55266	**Issue ID:**	SLXOS-55266
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-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-65379	**Issue ID:**	SLXOS-66289
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.		

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-54373	**Issue ID:**	SLXOS-67650

Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-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-68208	**Issue ID:**	SLXOS-68208
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-68264	**Issue ID:**	SLXOS-68264
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-69621	**Issue ID:**	SLXOS-70060
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-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-71395	**Issue ID:**	SLXOS-71655
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-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-72546	**Issue ID:**	SLXOS-72546
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-72267	**Issue ID:**	SLXOS-73137
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1cb
Technology Group:	Security	**Technology:**	ACLs - Access Control Lists
Symptom:	When ACL is configured with dscp-force value, ACL will not work to redirect configured traffic DSCP value at egress.		

Condition:	When there is high priority traffic with congestion and ACL is applied with dscp-force to 0, ACL will not work to redirect DSCP value at 0 egress.

Parent Defect ID:	SLXOS-73263	**Issue ID:**	SLXOS-73263
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	Some of the valid BGP routes are not selected as best and not installed in routing table.		
Condition:	eBGP routes nexthop is resolved recursively by other eBGP route.		

Parent Defect ID:	SLXOS-72665	**Issue ID:**	SLXOS-73288
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3ac
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD sessions are down on 8720 device		
Condition:	BFD sessions are down on 8720 device		

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-73637	**Issue ID:**	SLXOS-73637
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Other	**Technology:**	Other

Symptom:	Unable to login TPVM with LDAP user credentials
Condition:	Issue observed when Windows AD LDAP server is configured with TPVM.

Parent Defect ID:	SLXOS-73702	**Issue ID:**	SLXOS-73702
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-73769	**Issue ID:**	SLXOS-73769
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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:**	SLXOS 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:**	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-74014	**Issue ID:**	SLXOS-74014
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-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-74074	**Issue ID:**	SLXOS-74074
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-74075	**Issue ID:**	SLXOS-74075
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-74802	**Issue ID:**	SLXOS-74802
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:	BFD multihop ipv6 sessions flaps
Condition:	when bfd multihop session is configured on the 9740 40c device.

Parent Defect ID:	SLXOS-74888	**Issue ID:**	SLXOS-74888
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	Issue on ARP entries programming results on traffic loss.		
Condition:	On flapping Spine facing (EVPN) Ve interface on Leaf node.		

Parent Defect ID:	SLXOS-74984	**Issue ID:**	SLXOS-74984
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-74985	**Issue ID:**	SLXOS-74985
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-75006	**Issue ID:**	SLXOS-75006

Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-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		

Parent Defect ID:	SLXOS-75087	**Issue ID:**	SLXOS-75087
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 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.		

The following software defects are open in SLX-OS 20.5.2a as of September 2023:

Parent Defect ID:	SLXOS-73263	**Issue ID:**	SLXOS-74142
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	Some of the valid BGP routes are not selected as best and not installed in routing table.		
Condition:	eBGP routes nexthop is resolved recursively by other eBGP route.		

The following software defects are open in SLX-OS 20.5.2 as of September 2023:

Parent Defect ID:	SLXOS-52746	**Issue ID:**	SLXOS-53722
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1a
Technology Group:	Monitoring	**Technology:**	sFlow
Symptom:	S-flow will not work for Virtual leased lines interface		
Condition:	When Storm control is applied on Virtual leased lines interface		

Parent Defect ID:	SLXOS-55266	**Issue ID:**	SLXOS-55266
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-60302	**Issue ID:**	SLXOS-60754
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Static Routing (IPv4)
Symptom:	Shutting down the uplink port channel from the border leaf to the L3 gateway leads to traffic convergence of nearly 1 second		
Condition:	SLX-8720 is used as the border leaf pair and SLX-9640 as L3 gateway. There are 32 VRFs configured and there are IPv4 and IPv6 routes. There is a port-channel between the BL nodes and the gateway. The port-channel is shut at a border leaf node and the traffic is redirected from the border leaf node to its peer along the ICL. The convergence times for this are found to be more than expected. With static routes, the convergence times are in the order of 1 second. With only BGP routes and PIC enabled, it was upto around 730 msec.		

Parent Defect ID:	SLXOS-61347	**Issue ID:**	SLXOS-61598
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-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-65379	**Issue ID:**	SLXOS-66289
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.		

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-66825	**Issue ID:**	SLXOS-67000
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2fa
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD sessions flaps		
Condition:	Reload of Leaf node connected to SRIOV compute servers.		

Parent Defect ID:	SLXOS-54373	**Issue ID:**	SLXOS-67650
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-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-68208	**Issue ID:**	SLXOS-68208
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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:**	SLXOS 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-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-70473	**Issue ID:**	SLXOS-70473
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:	Traffic redirect to other port after doing clear ip route all on golden eagle.		
Condition:	Issue can be recovered either by removing or reapplying flowspec routemap distribution.		

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-71344	**Issue ID:**	SLXOS-71502
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	OSPF routes installed as result of Static route redistribution in NSSA area is getting deleted even though the same static route entry is present in another device and reachable from the former.		
Condition:	The static route entry is being added and deleted immediately within a interval of 5 secs from one of the advertising devices in NSSA area.		

Parent Defect ID:	SLXOS-68264	**Issue ID:**	SLXOS-71647
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-71395	**Issue ID:**	SLXOS-71655
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-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-71509	**Issue ID:**	SLXOS-72084
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	Forwarding address selection was very generic. We would pick any OSPF-INTERFACE that came up at the last during selection. Here there was no particular logic to fetch the loopback IP always when one is present.		
Condition:	When an external route is advertised into NSSA area as Type7 LSA, the forwarding address picked by the same was physical interface address.		

Parent Defect ID:	SLXOS-72212	**Issue ID:**	SLXOS-72696
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-71948	**Issue ID:**	SLXOS-72891
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2d
Technology Group:	IP Multicast	**Technology:**	IPv4 Multicast Routing
Symptom:	Multicast traffic drops for 5-6 secs or more.		

Condition:	When multiple hosts join and leave a set of groups, in a sequence , such that each group is joined by one host at a time, followed by leave and join the next group in the sequence.
Workaround:	Using static groups.

Parent Defect ID:	SLXOS-72629	**Issue ID:**	SLXOS-73071
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-72893	**Issue ID:**	SLXOS-73087
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	In the IP Fabric environment, 2-8 seconds traffic loss was observed during Maintenance Mode disable on one of the L2 MCT nodes.		
Condition:	In a rare timing scenario, 2-8 seconds of traffic loss is noticed in some East-West flows during Maintenance Mode disable operation on one of the MCT nodes.		
Recovery:	Traffic recovers automatically, but there is a transient drop in the traffic during the Maintenance Mode operation.		

Parent Defect ID:	SLXOS-72973	**Issue ID:**	SLXOS-73128
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	OSPF routing table is advertising the /16 subnet which was removed		
Condition:	Example: Add the following static routes on both Dist01 and Dist02 ip route 10.210.0.0/16 192.168.100.100 ip route 10.210.0.0/24 192.168.100.100 Remove static route 10.210.0.0/16 from both Dist01 and Dist02		
Workaround:	Clear OSPF routes		
Recovery:	clear OSPF routes		

Parent Defect ID:	SLXOS-73047	**Issue ID:**	SLXOS-73047
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2ae
Technology Group:	Management	**Technology:**	SNMP - Simple Network

			Management Protocol
Symptom:	After migrating from Port-channel 20 having Bandwidth of 30G to Port-channel 21 which is having bandwidth of 100G, VE statistics of migrated Vlans shows 30G instead of 100G with SNMP walk.		
Condition:	When port-channels with different Bandwidths are migrated to same VE interface(s), updated Bandwidth is not reflecting in SNMP Walk.		

Parent Defect ID:	SLXOS-72665	**Issue ID:**	SLXOS-73288
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3ac
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD sessions are down on 8720 device		
Condition:	BFD sessions are down on 8720 device		

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-73395	**Issue ID:**	SLXOS-73395
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Default route is not advertised in BGP by using the network command...		
Condition:	When the default route next hop matches with the local BGP peer Address then the BGP is rejecting the route.		
Workaround:	Users can advertise the default route in BGP by using the default originate command.		

Parent Defect ID:	SLXOS-72514	**Issue ID:**	SLXOS-72514
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom:	While transitioning from Backup to Master, the device does not wait for hold-timer in VRRP-E configuration.		
Condition:	When shutdown/no shutdown the VE or boot the router.		

Parent Defect ID:	SLXOS-73468	**Issue ID:**	SLXOS-73586
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.2.00bf
Technology Group:	Monitoring	**Technology:**	Hardware Monitoring
Symptom:	Unqualified Optic warning message thrown for connected ports during SLX bootup.		
Condition:	While connecting non-Extreme/Brocade Optic.		

Parent Defect ID:	SLXOS-73061	**Issue ID:**	SLXOS-73061
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	When TM debug command "show tm non-empty-queues" is executed there is no queue core information available in the command output.		
Condition:	On SLX 9740, SLX 9640, SLX 9540, and Extreme 8820 platforms.		

Parent Defect ID:	SLXOS-73629	**Issue ID:**	SLXOS-73629
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	Up Mep is not settled on SLX 9740/Extreme 8870 devices with VPLS configurations.		
Condition:	Up Mep is configured on breakout ports (: 2, :3 and :4) on the SLX 9740/Extreme 8870 ports 41-80.		
Workaround:	Reload the device with breakout ports(:2,:3,:4) configurations on ports 41-80.		

Parent Defect ID:	SLXOS-73646	**Issue ID:**	SLXOS-73646
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	GRE - Generic Routing Encapsulation
Symptom:	GRE Tunnel Termination statistics enabled by default		

Condition:	GRE Tunnel Termination statistics enabled by default in HW due to an ASIC limitation. Even though it is enabled by default, GRE Tunnel statistics will not be accounted until 'statistics' is configured for Tunnel.

Parent Defect ID:	SLXOS-73263	**Issue ID:**	SLXOS-73263
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	Some of the valid BGP routes are not selected as best and not installed in routing table.		
Condition:	eBGP routes nexthop is resolved recursively by other eBGP route.		

Parent Defect ID:	SLXOS-73712	**Issue ID:**	SLXOS-73712
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	Up Mep DM is not working as expected on SLX 9740/Extreme 8870 80C devices.		
Condition:	When Up Mep is configured on ports 41-80 on SLX 9740/Extreme 8870 80C devices.		

Parent Defect ID:	SLXOS-73637	**Issue ID:**	SLXOS-73637
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Other	**Technology:**	Other
Symptom:	Unable to login TPVM with LDAP user credentials		
Condition:	Issue observed when Windows AD LDAP server is configured with TPVM.		

Parent Defect ID:	SLXOS-73769	**Issue ID:**	SLXOS-73769
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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:**	SLXOS 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		

Defects Closed with Code Changes

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.		

The following software defects were closed in 20.5.3a with code changes as of December 2023:

Parent Defect ID:	SLXOS-74893	**Issue ID:**	SLXOS-75178
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-75183	**Issue ID:**	SLXOS-75185
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-75006	**Issue ID:**	SLXOS-75190
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-74802	**Issue ID:**	SLXOS-75220
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:	BFD multihop IPv6 sessions flap		
Condition:	When BFD multihop session is configured on the SLX 9740-40c device.		

Parent Defect ID:	SLXOS-75262	**Issue ID:**	SLXOS-75262
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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.		

Parent Defect ID:	SLXOS-74943	**Issue ID:**	SLXOS-75269
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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.		

The following software defects were closed in 20.5.3 with code changes as of November 2023:

Parent Defect ID:	SLXOS-71170	**Issue ID:**	SLXOS-71170
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 session flaps		
Condition:	port-channel ports span across different units		

Parent Defect ID:	SLXOS-71344	**Issue ID:**	SLXOS-71502
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	OSPF routes installed as result of Static route redistribution in NSSA area is getting deleted even though the same static route entry is present in another device and reachable from the former.		
Condition:	The static route entry is being added and deleted immediately within a interval of 5 secs from one of the advertising devices in NSSA area.		

Parent Defect ID:	SLXOS-71509	**Issue ID:**	SLXOS-72084
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	Forwarding address selection was very generic. We would pick any OSPF-INTERFACE that came up at the last during selection. Here there was no particular logic to fetch the loopback IP always when one is present.		
Condition:	When an external route is advertised into NSSA area as Type7 LSA, the forwarding address picked by the same was physical interface address.		

Parent Defect ID:	SLXOS-72267	**Issue ID:**	SLXOS-72267
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1cb
Technology Group:	Security	**Technology:**	ACLs - Access Control Lists
Symptom:	When ACL is configured with dscp-force value, ACL will not work to redirect configured traffic DSCP value at egress.		
Condition:	When there is high priority traffic with congestion and ACL is applied with dscp-force to 0, ACL will not work to redirect DSCP value at 0 egress.		

Parent Defect ID:	SLXOS-72271	**Issue ID:**	SLXOS-72271
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2c
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	When TM Queue size is changed and queues are congested on specific core, L2/L3 protocol packets may be dropped. When 'show tm non-empty' command is executed, the core queue information is not displayed to debug issue in SLX 9540/9640 platforms.		
Condition:	When TM Queue size is changed, and when 'show tm non-empty' command is executed.		

Parent Defect ID:	SLXOS-72294	**Issue ID:**	SLXOS-72294
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ICMP - Internet Control Message Protocol

Symptom:	Duplicate ICMP packet observed
Condition:	Duplicate ICMP packet is observed when Ping is initiated from Border Leaf

Parent Defect ID:	SLXOS-72514	**Issue ID:**	SLXOS-72514
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom:	While transitioning from Backup to Master, the device does not wait for hold-timer in VRRP-E configuration.		
Condition:	When shutdown/no shutdown the VE or boot the router.		

Parent Defect ID:	SLXOS-72524	**Issue ID:**	SLXOS-72524
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3j
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	When there is high data traffic coming to CPU with high TOS values, it may fill-up high priority queues and impact BGP sessions.		
Condition:	When there is high data traffic coming to CPU with high TOS values.		

Parent Defect ID:	SLXOS-72775	**Issue ID:**	SLXOS-72775
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	Traffic drop seen since ARP is not resolved at the client side.		
Condition:	ARP packets are being transmitted with non-zero padding.		

Parent Defect ID:	SLXOS-71948	**Issue ID:**	SLXOS-72891
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2d
Technology Group:	IP Multicast	**Technology:**	IPv4 Multicast Routing
Symptom:	Multicast traffic drops for 5-6 secs or more.		
Condition:	When multiple hosts join and leave a set of groups, in a sequence , such that each group is joined by one host at a time, followed by leave and join the next group in the sequence.		
Workaround:	Using static groups.		

Parent Defect ID:	SLXOS-72935	**Issue ID:**	SLXOS-72935
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Other	**Technology:**	Other
Symptom:	Extra link flap is observed during reboot.		
Condition:	When reloads the device.		

Parent Defect ID:	SLXOS-72973	**Issue ID:**	SLXOS-72973
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	OSPF routing table is advertising the /16 subnet which was removed		
Condition:	Example: Add the following static routes on both Dist01 and Dist02 ip route 10.210.0.0/16 192.168.100.100 ip route 10.210.0.0/24 192.168.100.100 Remove static route 10.210.0.0/16 from both Dist01 and Dist02		
Workaround:	Clear OSPF routes		
Recovery:	clear OSPF routes		

Parent Defect ID:	SLXOS-73047	**Issue ID:**	SLXOS-73047
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2ae
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	After migrating from Port-channel 20 having Bandwidth of 30G to Port-channel 21 which is having bandwidth of 100G, VE statistics of migrated Vlans shows 30G instead of 100G with SNMP walk.		
Condition:	When port-channels with different Bandwidths are migrated to same VE interface(s), updated Bandwidth is not reflecting in SNMP Walk.		

Parent Defect ID:	SLXOS-73061	**Issue ID:**	SLXOS-73061
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	When TM debug command "show tm non-empty-queues" is executed there is no queue core information available in the command output.		
Condition:	On SLX 9740, SLX 9640, SLX 9540, and Extreme 8820 platforms.		

Parent Defect ID:	SLXOS-73106	**Issue ID:**	SLXOS-73121
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	OSPF sometimes installs suboptimal path for a destination.		
Condition:	When there are 2 ECMP paths to a destination in NSSA area, the forwarding address chosen for Type-7 and Type-5 LSA was not of the optimal path.		

Parent Defect ID:	SLXOS-73148	**Issue ID:**	SLXOS-73148
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3ja
Technology Group:	Monitoring	**Technology:**	RAS - Reliability, Availability, and Serviceability
Symptom:	RASLOG messages for TCAM resources reached low threshold of a shared resource count is not clear, and the count of displayed high threshold of individual resource from shared pool is incorrect when reached after going to low threshold and back.		
Condition:	1. When shared resource reaches the low threshold watermark RASLOG was getting generated for last individual resource of shared resource whose count was used in display instead of total shared count of shared resource. 2. When shared resource total reached the high threshold watermark from low threshold RASLOG was showing incorrect count of individual resource in the RASLOG		

Parent Defect ID:	SLXOS-73445	**Issue ID:**	SLXOS-73445
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1d
Technology Group:	Security	**Technology:**	ACLs - Access Control Lists
Symptom:	Packet drops are observed when broadcast IP ACL is configured globally.		
Condition:	With /31 IPv4 netmask configured for the L3 interface.		

Parent Defect ID:	SLXOS-73557	**Issue ID:**	SLXOS-73557
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol

Symptom:	Received EVPN NLRI's are not imported.
Condition:	Received NlRI's RD matches with locally configured RD.

Parent Defect ID:	SLXOS-73600	**Issue ID:**	SLXOS-73600
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1a
Technology Group:	Security	**Technology:**	PBR - Policy-Based Routing
Symptom:	Cannot delete a route-map stanza if the route-map is applied to BGP. Error 'Route-map associated with a bgp neighbor' is seen.		
Condition:	Applying route-map on BGP neighbors		

Parent Defect ID:	SLXOS-73629	**Issue ID:**	SLXOS-73629
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	Up Mep is not settled on SLX 9740/Extreme 8870 devices with VPLS configurations.		
Condition:	Up Mep is configured on breakout ports (: 2, :3 and :4) on the SLX 9740/Extreme 8870 ports 41-80.		
Workaround:	Reload the device with breakout ports(:2,:3,:4) configurations on ports 41-80.		

Parent Defect ID:	SLXOS-73646	**Issue ID:**	SLXOS-73646
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	GRE - Generic Routing Encapsulation
Symptom:	GRE Tunnel Termination statistics enabled by default		
Condition:	GRE Tunnel Termination statistics enabled by default in HW due to an ASIC limitation. Even though it is enabled by default, GRE Tunnel statistics will not be accounted until 'statistics' is configured for Tunnel.		

Parent Defect ID:	SLXOS-73653	**Issue ID:**	SLXOS-73653
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2c
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	When TM Queue size is changed and queues are congested on specific core, L2/L3 protocol packets may be dropped. When 'show tm non-empty' command is executed, the core queue		

	information is not displayed to debug issue in SLX 9640/9740 platforms.
Condition:	When TM Queue size is changed, and when 'show tm non-empty' command is executed.

Parent Defect ID:	SLXOS-73701	**Issue ID:**	SLXOS-73701
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	Sometimes local hosts are not reachable on delete and re-creation of VE interface.		
Condition:	This is a timing issue which might be seen with XCO/EFA. The XCO/EFA ctag-range-delete operation triggers VE-unbind and VE-delete operations on the SLX in quick succession. And, sometimes the HAL layer receives messages in reverse order because of rapid configuration changes. The reversal of messages could leave a stale hardware L3 entry, thereby causing issues in subsequent VE re-creation.		
Workaround:	Try EFA ctag-range-delete followed by ctag-range-add again		
Recovery:	Delete and re-create VE using NOSCLI to recover from the situation		

Parent Defect ID:	SLXOS-73712	**Issue ID:**	SLXOS-73712
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	Up Mep DM is not working as expected on SLX 9740/Extreme 8870 80C devices.		
Condition:	When Up Mep is configured on ports 41-80 on SLX 9740/Extreme 8870 80C devices.		

Parent Defect ID:	SLXOS-73850	**Issue ID:**	SLXOS-73850
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3ja
Technology Group:	Management	**Technology:**	Configuration Fundamentals
Symptom:	"dampening" configuration under "router bgp" hierarchy is lost after device is restarted.		
Condition:	During upgrade/downgrade or reload operations, if configuration is applied from startup configuration file.		
Recovery:	Configure "dampening" via CLI after device is restarted.		

Parent Defect ID:	SLXOS-73931	**Issue ID:**	SLXOS-73931
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3b
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	Dcmd crash observed		
Condition:	radius-server host configuration exists with default-vrf or user vrf.		

Parent Defect ID:	SLXOS-74011	**Issue ID:**	SLXOS-74011
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3ac
Technology Group:	Other	**Technology:**	Other
Symptom:	All the port are detected as SFP ABSENT.		
Condition:	SLXOS upgrade and reload scenario.		

Parent Defect ID:	SLXOS-74092	**Issue ID:**	SLXOS-74092
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Security	**Technology:**	AAA - Authentication, Authorization, and Accounting
Symptom:	While setting GRUB password protection, an error message maybe observed.		
Condition:	While applying Grub password in Grub config mode: DUT(config-grub)# username grubuser password password Message Generic Error DUT(config-grub)#		

Parent Defect ID:	SLXOS-74115	**Issue ID:**	SLXOS-74115
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	When DHCPv4 Relay is re-configured with specific VE followed by VLAN creation, DHCP packets are not relayed from software and DHCP relayed stats don't show any packets.		
Condition:	When DHCPv4 Relay is re-configured VE followed by VLAN creation sequence.		

Parent Defect ID:	SLXOS-74157	**Issue ID:**	SLXOS-74157
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1a

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP daemon reload seen in Unified routing scenarios.		
Condition:	RIBOUT entries are not cleaned up before NLRI is freed, resulting in stale Ribout entries.		

Parent Defect ID:	SLXOS-73249	**Issue ID:**	SLXOS-74249
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2a
Technology Group:	Monitoring	**Technology:**	Hardware Monitoring
Symptom:	'show hw route-info linecard 0' command display may not be correct for IPv6 route entries with incorrect LPM add result values.		
Condition:	When 'show hw route-info linecard 0' is executed with IPv6 traffic.		

Parent Defect ID:	SLXOS-74258	**Issue ID:**	SLXOS-74258
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2c
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP daemon keeps reloading causing SLX to enter boot loop.		
Condition:	The issue is a combination of receiving 316 communities, which is the maximum can be accepted, and then the route-map which adds additional communities to the existing ones.		

Parent Defect ID:	SLXOS-74330	**Issue ID:**	SLXOS-74330
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1a
Technology Group:	Other	**Technology:**	Other
Symptom:	SLXOS upgrade and reload scenario.		
Condition:	all the port are detected as SFP ABSENT		

Parent Defect ID:	SLXOS-74499	**Issue ID:**	SLXOS-74499
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2ad
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Static Routing (IPv4)
Symptom:	Unexpected reload of device.		
Condition:	With static route of more than 128 ECMP paths, device may reload unexpectedly.		
Workaround:	Provision static route with less than or equal to 128 ECMP paths only		

Recovery:	Remove static routes with more than 128 ECMP paths.

Parent Defect ID:	SLXOS-74158	**Issue ID:**	SLXOS-74523
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2
Technology Group:	Security	**Technology:**	User Accounts & Passwords
Symptom:	On SLX8820 platform, root password cannot be changed properly.		
Condition:	1. On 8820 platform, go to shell using "start-shell" command 2. Using, "su" or "su -" commands, try to get into root-shell and then try changing the password, using "passwd" command. 3. Reload the device and again perform steps 1 & 2.		

Parent Defect ID:	SLXOS-74638	**Issue ID:**	SLXOS-74638
Severity:	S1 - Critical		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4b
Technology Group:	Layer 2 Switching	**Technology:**	VXLAN - Virtual Extensible LAN
Symptom:	In an IP fabric environment, L2 MAC from another leaf cluster is showing as having been learned on a port channel instead of the EVPN tunnel.		
Condition:	Some times, when a MAC moves from local port channel to remote logical VTEP, it remains inconsistent as local on one cluster node, but as EVPN on the peer node of the cluster. The expectation is to have the same MAC state on both MCT nodes, whether they are Local or EVPN in a consistent manner once the MAC move settles.		
Recovery:	Clearing the MAC on the local port channel may resolve the situation. The port channel flap should flush all local macs and relearn as EVPN if MAC clear does not resolve the issue.		

Parent Defect ID:	SLXOS-74662	**Issue ID:**	SLXOS-74662
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	Multiple stale entries observed in the Ifmacdb table.		
Condition:	When ARP entries move from one VE to another, the device adds the new node to the ifmacdb table and keeps the old node as stale.		

Parent Defect ID:	SLXOS-74694	**Issue ID:**	SLXOS-74694
Severity:	S3 - Moderate		

Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2a
Technology Group:	Monitoring	**Technology:**	Sysmon
Symptom:	Show media reports alarm status as high for optic even though values are within range		
Condition:	Below are the CLI's affected. "show media inter ethe <>" "show media optical-monitoring"		

Parent Defect ID:	SLXOS-74784	**Issue ID:**	SLXOS-74784
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1a
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Port channel is shown 'admin down' even though it is not shutdown during configuration		
Condition:	Port channel does not come up after a reload of the primary node, while the secondary node is undergoing Cluster bring up after an earlier reload.		

Parent Defect ID:	SLXOS-74797	**Issue ID:**	SLXOS-74957
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1da
Technology Group:	Traffic Management	**Technology:**	Rate Limiting and Shaping
Symptom:	When traffic requiring fragmentation is received at high rate, it may cause high CPU rate which may impact control traffic with protocols flaps.		
Condition:	When traffic requiring fragmentation is received at high rate, it may cause high CPU rate which may impact control traffic with protocols flaps.		

The following software defects were closed in 20.5.2a with code changes as of September 2023:

Parent Defect ID:	SLXOS-71948	**Issue ID:**	SLXOS-71948
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2d
Technology Group:	IP Multicast	**Technology:**	IPv4 Multicast Routing
Symptom:	Multicast traffic drops for 5-6 secs or more.		
Condition:	When multiple hosts join and leave a set of groups, in a sequence , such that each group is joined by one host at a time, followed by leave and join the next group in the sequence.		
Workaround:	Using static groups.		

Parent Defect ID:	SLXOS-72935	**Issue ID:**	SLXOS-73792
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Other	**Technology:**	Other
Symptom:	Extra link flap is observed during reboot.		
Condition:	When reloads the device.		

Parent Defect ID:	SLXOS-73712	**Issue ID:**	SLXOS-73994
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	Up Mep DM is not working as expected on SLX 9740/Extreme 8870 80C devices.		
Condition:	When Up Mep is configured on ports 41-80 on SLX 9740/Extreme 8870 80C devices.		

Parent Defect ID:	SLXOS-73629	**Issue ID:**	SLXOS-74018
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	Up Mep is not settled on SLX 9740/Extreme 8870 devices with VPLS configurations.		
Condition:	Up Mep is configured on breakout ports (: 2, :3 and :4) on the SLX 9740/Extreme 8870 ports 41-80.		
Workaround:	Reload the device with breakout ports(:2,:3,:4) configurations on ports 41-80.		

The following software defects were closed in 20.5.2 with code changes as of September 2023:

Parent Defect ID:	SLXOS-61208	**Issue ID:**	SLXOS-61283
Reason Code:	Not Reproducible	**Severity:**	S2 -– Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2b
Technology Group:	Other	**Technology:**	Other
Symptom:	SLX 9540 device does not respond		
Condition:	Taking suppotsave when the free memory is below 600Mb.		
Recovery:	Power off/on the device		

Parent Defect ID:	SLXOS-67049	**Issue ID:**	SLXOS-67663
Reason Code:	Will Not Fix	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4a
Technology Group:	Monitoring	**Technology:**	Hardware Monitoring
Symptom:	Flow based mirroring stopped working		

Condition:	On SLX-9150/9250 Platform port channel is configured as destination interface in monitor session in flow based mirroring.
Recovery:	Rebind ACL on the Source interface configured in flow based monitor session

Parent Defect ID:	SLXOS-66994	**Issue ID:**	SLXOS-67853
Reason Code:	Not Reproducible	**Severity:**	S2 -– Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2fa
Technology Group:	Monitoring	**Technology:**	Port Mirroring
Symptom:	For mirrored traffic ICMP reply packets are seen before ICM request packets.		
Condition:	When a PO is used as source interface for mirroring.		

Parent Defect ID:	SLXOS-68416	**Issue ID:**	SLXOS-68416
Reason Code:	Insufficient Information	**Severity:**	S2 -– Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Increase in NHID count for the 8K BFD scaled configuration		
Condition:	PIC is enabled/disabled and SLX device is rebooted		

Parent Defect ID:	SLXOS-69448	**Issue ID:**	SLXOS-69448
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1cb
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Unexpected reload on SLX device.		
Condition:	SLX is trying to process the unexpected flow spec rules sent from the peer device.		

Parent Defect ID:	SLXOS-69962	**Issue ID:**	SLXOS-69962
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1c
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Device may reload [with rpsd] when we try to clear the large number[>1024] of BGP flowspec rules/neighbor.		
Condition:	RPSD module and device may reload, once after clearing the BGP neighbor which has populated with large number of flowpsec rules[>1024].		

Parent Defect ID:	SLXOS-70482	**Issue ID:**	SLXOS-70828
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Security	**Technology:**	SSH - Secure Shell
Symptom:	SSH(sshd) process stops running after node reload.		
Condition:	Noticed in case of making remote side connection of management port DOWN.		

Parent Defect ID:	SLXOS-71312	**Issue ID:**	SLXOS-71373
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	MBGP - Multiprotocol Border Gateway Protocol
Symptom:	IP- Prefixes learnt via EVPN neighbor is not cleaned up properly.		
Condition:	EVPN Neighbor goes down and IP-Prefixes learned via particular neighbor are imported by multiple VRF's.		

Parent Defect ID:	SLXOS-71127	**Issue ID:**	SLXOS-71556
Reason Code:	Already Implemented	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1c
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) reporting very large value/zero CPU utilization.		
Condition:	While doing the snmpwalk for this OID (1.3.6.1.4.1.1588.3.1.12.1.1.1.3.1.60), it is displaying very large value/sometime Zero CPU utilization in SNMP response randomly.		

Parent Defect ID:	SLXOS-72014	**Issue ID:**	SLXOS-72192
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1cb
Technology Group:	Other	**Technology:**	Other
Symptom:	System may reload on executing CMSH DIAG command.		
Condition:	In execution of ‘show diag pp-fdt interface’ command for non-existing (loopback/port-channel) interface.		

Parent Defect ID:	SLXOS-72268	**Issue ID:**	SLXOS-72268
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3a
Technology Group:	Management	**Technology:**	SNMP - Simple Network

			Management Protocol
Symptom:	Device became unresponsive and Nsmd daemon reload was seen after upgrading to 20.4.3a.		
Condition:	SNMP query to fetch VE statistics for scaled VE interfaces may causing this issue.		

Parent Defect ID:	SLXOS-72298	**Issue ID:**	SLXOS-72298
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	IPv6 dynamic BGP failed to establish.		
Condition:	Flapping of MCT cluster's client interface.		

Parent Defect ID:	SLXOS-72163	**Issue ID:**	SLXOS-72388
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3ac
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	During an upgrade, loss is seen on some traffic streams		
Condition:	BFD and BGP sessions are not established since ICL drops the traffic passing through		
Recovery:	Flapping the ICL link would help to recover the traffic		

Parent Defect ID:	SLXOS-72010	**Issue ID:**	SLXOS-72483
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	EVPN Multi-homed peer is not updated with correct MAC and Port mapping		
Condition:	Host moves from one port-channel to other port-channel.		

Parent Defect ID:	SLXOS-72076	**Issue ID:**	SLXOS-72624
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	When the dynamic BGP peer goes down, the relevant SNMP trap is not generated.		
Condition:	The necessary condition for dynamic BGP peer goes down		

Parent Defect ID:	SLXOS-71969	**Issue ID:**	SLXOS-72637
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2
Technology Group:	Other	**Technology:**	Other
Symptom:	The 100G link does not come up online on platform SLX 9740		
Condition:	When FEC mode is configured as disabled and reload with full install.		

Parent Defect ID:	SLXOS-72639	**Issue ID:**	SLXOS-72639
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1ca
Technology Group:	Other	**Technology:**	Other
Symptom:	The "Unqualified SFP transceiver" message appears on the console during the reload or breakout.		
Condition:	When SPTSBP3PTCXT003 optic is used in the qsfp28 ports on SLX device.		

Parent Defect ID:	SLXOS-71903	**Issue ID:**	SLXOS-72756
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.1.00a
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP OID IF-MIB::ifType of port-channel returns value Other(1) instead of ieee8023adLag(161).		
Condition:	Configure port-channel.		

Parent Defect ID:	SLXOS-70648	**Issue ID:**	SLXOS-72766
Reason Code:	Will Not Fix	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.1.00m
Technology Group:	MPLS	**Technology:**	MPLS VPLS - Virtual Private LAN Services
Symptom:	Pseudowires flaps		
Condition:	After continuous link down event		

Parent Defect ID:	SLXOS-72770	**Issue ID:**	SLXOS-72829
Reason Code:	Working as Designed	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMPGet output not matches with its (Upper/Lower)case to SNMP trap output.		
Condition:	Validate both SNMP Get and SNMP trap(pcap) output.		

Parent Defect ID:	SLXOS-72611	**Issue ID:**	SLXOS-72837
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1d
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	Learning ARP from other subnet (non-connected) host.		
Condition:	Made IP with different subnet(host) to learn on SLX ARP table.		

Parent Defect ID:	SLXOS-72195	**Issue ID:**	SLXOS-72853
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3g
Technology Group:	Traffic Management	**Technology:**	Traffic Queueing and Scheduling
Symptom:	BFD and OSPF session flaps are observed in SLX 9540.		
Condition:	BFD and OSPF session flaps are observed if there is high latency due to internal CPU packet processing delays in hardware.		

Parent Defect ID:	SLXOS-72504	**Issue ID:**	SLXOS-72858
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2e
Technology Group:	Traffic Management	**Technology:**	Traffic Queueing and Scheduling
Symptom:	BFD and OSPF flaps are observed in SLX 9540.		
Condition:	BFD and OSPF flaps are observed if there is high latency due to internal CPU packet processing delays in hardware.		

Parent Defect ID:	SLXOS-71680	**Issue ID:**	SLXOS-72885
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1d
Technology Group:	Monitoring	**Technology:**	Hardware Monitoring
Symptom:	Speed failure trace seen on every SLX bootup.		
Condition:	SLX 9740 to be configured with 40G speed.		

Parent Defect ID:	SLXOS-72779	**Issue ID:**	SLXOS-72899
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2d
Technology Group:	IP Multicast	**Technology:**	IGMP - Internet Group Management Protocol
Symptom:	Multicast traffic drop of 1-2 minutes		
Condition:	When sending IGMPv3 report with source as 0.0.0.0, followed by sending IGMPv3 joins, and the configured version on switch is version v3.		

Workaround:	Configuring the switch with IGMP version v2 instead of version v3.

Parent Defect ID:	SLXOS-72880	**Issue ID:**	SLXOS-72917
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	IPv6 traffic loss seen for a few flows after a node reload or power cycle.		
Condition:	IPv6 Neighbor entries associated with wrong VE interface causing the packets to be blackholed.		

Parent Defect ID:	SLXOS-72912	**Issue ID:**	SLXOS-72923
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	IPv6 traffic loss seen for a few flows after a node reload or power cycle.		
Condition:	IPv6 Neighbor entries associated with wrong VE interface causing the packets to be blackholed.		

Parent Defect ID:	SLXOS-72886	**Issue ID:**	SLXOS-72928
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	IPv6 traffic loss seen for a few flows after a node reload or power cycle.		
Condition:	IPv6 Neighbor entries associated with wrong VE interface causing the packets to be blackholed.		

Parent Defect ID:	SLXOS-72907	**Issue ID:**	SLXOS-72933
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	IPv6 traffic loss seen for a few flows after a node reload or power cycle.		
Condition:	IPv6 Neighbor entries associated with wrong VE interface causing the packets to be blackholed.		

Parent Defect ID:	SLXOS-72945	**Issue ID:**	SLXOS-72952
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	IPv6 traffic loss seen for a few flows after a node reload or power cycle.		
Condition:	IPv6 Neighbor entries associated with wrong VE interface causing the packets to be blackholed.		

Parent Defect ID:	SLXOS-72305	**Issue ID:**	SLXOS-73025
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4a
Technology Group:	Layer 2 Switching	**Technology:**	VXLAN - Virtual Extensible LAN
Symptom:	VxLAN packets from VMWare VTEP are dropped on the trunk port in MCT/IP fabric environment.		
Condition:	In an MCT environment incoming VxLAN traffic from VMWare hosts is dropped when the ingress port is configured as a trunk port and the incoming traffic is tagged VxLAN. No drops are noticed when the ingress port is configured as an access port or router port and incoming traffic is untagged VxLAN.		
Workaround:	No known workarounds.		
Recovery:	No known recovery methods.		

Parent Defect ID:	SLXOS-72959	**Issue ID:**	SLXOS-73080
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2b
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Pseudo-wire clients configured under MCT Cluster is down		
Condition:	Post Maintenance-Mode upgrade, Pseudo-wire clients configured under MCT Cluster does not come up		

Parent Defect ID:	SLXOS-73082	**Issue ID:**	SLXOS-73082
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP filtered routes are stuck in the routing table (RIB/FIB)		
Condition:	1. Device runs e-BGP neighborship with 2 peers 2. Device learns a route from both these peers and installs both the routes as ECMP routes. 3. A prefix-list filter is applied to the DUT towards the peer from		

	which it learns the non-BEST route to deny the learned routes from this peer.

Parent Defect ID:	SLXOS-72780	**Issue ID:**	SLXOS-73142
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2d
Technology Group:	IP Multicast	**Technology:**	PIM - Protocol-Independent Multicast
Symptom:	Traffic loss seen on a few streams, attached to a prefix list with PIM RP		
Condition:	When more than one PIM RP with prefix list is present on a switch. Upon reload traffic drop for a few prefixes will be seen.		
Workaround:	Reconfigure PIM RPs, followed by PIM RP with prefix list.		

Parent Defect ID:	SLXOS-69469	**Issue ID:**	SLXOS-73282
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2
Technology Group:	Other	**Technology:**	Other
Symptom:	Interface displayed as SFP absent		
Condition:	When the device is reloaded multiple times.		

Parent Defect ID:	SLXOS-73107	**Issue ID:**	SLXOS-73368
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3ac
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	ARP is not resolved for few VE IP addresses		
Condition:	ARP is not resolved for few VE IP addresses after a Cluster client interface is toggled a few times		
Recovery:	Flap the cluster client interface again		

Parent Defect ID:	SLXOS-65710	**Issue ID:**	SLXOS-73374
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2d
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Cluster client stops forwarding traffic		
Condition:	When LACP state is toggled, Cluster client stops forwarding traffic		
Recovery:	Shutting down the Cluster client and re-enabling it		

Parent Defect ID:	SLXOS-72935	**Issue ID:**	SLXOS-73792
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Other	**Technology:**	Other

Symptom:	Extra link flap is observed during reboot.
Condition:	When reloads the device.

Defects Closed without Code Changes

NOTE: No defects were closed without code changes in 20.5.3c.

NOTE: No defects were closed without code changes in 20.5.3b.

NOTE: No defects were closed without code changes in 20.5.3a.

The following software defects were closed in 20.5.3 without code changes as of November 2023:

Parent Defect ID:	SLXOS-52746	**Issue ID:**	SLXOS-53722
Reason Code:	Design Limitation	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1a
Technology Group:	Monitoring	**Technology:**	sFlow
Symptom:	S-flow will not work for Virtual leased lines interface		
Condition:	When Storm control is applied on Virtual leased lines interface		

Parent Defect ID:	SLXOS-60302	**Issue ID:**	SLXOS-60754
Reason Code:	Not Reproducible	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Static Routing (IPv4)
Symptom:	Shutting down the uplink port channel from the border leaf to the L3 gateway leads to traffic convergence of nearly 1 second		
Condition:	SLX-8720 is used as the border leaf pair and SLX-9640 as L3 gateway. There are 32 VRFs configured and there are IPv4 and IPv6 routes. There is a port-channel between the BL nodes and the gateway. The port-channel is shut at a border leaf node and the traffic is redirected from the border leaf node to its peer along the ICL. The convergence times for this are found to be more than expected. With static routes, the convergence times are in the order of 1 second. With only BGP routes and PIC enabled, it was upto around 730 msec.		

Parent Defect ID:	SLXOS-66825	**Issue ID:**	SLXOS-67000
Reason Code:	Not Reproducible	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2fa
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD sessions flaps		
Condition:	Reload of Leaf node connected to SRIOV compute servers.		

Parent Defect ID:	SLXOS-70473	**Issue ID:**	SLXOS-70473
Reason Code:	Already Implemented	**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:	Traffic redirect to other port after doing clear ip route all on golden eagle.		
Condition:	Issue can be recovered either by removing or reapplying flowspec routemap distribution.		

Parent Defect ID:	SLXOS-72893	**Issue ID:**	SLXOS-73087
Reason Code:	Not Reproducible	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.1
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	In the IP Fabric environment, 2-8 seconds traffic loss was observed during Maintenance Mode disable on one of the L2 MCT nodes.		
Condition:	In a rare timing scenario, 2-8 seconds of traffic loss is noticed in some East-West flows during Maintenance Mode disable operation on one of the MCT nodes.		
Recovery:	Traffic recovers automatically, but there is a transient drop in the traffic during the Maintenance Mode operation.		

Parent Defect ID:	SLXOS-73395	**Issue ID:**	SLXOS-73395
Reason Code:	Insufficient Information	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Default route is not advertised in BGP by using the network command...		
Condition:	When the default route next hop matches with the local BGP peer Address then the BGP is rejecting the route.		
Workaround:	Users can advertise the default route in BGP by using the default originate command.		

Parent Defect ID:	SLXOS-73468	**Issue ID:**	SLXOS-73586
Reason Code:	Already Implemented	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.2.00bf
Technology Group:	Monitoring	**Technology:**	Hardware Monitoring
Symptom:	Unqualified Optic warning message thrown for connected ports during SLX bootup.		
Condition:	While connecting non-Extreme/Brocade Optic.		

Parent Defect ID:	SLXOS-74170	**Issue ID:**	SLXOS-74170
Reason Code:	Already Implemented	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3j
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	Interface packet statistics not display's run time traffic byte count.		
Condition:	Clearing counters will help to see this issue through SNMP MIB IfHCInOctets, IfHCOutOctets.		

Parent Defect ID:	SLXOS-74322	**Issue ID:**	SLXOS-74322
Reason Code:	Already Implemented	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1b
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD session flap across many interfaces.		
Condition:	Create BFD offload session.		

Parent Defect ID:	SLXOS-74357	**Issue ID:**	SLXOS-74357
Reason Code:	Already Implemented	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2ad
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	Spontaneous BFD session flap.		
Condition:	BFD session to be established with SRIOV.		

Parent Defect ID:	SLXOS-74372	**Issue ID:**	SLXOS-74372
Reason Code:	Insufficient Information	**Severity:**	S1 - Critical
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2
Technology Group:	Monitoring	**Technology:**	Syslog
Symptom:	SLX device experiences kernel panic with OOM and noticed sudden hike on syslog memory usage.		
Condition:	SLX receiving consistent syslog certificate expiry message as EFA/XCO installed with old.		

Parent Defect ID:	SLXOS-74530	**Issue ID:**	SLXOS-74530
Reason Code:	Already Implemented	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.3ac

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	Invalid ARP entry installed.		
Condition:	VE receiving GARP from another subnet.		

Parent Defect ID:	SLXOS-74862	**Issue ID:**	SLXOS-74862
Reason Code:	Already Implemented	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4b
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	MAC entry programmed only on one node of MCT Pair.		
Condition:	On condition of contiguous mac-move on MCT pair.		

The following software defects were closed in 20.5.2a without code changes as of September 2023:

Parent Defect ID:	SLXOS-73395	**Issue ID:**	SLXOS-73998
Reason Code:	Insufficient Information	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.5.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Default route is not advertised in BGP by using the network command...		
Condition:	When the default route next hop matches with the local BGP peer Address then the BGP is rejecting the route.		
Workaround:	Users can advertise the default route in BGP by using the default originate command.		