August 2023

Extreme SLX-OS 20.5.1b

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 9037771-02 Rev AA

Contents

Preface 5
Release Overview 7
Behavior Changes 8
Software Features 10
CLI Commands 16
Hardware Support 21
Supported FEC modes 25
Software Download and Upgrade 27
Limitations and Restrictions 33
Open Defects 38
Defects Closed with Code Changes 52
Defects Closed without Code Changes 62

Document History

Version	Summary of changes	Publication date
1.0	Initial version for 20.5.1b	August 2023

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 20.5.1b provides the following features:

- Critical defect fixes

Release SLX-OS 20.5.1a provides the following features:

- Critical defect fixes

Release SLX-OS 20.5.1 provides the following features:

- eBGP Nexthop Recursion
- BGP ADD-PATH support to receive 128-path routes advertised over eBGP
- Increasing BGP peer group scale to 1024
- Increasing ECMP scale to 128
- BMC Security Hardening
- NETCONF Bulking and DRC support for BGP related configurations
- EVPN-MH Enhancement - Deriving ES import extended RT from ESI
- Increasing sFlow sample rate values above 100K on SLX 9740 and Extreme 8820 platforms
- Add Description field for ACL, Route-maps, Static Routes
- Improvements for '`show media`' command
- Permissions for log files are changed to enhance their security

Release SLX-OS 20.4.3a provides the following features:

- Critical defect fixes

Release SLX-OS 20.4.3 provides the following features:

- A new HW platform – Extreme 8820 in two form factors – 40C and 80C.
- Delivers Trusted Delivery Solution on Extreme 8820
- VE interface config bulking (IP Fabric Upgrade Optimization)
- IP Fabric QoS Enhancements
- Removal of DF towards IP Fabric (local bias support for LVTEP)
- IPv6 Manageability on SLX TPVM – LDAP support
- IPv6 Egress based ACL rate limiting
- Recursive Next-hop resolution for PBR route-maps
- Notify user to activate BGP peer group to apply route-maps
- 100G Optics qualification

Release SLX-OS 20.4.2b provides the following features:

- Critical defect fixes

Release SLX-OS 20.4.2a provides the following features:

- Critical defect fixes

Release SLX-OS 20.4.2 provides the following features:

- Maintenance Mode Optimizations for IP Fabric Upgrade
- Ability to control service bindings for SNMP listening services
- Ability to disable processing of packets utilizing IP Options
- Support for Password Handling for special characters on SLX-OS
- Increased the allowed anycast-address entries per interface from 64 to 512
- Additional Ipv6 protocol support on TPVM
- Additional SNMP Notification Event support from SLX
- Prefix Independent Convergence (PIC) support for static routes
- IP Fabric QoS
- Enhanced Debug/RASLOG messages for FEC support status

Release SLX-OS 20.4.1c provides the following features:

- Critical defect fixes

Release SLX-OS 20.4.1b provides the following features:

- Critical defect fixes
- TPVM security patches till May 09, 2022 are included in TPVM 4.5.1

Release SLX-OS 20.4.1a provides the following features:

- Critical defect fixes

Release SLX-OS 20.4.1 provides the following features:

- SLX based TPVM upgrade optimization
- Additional SNMP notification event support
- SE Linux based IMA policy
- MAC (Mandatory Access Control) policy for user space binaries
- Ability to upgrade ONIE/GRUB
- Force port 1G speed/duplex via constrained advertised capabilities
- Processing ACL rule for Tunneled traffic
- BGP Dynamic Peering Scale Enhancement
- IPV6 configuration support in TPVM
- Ipv6 Support for Peer-Address in a Route Map for BGP
- BGP dampening for peer flaps
- TPVM security patches till April 03, 2022 are included in TPVM 4.5.0

Behavior Changes

The following are the behavioral changes for SLX-OS 20.5.1b

- No behavioral changes were introduced in this release

The following are the behavioral changes for SLX-OS 20.5.1a

- No behavioral changes were introduced in this release

The following are the behavioral changes for SLX-OS 20.5.1

- ICMP and ICMPv6 redirect are disabled by default on all SLX platforms. Configuration commands to enable/disable ICMP and ICMPv6 redirect are available only on SLX 9540 and SLX 9640 platforms.
- **sysObjectID** mib object value for different SLX-OS platform products is updated as follows -
    - In 8720-32C - OID:EXTREME-BASE-MIB::extreme872032CSLXOS (1.3.6.1.4.1.1916.2.505)
    - In 8520-48Y - OID:EXTREME-BASE-MIB::extreme852048YSLXOS (1.3.6.1.4.1.1916.2.506)
    - In 8520-48XT - OID:EXTREME-BASE-MIB::extreme852048XTSLXOS (1.3.6.1.4.1.1916.2.507)
    - In 8820-40C - OID: EXTREME-BASE-MIB::extreme882040CSLXOS (1.3.6.1.4.1.1916.2.508)
    - In 8820-80C - OID: EXTREME-BASE-MIB::extreme882080CSLXOS (1.3.6.1.4.1.1916.2.509)
- Following changes towards file and directory access permissions have been made –
    - Access permissions to /var/log directory is changed to '750'.
    - The "shell_activity.log" file is moved from /var/log directory to /var/local/ and access permission for the "shell_activity.log" is set to '622'
    - 'loggroup' group is added to the /var/log directory and /var/local/shell_activity.log file respectively to provide group access for administrators. Admin and root users are members of the 'loggroup' group.

The following are the behavioral changes for SLX-OS 20.4.3a

- No behavioral changes were introduced in this release

The following are the behavioral changes for SLX-OS 20.4.3

- As a part of SLX-OS hardening, access permission for log files have been modified to "r+w" for owners, "w" for groups, and no access for others. However, there are few exceptions to this new access permission scheme.
- In SNMP notifications, *snmpTrapAddress* OID is placed in the notification after the notification's object list
- For SNMP notifications for Maintenance mode (MM) Entry and Exit phases, overall convergence status is determined based on only MCT completion status. Previously, it was determined based on completion status of both MCT and BGP modules.

  From SLX-OS 20.4.3 and onwards, overall convergence status of MM operation – enable and disable, is determined as below:

  a) For *extremeMaintenanceModeEntryTrap*, based on MCT completion status. In case MCT module times out in any of the two stages of MM Enable operation, status will be timed out.
  b) For *extremeMaintenanceModeExitTrap*, based on MCT completion status (stage 1 of MM Disable operation).

The following are the behavioral changes for SLX-OS 20.4.2b

- No behavioral changes were introduced in this release

The following are the behavioral changes for SLX-OS 20.4.2a

- No behavioral changes were introduced in this release

The following are the behavioral changes for SLX-OS 20.4.2

- Default VRF bindings for SNMP listening services on SLX-OS are Management VRF and Default VRF.
- SNMP SET operation is completely unsupported.
- SNMP server view command does not take effect for the “write view” option
- SNMPv3 user delete operation requires SNMP agent to be stopped to take effect post reload.
- Boot up time for SNMP agent is delayed**.**
- The variable binding for ‘*InetAddress’* type variables in Enterprise MIBs related traps – BFD and MCT, is changed from ‘*IpAddress’* to ‘*InetAddress*’.

The following are the behavioral changes for SLX-OS 20.4.1c

- No behavioral changes were introduced in this release.

The following are the behavioral changes for SLX-OS 20.4.1b

- No behavioral changes were introduced in this release.
- TPVM security patches till May 09, 2022 are included in TPVM 4.5.1

The following are the behavioral changes for SLX-OS 20.4.1a

- No behavioral changes were introduced in this release.

The following are the behavioral changes for SLX-OS 20.4.1

- CLI `threshold-monitor` is modified as follows:
    - Default action is changed from RASlog to RASlog and SNMP Trap.
    - `threshold-monitor Memory` has removed parameters – limit and low-limit.
    - Default values for `threshold-monitor Cpu` and `threshold-monitor Memory` are changed.
- SNMP trap for BFD module contains additional info and is implemented via Enterprise BFD MIB. BFD Enterprise MIB is the default option. This means, snmp-server trap needs to be specifically configured for BFD standard MIB via newly added CLI in this release.
- TPVM patch upgrade (incremental upgrade) that helps upgrading only the patches without stopping the running TPVM instance. Use the command `tpvm upgrade incremental`.
- TPVM Ipv6 support
- Added security patches till April 03, 2022, in TPVM 4.5.0

Software Features

The following key software features are added in the SLX-OS 20.5.1b release

- No new feature is added in this release.

The following key software features are added in the SLX-OS 20.5.1a release

- No new feature is added in this release.

The following key software features are added in the SLX-OS 20.5.1 release

Feature Name	Supported SLX Platforms	Description
eBGP Nexthop recursion	All	BGP nexthop recursion support is extended to eBGP routes as well.
BGP ADD-PATH support to receive 128-path routes advertised over eBGP	All	Ability to receive 128-path routes advertised over eBGP.
Increasing BGP peer group scale to 1024	All	BGP Peer group scale is increased from current 250 to 1024.
ECMP scale increase to 128	SLX 9150, SLX 9250, SLX 9740, Extreme 8520, Extreme 8720, and Extreme 8820	ECMP scale is increased from current 64 to 128.
BMC Security Hardening	Extreme 8520, Extreme 8720, Extreme 8820, and SLX 9740	An user will be able to change default passwords and default IPv4 configuration on BMC ethernet interface.
IPv6 NETCONF Bulking and DRC support for BGP related configurations	All	NETCONF Bulking and DRC support is added for BGP related configurations - • BGP standard, extended and large communities • BGP AS-Path • IPv6-based Prefix list
EVPN-MH Enhancement - Deriving ES import extended RT from ESI	Extreme 8520, Extreme 8720, SLX 9150, and SLX 9250	This enhancement corrects Route Target (RT) encoding from ESI as per RFC. ES-Import RT is derived from the first 6 octets of 9-octet ESI value.
Increasing sFlow sample rate values above 100K	Extreme 8820 and SLX 9740	sFlow sample rate can be configured beyond 100K value up to 16M on SLX 9740 and Extreme 8820 platforms
Add Description field for ACL, Route-maps, Static Routes	All	User can add description to configured IPv4 and IPv6 static routes, ACL rules, and route-maps for better configuration readability.

Improvements over '`show media`' command	All	"`show media`" command has been enhanced to display qualitative info about certain parameters - High-Alarm, High-Warning, Low-Alarm, or Low-Warning.

The following key software features are added in the SLX-OS 20.4.3a release

- No new feature is added in this release.

The following key software features are added in the SLX-OS 20.4.3 release

Feature Name	Supported SLX Platforms	Description
New HW platform – Extreme 8820	Extreme 8820	• Available in two form factors – 40C and 80C • Validated Trusted Delivery solution • Software validation and feature parity with SLX 9740
VE interface config bulking (IP Fabric Upgrade Optimization)	All	Reduced boot up time for SLX-OS through optimization of the 'config replay' of VE interface configurations.
IP Fabric QoS	Extreme 8520, Extreme 8720, SLX 9150, and SLX 9250	Support added for user-configured QoS maps and DSCP Trust.
Removal of DF towards IP Fabric (local bias support for LVTEP)	SLX 9150, SLX 9250, SLX 9740, Extreme 8520, and Extreme 8720	It is recommended to enable 'Local-bias for LVTEP' when SR-IOV clients are used with an MCT pair.
IPv6 Manageability on SLX TPVM – LDAP support	All	IPv6 support for LDAP service added for managing TPVM.
IPv6 Egress based ACL rate limiting	SLX 9740 and Extreme 8820	Support added for IPv6 ACL based rate limiting on egress interfaces.
Recursive Next-hop resolution for PBR route-maps	All	Recursive next-hop resolution support added for policy-based route maps. This is supported for both IPv4 and IPv6 next hops
Notify user to activate BGP peer group to apply route-maps	All	Notify the user to activate BGP peer group before applying route-maps
Optics qualification	All	100G (QSFP) – LR (10KM), FR (2KM) and DR (500M)

The following key software features are added in the SLX-OS 20.4.2b release

- No new feature is added in this release.

The following key software features are added in the SLX-OS 20.4.2a release

- No new feature is added in this release.

The following key software features are added in the SLX-OS 20.4.2 release

Feature Name	**Supported SLX Platforms**	**Description**
Maintenance Mode Optimizations for IP Fabric Upgrade	All	Maintenance mode, which plays a key role for seamless upgrade via EFA, has been optimized to reduce the waiting time from current 300 sec to a much smaller number, say 60 sec. Also, link utilization on spine uplinks is monitored and based on link utilization drop, SLX device comes out of the Maintenance Mode enable stage instead of waiting for user-configured wait time (default is 300 sec).
Ability to control service bindings for SNMP listening services	All	Allows user to enable SNMP services listening on a specific VRF, incl. default and Management VRFs. User can configure up to 32 VRFs.
Ability to disable processing of packets utilizing IP Options	Extreme 8520, Extreme 8720, SLX 9150, SLX 9250, and SLX 9740	Allows to disable CPU processing of the IPv4 datagrams with IP header option fields.
Support for Password Handling for special characters on SLX-OS	All	Adds capability to support all special characters to configure a password on SLX-OS.
Increased the allowed anycast-address entries per interface from 64 to 512	All	Allows to configure anycast addresses per Virtual Ethernet (VE) interface scale up to 512. The overall system scale remains at 8000.
Additional IPv6 protocol support on TPVM	All	Extends IPv6 Manageability support on TPVM. Network services such as DNS and NTP can be configured with IPv6 address. Dynamic support for Default Gateway (DGW) is also added.
Additional SNMP Notification Event support from SLX	All	SNMP Notifications for events related to hardware tables such as MAC Table, LIF, VxLAN and BFD session tables have been added

Feature Name	Supported SLX Platforms	Description
PIC support for static routes	Extreme 8520, Extreme 8720, SLX 9150, SLX 9250, and SLX 9740	PIC (Prefix Independent Convergence) support for static routes feature is added In an IP Fabric deployment, enabling this feature on a Border Leaf device will help reduce the BFD convergence time b/w Border leaf and Border/Edge gateway
IP Fabric QoS	Extreme 8520, Extreme 8720, SLX 9150, SLX 9250, and SLX 9740	Default class maps support is added for L2 and L3 VxLAN gateways.
Enhanced Debug/RASLOG messages for FEC support status	All	Display RASlog message for the FEC support on various SLX platforms

The following key software features are added in the SLX-OS 20.4.1c release

- No new feature is added in this release.

The following key software features are added in the SLX-OS 20.4.1b release

- No new feature is added in this release.

The following key software features are added in the SLX-OS 20.4.1a release

- No new feature is added in this release.

The following key software features are added in the SLX-OS 20.4.1 release

Feature Name	Supported SLX Platforms	Description

SLX based TPVM upgrade optimization	All	`tpvm upgrade incremental` command is introduced.
		• avoids reinstallation of TPVM and EFA during upgrade
		• 2 Debian files for each installation type
		  ○ One for full installation
		  ○ One for upgrade installation

Feature Name	Supported SLX Platforms	Description
Additional SNMP Notification Event support	All	New and enhanced SNMP notifications are added: • BFD enterprise notifications with BFD session specific information • Cluster up and down notifications for MCT cluster • Maintenance mode traps for entry and exit transitions • CPU and memory threshold monitoring traps. • NTP status change trap • Enhanced BGP IPv6 notifications - Established & BackwardTransition traps • Enhanced Fan failure / recovery traps • Enhanced Power Supply failure / recovery traps
SE Linux based IMA policy	All	Security Enhanced Linux is added as an additional layer of system security for access controls for the applications, processes, and files on the SLXOS system.
MAC policy for user space binaries	All	Security Enhanced Linux (SE Linux) implements Mandatory Access Control (MAC). Every process and system resource is issued a special security label called an SE Linux context.
Ability to upgrade ONIE/GRUB	SLX 9150, SLX 9250, Extreme 8720, and Extreme 8520	Provides the ability to install *onie, diag* and *onie-grub* images from SLXOS
Force port 1G speed/duplex via constrained advertised capabilities	SLX 9150 and Extreme 8520	Adds the support of 10G port in 1G forced mode in full duplex with clock parameter to auto negotiate based on peer capabilities
Processing ACL rule for Tunneled traffic	SLX 9740	Supports ingress ACL on tunnels to match the inner headers for VxLAN, GRE and MPLS tunnels
BGP Dynamic Peering Scale Enhancement	All	Increases the number of BGP peers for Dynamic BGP Peers
IPV6 protocol support on TPVM	All	Introduces the initial support of IPv6 protocol for TPVM
IPv6 Support for Peer-Address in a Route Map for BGP	All	Supports of `set ipv6 next-hop peer-address` in route-map for BGP
BGP dampening for peer flaps	All	Adds the BGP peer dampening capability for unusable BGP peers

CLI Commands

The following commands were added, modified, or deprecated for the 20.5.1b program

New commands for 20.5.1b

No commands were added in this release

Modified commands for 20.5.1b

No commands were modified in this release

Deprecated commands for 20.5.1b

No commands were deprecated in this release

The following commands were added, modified, or deprecated for the 20.5.1a program

New commands for 20.5.1a

No commands were added in this release

Modified commands for 20.5.1a

No commands were modified in this release

Deprecated commands for 20.5.1a

No commands were deprecated in this release

The following commands were added, modified, or deprecated for the 20.5.1 program

New commands for 20.5.1

- remark
- rule-name
- bmc user
- bmc lan ipsrc
- bmc lan ipaddr
- bmc lan netmask
- bmc lan gateway
- bmc factory reset
- show bmc status

Modified commands for 20.5.1

- ip route
- ipv6 route
- ip icmp redirect
- ipv6 icmpv6 redirect
- profile route
- resilient-hash
- maximum paths (BGP)
- sflow enable
- sflow sample-rate

- show media interface
- show media optical-monitoring
- show hardware profile
- show running-config

Deprecated commands for 20.5.1

No commands were deprecated in this release

The following commands were added, modified, or deprecated for the 20.4.3a program

New commands for 20.4.3a

No commands were added in this release

Modified commands for 20.4.3a

No commands were modified in this release

Deprecated commands for 20.4.3a

No commands were deprecated in this release

The following commands were added, modified, or deprecated for the 20.4.3 program

New commands for 20.4.3

- lvtep broadcast-local-bias
- ingress-vlan-mapped-ve-counter
- qos trust dscp
- qos remark dscp
- next-hop-recursion

Modified commands for 20.4.3

- tpvm ldap ca-cert
- tpvm ldap
- neighbor peer-group
- show cluster
- show interface stats detail
- show qos maps traffic-class-dscp
- show route-map

Deprecated commands for 20.4.3

No commands were deprecated in this release

The following commands were added, modified, or deprecated for the 20.4.2b program

New commands for 20.4.2b

No commands were added in this release

Modified commands for 20.4.2b

No commands were modified in this release

Deprecated commands for 20.4.2b

No commands were deprecated in this release

The following commands were added, modified, or deprecated for the 20.4.2a program

New commands for 20.4.2a

No commands were added in this release

Modified commands for 20.4.2a

No commands were modified in this release

Deprecated commands for 20.4.2a

No commands were deprecated in this release

The following commands were added, modified, or deprecated for the 20.4.2 program

New commands for 20.4.2

- convergence-time (maintenance mode)
- efa deploy
- enable-on-reboot (maintenance mode)
- maintenance-mode
- prefix-independent-convergence-static
- qos-dscp-mode
- rate-monitoring (maintenance mode)
- snmp-server use-vrf
- threshold-monitor bfd-session
- threshold-monitor lif
- threshold-monitor mac-table
- threshold-monitor vxlan-tunnel
- shutdown-time (maintenance mode)

Modified commands for 20.4.2

- dns (TPVM)
- enable (maintenance mode)
- ip option
- ntp (TPVM)
- system maintenance
- system maintenance turn-off
- trusted-peer (tpvm mode)
- tpvm download

- interface management (tpvm mode)
- snmp-server group
- snmp-server user
- show overlay-gateway
- show tunnel
- show system maintenance
- show system maintenance rate-monitoring

Deprecated commands for 20.4.2

- qos-ttl-mode

The following commands were added, modified, or deprecated for the 20.4.1c program

New commands for 20.4.1c

No commands were added in this release.

Modified commands for 20.4.1c

No commands were modified in this release.

Deprecated commands for 20.4.1c

No commands were deprecated in this release.

The following commands were added, modified, or deprecated for the 20.4.1b program

New commands for 20.4.1b

No commands were added in this release.

Modified commands for 20.4.1b

No commands were modified in this release.

Deprecated commands for 20.4.1b

No commands were deprecated in this release.

The following commands were added, modified, or deprecated for the 20.4.1a program

New commands for 20.4.1a

No commands were added in this release.

Modified commands for 20.4.1a

No commands were modified in this release.

Deprecated commands for 20.4.1a

No commands were deprecated in this release.

The following commands were added, modified, or deprecated for the 20.4.1 program

New commands for 20.4.1

- neighbor peer-dampening
- neighbor peer-dampening (peer-group)
- peer-dampening
- show grubversion
- show [ip|ipv6] bgp peer-dampened
- show onieversion
- show selinux status
- snmp-server trap
- update onie

Modified commands for 20.4.1

- dns (tpvm mode)
- interface management (tpvm mode)
- ntp (tpvm mode)
- set ip next-hop
- set ipv6 next-hop
- speed
- threshold-monitor Cpu
- threshold-monitor Memory
- tpvm download
- tpvm upgrade (tpvm mode)
- vrf-lite-capability

The following show commands were enhanced to show additional information.

- show interface ethernet
- show interface status
- show ipv6 bgp routes

Deprecated commands for 20.4.1

No commands were deprecated in this release.

Hardware Support

Supported devices and software licenses

Supported devices	Description
SLX9740-40C	Extreme SLX 9740-40C Router. Base unit with 40x100GE/40GE capable QSFP28 ports, 2 unpopulated power supply slots, 6 unpopulated fan slots
SLX9740-40C-AC-F	Extreme SLX 9740-40C-AC-F Router. Base unit with 40x100GE/40GE capable QSFP28 ports, 2 AC power supplies, 6 fan modules
SLX9740-80C	Extreme SLX 9740-80C Router. Base unit with 80x100GE/40GE capable QSFP28 ports, 4 unpopulated power supply slots, 4 unpopulated fan slots
SLX9740-80C-AC-F	Extreme SLX 9740-80C-AC-F Router. Base unit with 80x100GE/40GE capable QSFP28 ports, 4AC power supplies, 4 fan modules
SLX9740-ADV-LIC-P	Advanced Feature License for MPLS, BGP-EVPN and Integrated Application Hosting for Extreme SLX 9740
SLX9150-48Y-8C	Extreme SLX 9150-48Y Switch with two empty power supply slots, six empty fan slots. Supports 48x25GE/10GE/1GE + 8x100GE/40GE.
SLX9150-48Y-8C-AC-F	Extreme SLX 9150-48Y Switch AC with Front to Back Airflow. Supports 48x25GE/10GE/1GE + 8x100GE/40GE with dual power supplies, six fans.
SLX9150-48Y-8C-AC-R	Extreme SLX 9150-48Y Switch AC with Back to Front Airflow. Supports 48x25GE/10GE/1GE + 8x100GE/40GE with dual power supplies, six fans.
SLX9150-48XT-6C	Extreme SLX 9150-48XT 10GBaseT Switch with two empty power supply slots, six empty fan slots, Supports 48x10GE/1GE + 6x100GE/40GE.
SLX9150-48XT-6C-AC-F	Extreme SLX 9150-48XT 10GBaseT Switch AC with Front to Back Airflow, Supports 48x10GE/1GE + 6x100GE/40GE with dual power supplies, six fans.
SLX9150-48XT-6C-AC-R	Extreme SLX 9150-48XT 10GBaseT Switch AC with Back to Front Airflow, Supports 48x10GE/1GE + 6x100GE/40GE with dual power supplies, six fans.
SLX9150-ADV-LIC-P	SLX 9150 Advanced Feature License for GuestVM, Analytics Path, PTP, BGP-EVPN.
SLX9250-32C	SLX 9250-32C Switch with two empty power supply slots, six empty fan slots. Supports 32x100/40GE.
SLX9250-32C-AC-F	SLX 9250-32C Switch AC with Front to Back Airflow. Supports 32x100GE/40GE with dual power supplies, six fans.
SLX9250-32C-AC-R	SLX 9250-32C Switch AC with Back to Front Airflow. Supports 32x100GE/40GE with dual power supplies, six fans.
SLX9250-ADV-LIC-P	SLX 9250 Advanced Feature License for GuestVM, Analytics Path, BGP-EVPN.
BR-SLX-9540-48S-AC-R	SLX 9540-48S Switch AC with Back to Front airflow (Non-port Side to port side airflow). Supports 48x10GE/1GE + 6x100GE/40GE. (1+1) redundant power supplies and (4+1) redundant fans included.
BR-SLX-9540-48S-AC-F	SLX 9540-48S Switch AC with Front to Back airflow (Port-side to non-port side airflow). Supports 48x10GE/1GE + 6x100GE/40GE. (1+1) redundant power supplies and (4+1) redundant fans included.
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.

Supported devices	Description
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
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

Supported devices	Description
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
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

Supported devices	Description
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

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

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

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

Software Download and Upgrade

For more information about the various methods of upgrading to SLX-OS 20.5.1b see the *Extreme SLX-OS Software Upgrade Guide.*

Image files

Download the following images from www.extremenetworks.com.

Image file name	Description
SLX-OS_20.5.1b.tar.gz	SLX-OS 20.5.1b software
SLX-OS_20.5.1b_mibs.tar.gz	SLX-OS 20.5.1b MIBS
SLX-OS_20.5.1b.md5	SLX-OS 20.5.1b md5 checksum
SLX-OS_20.5.1b-digests.tar.gz	SLX-OS 20.5.1b sha checksum
SLX-OS_20.5.1b-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/b
20.4.3 (Factory Image)	For upgrade: normal firmware download / coldboot	
20.5.1/a/b		

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/b
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/b					

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/b
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/b					

Note:

For upgrade and downgrade procedure on SLX platforms, involving releases earlier to SLX-OS 20.3.2, full install is recommended.

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/b
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/b					

Note:

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

SLX 9540 and SLX 9640

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/b
18r.2.00/a-d	**For SLX 9540** 1. First upgrade to 20.1.2h, using full install 2. Then upgrade to target version, using full install **For SLX 9640** 1. First upgrade to 18r.2.00d, using full install 2. Then upgrade to 20.1.2h, using full install 3. Then upgrade to target version, using full install				
20.1.1	**For SLX 9540** 1. First upgrade to 20.1.2h, using full install 2. Then upgrade to target version, using full install **For SLX 9640** Full install				
20.1.2e, g 20.2.x	Full install				
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					

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/b
20.5.1/a/b					

Notes:

- When upgrading from the 18r.1.00x and 18r.2.00a and earlier patches, upgrade first to 18r.2.00bx and then to 20.2.2x, which is a two-step upgrade procedure.
- The MCT upgrade procedure from 18r.2.00bc to 20.2.x is detailed in the *Extreme SLX-OS Software Upgrade Guide.*
- Because SLX 9540 is a bare metal device, use the "fullinstall" option to migrate between the SLX-OS 20.2.2x and SLX-OS 20.1.x releases.
- Because SLX 9540 is moved to the bare metal mode in 20.2.1, use 'fullinstall' when migrating between SLX-OS 20.2.2x and SLX-OS 2.1.x releases.
- 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/b
20.1.x	Full install				
20.2.x					
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/b					

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/b	TPVM 4.2.5 and later	TPVM 4.4.0 and later	TPVM 4.2.5 and later

Upgrading the TPVM without configuration persistence (Legacy upgrade method)

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

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

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

remove name <disk name> to remove each additional disk manually. For example, `tpvm disk remove name vdb`.

- To perform patch upgrade from TPVM 4.5.x to latest, do the following:
  - Upgrade to SLX-OS 20.5.x while the existing TPVM 4.5.x installation continues to run
  - Copy the new *tpvm_inc_upg-4.5.X-X.amd64.deb* to */tftpboot/SWBD2900* directory on the SLX device.
  - Install latest TPVM 4.5.x using **tpvm upgrade incremental** command

Notes:

- TPVM 4.5.4 can be incrementally upgraded from TPVM 4.2.5 and beyond.
- TPVM 4.5.4 supports full install upgrade/downgrade from TPVM 4.2.5.

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 ~2.7 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 4.5.12 has security updates till April 30th , 2023.
VDB disk size for EFA has changed to 40 GB to accommodate storage for snapshot and the remaining space is considered as reserved space, for the new TPVM installation.

Upgrading the TPVM with configuration persistence – Recommended method

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

1. SLX-OS old version with tpvm instance installed/deployed and few related config may be set.
2. SLX-OS upgrade done vide `firmware download` CLI command.
3. Across SLX-OS reboots, old TPVM too shall reboot if auto-boot config was there, else shall be there in installed state.
    - **a.** tpvm stop
    - **b.** tpvm uninstall
        - **i.** (or) tpvm uninstall force – if you plan to delete disk vdb (i.e. the TPVM /apps partition).
        - **ii.** Note:
            1. New mode like old mode, create disk vdb (/apps) by default upon first install/deploy or reuse previously existing partition.
            2. Currently the new mode does not support new disk creation. The **tpvm disk add** command can be used.
4. As simple example for new mode of deploying TPVM:
    a. Copy new TPVM debian Image under /tftpboot/SWBD2900. Only one file should be there and no subfolder should be present/created within this folder.
    b. Deploy TPVM in Config Mode:

```
SLX # config terminal

SLX (config)# tpvm TPVM

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

Above will install and start any TPVM image kept under /tftpboot/SWBD2900.

    c. Deploy TPVM with some configuration and later update any runtime configuration:

```
SLX # config terminal

SLX (config)# tpvm TPVM

SLX (config-tpvm-TPVM) # password newpassword
SLX (config-tpvm-TPVM) # interface management ip 10.25.24.21/24
SLX (config-tpvm-TPVM) # auto-boot
SLX (config-tpvm-TPVM) # hostname newhostname
SLX (config-tpvm-TPVM) # timezone Europe/Stockholm
SLX (config-tpvm-TPVM) # deploy
SLX (config-tpvm-TPVM) # end

SLX # config terminal

SLX (config)# tpvm TPVM

SLX (config-tpvm-TPVM) # hostname oldhostname
SLX (config-tpvm-TPVM) # no timezone

SLX (config-tpvm-TPVM) # exit
```

5. Note:
    a. Now, say, if the **tpvm config hostname xyz** command is used. It will still work and apply on TPVM instance. But this configuration shall not be persisted in SLX Database and will become inconsistent. Same is true for any other configuration done in old way.
    b. As in above example, password, management configuration should always be set before deploy. If required later, refer User Guide and use tpvm stop, start for such update/maintenance reason.
    c. If **tpvm unstall force** command is used, then you will need to perform a **no deploy** and **deploy** in the new mode.

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

TPVM Migration

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

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

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

Limitations and Restrictions

Copy flash to startup and reload with TPVM

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

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

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

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

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

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

TPVM Migration

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

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

PM Configuration	Examples
If 4x25G breakout is configured, no 40G or 4x10G.	• If 0/1 is configured as 4x25G breakout, you cannot configure 0/3 or 0/4 as 40G. • If 0/1 is configured as 4x25G breakout, you cannot configure 0/3 as 4x10G breakout. • If 0/3 is configured as 4x25G breakout, you cannot configure 0/1 or 0/2 as 40G. • If 0/3 is configured as 4x25G breakout, you cannot configure 0/1 as 4x10G breakout.

QoS

- PCP remarking is not supported for SLX 9740.
- Conformed and Violated counters are not supported for egress rate limiting for SLX 9740.
- Egress rate limiting in a Bridge Domain configuration is not supported for SLX 9740.
- DSCP-COS map is not work correctly for SLX 9740.

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 13183. 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 13183 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.

Open Defects

The following software defects are open in SLX-OS 20.5.1b as of August 2023:

Parent Defect ID:	SLXOS-72935	**Issue ID:**	SLXOS-72935
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-73263	**Issue ID:**	SLXOS-73263
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-69469	**Issue ID:**	SLXOS-73281
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72514	**Issue ID:**	SLXOS-73578
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-73585
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-73591
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-73600	**Issue ID:**	SLXOS-73600
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-73637	**Issue ID:**	SLXOS-73637
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72298	**Issue ID:**	SLXOS-73783
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-73834	**Issue ID:**	SLXOS-73835
Severity:	S4 - Minor		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 16r.1.01a
Technology Group:	Layer 2 Switching	**Technology:**	VXLAN - Virtual Extensible LAN

The following software defects are open in SLX-OS 20.5.1a as of June 2023:

Parent Defect ID:	SLXOS-71127	**Issue ID:**	SLXOS-72816
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72770	**Issue ID:**	SLXOS-72825
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72834
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-71680	**Issue ID:**	SLXOS-72882
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-71948	**Issue ID:**	SLXOS-72888
Severity:	S2 - Major		

Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72779	**Issue ID:**	SLXOS-72896
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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 v3.		
Workaround:	Configuring the switch with IGMP version v2 instead of v3.		

The following software defects are open in SLX-OS 20.5.1 as of April 2023:

Parent Defect ID:	SLXOS-52746	**Issue ID:**	SLXOS-53722
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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:**	SLX-OS 20.2.2
Technology Group:	Layer 2 Switching	**Technology:**	VLAN - Virtual LAN
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-55211	**Issue ID:**	SLXOS-57437
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.2
Technology Group:	Management	**Technology:**	Other

Symptom:	Command is not successful and displays an error saying "Cannot resolve hostname"
Condition:	Usage of "copy" command with FTP protocol and IPV6 address .
Workaround:	Use IPv4 interface address

Parent Defect ID:	SLXOS-56740	**Issue ID:**	SLXOS-57454
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Convergence times > 500 msec are seen for South - North traffic when a port from Border Leaf to L3 gateway is shut		
Condition:	This is a test for convergence numbers. The port between a Border Leaf and an L3 gateway is shut which forces the BL to reprogram the next hop for the South - North traffic to go over the ICL. The convergence times vary and there are occasional spikes between 800 to 1000 msec.		

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

Parent Defect ID:	SLXOS-60302	**Issue ID:**	SLXOS-60754
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-61208	**Issue ID:**	SLXOS-61283
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-61347	**Issue ID:**	SLXOS-61598
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.3.2c
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	In Multi-homed environment, shutdown of an LACP ES Port-channel may cause traffic flooding to other ES interfaces if the client/host device is not able to detect link flap and continue to send the traffic. Whenever LACP port-channel is shut, member ports will be disaggregated and laser will be down for few msec(around 100ms) to allow peer device to detect link event. After that link comes up and member port will be transitioned to disaggregated individual port. Some old devices may not be able to detect link flap and continue to send traffic for some more time till LACP timeout.		
Condition:	Some old hosts may not be able to detect link flap when the link goes down for short period of time. SLX 9150/9250 keep the link down for 100msec before bring up the link as lacp individual. If the dual homed host is not able to detect the link flap on LACP ESI shut, the host continues to send the traffic till LACP timeout. SLX device may flood the traffic (in vlan) during that period.		
Workaround:	Shutting the individual member ports along with ES port-channel avoids flooding in this scenario.		
Recovery:	This situation will be recovered automatically after LACP timeout. Client device detects LACP timeout after 3sec (in case of short lacp interval), and stops traffic.		

Parent Defect ID:	SLXOS-62671	**Issue ID:**	SLXOS-62995
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	Latency of around 250ms to 1second is observed on SLX device.		
Condition:	SLX node has experienced the CPU congestion		

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

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

Parent Defect ID:	SLXOS-66144	**Issue ID:**	SLXOS-66144
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	Traffic takes more than 900 msec in the N-S direction when a port channel between the Gateway and Border Leaf fails. Minimum link is configured over this port channel and the trigger is the shutdown of one interface belonging to the port channel.		
Condition:	Minimum-link is configured between border leaf and gateway. When a port channel member between them is shutdown in the BL side, the PO is expected to fail. The GW should redirect the traffic to the other border leaf. This was seen to take more than 900 ms. The GW is a SLX 9640.		

Parent Defect ID:	SLXOS-65379	**Issue ID:**	SLXOS-66289
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.3j
Technology Group:	MPLS	**Technology:**	MPLS VPLS - Virtual Private LAN Services
Symptom:	MPLS encapsulated 'Unicast ICMP with destination MAC starts on 4' traffic fails to forward from 9740(PHP/P) to 9850(PE).		

Condition:	a) Establish VPLS session between 9850 & MLX with adding 9740 as Transit Node. b) Initiate traffic with destination MAC starts with 4 from CE to CE.

Parent Defect ID:	SLXOS-66738	**Issue ID:**	SLXOS-66738
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1
Technology Group:	Monitoring	**Technology:**	Port Mirroring
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:**	SLX-OS 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:**	SLX-OS 20.2.1
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	Interface MTU value not set		
Condition:	Sometimes a reload will not set MTU value		
Workaround:	Re-configure MTU value		

Parent Defect ID:	SLXOS-67049	**Issue ID:**	SLXOS-67663
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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

Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-68095	**Issue ID:**	SLXOS-68095
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	Convergence of L3VNI Asymmetric traffic takes 30 seconds.		
Condition:	Reloading one of the Multi-homed peer.		

Parent Defect ID:	SLXOS-68416	**Issue ID:**	SLXOS-68416
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-68208	**Issue ID:**	SLXOS-69895
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.3.2f
Technology Group:	Monitoring	**Technology:**	OAM - Operations, Admin & Maintenance
Symptom:	Failed to fetch the utilization-watermark stats on the "show interface stats utilization-watermark interface ethernet <x/x>".		
Condition:	In SLX 9540 device configured with "system interface utilization-watermark".		

Parent Defect ID:	SLXOS-69448	**Issue ID:**	SLXOS-69959
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1cb
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	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-69621	**Issue ID:**	SLXOS-70060
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.3.2g
Technology Group:	Layer 2 Switching	**Technology:**	LAG - Link Aggregation Group
Symptom:	Fail to add port to Link Aggregation Group		
Condition:	On removing a port from LACP LAG and add it again to same LAG, port fails to be part of LAG and will throw "[LACP-1005]" RAS log		
Workaround:	Remove all member ports of LAG and add them again.		

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

Parent Defect ID:	SLXOS-70473	**Issue ID:**	SLXOS-70473
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	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:**	SLX-OS 20.4.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD sessions flap while rebooting a leaf node		
Condition:	In an MCT pair, BFD sessions flap while rebooting a leaf node with SRIOV clients		

Parent Defect ID:	SLXOS-69962	**Issue ID:**	SLXOS-70821
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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:**	SLX-OS 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:**	SLX-OS 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-71344	**Issue ID:**	SLXOS-71502
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-71127	**Issue ID:**	SLXOS-71556
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-68264	**Issue ID:**	SLXOS-71647
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1b
Technology Group:	Other	**Technology:**	Other
Symptom:	Link not coming up after reload. And if it comes up, after certain time (in secs) pld algorithm kicks in and link goes down after which it comes up again based on the configured time. This happens in loop.		
Condition:	When port link dampening CLI is configured. link-error-disable 2 120 300		

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

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

Condition:	MPLSD module reset due to the message queue becoming full on MPLS.

Parent Defect ID:	SLXOS-71509	**Issue ID:**	SLXOS-72084
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72014	**Issue ID:**	SLXOS-72192
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72163	**Issue ID:**	SLXOS-72388
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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:**	SLX-OS 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.

Defects Closed with Code Changes

The following software defects were closed in 20.5.1b with code changes as of August 2023:

Parent Defect ID:	SLXOS-73107	**Issue ID:**	SLXOS-73367
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72268	**Issue ID:**	SLXOS-73665
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-74057	**Issue ID:**	SLXOS-74057
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.1a
Technology Group:	Other	**Technology:**	Other
Symptom:	Rasdecode traces are not generated for BGP module.		
Condition:	No specific triggers.		

Parent Defect ID:	SLXOS-73198	**Issue ID:**	SLXOS-74118
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.5.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	BGP daemon reload is observed.		
Condition:	MAC route is learnt locally and imported as EVPN route.		

The following software defects were closed in 20.5.1a with code changes as of June 2023:

Parent Defect ID:	SLXOS-72076	**Issue ID:**	SLXOS-72768

Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72769
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72163	**Issue ID:**	SLXOS-72840
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72195	**Issue ID:**	SLXOS-72850
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72855
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72010	**Issue ID:**	SLXOS-72867
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72880	**Issue ID:**	SLXOS-72880
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72886
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72907
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72912
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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-72945
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 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.		

The following software defects were closed in 20.5.1 with code change as of April 2023:

Parent Defect ID:	SLXOS-66842	**Issue ID:**	SLXOS-68904
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.3.4a
Technology Group:	Security	**Technology:**	SSH - Secure Shell
Symptom:	Public key authentication does not work sometimes.		
Condition:	Running "ssh" exec mode command.		

Parent Defect ID:	SLXOS-68731	**Issue ID:**	SLXOS-68914
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.1.00m
Technology Group:	Security	**Technology:**	AAA - Authentication, Authorization, and Accounting
Symptom:	Disabling AAA accounting does not appear in accounting log.		
Condition:	Disabling AAA accounting.		

Parent Defect ID:	SLXOS-69102	**Issue ID:**	SLXOS-69369
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.3.2f

Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	When trying to create a port configuration map using ifIndex as the key value, It is not possible to make a port configuration map because the key value(ifIndex) of the management port is not supported.		
Condition:	on SLX 9250 in 20.4.2a, issue is seen only after reloading, after reloading if SNMP walk is issued for IfIndex and later SNMP walk is issued for the IP Address table issue is not seen.		

Parent Defect ID:	SLXOS-69413	**Issue ID:**	SLXOS-69459
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.2
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	Link up/down interfaces are not generated for insight interface.		
Condition:	When TPVM STOP / START is configured		

Parent Defect ID:	SLXOS-69474	**Issue ID:**	SLXOS-69474
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1
Technology Group:	Monitoring	**Technology:**	Hardware Monitoring
Symptom:	Occasional RAS logs suggesting there is FAN airflow mismatch and to replace the FAN module. There is no issue with the HW when the symptom is observed		
Condition:	As part of the hardware monitoring, the symptoms may be observed randomly		

Parent Defect ID:	SLXOS-70700	**Issue ID:**	SLXOS-70700
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	MBGP - Multiprotocol Border Gateway Protocol
Symptom:	Traffic loss observed for 20 to 25 seconds.		
Condition:	Exiting Core isolation in EVPN Multihomed Router .		

Parent Defect ID:	SLXOS-70005	**Issue ID:**	SLXOS-70714
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.2

Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Cluster peer keepalive is down		
Condition:	When management IP is changed, Cluster keepalive is not coming up		
Recovery:	Shutting down the cluster and re-enabling it		

Parent Defect ID:	SLXOS-68899	**Issue ID:**	SLXOS-70787
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 18s.1.03e
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Invalid Ethernet-tag value is seen in BGP-EVPN Routes.		
Condition:	SLX acts as Spine for EVPN Routes and Ethernet tag is set in EVPN routes.		

Parent Defect ID:	SLXOS-69717	**Issue ID:**	SLXOS-71025
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.3.2ae
Technology Group:	Traffic Management	**Technology:**	Rate Limiting and Shaping
Symptom:	ICMP packets may cause drops once exception queue limit is hit in SLX 9540/9640 platforms.		
Condition:	When ICMP packets are sent with TTL1 with MTR or traceroute tool, they may cause drops once exception queue limit is hit in SLX 9540/9640 platforms.		

Parent Defect ID:	SLXOS-70883	**Issue ID:**	SLXOS-71072
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.2a
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	For SNMP requests made to loopback interface address, SNMP response is sent with source IP address as outgoing interface address.		
Condition:	SNMP request made to loopback interface address.		

Parent Defect ID:	SLXOS-70795	**Issue ID:**	SLXOS-71077
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1cb
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol

Symptom:	High volume BGP TTL1 packets received could cause BGP flaps.
Condition:	BGP TTL1 packets may get classified to Exception queue with threshold limit hit which may result in BGP flaps due to IP-FEC issue.

Parent Defect ID:	SLXOS-70451	**Issue ID:**	SLXOS-71126
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.2ac
Technology Group:	Other	**Technology:**	Other
Symptom:	Device reload was seen due to NSM module reset.		
Condition:	One Netconf session polling the PO status repeatedly and another Netconf session adding and removing the PO repeatedly.		

Parent Defect ID:	SLXOS-70200	**Issue ID:**	SLXOS-71208
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1
Technology Group:	Management	**Technology:**	LLDP - Link Layer Discovery Protocol
Symptom:	LLDP frames with error counter increasing.		
Condition:	LLDP frames received with two or more management TLV are considered erroneous and LLDP frames with error counter is incremented. This will not cause any functional issue.		

Parent Defect ID:	SLXOS-69875	**Issue ID:**	SLXOS-71386
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.1.00m
Technology Group:	Layer 2 Switching	**Technology:**	LAG - Link Aggregation Group
Symptom:	Invalid "Time since last interface status change" value for Port-channel.		
Condition:	Member port flap.		
Workaround:	No		

Parent Defect ID:	SLXOS-71230	**Issue ID:**	SLXOS-71435
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.3.4a
Technology Group:	IP Multicast	**Technology:**	IPv4 Multicast Routing
Symptom:	Node reboot while processing a Multicast packet		
Condition:	Multicast daemon reset while processing an IPv6 Multicast packet leading to a node reboot		

Parent Defect ID:	SLXOS-71300	**Issue ID:**	SLXOS-71506
Severity:	S3 - Moderate		

Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.2
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	When tm voq-stats CLI command is executed, destination port shown as N/A when there are CPU discards.		
Condition:	During execution of "show tm voq-stat ingress-device all discards" command.		

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

Parent Defect ID:	SLXOS-70559	**Issue ID:**	SLXOS-71575
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.3ja
Technology Group:	Layer 2 Switching	**Technology:**	xSTP - Spanning Tree Protocols
Symptom:	When no switch-port is initiated on PO interface, the device might block traffic on other interface as it updates wrong h/w entry with drop.		
Condition:	When no switch-port is done on PO interface.		

Parent Defect ID:	SLXOS-71199	**Issue ID:**	SLXOS-71697
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	IPv6 traffic loss seen 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-71581	**Issue ID:**	SLXOS-71874
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.3.2h

Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	For SNMP requests made to loopback interface address, SNMP response is sent with source IP address as outgoing interface address.		
Condition:	SNMP request made to loopback interface address.		

Parent Defect ID:	SLXOS-70677	**Issue ID:**	SLXOS-71879
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1c
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	Traffic loss is observed with URPF		
Condition:	Traffic loss is observed when 'profile route enable urpf' is configured		

Parent Defect ID:	SLXOS-71968	**Issue ID:**	SLXOS-71979
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1c
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	Seen in 9150/9250/8720/8750, "Hardware resource allocation failed" message in the console. This can be followed by some flows being blackholed or routed over wrong interfaces.		
Condition:	Usually seen when BGP-EVPN is enabled and the switch has been up for a long time, or has been through network churn. There is a case where the nexthops in the hardware are leaked. After the switch runs for a while, the nexthops can get exhausted and fresh hardware programming may fail.		

Parent Defect ID:	SLXOS-70832	**Issue ID:**	SLXOS-71992
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	Duplicate CPU/memory threshold monitoring SNMP traps seen.		
Condition:	CPU/memory usage in SLX reaching its configured threshold limits.		

Parent Defect ID:	SLXOS-72554	**Issue ID:**	SLXOS-72608

Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.3a
Technology Group:	Other	**Technology:**	Other
Symptom:	TPVM deploy has failed		
Condition:	deploying tpvm 4.5.11 failed.		

Defects Closed without Code Changes

The following software defects were closed in 20.5.1 without code changes as of April 2023:

Parent Defect ID:	SLXOS-55243	**Issue ID:**	SLXOS-55243
Reason Code:	Not Reproducible	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.2
Technology Group:	Security	**Technology:**	HTTP/HTTPS
Symptom:	Extreme switch bootup logs reports(sometimes) unavailable file (/usr/sbin/httpd.0)		
Condition:	Issue is seen after restarting HTTP(S) server multiple times		

Parent Defect ID:	SLXOS-57738	**Issue ID:**	SLXOS-57738
Reason Code:	Working as Designed	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.1.2f
Technology Group:	MPLS	**Technology:**	IP over MPLS
Symptom:	Hops are not displayed in IPoMPLS trace		
Condition:	During traceroute of IPoMPLS traffic		

Parent Defect ID:	SLXOS-61178	**Issue ID:**	SLXOS-62976
Reason Code:	Not Reproducible	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.2.3d
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ICMP - Internet Control Message Protocol
Symptom:	Slowness on the ping responses on SLX.		
Condition:	On SLX node, CPU is busy with the higher priority packets.		

Parent Defect ID:	SLXOS-66740	**Issue ID:**	SLXOS-66740
Reason Code:	Not Reproducible	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD daemon reboot may be seen.		
Condition:	Multiple times add and remove of EPGs from EFA.		

Parent Defect ID:	SLXOS-66741	**Issue ID:**	SLXOS-66741
Reason Code:	Not Reproducible	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	RH entries are exhausting. Utilizing more resources		

Condition:	Enabling Maintenance mode makes RH entries exhaust and utilize more resources

Parent Defect ID:	SLXOS-69858	**Issue ID:**	SLXOS-69942
Reason Code:	Working as Designed	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLX-OS 20.4.2
Technology Group:	Management	**Technology:**	NTP - Network Time Protocol
Symptom:	Delayed NTP synchronization (>30 mins sometimes) after creating NTP server.		
Condition:	Creation of NTP server on SLX.		

Parent Defect ID:	SLXOS-70057	**Issue ID:**	SLXOS-71224
Reason Code:	Not Applicable	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.1.00m
Technology Group:	MPLS	**Technology:**	MPLS Traffic Engineering
Symptom:	Device reload was seen due to MPLSD reset when the interfaces are going down.		
Condition:	When the interfaces are going down, triggering the bandwidth calculation.		