November 2022

Extreme SLX-OS 20.4.2

Release Notes

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

Part Number 9037617-00 Rev AB

Contents

Document History

Version	Summary of changes	Publication date
1.0	Initial version for 20.4.2	September 2022
2.0	Added restrictions for Resilient Hashing in the 'Others' section of 'Limitations and Restrictions'	November 2022

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 20.4.2 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 20.4.2

- 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 20.4.2 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).

Feature Name	Supported SLX Platforms	Description
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, 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
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

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.

Feature Name	Supported SLX Platforms	Description
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, 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 20.4.2 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
8000-PRMR-LIC-P	Extreme 8000 Premier Feature License (includes Integrated Application Hosting)
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)

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.
XN-ACPWR-1600W-R	SLX 9740 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.
XN-ACPWR-1600W-F	SLX 9740 Fixed AC 1600W Power Supply Front to Back. Power cords not included.
XN-FAN-003-F	SLX 9740 FAN Front to Back airflow for SLX9740-40C
XN-FAN-003-R	SLX 9740 FAN Back to Front airflow for SLX9740-40C
XN-FAN-004-F	SLX 9740 FAN Front to Back airflow for SLX9740-80C
XN-FAN-004-R	SLX 9740 FAN Back to Front airflow for SLX9740-80C
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

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

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

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
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 20.4.2 see the *Extreme SLX-OS Software Upgrade Guide.*

Image files

Download the following images from www.extremenetworks.com.

Image file name	Description
SLX-OS_20.4.2.tar.gz	SLX-OS 20.4.2 software
SLX-OS_20.4.2_mibs.tar.gz	SLX-OS 20.4.2 MIBS
SLX-OS_20.4.2.md5	SLX-OS 20.4.2 md5 checksum
SLX-OS_20.4.2-digests.tar.gz	SLX-OS 20.4.2 sha checksum
SLX-OS_20.4.2-releasenotes.pdf	Release Notes

Notes:

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

Extreme 8720

To / From	20.2.3x	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1/a/b	20.4.1c	20.4.2
20.2.3(MFG)	Use the normal Firmware Download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.3ab	Use the normal Firmware Download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.3x	NA	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.3.2/a/b	Use fullinstall	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.

To / From	20.2.3x	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1/a/b	20.4.1c	20.4.2
20.3.2c/d	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.
20.3.3	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.3.4	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.3.4a/ac	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.4.1/a/b	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot

To / From	20.2.3x	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1/a/b	20.4.1c	20.4.2
20.4.1c	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot
20.4.2	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA

SLX 9740

To / From	20.2.2x	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1/a/b	20.4.1c	20.4.2
20.2.1a	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.2x	Use the normal Firmware Download / coldboot *	Use the normal Firmware Download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall

To / From	20.2.2x	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1/a/b	20.4.1c	20.4.2
20.2.3x	Use the normal Firmware Download / coldboot	NA	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.3.1	Use fullinstall	Use fullinstall	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.
20.3.2/a/b	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.

To / From	20.2.2x	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1/a/b	20.4.1c	20.4.2
20.3.2c/d	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.
20.3.3	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot.	Use the normal Firmware Download / coldboot.	Use the normal Firmware Download / coldboot.	Use the normal Firmware Download / coldboot.	Use the normal Firmware Download / coldboot.
20.3.4	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot.	Use the normal Firmware Download / coldboot.

To / From	20.2.2x	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1/a/b	20.4.1c	20.4.2
20.3.4a/ac	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot.	Use the normal Firmware Download / coldboot.	Use the normal Firmware Download / coldboot.
20.4.1/a/b	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot.	Use the normal Firmware Download / coldboot.
20.4.1c	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot.	Use the normal Firmware Download / coldboot.	NA	Use the normal Firmware Download / coldboot.
20.4.2	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot.	Use the normal Firmware Download / coldboot.	Use the normal Firmware Download / coldboot	NA

*within the patches

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	20.2.2a/ b/c	20.2.3a to 20.2.3h	20.3.1	20.3.2/a/ b	20.3.2c/ d	20.3.3	20.3.4	20.3.4a/ ac	20.4.1/a/ b	20.4.1c	20.4.2
18r.2.00, 18r.2.00a /b/c	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.2.2a/ b/c using fullinstall . For SLX 9640: 1. First upgrade	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to targeted 20.2.3 version using fullinstall . For SLX 9640:	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.3.1 version using fullinstall . For SLX 9640: 1. First upgrade	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to targeted 20.3.2 version using fullinstall . For SLX 9640:	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.3.2d version using fullinstall . For SLX 9640:	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.3.3 version using fullinstall . For SLX 9640: 1. First upgrade	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.3.4 version using fullinstall . For SLX 9640: 1. First upgrade	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.3.4a version using fullinstall . For SLX 9640:	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.4.1/a/ b version using fullinstall . For SLX 9640:	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.4.1c version using fullinstall . For SLX 9640:	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.4.2 version using fullinstall . For SLX 9640:

To / From	20.2.2a/b/c	20.2.3a to 20.2.3h	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1/a/b	20.4.1c	20.4.2
	to 18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to 20.2.2a/b/c using fullinstall.	1. First upgrade to 18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to targeted 20.2.3 version using fullinstall.	to 18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to 20.3.1 version using fullinstall.	1. First upgrade to 18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to targeted 20.3.2 version using fullinstall.	1. First upgrade to 18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to 20.3.2d version using fullinstall.	to 18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to 20.3.3 version using fullinstall.	to 18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to 20.3.4 version using fullinstall.	1. First upgrade to 18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to 20.3.4a version using fullinstall.	1. First upgrade to 18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to 20.4.1/a/b version using fullinstall.	1. First upgrade to 18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to 20.4.1c version using fullinstall.	1. First upgrade to 18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to 20.4.2 version using fullinstall.
18r.2.00d	For SLX 9540 : 1. First upgrade to 20.1.2h using	For SLX 9540 : 1. First upgrade to 20.1.2h using	For SLX 9540 : 1. First upgrade to 20.1.2h using	For SLX 9540 : 1. First upgrade to 20.1.2h using	For SLX 9540 : 1. First upgrade to 20.1.2h using	For SLX 9540 : 1. First upgrade to 20.1.2h using	For SLX 9540 : 1. First upgrade to 20.1.2h using	For SLX 9540 : 1. First upgrade to 20.1.2h using	For SLX 9540 : 1. First upgrade to 20.1.2h using	For SLX 9540 : 1. First upgrade to 20.1.2h using	For SLX 9540 : 1. First upgrade to 20.1.2h using

To / From	20.2.2a/ b/c	20.2.3a to 20.2.3h	20.3.1	20.3.2/a/ b	20.3.2c/ d	20.3.3	20.3.4	20.3.4a/ ac	20.4.1/a/ b	20.4.1c	20.4.2
	fullinstall. 2. Then upgrade to 20.2.2a/ b/c using fullinstall. For SLX 9640: 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.2.2a/ b/c using fullinstall.	fullinstall. 2. Then upgrade to targeted 20.2.3 version using fullinstall. For SLX 9640: 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to targeted 20.2.3 version using fullinstall.	fullinstall. 2. Then upgrade to 20.3.1 version using fullinstall. For SLX 9640: 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.1 version using fullinstall.	fullinstall. 2. Then upgrade to targeted 20.3.2 version using fullinstall. For SLX 9640: 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to targeted 20.3.2 version using fullinstall.	fullinstall. 2. Then upgrade to 20.3.2d version using fullinstall. For SLX 9640: 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.2d version using fullinstall.	fullinstall. 2. Then upgrade to 20.3.3 version using fullinstall. For SLX 9640: 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.3 version using fullinstall.	fullinstall. 2. Then upgrade to 20.3.4 version using fullinstall. For SLX 9640: 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.4 version using fullinstall.	fullinstall. 2. Then upgrade to 20.3.4a version using fullinstall. For SLX 9640: 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.3.4a version using fullinstall.	fullinstall. 2. Then upgrade to 20.4.1/a/ b version using fullinstall. For SLX 9640: 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.4.1/a/ b version using fullinstall.	fullinstall. 2. Then upgrade to 20.4.1c version using fullinstall. For SLX 9640: 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.4.1c version using fullinstall.	fullinstall. 2. Then upgrade to 20.4.2 version using fullinstall. For SLX 9640: 1. First upgrade to 20.1.2h using fullinstall. 2. Then upgrade to 20.4.2 version using fullinstall.

To / From	20.2.2a/ b/c	20.2.3a to 20.2.3h	20.3.1	20.3.2/a/ b	20.3.2c/ d	20.3.3	20.3.4	20.3.4a/ ac	20.4.1/a/ b	20.4.1c	20.4.2
20.1.1	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.2.2a/ b/c using fullinstall . For SLX 9640: Use fullinstall .	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to targeted 20.2.3 version using fullinstall . For SLX 9640: Use fullinstall .	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.3.1 version using fullinstall . For SLX 9640: Use fullinstall .	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to targeted 20.3.2 version using fullinstall . For SLX 9640: Use fullinstall .	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.3.2d version using fullinstall . For SLX 9640: Use fullinstall .	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.3.3 version using fullinstall . For SLX 9640: Use fullinstall .	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.3.4 version using fullinstall . For SLX 9640: Use fullinstall .	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.3.4a version using fullinstall . For SLX 9640: Use fullinstall .	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.4.1/a/ b version using fullinstall . For SLX 9640: Use fullinstall .	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.4.1c version using fullinstall . For SLX 9640: Use fullinstall .	For SLX 9540 : 1. First upgrade to 20.1.2h using fullinstall . 2. Then upgrade to 20.4.2 version using fullinstall . For SLX 9640: Use fullinstall .
20.1.2e, g	Use fullin stall	Use fullin stall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.1a	Use the normal Firmware	Use the normal Firmware	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall

To / From	20.2.2a/ b/c	20.2.3a to 20.2.3h	20.3.1	20.3.2/a/ b	20.3.2c/ d	20.3.3	20.3.4	20.3.4a/ ac	20.4.1/a/ b	20.4.1c	20.4.2
	Download / coldboot	Download / coldboot									
20.2.2x	NA	Use the normal Firmware Download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.3x	Use the normal Firmware Download / coldboot	NA	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.3.1	Use fullinstall	Use fullinstall	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.
20.3.2/a/ b	Use fullinstall	Use fullinstall	Use the normal Firmware	Use the normal Firmware	Use the normal Firmware	Use the normal Firmware	Use the normal Firmware	Use the normal Firmware	Use the normal Firmware	Use the normal Firmware	Use the normal Firmware

To / From	20.2.2a/ b/c	20.2.3a to 20.2.3h	20.3.1	20.3.2/a/ b	20.3.2c/ d	20.3.3	20.3.4	20.3.4a/ ac	20.4.1/a/ b	20.4.1c	20.4.2
			Download / coldboot	Download / coldboot	Download / coldboot. For downgrade use fullinstall.	Download / coldboot. For downgrade use fullinstall.	Download / coldboot. For downgrade use fullinstall.	Download / coldboot. For downgrade use fullinstall.	Download / coldboot. For downgrade use fullinstall.	Download / coldboot. For downgrade use fullinstall.	Download / coldboot. For downgrade use fullinstall.
20.3.2c/ d	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.	Use the normal Firmware Download / coldboot. For downgrade use fullinstall.
20.3.3	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.3.4	Use fullinstall	Use fullinstall	Use the normal Firmware Download	Use the normal Firmware Download	Use the normal Firmware Download	Use the normal Firmware Download	NA	Use the normal Firmware Download	Use the normal Firmware Download	Use the normal Firmware Download	Use the normal Firmware Download

To / From	20.2.2a/ b/c	20.2.3a to 20.2.3h	20.3.1	20.3.2/a/ b	20.3.2c/ d	20.3.3	20.3.4	20.3.4a/ ac	20.4.1/a/ b	20.4.1c	20.4.2
			/ coldboot	/ coldboot	/ coldboot	/ coldboot		/ coldboot	/ coldboot	/ coldboot	/ coldboot
20.3.4a/ ac	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.4.1/a/ b	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.4.1c	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot
20.4.2	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA

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 SLX9540 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	20.2.2x	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1/a/b	20.4.1c	20.4.2
20.1.1	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.1.2x	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall

To / From	20.2.2x	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1/a/b	20.4.1c	20.4.2
20.2.1x	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.2x	Use the normal firmware download / coldboot*	Use the normal firmware download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.3x	Use the normal firmware download / coldboot	NA	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.3.1	Use fullinstall	Use fullinstall	NA	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot

To / From	20.2.2x	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1/a/b	20.4.1c	20.4.2
20.3.2/a/b	Use fullinstall	Use fullinstall	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot
20.3.2c/d	Use fullinstall	Use fullinstall	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot
20.3.3	Use fullinstall	Use fullinstall	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	NA	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot
20.3.4	Use fullinstall	Use fullinstall	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	NA	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot

To / From	20.2.2x	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a/ac	20.4.1/a/b	20.4.1c	20.4.2
20.3.4a/ac	Use fullinstall	Use fullinstall	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot
20.4.1/a/b	Use fullinstall	Use fullinstall	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot
20.4.1c	Use fullinstall	Use fullinstall	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	NA	Use the normal firmware download / coldboot
20.4.2	Use fullinstall	Use fullinstall	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	NA

*within the patches

Extreme 8520

To / From	20.3.3	20.3.4	20.3.4a/ac	20.4.1/a	20.4.1b	20.4.1c	20.4.2
20.3.3	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.3.4	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.3.4a/ac	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.4.1/a	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.4.1b	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot
20.4.1c	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot
20.4.2	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA

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	SLX 9250	Extreme 8520	Extreme 8720
20.4.2	TPVM 4.1.1 and later	TPVM 4.1.1 and later	TPVM 4.4.0 and later	TPVM 4.2.2 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

- 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 20.4.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 4.1.1 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.

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, only "/apps" partition and its data are 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" 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 ~2.6 GB and the TPVM incremental update Debian file size is ~0.5 GB. These TPVM packages contain Ubuntu security patches available up to August 30, 2022 in TPVM 4.5.4. You must have at least 1GB of free space on the switch before proceeding with the `tpvm upgrade incremental` command

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 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

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.

Configuration	Migration State	Notes
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 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

- SNMPv3 feature-set esp. informs, and user-groups is not fully supported.
- VarBinds and Traps related to RMON (Remote Network Monitoring), HA (High Availability), VACM (view-based Access Control Mode) are partially functional.
- 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 Interfaces or LIFs (Port-VLAN or Port-Bridge domain (BD) association supported on SLX 9150, SLX 9250, Extreme 8520, Extreme 8720 is 13183. Since VLAN, BD resources share the same hardware table memory space, max scale for one has a trade-off with scale for other. For

e.g., maximum port-BD associations cannot be scaled to 13183 when VLAN and BDs combined scale has reached 8096.

Open Defects

The following software defects are open in SLX-OS 20.4.2 as of September 2022:

Parent Defect ID:	SLXOS-50693	**Issue ID:**	SLXOS-50693
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Traffic Management	**Technology:**	Rate Limiting and Shaping
Symptom:	Display summation of forwarded and dropped packets for the confirmed counter		
Condition:	Applying Egress Rate Limit on bridge domain and checking the statistics with "show stat bridge-domain x"		

Parent Defect ID:	SLXOS-52599	**Issue ID:**	SLXOS-52599
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	IPv6 Addressing
Symptom:	/127 prefix routes are accepted and traffic is dropped for them.		
Condition:	If route profile "ipv6-max-prefix64" is enabled on SLX 9150, or SLX 9250		

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

Parent Defect ID:	SLXOS-55243	**Issue ID:**	SLXOS-55243
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-55266	**Issue ID:**	SLXOS-55266
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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.
Recovery:	No known recovery methods available.

Parent Defect ID:	SLXOS-56576	**Issue ID:**	SLXOS-56576
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2
Technology Group:	Other	**Technology:**	Other
Symptom:	On SLX 9740, when the user upgrades software from 20.2.2a to a later release, device becomes unreachable when accessing through an in-band port.		
Condition:	Software upgrade through in-band port.		

Parent Defect ID:	SLXOS-57174	**Issue ID:**	SLXOS-57432
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3b
Technology Group:	Management	**Technology:**	Other
Symptom:	System memory usage increases slowly over time while being managed by EFA		
Condition:	Memory increase is seen when EFA frequently polls SLX for updates and health checks		

Parent Defect ID:	SLXOS-55211	**Issue ID:**	SLXOS-57437
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-57721	**Issue ID:**	SLXOS-57721
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	When we are pinging the destination with the domain name, output will be in decimal format(IP address instead of domain name)		
Condition:	When the firmware is SLXOS 20.1.2, SLXOS 20.2.1 or above ping will have the output in IP address instead of domain name.		

Parent Defect ID:	SLXOS-57738	**Issue ID:**	SLXOS-57738
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-58198	**Issue ID:**	SLXOS-58198
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3c
Technology Group:	Other	**Technology:**	Other
Symptom:	ICL interface is not coming up.		
Condition:	After the BGP process is killed.		

Parent Defect ID:	SLXOS-60970	**Issue ID:**	SLXOS-60970
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.3
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	On SLX 9640. while programming 500 flowspec rules to hardware, a BFD session is down due to "Detection Time Expired" which in turn terminates BGP session. Some BGP sessions flapping are due to this.		
Condition:	In scaled setup, 500 BGP-flow spec rules are programmed in hardware		

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

Parent Defect ID:	SLXOS-61458	**Issue ID:**	SLXOS-61527
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2b
Technology Group:	Other	**Technology:**	Other
Symptom:	When the encrypted password string has “\” or “?” in the startup config, ? or \ is missed in the running-config after config restore and TPVM login will be failed		
Condition:	Encrypted password string should not have these charater “\” or “?”		
Workaround:	TPVM password command needs to be executed till the encrypted password string doesn't have the '\' and '?'.		

Recovery:	TPVM password command needs to be executed again to recover TPVM login

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

Parent Defect ID:	SLXOS-61510	**Issue ID:**	SLXOS-62106
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2c
Technology Group:	Management	**Technology:**	Software Installation & Upgrade
Symptom:	a) If the device is reloaded, running-configs is not retained with auto persistence enable as dcmd database is not present. b) If the device is not reloaded and do a normal fwdl or fullinstall, no issue will be seen.		
Condition:	If “firmware download + noreboot” is issued and later if the “firmware commit” is done and rebooted the device.		

Parent Defect ID:	SLXOS-62773	**Issue ID:**	SLXOS-62773
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Some BGP EVPN ND routes are not flushed in BGP EVPN table alone when one MH node comes out from MM and traffic is not getting forwarded for those ND routes		
Condition:	This EVPN ND routes sync issue happens inconsistently when one MH node comes out from MM		

Parent Defect ID:	SLXOS-61178	**Issue ID:**	SLXOS-62976
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-62671	**Issue ID:**	SLXOS-62995
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	Latency of around 250ms to 1second is observed on SLX device.		
Condition:	SLX node has experienced the CPU congestion		

Parent Defect ID:	SLXOS-63182	**Issue ID:**	SLXOS-63182
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Sometimes the switch reload is seen in a scaled environment.		
Condition:	In scaled environment and BGP PIC configuration is enabled, when routes are learned through BGP and are getting processed.		

Parent Defect ID:	SLXOS-63023	**Issue ID:**	SLXOS-63982
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.2g
Technology Group:	Management	**Technology:**	Software Installation & Upgrade
Symptom:	Device will boot to ONIE on bootrom, and waits for ever.		
Condition:	Doing firmware downgrade from 20.2.3 to 20.1.2 via USB.		

Workaround:	Use methods of firmware download, other than the USB.

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

Parent Defect ID:	SLXOS-64255	**Issue ID:**	SLXOS-65234
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.1.00j
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	ARP not resolved for the peer entry		
Condition:	When link fault is cleared.		

Parent Defect ID:	SLXOS-65700	**Issue ID:**	SLXOS-65700
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	MPLS	**Technology:**	MPLS VPLS - Virtual Private LAN Services
Symptom:	LACP configured Port channels may flap after clearing MACs.		
Condition:	Executing "clear mac dynamic" command on a Provider Edge node with more than 600 VPLS bridge domain configuration may cause LACP port channels to flap.		
Workaround:	MACs can be cleared one at a time or clear MAC by one VLAN at a time		

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

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

Parent Defect ID:	SLXOS-66290	**Issue ID:**	SLXOS-66290
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom:	SAG mac is not programmed in hardware.		
Condition:	ESI flap on port-channel interface.		

Parent Defect ID:	SLXOS-66262	**Issue ID:**	SLXOS-66385
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4a
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	Response is not seen for Neighbor Solicitation		
Condition:	On capturing packets using port mirroring while receiving ICMP6 Neighbor Solicitations at the rate of 1pkt/sec or more, a sporadic miss of Neighbor Advertisements (NA) is seen in the pcap file, though SLX responds with NA for each of them.		

Parent Defect ID:	SLXOS-66718	**Issue ID:**	SLXOS-66718
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Other	**Technology:**	Other
Symptom:	Observed the optics removed for all ports.		
Condition:	After multiple device reloads on 9740 device.		

Parent Defect ID:	SLXOS-66738	**Issue ID:**	SLXOS-66738
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-66740	**Issue ID:**	SLXOS-66740

Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 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-66742	**Issue ID:**	SLXOS-66742
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	BUM packets failed to go out over CCEP(cluster client endpoint) ports		
Condition:	Below is the sequence of trigger: -Maintenance mode enable -Vlan delete/add against CCEP Interface -Disable Maintenance mode		

Parent Defect ID:	SLXOS-64538	**Issue ID:**	SLXOS-66864
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Other	**Technology:**	Other
Symptom:	RME port may be down		
Condition:	Redundant management ports on slx 9740 may not come up for certain ports in certain scenarios		
Workaround:	Reconfigure breakout cable and sh/no shut to resolve the issue		
Recovery:	Reconfigure breakout cable and sh/no shut to resolve the issue		

Parent Defect ID:	SLXOS-66951	**Issue ID:**	SLXOS-66988
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Other	**Technology:**	Other
Symptom:	"Last Runtime error" in the "show tpvm status" after power cycle.		

Condition:	While trying to get the tpvm status before TPVM is coming to alive.
Recovery:	After executing "show tpvm ip" with proper ip, issue will be resolved.

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

Parent Defect ID:	SLXOS-67058	**Issue ID:**	SLXOS-67177
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Other	**Technology:**	Other
Symptom:	BGP IPV6 trap with BGP peer remote address in its varbind list.		
Condition:	During BGP IPV6 traps generation, the bgp peer remote address got stored in ipAddress value type.		

Parent Defect ID:	SLXOS-67321	**Issue ID:**	SLXOS-67373
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Security	**Technology:**	SSH - Secure Shell
Symptom:	After deleting the SSH key from flash it come up again after reload.		
Condition:	After deleting the SSH key from flash it come up again after reload.		

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

Parent Defect ID:	SLXOS-67049	**Issue ID:**	SLXOS-67663
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4a
Technology Group:	Monitoring	**Technology:**	Hardware Monitoring
Symptom:	Flow based mirroring stopped working		
Condition:	On SLX-9150/9250 Platform port channel is configured as destination interface in monitor session in flow based mirroring.		

Workaround:	Rebind ACL on the Source interface configured in flow based monitor session

Parent Defect ID:	SLXOS-66416	**Issue ID:**	SLXOS-67705
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2e
Technology Group:	Security	**Technology:**	User Accounts & Passwords
Symptom:	Unable to login to the device on SLX9740.		
Condition:	When following the password recovery method.		

Parent Defect ID:	SLXOS-66994	**Issue ID:**	SLXOS-67853
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2fa
Technology Group:	Monitoring	**Technology:**	Port Mirroring
Symptom:	For mirrored traffic ICMP reply packets are seen before ICM request packets.		
Condition:	When a PO is used as source interface for mirroring.		

Parent Defect ID:	SLXOS-67492	**Issue ID:**	SLXOS-67928
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1a
Technology Group:	Management	**Technology:**	Other
Symptom:	Failed to bring up the interfaces(0/49:1 & 0/54:1) on SLX9150-48XT.		
Condition:	With presence of QSFP-SFPP-ADPT and 10G SR SFP+ optics on 0/49 or 0/54.		

Parent Defect ID:	SLXOS-67965	**Issue ID:**	SLXOS-67965
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2
Technology Group:	Monitoring	**Technology:**	RAS - Reliability, Availability, and Serviceability
Symptom:	Dcmd core file will be generated and system will boot up.		
Condition:	When support save is started if there is a network connectivity issue and file transfer takes a very long time.		

Parent Defect ID:	SLXOS-67837	**Issue ID:**	SLXOS-68001
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2fb
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol

Symptom:	In routing table, POD prefixes with /25 routes are not added instead the route which has next-hop points to gateway is added.
Condition:	During POD reboot the routes are installed with gateway's next-hop address.

Parent Defect ID:	SLXOS-68053	**Issue ID:**	SLXOS-68053
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	Delay in delivering SNMP traps		
Condition:	With SNMPv3 informs configuration		

Parent Defect ID:	SLXOS-67941	**Issue ID:**	SLXOS-68061
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4b
Technology Group:	Monitoring	**Technology:**	Hardware Monitoring
Symptom:	SLXCLI route command "show hw route-info linecard 0" will show invalid values in the LPM output display.		
Condition:	When route command "show hw route-info linecard 0" is executed from SLXCLI.		

Parent Defect ID:	SLXOS-68101	**Issue ID:**	SLXOS-68101
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Multi-VRF
Symptom:	During VRF delete, user notices brindge-domain VE number being displayed incorrectly as “Ve 0” in NSM raslogs as shown below: <date>, [NSM-1003], 109517, DCE, INFO, BL-1, interface Ve 0 is link down. <date>, [NSM-1001], 109518, DCE, INFO, BL-1, interface Ve 8150 is online. This is cosmetic display error, and no impact to VE functionality.		
Condition:	During VRF delete, when all bounded VE interfaces goes for reset. During VE down, brindge-domain VE number will be displayed incorrectly as “Ve 0” in NSM raslogs. This issue is not observed for Vlan VEs.		

Parent Defect ID:	SLXOS-68166	**Issue ID:**	SLXOS-68166
Severity:	S2 - Major		

Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	After changing any SNMP configuration, snmpwalk of Entity MIB, HA MIB and SW MIB may sometimes result in "No Such Instance".		
Condition:	After changing any SNMP configuration, snmpwalk of Entity MIB, HA MIB and SW MIB may sometimes result in "No Such Instance".		
Recovery:	Restart SNMP agent. This can be achieved by shut/noshut of SNMP service on any VRF. SLX(config)# snmp-server use-vrf mgmt-vrf shut SLX(config)# no snmp-server use-vrf mgmt-vrf shut		

Parent Defect ID:	SLXOS-66943	**Issue ID:**	SLXOS-68200
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.1.00j
Technology Group:	MPLS	**Technology:**	LDP - Label Distribution Protocol
Symptom:	SLX ignores the LDP MAC withdrawal from juniper.		
Condition:	SLX ignores the LDP MAC withdrawal from juniper when juniper sets the IP address as 0.0.0.0.		

Parent Defect ID:	SLXOS-67899	**Issue ID:**	SLXOS-68239
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2fb
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Route entries with 2 next-hops are added where one next-hop is inactive.		
Condition:	During the POD reboot scenario, PODs advertise different next-hop address. Though one of the next-hop is detected as BFD DOWN, route with this next-hop still present in routing table.		
Recovery:	Execute "clear ip route <route>"		

Parent Defect ID:	SLXOS-67978	**Issue ID:**	SLXOS-68324
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3ab

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	Crash is seen in Fibagt module.		
Condition:	1 million BGP routes are advertised and withdrawn in a loop with a gap of 5 seconds in between.		
Workaround:	None.		

Parent Defect ID:	SLXOS-67850	**Issue ID:**	SLXOS-68337
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2ae
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP learnt best route is getting withdrawn and re-programmed once new additional path route is programmed.		
Condition:	Additional Path feature is enabled for BGP.		

Parent Defect ID:	SLXOS-67973	**Issue ID:**	SLXOS-68392
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2d
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD session is not coming up		
Condition:	AMF POD reset		

Parent Defect ID:	SLXOS-68393	**Issue ID:**	SLXOS-68393
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD session will remain in down state.		
Condition:	BFD packet is transmitted with wrong UDP checksum value.		
Recovery:	Flap the IP interface once over which BFD Session is created.		

Parent Defect ID:	SLXOS-68416	**Issue ID:**	SLXOS-68416
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Increase in NHID count for the 8K BFD scaled configuration		

Condition:	PIC is enabled/disabled and SLX device is rebooted

Parent Defect ID:	SLXOS-68429	**Issue ID:**	SLXOS-68429
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	Console message maybe seen - [RTM-1033], 65963, DCE, ERROR, BL-1, System Next-Hop limits exceeded. Current Profile Nexthop 2000. Configured Next-Hops 1003		
Condition:	When Clear bfd neighbors command is issued.		

Parent Defect ID:	SLXOS-68374	**Issue ID:**	SLXOS-68435
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2fd
Technology Group:	Traffic Management	**Technology:**	Rate Limiting and Shaping
Symptom:	When high rate of IGMP traffic is received, device may experience OSPF and BFD sessions flaps.		
Condition:	When high rate of IGMP traffic is received with destination IP address 224.224.224.224.		

Parent Defect ID:	SLXOS-67423	**Issue ID:**	SLXOS-68447
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4ab
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP crash and sessions went down		
Condition:	redeployment of VMs that causes MACs to be advertised		

Parent Defect ID:	SLXOS-68498	**Issue ID:**	SLXOS-68498
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	Delay in delivering traps		
Condition:	When there is flood of traps observed that traps are delivered slowly		

Parent Defect ID:	SLXOS-68190	**Issue ID:**	SLXOS-68561

Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2fd
Technology Group:	IP Multicast	**Technology:**	MLD - Multicast Listener Discovery
Symptom:	Crash is observed in MLD module, followed by node reload and link flaps.		
Condition:	The node receives MLD traffic from peer (with a large length value), on an L3 interface with no multicast configuration.		

Defects Closed with Code Changes

The following software defects were closed in 20.4.2 with code change as of September 2022:

Parent Defect ID:	SLXOS-62115	**Issue ID:**	SLXOS-62126
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2b
Technology Group:	Management	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	SNMP trap is not sent for Loopback interface which is a VTEP, during cluster bring-up after a reload.		
Condition:	Reload of switch that is in a MCT cluster. SNMP trap is not sent when an interface comes up. Issue is seen when VTEP comes up as part of cluster bring-up after reload.		

Parent Defect ID:	SLXOS-65436	**Issue ID:**	SLXOS-65436
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	Not able to delete a logical interface.		
Condition:	When a new BD/LIF was created after LIF limit is reached.		

Parent Defect ID:	SLXOS-66708	**Issue ID:**	SLXOS-66708
Severity:	S1 - Critical		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Other	**Technology:**	Other
Symptom:	observed the crash		
Condition:	when kernel panic is done on the device.		

Parent Defect ID:	SLXOS-66716	**Issue ID:**	SLXOS-66727
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4a
Technology Group:	MPLS	**Technology:**	MPLS VPLS - Virtual Private LAN Services
Symptom:	show bridge-domain <BD#> logical-interface" displays the LIF as untagged, when it is configured as a tagged interface. This is cosmetic issue.		
Condition:	This is only cosmetic bug as traffic was working as tagged. When bridge-domain is configured with tagged interface, show command show it as untagged.		

Parent Defect ID:	SLXOS-66305	**Issue ID:**	SLXOS-66802
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Other	**Technology:**	Other
Symptom:	In 9640, other unrelated 1G ports go down when one particular 1G port is reseated.		
Condition:	In 9640, for example, if ports 0/13, 0/14, 0/16, 0/17 have 1G optics and are UP, and when 0/13 optic is reseated, 0/14 and 0/16 also go down.		

Parent Defect ID:	SLXOS-66829	**Issue ID:**	SLXOS-66836
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3j
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	Switch does not allow new tag-type or TPID to be configured.		
Condition:	While trying to configure a new tag-type the node throws an error - Exceeded the system max on how many different Tag Type can be configured.		

Parent Defect ID:	SLXOS-66826	**Issue ID:**	SLXOS-66850
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2fa
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD session state mismatch between SLX and neighbor.		
Condition:	In SLX-9740,during BFD sessions bringup.		

Parent Defect ID:	SLXOS-66426	**Issue ID:**	SLXOS-66859
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 2 Switching	**Technology:**	VLAN - Virtual LAN
Symptom:	'show interface <phy/po> switchport' output has incorrect Active VLANs after a VLAN is removed from the interface.		
Condition:	When a Vlan is added on to an interface in the order 'switchport trunk native-vlan <vlan-id>' and 'switchport trunk allowed vlan add <vlan-id>', due to cleanup issue, even after removing the vlan using 'switchport trunk allowed vlan remove <vlan-id>', vlan is still showing up in 'show interface <phy/po> switchport' output and also in LIF output associated to vlan.		

Parent Defect ID:	SLXOS-66893	**Issue ID:**	SLXOS-66940
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2fa

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD Sessions enabled stays down.		
Condition:	In SLX-9250/SLX-9150/SLX-8720, BFD Sessions over CEP interface enabled with "bfd-software-session".		

Parent Defect ID:	SLXOS-67323	**Issue ID:**	SLXOS-67333
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom:	TCP packets received from a VxLAN tunnel maybe copied to CPU and forwarded as duplicate packets to host.		
Condition:	When a specific TCP packet with the Acknowledgement number matches with a certain pattern, the packet maybe incorrectly copied to CPU and forwarded as duplicate packet to end host.		

Parent Defect ID:	SLXOS-67007	**Issue ID:**	SLXOS-67379
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2fa
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	Some of the BFD sessions are going down		
Condition:	SRIOV ports are connected with a Leaf pair in Active-Standby mode. When the port connected to active SRIOV is shutdown, some of the BFD sessions go down.		

Parent Defect ID:	SLXOS-67430	**Issue ID:**	SLXOS-67640
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	When IGMP packets are received at high rate via VXLAN tunnel, OSPF sessions may flap.		
Condition:	When IGMP packets are received at high rate via VXLAN tunnel.		

Parent Defect ID:	SLXOS-66927	**Issue ID:**	SLXOS-67670
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4

Technology Group:	Monitoring	**Technology:**	OAM - Operations, Admin & Maintenance
Symptom:	SLX 9540/9640 does not reply with DMR pkts when CFM y.1731 DMM pkts are received from other devices.		
Condition:	SLX 9540/9640 does not reply with DMR response when CFM y.1731 DMM pkts are received from other devices.		

Parent Defect ID:	SLXOS-67528	**Issue ID:**	SLXOS-67676
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.2d
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	May encounter continuous Tx Discard count increment on Ports.		
Condition:	Reported behavior specific to MCT-ICL ports on SLX Leaf switch.		

Parent Defect ID:	SLXOS-67588	**Issue ID:**	SLXOS-67765
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4ab
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	May encounter continuous Tx Discard count increment on Ports.		
Condition:	Reported behavior specific to MCT-ICL ports on SLX Leaf switch.		

Parent Defect ID:	SLXOS-67934	**Issue ID:**	SLXOS-67946
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1b
Technology Group:	Management	**Technology:**	Other
Symptom:	Upon the boot up of SLX, system persists directory file /TPVM/tpvm_disk_pool/		
Condition:	When "write erase all" issued without issuing command, "tpvm uninstall force"		

Parent Defect ID:	SLXOS-67995	**Issue ID:**	SLXOS-68182
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP EVPN MH AD-per-EVI route incorrectly setting VNI value to 0 rather than global value		
Condition:	For BGP EVPN MH, when generated AD-per-EVI route contains VNI field in the NLRI		

Defects Closed without Code Changes

The following software defects were closed in 20.4.2 without code changes as of September 2022.

Parent Defect ID:	SLXOS-63118	**Issue ID:**	SLXOS-63118
Reason Code:	Not Reproducible	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Other	**Technology:**	Other
Symptom:	2nd and 3rd BO ports of 8520-48XT and 8520-48Y do not come up when OIR is done and they are connected to Spirent or a SLX 9150 respectively.		
Condition:	When OIR is done on 8520-48XT or 8520-48Y devices.		
Workaround:	Remove and configure the breakout config or reload the device.		

Parent Defect ID:	SLXOS-66291	**Issue ID:**	SLXOS-66291
Reason Code:	Working as Designed	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Peer group command not accepted under router bgp user vrf		
Condition:	While trying to add peer group for BGP under user vrf.		

Parent Defect ID:	SLXOS-66494	**Issue ID:**	SLXOS-66494
Reason Code:	Not a Software Defect	**Severity:**	S1 - Critical
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Other	**Technology:**	Other
Symptom:	With FEC mode RS-FEC/FC-FEC configuration, the link is not coming up.		
Condition:	When configuring the "no shutdown" on the port, with FEC mode as RS-FEC /FC-FEC.		

Parent Defect ID:	SLXOS-66686	**Issue ID:**	SLXOS-66686
Reason Code:	Already Implemented	**Severity:**	S3 - Moderate
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.1
Technology Group:	Other	**Technology:**	Other
Symptom:	"show efa status" is not getting the status from EFA and throwing the error		
Condition:	While doing multiple EFA upgrade without "no efa deploy", "show efa status" is not getting the status from EFA		
Workaround:	Execute "no efa deploy" before doing the "efa deploy" on the node with already EFA deployed.		

Parent Defect ID:	SLXOS-67955	**Issue ID:**	SLXOS-67955
Reason Code:	Question Answered	**Severity:**	S2 - Major
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.4.2
Technology Group:	MPLS	**Technology:**	MPLS Traffic Engineering
Symptom:	LSP is not coming up between MLX and SLX devices.		
Condition:	SLX MPLS TE is not able to find link between MLX and SLX. Also seeing the delay on hello packets.		