February 2022

Extreme SLX-OS 20.3.4a

Release Notes

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

Contents

Document History

Version	Summary of changes	Publication date
1.0	Initial version for 20.3.4a	February 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 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 20.3.4a is mainly focused on:

- Critical defect fixes
- Mirroring support for Port channel Interface on SLX 9150, SLX 9250, Extreme 8520 and Extreme 8720 platforms
- Smart drift detection method on SLX-OS configuration

Release SLX-OS 20.3.4 is mainly focused on:

- SLX-OS Hardening features
- Augmented ACL and rate-limiting capabilities on SLX 9740 platform
    - IPv4 Ingress ACL based rate-limiting on VE.
    - IPv4 Egress ACL based rate-limiting.
    - IPv6 Egress ACL filtering (Both Source and Destination IPv6 with full address length)
- Forward Error Correction (FEC) changes
- Manual speed configuration for 1G ports on SLX 9150-XT & Extreme 8520-XT.

Release SLX-OS 20.3.3 is mainly focused on:

- Bring up the new hardware platforms – Extreme 8520 and Extreme 8720
- Deliver IP Fabric and data center use cases on newer HW platforms – Extreme 8520 and Extreme 8720
- Provide Trusted Delivery Solution on Service Provider Product portfolio
- Add Security features towards hardening SLX-OS

Release SLX-OS 20.3.2c provides the following features:

No new feature is added in this release.

Release SLX-OS 20.3.2b provides the following features:

- Automatic re-installation of TPVM image after device reload.
- MD5 Password support extended to BGP Dynamic Range.
- Increased the number of supported L3 MTU Profiles to seven (7) on SLX 9740.

Release SLX-OS 20.3.2a provides the following features:

- Single folder/directory support for supportsave collection
- TPVM - NETConf RPC to perform TPVM image sanity
- TPVM Upgrade enhancements – TPVM migration on legacy to config mode
- BGP multihoming with EVPN VxLAN – additional capabilities

Release SLX-OS 20.3.2 provides the following features:

- BGP Multi-homing with EVPN VxLAN
- BGP neighbor teardown-restart-interval

- Allowing 64-character length VRF name
- TPVM Enhancements for EFA use case.
    - TPVM configuration persistence.
    - SLX OS Image upgrade
    - SLX OS configuration snapshot for upgrade and rollback.
- Connection limit option for IP ACL (Management port only)
- BFD timer config at global for both single hop and multi-hop sessions
- Secure (TLS 1.2) support for gNMI streaming
- RSPAN and ERSPAN support for VLAN mirroring
- Optimize Supportsave creation in low memory conditions
- Strong encryption support
- Confidentiality and integrity of O&M traffic

Release SLX-OS 20.3.1 provides the following features:

- Support for BGP Resource Public Key Infrastructure Prefix Origin Validation
- Added support for Unified Routing
- Maintenance Mode support is now available for all devices
- Enhanced Transmission Selection is now supported
- Forced password change on first login is now enforced
- Up to 6 DNS name servers can now be assigned
- Enhanced reporting for VE Statistics for SLX 9540 and SLX 9640
- Option available to drop BPDUs on L2 ports of the switch

Behavior Changes

The following are the behavioral changes for SLX-OS 20.3.4a

No behavioral changes were introduced in this release.

The following are the behavioral changes for SLX-OS 20.3.4

- Availability of HTTP and SSH services for a newly added or operationally up interface in mgmt-vrf, requires the user to restart services.
- Similarly, after removing any interface from the mgmt.-vrf, the user must restart HTTP and SSH services.

The following are the behavioral changes for SLX-OS 20.3.3

No behavioral changes were introduced in this release.

The following are the behavioral changes for SLX-OS 20.3.2c

No behavioral changes were introduced in this release.

The following are the behavioral changes for SLX-OS 20.3.2b

- The copy default-config startup-config command now restores the TPVM (when installed).

  TPVM must be explicitly removed using the below command:

  *copy default-config startup-config **remove-tpvm***

The following are behavioral changes for SLX-OS 20.3.2a.

- Supportsave files will be copied under a **sub directory** under the remote path provided in the support save command. *Please refer the SLX OS 20.3.2a Manageability Guide for more information.*

The following are behavioral changes for SLX-OS 20.3.2.

- TPVM CLI commands are now available under config mode.
- LIF scale reduced to 13150 with EVPN MH feature addition.
- Supportsave threshold for low memory condition is changed from 200 MB to 500 MB.

Software Features

The following key software features are added in the SLX-OS 20.3.4a release

Feature Name	Supported SLX Platforms	Description
Mirroring support on Port channel (PO) interface	SLX 9150 SLX 9250 Extreme 8520 Extreme 8720	Allows user to configure a port channel interface as source mirror port. Currently, user is required to configure this on individual member ports of a port channel

Smart Drift Detection method for SLX-OS configuration	All	Enables Manageability Applications such as Extreme Fabric Automation (EFA) to quickly detect differences in the application stored configuration and SLX-OS configuration and perform reconciliation only when required

The following key software features are added in the SLX-OS 20.3.4 release:

Feature Name	Supported SLX Platforms	Description
Transmission of log event records to central log collection server	All	Supports for system logging using rsyslog over Reliable Event Logging Protocol (RELP).
Ability to control service bindings for listening services	All	Provides flexibility to start/stop HTTP and SSH services on VRFs by hardening the code to bind to specific VRFs
Ability to disable processing of packets utilizing IP Options	All	Enables the ability to disable processing of IPv4 and IPv6 packets using IP Options
IPv4 Egress Rate Limiting	SLX 9740	Adds the IPv4 ingress rate limiting support on VE interfaces, and IPv4 egress rate limiting support on all interface types (physical, PO and VE)
IPv6 ACL enhancement	SLX 9740	New support for egress IPv6 ACL. IPv6 source and destination match is now supported on egress IPv6 ACL in a new ipv6-optimized profile.
BGP Dynamic Peering Scale Enhancement	All	Max. number of BGP Dynamic Peering sessions is increased to 1024.
IPv4 SNMP trap for BGP connection states as supported with IPv6	All	Enables SNMP trap support for IPv4 BGP connection state transition.
1G port on SLX 9150 and Extreme 8520	SLX 9150-T and Extreme 8520-XT	Enables manual configuring of 1G port speed on SLX 9150-XT and Extreme 8520-XT.
FEC mode enhancement	SLX 9150, SLX 9250, Extreme 8720, Extreme 8520 and SLX 9740	"no FEC" support is added.

The following key software features are added in the SLX-OS 20.3.3 release:

Feature Name	Supported SLX Platforms	Description
Measured Boot with Remote Attestation	Extreme 8520 Extreme 8720	Measured boot allows malware detection in the boot components of an SLX switch Remote Attestation allows SLX switches to authenticate hardware and software components to a remote server (attestation server)
GRUB bootloader password protection	All	Add password protection to access the GRUB boot loader.
Support network element authentication (mutual authentication)	All	Introduces mutual authentication where client certificate is validated by a TLS party acting as a server
Support preservation of SSH Host Keys during all upgrades (mutual authentication)	All	Ensures SSH host keys are preserved after all upgrade procedures, esp. with fullinstall and netinstall
Support inactivity for user account	All	Informs user about account inactivity and lock user accounts on SLX OS for exceeded inactivity periods
Enforcement of least privilege	All	Enforces least access privilege for log files, bin files and text file permissions on SLX OS to minimize potential impact in the wake of any malicious attacks
Certificate management – expiry alert	All	Allows users to receive an early notification when Cryptographic certificates on SLX OS are nearing expiry. User can configure severity levels and period (number of days for certificate expiry)
Platform and Software Bring up on Extreme 8520 and Extreme 8720	Extreme 8520 Extreme 8720	Bring up new hardware platforms (Extreme 8520 and 8720) and support IP Fabric and data center feature set
L3 MTU profile support	SLX 9250 Extreme 8720	Increases number of supported L3 MTU profiles
Per neighbor support for BGP Graceful Restart	All	Allowing to configure BGP Graceful Restart feature on a per-neighbor basis
Per-Interface Neighbor Discovery Cache Limit	All	Mitigates certain DoS attacks in IPv6 deployments that involves advertising large numbers of hosts in the same subnet and filling the IPv6 ND Cache table
BGP MIB support for bgp4V2PrefixGaugesTable	All	SNMP MIB support for BGP prefix gauge table

The following key software features are added in the SLX-OS 20.3.2c release:
No new feature is added in this release.

The following key software features are added in the SLX-OS 20.3.2b release:

Feature Name	Supported SLX Platforms	Description
MTU Profiles support	SLX 9740	Increased the number of supported L3 MTU Profiles to 7.
MD5 Password support extended to BGP Dynamic Range	All Platforms	MD5 password is supported on dynamic BGP neighbors with range options.
Automatic re-installation of TPVM image after resetting the device	All Platforms	By default, TPVM configuration will be retained after issuing "coping default to startup-config". User needs to explicitly configure **'remove-tpvm'** parameter of this command to prevent TPVM being automatically reinstalled.

The following key software features are added in the SLX-OS 20.3.2a release:

Feature Name	Supported SLX Platforms	Description
Single folder/directory support for supportsave collection	All Platforms	Provide support to create a sub directory under the remote path provided in the support save command
TPVM - NETConf RPC to perform TPVM image sanity	All Platforms	Augments current "tpvm upgrade" command to sanitize image before downloading for parameters such as length, version, host access, user/credential authentication
TPVM Upgrade enhancement – TPVM migration support	All Platforms	Migrate the TPVM configurations done using legacy exec commands (in releases before SLX OS 20.3.2), to running-config, during the firmware download to SLX OS 20.3.2a.
BGP multihoming with EVPN VxLAN	SLX 9150, SLX 9250	Additional EVPN Multihoming support for 1) Core Isolation (Disable case) 2) IRB in multi-homed topology - L3 VNI 3) Maintenance Mode

The following key software features are added in the SLX-OS 20.3.2 release.

Feature Name	Supported SLX Platforms	Description
BGP Multi-homing with EVPN VxLAN	SLX 9150 SLX 9250 Extreme 8720	Supporting BGP EVPN VxLAN based multi-homing clients.
BGP neighbor teardown-restart-interval	All Platforms	To support automatic restart of BGP neighbor restarts after a teardown due to prefix-limit.
Allowing 64-character length VRF name	All Platforms	VRF name length is increased to 64 characters.
TPVM Image Upgrade via EFA and Configuration Persistence	All Platforms	TPVM Image can be upgrade via EFA and configuration preserved.
Connection limit option for IP ACL (Management port only)	All Platforms	Number of connection per-IP can be limited via ConnTrack module in IP tables.
BFD timer config at global for both single hop and multi-hop sessions	All Platforms	BFD timer value can be configured at global level for all session.
Secure (TLS 1.2) support for gNMI streaming	All Platforms	Interface counters can be streamed up via gNMI to gNMI clients.
RSPAN and ERSPAN support for VLAN mirroring	SLX 9150 SLX 9250 SLX 9740 Extreme 8720	Support port and flow based span
Strong encryption support	All Platforms	Capability to control the TLS version used by SLX-OS services
Confidentiality and integrity of O&M traffic	All Platforms	4096-bit SSH host key support.
Optimize Supportsave creation in low memory conditions	All Platforms	Depending on low system memory conditions hitting threshold (500 MB), support save creation will automatically move to basic support save.

Feature Name	Supported SLX Platforms	Description
TPVM Configuration Persistence	All Platforms	New config mode added to `deploy tpvm` and related TPVM configurations. When these TPVM configuration are persisted at SLX-OS config database too, they can be displayed by `show running-config tpvm` and other `show` commands Earlier, TPVM could be installed using the `tpvm install` or `tpvm deploy` or other similar commands. The configurations were applied using the `tpvm config` set of commands. These applied configurations were retained by the TPVM Guest OS. These configurations were available for use only when the switch rebooted. But across upgrade and SLX switch RMA, manual re-applying was needed on new installation. In the new mode, along with the new TPVM Upgrade CLIs, upgrade or RMA like operation becomes seamless and the device admin need not re-apply previously configured TPVM settings. For more information on configuring TPVM Configuration Persistence, refer the 'Management Configuration Guide' for SLX-OS 20.3.2. Note: Both modes of installation are allowed for backward compatibility, However, only one TPVM can be installed. It is recommended to use one of these two modes and not mix.
TPVM Upgrade	All Platforms	New CLI to download new TPVM image. If SLX had any previously deployed TPVM as per new mode introduced in this release SLX-OS 20.3.2, then that will be stop/uninstalled and new image shall be deployed and previously set TPVM configurations will be applied too. For more information on configuring TPVM Configuration Persistence, refer the 'Management Configuration Guide' for SLX-OS 20.3.2.

Feature Name	Supported SLX Platforms	Description
TPVM snapshot	All Platforms	Installed TPVM snapshot (backup) can be taken manually or as part of `tpvm upgrade` CLI. If admin finds upgrade failed or for any reason, TPVM instance can be reverted to backup instance. Note: in-between configs should not be updated and only one snapshot instance is supported. For more information on configuring TPVM Configuration Persistence, refer the 'Management Configuration Guide' for SLX-OS 20.3.2.

CLI Commands

The following commands were added, modified, or deprecated for the 20.3.4a program

New commands for 20.3.4a

- config-drift-track
- show config-drift-track

Modified commands for 20.3.4a

No commands were modified in this release.

Deprecated commands for 20.3.4a

No commands were deprecated in this release.

The following commands were added, modified, or deprecated for the 20.3.4 program

New commands for 20.3.4

- logging utility
- ipv6 option disable
- undeploy-force (tpvm)

Modified commands for 20.3.4

- speed (ethernet)
- service-policy (interface)
- fec mode (interface)
- ip option disable

Deprecated commands for 20.3.4

No commands were deprecated in this release.

The following commands were added, modified, or deprecated for the 20.3.3 program

New commands for 20.3.3

- agent-enable
- agent-uuid
- agent-port
- core-isolation-track
- crypto cert
- enable (GRUB)
- grub
- measured-boot enable
- neighbor graceful-restart
- registrar-server
- registrar-port
- show core-isolation track
- show remote-attestation
- username (GRUB)

Modified commands for 20.3.3

- crypto ca import-pkcs
- crypto import
- ipv6 nd cache interface-limit
- show policy-map
- tpvm config hostname
- username
- hostname (tpvm mode)

Deprecated commands for 20.3.3

No commands were deprecated in this release.

The following commands were added, modified, or deprecated for the 20.3.2c program

New commands for 20.3.2c

No commands are added in this release.

Modified commands for 20.3.2c

No commands are modified in this release.

Deprecated commands for 20.3.2c

No commands are deprecated in this release.

The following commands were added, modified, or deprecated for the 20.3.2b program

New commands for 20.3.2b

No commands are added in this release

Modified commands for 20.3.2b

- copy default-config startup-config

Deprecated commands for 20.3.2b

No commands are deprecated in this release.

The following commands were added, modified, or deprecated for the 20.3.2a program

New commands for 20.3.2a

- tpvm fileinfo
- tpvm download
- core-isolation-disable
- lacp system-id

Modified commands for 20.3.2a

- neighbor password
- ip ospf md5-authentication
- area authentication
- ip vrrp-extended auth-type

- auth-key
- isis auth-key
- tpvm upgrade

Deprecated commands for 20.3.2a

- neighbor accept-lldp-neighbors

The following commands were added, modified, or deprecated for the 20.3.2 program

New commands for 20.3.2

- auto-boot (tpvm mode)
- Ethernet-segment
- Esi
- gnmi server
- interface management (tpvm mode)
- ip route static bfd
- management-security
- neighbor <IPv4/v6> maximum-prefix <maxprefixcount> teardown restart-interval <interval>
- password (tpvm mode)
- ssl-profile
- tls min-version
- tpvm (mode)
- hostname (tpvm mode)
- timezone (tpvm mode)
- dns (tpvm mode)
- ntp (tpvm mode)
- ldap (tpvm mode)
- ldap ca-cert (tpvm mode)
- trusted-peer (tpvm mode)
- tpvm deploy (tpvm mode)
- tpvm snapshot
- tpvm upgrade (tpvm mode)

Modified commands for 20.3.2

- acl-mirror
- crypto ca import-pkcs
- crypto import
- ip access-list extended
- ipv6 access-list extended
- ip route static bfd
- ssh server key
- show ip/ipv6 bgp neighbor
- show tpvm status

    It adds one additional line of information to indicate "*additional status*".

E.g.

```
SLX# show tpvm status
SSH and Sudo passwordless      :Enabled
AutoStart                      :Enabled
Tpvm status                    :Running
Tpvm version                   :4.2.5
Tpvm additional status         :normal
```

It is mainly set to **normal**, implying rest of above fields are normal. But if upgrade or deploy, is issued, then it reflects transiting state of that operation. For success completion, it again gets value "normal" else reflect error state.

- switchport access
- switchport trunk allowed

Deprecated commands for 20.3.2

- qos cos cos_value

The following commands were added, modified, or deprecated for the 20.3.1 program

New commands for 20.3.1

- bestpath prefix-validation disable
- bestpath prefix-validation disallow-invalid
- cee
- cee-map
- import l2vpn evpn reoriginate
- import vpnv4 unicast reoriginate
- import vpnv6 unicast reoriginate
- match rpki
- neighbor announce rpki state
- priority-group-table
- priority-table
- rpki priority
- server ssh
- server tcp
- show cee-map default

Modified commands for 20.3.1

- bpdu-drop-enable
- clear ip bgp rpki server
- clear counters
- clear counters access-list
- ip dns
- ip access-list
- password-attributes
- profile counters
- monitor session

- show lldp neighbors
- show system maintenance
- show ip bgp rpki details
- show ip bgp rpki server summary
- show ip bgp rpki table
- show ip bgp routes
- show hardware profile
- show interface stats detail
- show access-list
- show statistics access-list
- system maintenance
- system maintenance turn-off

Deprecated commands for 20.3.1

- match uda
- seq (deny/permit rules in UDAs)
- set uda interface null0
- show running-config uda access-list
- show running-config uda-key profile
- uda access-group
- uda access-list
- uda policy route-map
- uda-key profile
- uda-offsets
- uda-profile-apply

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

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 20.3.4a, see the *Extreme SLX-OS Software Upgrade Guide.*

Image files

Download the following images from www.extremenetworks.com.

Image file name	Description
SLX-OS_20.3.4a.tar.gz	SLX-OS 20.3.4a software
SLX-OS_20.3.4a_mibs.tar.gz	SLX-OS 20.3.4a MIBS
SLX-OS_20.3.4a.md5	SLX-OS 20.3.4a md5 checksum
SLX-OS_20.3.4a-digests.tar.gz	SLX-OS 20.3.4a sha checksum
SLX-OS_20.3.4a-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
20.2.3(MFG)	Use the normal Firmware Download / coldboot	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
20.2.3x	NA	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.3.2/a/b	Use fullinstall	NA	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.
20.3.2c/d	Use fullinstall	Use the normal Firmware Download / coldboot	NA	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

To From	20.2.3x	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a
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
20.3.4a	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

SLX 9740

To From	20.2.2x	20.2.3_CR	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a
20.2.1a	Usethe normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	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 the normal Firmware Download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.3_CR	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.3x	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.3.1	Use fullinstall	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.

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

To From	20.2.2x	20.2.3_CR	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a
20.3.4a	Use fullinstall	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	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 there 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
18r.2.00, 18r.2.00 a/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:	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:	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: 1. First upgrade to	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 to	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 to	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: 1. First upgrade to

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
	1. First upgrade 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.	1. First upgrade 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.	18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to 20.3.2d version using fullinstall.	18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to 20.3.3 version using fullinstall.	18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to 20.3.4 version using fullinstall.	18r.2.00d via fullinstall. 2. Then upgrade to 20.1.2h using fullinstall. 3. Then upgrade to 20.3.4a version using fullinstall.
18r.2.00d	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 to	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: 1. First upgrade to	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 to	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: 1. First upgrade to	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: 1. First upgrade to 20.1.2h using 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: 1. First upgrade to 20.1.2h using 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: 1. First upgrade to 20.1.2h using 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: 1. First upgrade to 20.1.2h 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
	20.1.2h using fullinstall. 2. Then upgrade to 20.2.2a/b/c using fullinstall.	20.1.2h using fullinstall. 2. Then upgrade to targeted 20.2.3 version using fullinstall.	20.1.2h using fullinstall. 2. Then upgrade to 20.3.1 version using fullinstall.	20.1.2h using fullinstall. 2. Then upgrade to targeted 20.3.2 version using fullinstall.	2. Then upgrade to 20.3.2d version using fullinstall.	2. Then upgrade to 20.3.3 version using fullinstall.	2. Then upgrade to 20.3.4 version using fullinstall.	2. Then upgrade to 20.3.4a version using fullinstall.
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..
20.1.2e, g	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
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

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
20.2.2x	NA	Use the normal Firmware Download / coldboot	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
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.
20.3.2/a /b	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	NA	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.
20.3.2c/ d	Use fullinstall	Use fullinstall	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA	Use the normal Firmware Download / coldboot. For	Use the normal Firmware Download / coldboot. For	Use the normal Firmware Download / coldboot. For

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
						downgrade use fullinstall.	downgrade use fullinstall.	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
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
20.3.4a	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	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	20.2.3_CR	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a
20.1.1	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	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 the normal firmware download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.1x	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	Use the normal firmware download / coldboot	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 the normal firmware download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall
20.2.3_CR	Use the normal firmware download / coldboot	NA	Use the normal firmware download / coldboot	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall	Use fullinstall

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

To / From	20.2.2x	20.2.3_CR	20.2.3x	20.3.1	20.3.2/a/b	20.3.2c/d	20.3.3	20.3.4	20.3.4a
20.3.4	Use fullinstall	Use fullinstall	Use fullinstall	Use the normal firm ware download / coldboot	Use the normal firm ware download / coldboot	Use the normal firm ware download / coldboot	Use the normal firm ware download / coldboot	NA	Use the normal firm ware download / coldboot
20.3.4a	Use fullinstall	Use fullinstall	Use fullinstall	Use the normal firm ware download / coldboot	Use the normal firm ware download / coldboot	Use the normal firm ware download / coldboot	Use the normal firm ware download / coldboot	Use the normal firm ware download / coldboot	NA

*within the patches

Extreme 8520

To ⟍ From	20.3.3	20.3.4	20.3.4a
20.3.3	NA	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
20.3.4a	Use the normal Firmware Download / coldboot	Use the normal Firmware Download / coldboot	NA

SLX TPVM Support Matrix for 9150 and 9250, Extreme 8520 and Extreme 8720

SLX Build	TPVM – Fresh Install Supported	EFA
20.2.2	TPVM-4.1.1	EFA-2.3
20.2.2a	TPVM-4.1.2	EFA-2.3.x
20.2.2b	TPVM-4.1.2	EFA-2.3.x
20.2.3	TPVM-4.2.2	EFA-2.4.x, EFA-2.3.x
20.2.3a	TPVM-4.2.3	EFA-2.4.x, EFA-2.3.x, EFA-2.5x *
20.3.1	TPVM-4.2.4	EFA-2.4.x
20.3.2/a/b/c	TPVM-4.2.5	EFA-2.4.x, EFA-2.5x
20.3.2d	TPVM-4.3.0	EFA-2.4.x, EFA-2.5x
20.3.3	TPVM-4.2.5	EFA-2.5x
20.3.4	TPVM-4.4.0	EFA-2.5x
20.3.4a	TPVM-4.4.0	EFA-2.6.0

* EFA-2.4.x feature parity in 20.2.3d

Note:

Extreme 8720 and Extreme 8520 are supported from 20.3.3 onwards.

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

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

- 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, take the following steps:
  - Upgrade to SLX-OS 20.3.x, 20.2.3/x with existing TPVM continue to run

- Remove 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`.

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, as a best practice make a backup and then delete the old disks. Use the **tpvm disk remove name <disk name>** command, 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 the 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 backup of EFA installation.**"

Notes:

Security updates are added to the TPVM, there is a change in size of TPVM image to ~2.3 GB. This TPVM package contains Ubuntu security patches available up to 11th November, 2021.
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

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 plan to delete disk vdb (i.e. 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 new mode does not support new disk creation. Old "tpvm disk add" can be used.
4. As simple example for new mode deploy:
   a. Copy new TPVM debian Image under /tftpboot/SWBD2900. Only one file should be there and no subfolder.
   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 if say "tpvm config hostname xyz" command is used. It will still work and apply on TPVM instance. But this config shall not be persisted in SLX Database and will become inconsistent. Same true for any other config done in old way.

b. As in above example, password, management config should always be set before deploy. If required later, refer User Guide and use tpvm stop, start for such update/maintenance reason.

c. tpvm uninstall [force], if used, then you shall need "no deploy" and deploy, in new mode.

For more information on configuring TPVM Configuration Persistence, refer the 'Management Configuration Guide' for SLX-OS 20.3.2x.

TPVM Migration

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

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

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 … `"

Limitations and Restrictions

Copy flash to startup and reload with TPVM

setNTPServer and setLDAPServer statuses are reported as failed in "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.

TPVM Migration

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

Configuration	Migration State	Notes
tpvm auto-boot	Migrated	
tpvm disk	Not Migrated	Disk configuration is not supported in the configuration mode, and therefore, not migrated.
tpvm password	Migrated	Only the old password is migrated. This is due to the password being encrypted and stored and it is not

		possible to know if the password was changed during the migration.
tpvm config ntp	Migrated	
tpvm config dns	Migrated	
tpvm config ldap	Migrated	Secure LDAP require certificates. It is assumed that certificates are already downloaded and installed. Certificates are not validated during this migration. A notification will be sent to the user to reconfigure LDAP certificate settings.
tpvm config hostname	Migrated	
tpvm config timezone	Migrated	
tpvm deploy <interface> allow-pwless	Not Migrated	This is the new default configuration and is not migrated.
tpvm deploy mgmt [dhcp | static]	Migrated	
tpvm deploy insight	Not Migrated	Insight interface configuration is not supported when configuring using the Privilege Execution Mode commands.
tpvm config ldap ca-cert	Not Migrated	
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.
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 is not working 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.
- The **show running ip prefix-list <name>** command can take a long time to complete in a scaled prefix-list configuration.

- 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 supports 16K flowset entries for SLX 9740, and 32K flowset entries for SLX 9150/9250.

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.

Open Defects

The following software defects are open in SLX-OS 20.3.4a as of **February 2022**:

Parent Defect ID:	SLXOS-63282	Issue ID:	SLXOS-63956
Severity:	S1 - Critical		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Monitoring	**Technology:**	Port Mirroring
Symptom:	On SLX 9740, flow based mirroring is not working for flow matching deny rules with the configured ACL		
Condition:	configure mirror action in deny rule , traffic matching deny rule are not mirrored.		

Parent Defect ID:	SLXOS-63941	Issue ID:	SLXOS-63959
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2bb
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Unexpected reload of the switch		
Condition:	During the SNMP walk with 1 M routes learnt from real internet feed, when any route among the learnt routes has a longer BGP AS path attribute.		

Parent Defect ID:	SLXOS-63121	Issue ID:	SLXOS-63966
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.4
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	"show cluster track" command does not display correct interface status		
Condition:	Interface status is not displayed as 'down' under 'show cluster track' when port-channel becomes down due to the minimum-link criteria not being met.		

Parent Defect ID:	SLXOS-62863	Issue ID:	SLXOS-63967
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:	1+ sec of traffic loss is observed during a border leaf reload.		
Condition:	Reloading one of SLX-9740 border leaf's in a MCT configuration		

Parent Defect ID:	SLXOS-63023	Issue ID:	SLXOS-63981
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-63253	Issue ID:	SLXOS-63990
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.4
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	MCT Cluster peer-interface Port-channel flaps few times		
Condition:	On reloading one of the border leaf nodes in the MCT configuration, ICL port-channel flaps, while the reloaded node is coming online. This happens when more than 5000 BFD sessions are established over the VxLAN tunnel.		

Parent Defect ID:	SLXOS-63118	Issue ID:	SLXOS-63991
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-62353	Issue ID:	SLXOS-63992
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2b
Technology Group:	Layer 2 Switching	Technology:	VXLAN - Virtual Extensible LAN
Symptom:	VRF traffic loss is greater than 1sec upon spine node reboot.		
Condition:	Upon spine reboot, few BFD sessions from compute nodes to border-leaf flap and traffic loss for 1-2 sec is observed.		

Parent Defect ID:	SLXOS-63092	Issue ID:	SLXOS-63993
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:	Convergence times of upto 800 msec is seen when an interface from the Gateway towards the Border Leaf is shut down		
Condition:	There is a port channel between PE router and the Border leaf. The minimum-links is configured in the port channel. One of the physical interfaces in the port channel is shut and the minimum-link configuration brings down the port channel. The convergence time for the traffic from the border leaf towards the gateway is sometimes seen to be in the range of 500-800 msec.		
Workaround:	Using only BGP routes and configuring Prefix-Independent-Convergence can provide better convergence times than having static routes.		

Parent Defect ID:	SLXOS-62668	Issue ID:	SLXOS-63994
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.3
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	L2sys daemon terminates on one of the MCT cluster node		
Condition:	During MCT cluster node bring up after transitioning the Multi Homing EVPN config to MCT config using config script		

Parent Defect ID:	SLXOS-61371	Issue ID:	SLXOS-63996
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2
Technology Group:	Other	Technology:	Other
Symptom:	On SLX 9740, and breakout port cli command on a port-macro group, can cause other ports in same group to flap sometimes.		
Condition:	Issue is seen when the breakout command is configured.		

Parent Defect ID:	SLXOS-62922	Issue ID:	SLXOS-64001
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2d
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Some IPV4 BGP sessions gets deleted only after BGP hold timer expires even though BFD has gone down		
Condition:	When configuring with Extreme Fabric Automation(EFA), and EPG(End Point Group) is removed in the local node. Issue in the symptom is seen on the remote node.		

Parent Defect ID:	SLXOS-63182	Issue ID:	SLXOS-64025
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-59118	Issue ID:	SLXOS-64026
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Overlay traffic loss of 2+ second		
Condition:	In BGP EVPN based Multihoming solution, one of the leaf node going through reload.		

Parent Defect ID:	SLXOS-60298	Issue ID:	SLXOS-64028
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2a
Technology Group:	Other	Technology:	Other
Symptom:	One of the BFD session over MCT flaps on cluster node. There is no visible traffic loss as such because the other MCT peer takes the traffic over ICL and forwards it to CCEP DUT (from L3 GW).		
Condition:	On reload and system maintenance turn-off on an SLX8720 cluster node. System scale: 32 VRFs, at least 2 BFD over MCT, 2 HW BFD and 2 BFD over VxLAN session per VRF. (one IPv4 and one IPv6) (First 20 VRFs have 10+ BFD over MCT sessions towards CCEP DUTs, last 12 VRFs have 2 BFD over MCT sessions towards CCEP DUTs) All VE interfaces configured across all devices are dual stack. SW BFD sessions: 393 HW BFD sessions: 65 960 IPv4 routes, 960 IPv6 routes from L3 GW. 960 IPv4 routes, 960 IPv6 routes from CCEP DUTs. System-wide route scale: 3K IPv4 and 3K IPv6		
Workaround:	issue seen on Ve's attached to BDs. Remove the VE from BD and reconfigure.		

Parent Defect ID:	SLXOS-58198	Issue ID:	SLXOS-64030
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-62135	Issue ID:	SLXOS-64194
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00b
Technology Group:	Monitoring	Technology:	RAS - Reliability, Availability, and Serviceability
Symptom:	Logs indicating flash size usage crossing high boundary		
Condition:	/var/log/hasm.log file size is large, with no impact on functionality		

Parent Defect ID:	SLXOS-64409	Issue ID:	SLXOS-64409
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.		

The following software defects are open in SLX-OS 20.3.4 as of **December 2021**:

Parent Defect ID:	SLXOS-40754	Issue ID:	SLXOS-40754
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BFD - BiDirectional Forwarding Detection
Symptom:	BFD sessions will flap and bring down associated client sessions bound to it.		
Condition:	Maximum Supported IPv4 Multi-hop BFD session is 16. When IPv4 BFD Multi-hop session count exceeds 16, BFD sessions will flap.		

Parent Defect ID:	SLXOS-42488	Issue ID:	SLXOS-42488
Severity:	S3 - Moderate		

Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Other	Technology:	Other
Symptom:	"show running-config ip prefix-list <list-name>" on specific prefix-list sometimes doesnt work		
Condition:	issue is observed during highly scaled scale prefix-list configurations		
Workaround:	use show running-config ip prefix-list show running-config show running-config ip prefix-list | include <prefix-list-name>		

Parent Defect ID:	SLXOS-46276	Issue ID:	SLXOS-46276
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	The remote end tunnel retains old VTEP IP when VTEP IP is changed at the local end		
Condition:	When tunnel VTEP IP is changed locally, some of the evpn IMR routes for old VTEP IP are not withdrawn. Hence old tunnel exists at remote end.		
Workaround:	When VTEP IP is modified, please issue "clear bgp evpn neighbor all"		

Parent Defect ID:	SLXOS-46419	Issue ID:	SLXOS-46419
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Monitoring	Technology:	Port Mirroring
Symptom:	QoS service-policy configuration is not allowed on a mirror destination port-channel.		
Condition:	Configure a port-channel as mirror destination and configure a service-policy under this port-channel.		
Workaround:	Remove mirror configuration and add service-policy under this port-channel. Reconfigure mirror session with this port-channel as mirror destination.		

Parent Defect ID:	SLXOS-47644	Issue ID:	SLXOS-47644
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Security	Technology:	ACLs - Access Control Lists
Symptom:	OSPF neighbourship doesn't go down after applying IP ACL on the interface		
Condition:	Applying IP ACL after OSPF neighbourship up.		
Workaround:	Clear OSPF neighbourship after IP ACL applied.		

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-51794	Issue ID:	SLXOS-51822
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.1
Technology Group:	Traffic Management	Technology:	QoS - Quality of Service
Symptom:	Virtual output queue statistics of traffic manager are not incrementing for priority traffic classes.		
Condition:	Traffic manager CLI command: "show tm voq-stat" is executed.		

Parent Defect ID:	SLXOS-49454	Issue ID:	SLXOS-52076
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.1
Technology Group:	Management	Technology:	CLI - Command Line Interface
Symptom:	Sometimes, show running-config ip prefix-list <name> takes around 25 mins to display output		
Condition:	Issue is seen when the user is querying for a specific prefix-list while the device has highly scaled prefix list configuration		
Workaround:	Use "show running-config ip prefix-list" or "show ip prefix-list <name>"		

Parent Defect ID:	SLXOS-52329	Issue ID:	SLXOS-52329
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.1a
Technology Group:	IP Multicast	Technology:	IGMP - Internet Group Management Protocol
Symptom:	The IGMP querier node does not receive IGMP joins on Multicast tunnel even though there are receivers present on other LVTEP. This causes IGMP group entry expiry after the time-out.		
Condition:	1. There should be MCT nodes acting as a leaf (LVTEP) and receiver should be connected to CCEP client or CEP port. 2. The MDT Rx path is on one MCT peer and MDT Tx path is on other		

	MCT peer. 3. IGMP Query should be received on Multicast tunnel. 4. IGMP report should land on the peer which is having MDT Rx path.		
Workaround:	If Source or Receiver is connected to one of the MCT nodes, then it is recommended to configure IGMP snooping querier for the vlan or Bridge domain on both the MCT peers.		

Parent Defect ID:	SLXOS-52506	**Issue ID:**	SLXOS-52506
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1a
Technology Group:	Management	**Technology:**	Other
Symptom:	Netconf request to configure ip prefix-list without providing sequence number fails and returns error.		
Condition:	Issue exists only for configuration via Netconf		
Workaround:	Workaround is to provide sequence number value in the Netconf request while configuring ip prefix-list		

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-55198	**Issue ID:**	SLXOS-55198
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.2a
Technology Group:	Management	**Technology:**	Other
Symptom:	"no fec mode " CLI support is removed		
Condition:	"no fec mode " CLI support is removed and due to this the User will not be able to go to Default FEC mode on specified port.		
Workaround:	User can do Explicit FEC Configuration either Enable with appropriate FEC mode or Disable FEC for specified port.		

Parent Defect ID:	SLXOS-55243	Issue ID:	SLXOS-55243
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.2a
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 20.2.2a
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-55569	Issue ID:	SLXOS-55569
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2c
Technology Group:	Layer 2 Switching	Technology:	VLAN - Virtual LAN
Symptom:	L2 Loop not detected and blocked		
Condition:	Loop-detection feature doesn't detect and block L2 loop when provisioned on Ethernet or Port-channel interface		
Workaround:	Configure loop-detection on VLAN to which Ethernet or Port-channel is member. This will detect the loop and block it.		

Parent Defect ID:	SLXOS-55586	Issue ID:	SLXOS-55586
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2a
Technology Group:	Monitoring	Technology:	sFlow
Symptom:	SFLOW not working as expected		
Condition:	monitoring inbound and outbound traffic with Netflow		

Parent Defect ID:	SLXOS-56576	Issue ID:	SLXOS-56576
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.2a
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-56675	Issue ID:	SLXOS-56675
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3a
Technology Group:	Other	Technology:	Other
Symptom:	WARNING message, Unqualified SFP transceiver for interface Ethernet 0/x is detected.		
Condition:	Insert 100G LR4 optic (EQPT1H4LR4LCL100) optics.		

Parent Defect ID:	SLXOS-56861	Issue ID:	SLXOS-56861
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.2b
Technology Group:	Other	Technology:	Other
Symptom:	Sometimes, a unrelated interface can go down when an optic is inserted.		
Condition:	A new optic is inserted in SLX 9740.		

Parent Defect ID:	SLXOS-57031	Issue ID:	SLXOS-57031
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.1
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	SLXOS BGP process may crash and router will get rebooted		
Condition:	If the user tries to remove L2VPN EVPN address family		
Workaround:	Deactivate BGP neighbors under L2VPN EVPN address family. And then remove the L2VPN EVPN address family.		

Parent Defect ID:	SLXOS-57274	Issue ID:	SLXOS-57274
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.2b
Technology Group:	Management	Technology:	CLI - Command Line Interface
Symptom:	On execution of "show run route-map" command with route map name like "show run route-map <route-map-name>" it throws error.		
Condition:	Issue is seen when "show run route-map" command is invoked with route map name.		
Workaround:	As a workaround command "show run route-map" can be executed and it will display the output for all configured route maps.		

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 20.2.2a
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-56401	Issue ID:	SLXOS-57443
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3
Technology Group:	Other	Technology:	Other
Symptom:	The following Brocade branded 4x10G breakout DAC modules are not detected sometimes. The affected module SKU's are 40G-DACP-QSFP4SFP1M, 40G-DACP-QSFP4SFP3M, 40G-DACP-QSFP4SFP5M		
Condition:	Over a period of time, the issue is seen from a corruption in the EEPROM MSA programming		

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

Parent Defect ID:	SLXOS-57371	Issue ID:	SLXOS-57471
Severity:	S3 - Moderate		

Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3b
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BFD - BiDirectional Forwarding Detection
Symptom:	Few BFD sessions will flap once during system bring up.		
Condition:	On 9740,during system bring up after reload.		

Parent Defect ID:	SLXOS-57721	Issue ID:	SLXOS-57721
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.2b
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-57753	Issue ID:	SLXOS-57853
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00h
Technology Group:	MPLS	Technology:	LDP - Label Distribution Protocol
Symptom:	Unexpected reload.		
Condition:	On continuous MPLS interface flap for every 60 seconds run for minimum 5 hrs, to re-establish LDP tunnels.		

Parent Defect ID:	SLXOS-57929	Issue ID:	SLXOS-57929
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00b
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Possible unexpected reload may be observed		
Condition:	User uses cmsh CLI mode to display BGP process internal data using "show ip bgp debug command"		

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-58576	Issue ID:	SLXOS-58798
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3c
Technology Group:	Management	Technology:	Other
Symptom:	https not started after registration		
Condition:	Device registeration. Not reproduced after last occurence.		
Workaround:	Reimport certificates and perform https restart via CLI - http server use-vrf mgmt-vrf shut and no http server use-vrf mgmt-vrf shut		

Parent Defect ID:	SLXOS-59050	Issue ID:	SLXOS-59050
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	Discrepancy between the configured interface status and displayed status		
Condition:	Running config shows that the interface is "no shutdown" but the interface state is shown as administratively down		

Parent Defect ID:	SLXOS-59440	Issue ID:	SLXOS-59440
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Dynamic BGP session won't come up		
Condition:	BGP session won't come up with MD5 password configuration		

Parent Defect ID:	SLXOS-59457	Issue ID:	SLXOS-59457
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.1
Technology Group:	Security	Technology:	RADIUS
Symptom:	Unexpected reload of SLX.		
Condition:	SLX may reload after many REST queries on behalf of RADIUS users when "peap-mschap" is configured as RADIUS protocol.		

Parent Defect ID:	SLXOS-60172	Issue ID:	SLXOS-60176
Severity:	S1 - Critical		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3ea
Technology Group:	Other	Technology:	Other
Symptom:	We may see flap of any random interface during the bootup time of the device. The device can be SLX 9740, SLX 9250, Extreme 8720, SLX 9150.		
Condition:	Sometimes Port flap is seen on a device during bootup.		

Parent Defect ID:	SLXOS-60308	Issue ID:	SLXOS-60308
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.1
Technology Group:	Other	Technology:	Other
Symptom:	On SLX 9740, traffic egressing out of a router port or an L3 port channel show incorrect statistics value.		
Condition:	L3 route traffic egressing out of a router port or an l3 port channel.		
Workaround:	1. Create a new VE and move the ve configuration that is exhibiting this extra counter display to the new VE. 2. Leave the previous VE in its place (it will still display all egressing traffic out of a router port or l3 po on it).		

Parent Defect ID:	SLXOS-60682	Issue ID:	SLXOS-60682
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.1
Technology Group:	Other	Technology:	Other
Symptom:	Interface Link flap is observed.		
Condition:	Speed is configured on the interface		

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

With static routes, the convergence times are in the order of 1 second. With only BGP routes and PIC enabled, it was upto around 730 msec.	

Parent Defect ID:	SLXOS-60298	Issue ID:	SLXOS-60757
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2a
Technology Group:	Other	Technology:	Other
Symptom:	One of the BFD session over MCT flaps on cluster node. There is no visible traffic loss as such because the other MCT peer takes the traffic over ICL and forwards it to CCEP DUT (from L3 GW).		
Condition:	On reload and system maintenance turn-off on an Extreme 8720 cluster node. System scale: 32 VRFs, at least 2 BFD over MCT, 2 HW BFD and 2 BFD over VxLAN session per VRF. (one IPv4 and one IPv6) (First 20 VRFs have 10+ BFD over MCT sessions towards CCEP DUTs, last 12 VRFs have 2 BFD over MCT sessions towards CCEP DUTs) All VE interfaces configured across all devices are dual stack. SW BFD sessions: 393 HW BFD sessions: 65 960 IPv4 routes, 960 IPv6 routes from L3 GW. 960 IPv4 routes, 960 IPv6 routes from CCEP DUTs. System-wide route scale: 3K IPv4 and 3K IPv6		
Workaround:	issue seen on Ve's attached to BDs. Remove the VE from BD and reconfigure.		

Parent Defect ID:	SLXOS-60534	Issue ID:	SLXOS-60767
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2a
Technology Group:	Layer 3 Routing/Network Layer	Technology:	ARP - Address Resolution Protocol
Symptom:	Traffic loss maybe seen for any particular Host.		
Condition:	1. Centralized Routing and Border Leaf has MCT cluster configured. 2. One of the MCT nodes goes for a reload.		

Parent Defect ID:	SLXOS-60895	Issue ID:	SLXOS-60895
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.1
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	The switch reloads sometime due to hslagtd deamon termination on illeagal memory access.		

Condition:	In a scaled up configuration and with a very high number of routes learnt with BGP protocol.

Parent Defect ID:	SLXOS-60448	Issue ID:	SLXOS-60912
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.2a
Technology Group:	Management	Technology:	Configuration Fundamentals
Symptom:	DHCP/BOOTP request is seen sending out from mgmt. interface event after disable DHCP.		
Condition:	BMC is configured as DHCP client.		
Recovery:	Manually disable DHCP option from BMC .		

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-61003	Issue ID:	SLXOS-61003
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.1
Technology Group:	IP Multicast	Technology:	IGMP - Internet Group Management Protocol
Symptom:	PING may take more time than expected.		
Condition:	1. There should be L2 loop in the topology for a given vlan. 2. IGMP snooping OR PIM-SM is enabled on this interface. 3. IGMP query should be either received OR Generated by the node.		
Workaround:	Please remove the L2 loop.		

Parent Defect ID:	SLXOS-60989	Issue ID:	SLXOS-61096
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2b
Technology Group:	Layer 3 Routing/Network Layer	Technology:	ARP - Address Resolution Protocol
Symptom:	Traffic loss maybe seen for ~4 seconds for few traffic streams		

Condition:	Enable and Disable maintenance mode in one of the BL node

Parent Defect ID:	SLXOS-61120	Issue ID:	SLXOS-61167
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3b
Technology Group:	Layer 2 Switching	Technology:	VLAN - Virtual LAN
Symptom:	Access to SLX management port is not working.		
Condition:	Ping packet drop is seen if it passes through VLAN before turning back on the mgmt. interface.		
Workaround:	Enable L3 VE interface on the VLAN		

Parent Defect ID:	SLXOS-61209	Issue ID:	SLXOS-61209
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.3
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	Broadcast, unknown unicast and Multicast traffic loss		
Condition:	Remote client interface shutdown followed by no cluster-client auto and cluster-client auto under local client interface		

Parent Defect ID:	SLXOS-60632	Issue ID:	SLXOS-61217
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2a
Technology Group:	Other	Technology:	Other
Symptom:	Tpvm status shows "Last Runtime error"		
Condition:	Upon upgrading from 20.3.2a to 20.3.2b		
Recovery:	tpvm stop and tpvm start		

Parent Defect ID:	SLXOS-60946	Issue ID:	SLXOS-61257
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2
Technology Group:	MPLS	Technology:	LDP - Label Distribution Protocol
Symptom:	Juniper rejects the LDP init messages sent by SLX when SLX is active, when the max pdu field is set to a value higher than default of 4096		
Condition:	SLX is active peer, and link PDU for l3 has been set to higher than 4096		

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-60951	Issue ID:	SLXOS-61576
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3e
Technology Group:	Layer 2 Switching	Technology:	LAG - Link Aggregation Group
Symptom:	MAC address of port-channel INTF changes when system is reloaded after performing un-config and then config of port channel interfaces.		
Condition:	MAC address of port channel interfaces change in below two cases; 1. Without reload - Port-channel interfaces are configured. Some of the port-channel interfaces are un-configured, and configured again without any specific sequence. 2. Port-channel Interfaces config and un-config is done without any particular sequence. Then config is saved and system is reloaded.		
Workaround:	For SLX 9540, SLX 9640 and SLX 9740, Some number of port-channel INTF can be created in the incremental order interface index. (say , port-channel 1, then port-channel 2, …, then port-channel 10). Now, config can be saved, and these port-channel are kind or reserved for future use. With these steps followed, MAC address of port-channel interfaces will not change with reload as well.		

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-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-61371	Issue ID:	SLXOS-62218
Severity:	S2 - Major		

Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2
Technology Group:	Other	Technology:	Other
Symptom:	Breakout port cli command on a port-macro group, can cause other ports in same group to flap sometimes.		
Condition:	Issue is seen when the breakout command is configured		

Parent Defect ID:	SLXOS-62256	Issue ID:	SLXOS-62256
Severity:	S1 - Critical		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.3
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	CCEP Port-channel flaps		
Condition:	With more than 96 Port-channels as MCT clients, and traffic running with COS priority of 6 or 7 - when one of the MCT node is reloaded, we see some of the CCEP Port-channels flapping on other MCT node.		

Parent Defect ID:	SLXOS-62220	Issue ID:	SLXOS-62276
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.2b
Technology Group:	IP Multicast	Technology:	IGMP - Internet Group Management Protocol
Symptom:	Switch reload and Link flaps on interface.		
Condition:	The switch receives igmp traffic from peer (with a large length value), on an L3 interface with no multicast configuration.		

Parent Defect ID:	SLXOS-62270	Issue ID:	SLXOS-62361
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2c
Technology Group:	Monitoring	Technology:	Port Mirroring
Symptom:	When VLAN is configured as source in monitor session , mirroring stops working after rebooting device		
Condition:	Configure flow based mirroring session with VLAN as source		
Workaround:	1)Delete Monitor configuration 2)Remove the ACL binding from the VLAN interface 3)Configure monitor session with VLAN as source 4)Bind L2 ACL on the VLAN interface.		

Parent Defect ID:	SLXOS-62440	Issue ID:	SLXOS-62454
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2d
Technology Group:	Monitoring	Technology:	Port Mirroring
Symptom:	Flow based mirroring keeps mirroring the packets, after the monitor session is deleted.		

Condition:	Flow based mirroring is configured with source as normal ethernet and L3 ACL is applied on the interface. Then monitor configuration is deleted.
Recovery:	Rebind the ACL on the mirror source interface.

Parent Defect ID:	SLXOS-62507	Issue ID:	SLXOS-62712
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2c
Technology Group:	Layer 2 Switching	Technology:	VXLAN - Virtual Extensible LAN
Symptom:	HSLagt daemon crash		
Condition:	HSLagt daemon termination is seen when VxLAN tunnel creation and deletion operations happen at very quick interval		

Parent Defect ID:	SLXOS-62754	Issue ID:	SLXOS-62754
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.4
Technology Group:	Security	Technology:	ACLs - Access Control Lists
Symptom:	On SLXOS 9740 only, BFD session flaps on an interface.		
Condition:	Egress ACL and BFD are configured on the specific interface.		

Workaround:	Use below permit rule for allowing the BFD packets
	        permit udp any any eq 3784
	        permit udp any any eq 4784		

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-62525	Issue ID:	SLXOS-62811
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2b
Technology Group:	Other	Technology:	Other
Symptom:	Traffic may be dropped when packets come in via VEoVPLS tunnel.		
Condition:	MAC learning events may fail when packets come in via VEoVPLS tunnel for MAC learning.		

Parent Defect ID:	SLXOS-62863	Issue ID:	SLXOS-62863
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:	1+ sec of traffic loss is observed during a border leaf reload.		
Condition:	Reloading one of SLX-9740 border leaf's in a MCT configuration		

Parent Defect ID:	SLXOS-60455	Issue ID:	SLXOS-62870
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Layer 2 Switching	Technology:	xSTP - Spanning Tree Protocols
Symptom:	RPVST flaps on SLX device		
Condition:	when root bridge change occurs without any user intervention		

Parent Defect ID:	SLXOS-62861	Issue ID:	SLXOS-62897
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3g
Technology Group:	Layer 3 Routing/Network Layer	Technology:	VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom:	SAG will become inactive after boot		
Condition:	When multiple VE interfaces are configured with same gateway-address, after reboot, the SAG will become inactive.		
Workaround:	Remove and reconfigure the anycast address		

Parent Defect ID:	SLXOS-62540	Issue ID:	SLXOS-62902
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	A cluster link port towards primary border leaf (BL2) does not come up after doing "shut"/"no-shutdown"		
Condition:	One of the cluster link ports towards primary border leaf (BL2) was shutdown. After about 30 seconds no shut was performed on the same port.		
Workaround:	Perform a "shutdown"/"no shutdown" on the link		

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-62308	Issue ID:	SLXOS-62979
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3g
Technology Group:	Management	Technology:	Other
Symptom:	Unexpected reload of SLX switch.		
Condition:	Unqualified QSFP inserted on SLX switch and causes the SLX node to reload.		

Parent Defect ID:	SLXOS-61558	Issue ID:	SLXOS-62992
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3d
Technology Group:	Management	Technology:	Other
Symptom:	Occasional TPVM CPU spike above 90% noticed for 1-2 sec.		
Condition:	Collecting EFA support-save on TPVM.		

Parent Defect ID:	SLXOS-62671	Issue ID:	SLXOS-62995
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.2b
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-62230	Issue ID:	SLXOS-62998
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.2c
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	On SLX 9640, BGP flaps are seen sometimes		
Condition:	In a scaled environment, and when high rate of control packets are processed on CPU, it can lead to lead loss of BGP packets.		

Parent Defect ID:	SLXOS-62722	Issue ID:	SLXOS-63001
Severity:	S2 - Major		

Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3c
Technology Group:	Traffic Management	Technology:	QoS - Quality of Service
Symptom:	Packets are egressing with DSCP value as 0 value, irrespective of incoming DSCP value.		
Condition:	In IP fabric environment, packets ingress at the SLX 9150 leaf switch with non-zero DSCP values and egress the SLX 9250 border leaf switch.		

Parent Defect ID:	SLXOS-62849	Issue ID:	SLXOS-63004
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3g
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	May experience 20-60 seconds of traffic loss.		
Condition:	On BGP re-convergence on network with below scale values, where 873k+ bgp ipv4 routes + 136k+ bgp ipv6 routes made to switch other path because of manual shut on working path.		

Parent Defect ID:	SLXOS-60943	Issue ID:	SLXOS-63018
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2g
Technology Group:	Monitoring	Technology:	sFlow
Symptom:	Sflow collector is configured for user vrf		
Condition:	Sflow sample reaching sflow collector via default vrf.		

Parent Defect ID:	SLXOS-63092	Issue ID:	SLXOS-63092
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:	Convergence times of upto 800 msec is seen when an interface from the Gateway towards the Border Leaf is shut down		
Condition:	There is a port channel between PE router and the Border leaf. The minimum-links is configured in the port channel. One of the physical interfaces in the port channel is shut and the minimum-link configuration brings down the port channel. The convergence time for the traffic from the border leaf towards the gateway is sometimes seen to be in the range of 500-800 msec.		
Workaround:	Using only BGP routes and configuring Prefix-Independent-Convergence can provide better convergence times than having static routes.		

Parent Defect ID:	SLXOS-62353	Issue ID:	SLXOS-63106
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2b
Technology Group:	Layer 2 Switching	Technology:	VXLAN - Virtual Extensible LAN
Symptom:	VRF traffic loss is greater than 1sec upon spine node reboot.		
Condition:	Upon spine reboot, few BFD sessions from compute nodes to border-leaf flap and see a traffic loss for 1-2 sec		

Parent Defect ID:	SLXOS-63115	Issue ID:	SLXOS-63115
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.4
Technology Group:	Security	Technology:	ACLs - Access Control Lists
Symptom:	On SLX 9740, Ingress ipv6 access-list counters do not increment in ipv6-optimised tcam profile		
Condition:	User has configured to use ipv6-optimised tcam profile and has configured counters for matching ipv6 access-list rules. Issued "clear counters" cli command.		

Parent Defect ID:	SLXOS-63118	Issue ID:	SLXOS-63118
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 Extreme 8520-48XT and Extreme 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 Extreme 8520-48XT or Extreme 8520-48Y devices.		
Workaround:	Remove and configure the breakout config or reload the device.		

Parent Defect ID:	SLXOS-63121	Issue ID:	SLXOS-63121
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.4
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	"show cluster track" command does not display correct interface status		
Condition:	Interface status is not displayed as 'down' under 'show cluster track' when port-channel becomes down due to the minimum-link criteria not being met.		

Parent Defect ID:	SLXOS-61254	Issue ID:	SLXOS-63124
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ca
Technology Group:	MPLS	Technology:	LDP - Label Distribution Protocol
Symptom:	Duplicate LDP Address Withdraw Message sent from LDP for each VC-Peer.		
Condition:	Issue is seen when we do "clear mac-address" under a bridge domain.		

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-63253	Issue ID:	SLXOS-63253
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.4
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	MCT Cluster peer-interface Port-channel flaps few times		
Condition:	On reloading one of the border leaf nodes in the MCT configuration, ICL port-channel flaps, while the reloaded node is coming online. This happens when more than 5000 BFD sessions are established over the VxLAN tunnel.		

Parent Defect ID:	SLXOS-63282	Issue ID:	SLXOS-63282
Severity:	S1 - Critical		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.4
Technology Group:	Monitoring	Technology:	Port Mirroring
Symptom:	On SLX 9740, flow based mirroring is not working for flow matching deny rules with the configured ACL		
Condition:	configure mirror action in deny rule , traffic matching deny rule are not mirrored.		

Parent Defect ID:	SLXOS-63289	Issue ID:	SLXOS-63289
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.4
Technology Group:	Monitoring	Technology:	sFlow
Symptom:	Flow based ERSPAN mirroring is not working in the ingress direction.		

Condition:	If the configured ERSPAN id is more than 255.
Workaround:	Configure ERSPAN is to be less than 25

Parent Defect ID:	SLXOS-63125	Issue ID:	SLXOS-63317
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3g
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	MAC address is not updated properly when there is MAC move between MCT peer nodes multiple times.		
Condition:	In the IP fabric, the MAC move happens between the MCT peer nodes.		

Defects Closed with Code Changes

The following software defects were closed in 20.3.4a with a code change as of **February 2022**:

Parent Defect ID:	SLXOS-62526	Issue ID:	SLXOS-62534
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.3
Technology Group:	Layer 2 Switching	**Technology:**	VXLAN - Virtual Extensible LAN
Symptom:	Multicast traffic from remote leaf loops back to the source node and multi-home client receives duplicate traffic		
Condition:	When multicast traffic sent over the VxLAN tunnel to EVPN Multi-homing node, the traffic is not dropped at the non-DF multi-homing node. The traffic is looped back to the source node and multi-homed clients receives duplicate traffic.		

Parent Defect ID:	SLXOS-63125	Issue ID:	SLXOS-63316
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3g
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	MAC address is not updated properly when there is MAC move between MCT peer nodes multiple times.		
Condition:	In the IP fabric, the MAC move happens between the MCT peer nodes.		

Parent Defect ID:	SLXOS-61209	Issue ID:	SLXOS-63964
Severity:	S2 - Major		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.3.3
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Broadcast, unknown unicast and Multicast traffic loss		
Condition:	Remote client interface shutdown followed by no cluster-client auto and cluster-client auto under local client interface		

Parent Defect ID:	SLXOS-61120	Issue ID:	SLXOS-63969
Severity:	S3 - Moderate		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.3b
Technology Group:	Layer 2 Switching	**Technology:**	VLAN - Virtual LAN
Symptom:	Access to SLX management port is not working.		
Condition:	Ping packet drop is seen if it passes through VLAN before turning back on the mgmt. interface.		

Parent Defect ID:	SLXOS-63974	Issue ID:	SLXOS-63977
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3g
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP flaps could be seen during high scale of BGP packets to CPU if it hits threshold rate-limit.		
Condition:	BGP flaps could be seen during high scale of BGP packets to CPU if it hits threshold rate-limit.		

Parent Defect ID:	SLXOS-63289	Issue ID:	SLXOS-63989
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.4
Technology Group:	Monitoring	Technology:	sFlow
Symptom:	Flow based ERSPAN mirroring is not working in the ingress direction.		
Condition:	If the configured ERSPAN id is more than 255.		

Parent Defect ID:	SLXOS-62256	Issue ID:	SLXOS-63995
Severity:	S1 - Critical		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.3
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	CCEP Port-channel flaps		
Condition:	With more than 96 Port-channels as MCT clients, and traffic running with COS priority of 6 or 7 - when one of the MCT node is reloaded, we see some of the CCEP Port-channels flapping on other MCT node.		

Parent Defect ID:	SLXOS-64022	Issue ID:	SLXOS-64022
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.4
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	MAC address is not updated properly when there is MAC move between MCT peer nodes multiple times.		
Condition:	In the IP fabric, the MAC move happens between the MCT peer nodes.		

Parent Defect ID:	SLXOS-63334	Issue ID:	SLXOS-64110
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00j
Technology Group:	MPLS	Technology:	MPLS VLL - Virtual Leased Line

Symptom:	User may experiences one way traffic over VLL usually during failover to bypass path.
Condition:	Rarely, hardware fails to delete transit cross-connect, and hardware continues to have stale Label in MPLS forwarding table.
Workaround:	Software state can be brought in sync by flapping all the MPLS enabled interfaces.

Parent Defect ID:	SLXOS-64141	Issue ID:	SLXOS-64142
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2d
Technology Group:	Management	Technology:	Other
Symptom:	In case, when file replay takes place during reboot of the switch and the configuration file contains CLI for Maintenance Mode - "enable-on-reboot", then log "RASLOG SMAN-1004" is generated twice. This indicates system is entering into maintenance Mode.		
Condition:	During system reload, when the configuration file replay takes place as in case of "full-install"		

Parent Defect ID:	SLXOS-63036	Issue ID:	SLXOS-64415
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2b
Technology Group:	Management	Technology:	SNMP - Simple Network Management Protocol
Symptom:	During bootup, SNMP traps for link status of VE and loopback interfaces are sent even when "snmp trap lnk-status disable" is configured for the interfaces		
Condition:	Issue is seen only during bootup for VE and loopback interfaces that are not shutdown.		

The following software defects were closed in 20.3.4 with a code change as of **December 2021**:

Parent Defect ID:	SLXOS-51569	Issue ID:	SLXOS-51843
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.1
Technology Group:	Monitoring	Technology:	OAM - Operations, Admin & Maintenance
Symptom:	On 9740-80, CFM session doesn't come-up when a bridge domain (BD) is configured with logical interfaces on breakout front panel ports (in the series 0/41-80). On BD deletion, the CFM sessions are up		
Condition:	Bridge domain (BD) is configured with logical interfaces on breakout front panel ports of the series 0/41-80.		

Parent Defect ID:	SLXOS-56079	Issue ID:	SLXOS-56079
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.2b
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	The switch might reload unexpectedly after a BGP process failure.		
Condition:	On SLX 9740, that is configured as a border leaf MCT node, and BGP is configured with BFD is enabled for all the BGP peering sessions. Sometimes on a reload of one of the border leaf switch, BFD sessions flap unexpectedly and can cause BGP session reset.		

Parent Defect ID:	SLXOS-58073	Issue ID:	SLXOS-58073
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3b
Technology Group:	Layer 2 Switching	Technology:	Other
Symptom:	VPLS traffic terminating towards TPVM insight interface is trapped to CPU instead of forwarding it out of switch.		
Condition:	TPVM insight interface is the AC interface(attachment circuit) for the VPLS terminating packets.		

Parent Defect ID:	SLXOS-58421	Issue ID:	SLXOS-58421
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3b_CVR
Technology Group:	Other	Technology:	Other
Symptom:	Console is not able to use, due to continuously getting the SMBus Message "i801_smbus 0000:00:1f.4: SMBus is busy".		
Condition:	After reload the device. the console is getting continuously "i801_smbus 0000:00:1f.4": SMBus Message.		

Parent Defect ID:	SLXOS-59936	Issue ID:	SLXOS-59936
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2
Technology Group:	Monitoring	Technology:	Port Mirroring
Symptom:	On SLX-9740, ACL based Egress mirroring does not mirror traffic from source port in the transmit direction.		
Condition:	Monitor session is created with "tx" direction and flow-based. After Egress ACL is applied with "mirror" action on the source port, the transmit direction traffic is not mirrored.		

Parent Defect ID:	SLXOS-60558	Issue ID:	SLXOS-60963
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3d

Technology Group:	Management	Technology:	CLI - Command Line Interface
Symptom:	"ip ospf area" configuration missing on some interfaces associated with OSPF instance enabled on non-default VRF		
Condition:	upgrade from 20.1.2x to 20.2.3x code		

Parent Defect ID:	SLXOS-61077	Issue ID:	SLXOS-61094
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2b
Technology Group:	Layer 2 Switching	Technology:	VXLAN - Virtual Extensible LAN
Symptom:	L2agt daemon terminates on EVPN-MH Leaf node		
Condition:	Sometimes l2agt daemon reload may be seen when the uplink port is flapped a few times on a EVPN multihoming node		

Parent Defect ID:	SLXOS-61014	Issue ID:	SLXOS-61273
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2a
Technology Group:	Management	Technology:	SNMP - Simple Network Management Protocol
Symptom:	BGP ipv4 traps will not be sent from SLX.		
Condition:	When bgp ipv4 session is established and if the bgp session is made up or down, default bgp ipv4 traps meant for session up/down for ipv4 peers will not be sent from slx.		

Parent Defect ID:	SLXOS-61332	Issue ID:	SLXOS-61332
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.3
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	The ICL port link is flapping for some time, and traffic convergence takes more than 10 sec.		
Condition:	Reloading the CCEP device.		

Parent Defect ID:	SLXOS-61339	Issue ID:	SLXOS-61409
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2a
Technology Group:	Layer 2 Switching	Technology:	Other
Symptom:	When QOS profile is set as "lossless" and cee default exists, the interfaces which are in LLDP UP state sends DOT1-TLV also. This is not exepcted.		
Condition:	When QOS profile is set as "lossless" and cee default exists.		

Parent Defect ID:	SLXOS-61523	Issue ID:	SLXOS-61523
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.3
Technology Group:	Management	Technology:	Other
Symptom:	Bootup can sometimes fail on Extreme 8720/8520 and sometimes the management link fails to come up.		
Condition:	On switch bootup.		

Parent Defect ID:	SLXOS-61515	Issue ID:	SLXOS-61557
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3g
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	After mac-move the MAC is still displayed as Dynamic-CCL		
Condition:	After a mac-move from remote leaf and then between a MCT peers, the MAC is displayed as Dynamic-CCL instead of CCR		

Parent Defect ID:	SLXOS-61573	Issue ID:	SLXOS-61573
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.3
Technology Group:	Layer 3 Routing/Network Layer	Technology:	ARP - Address Resolution Protocol
Symptom:	Ipv6 Neighbor is not updated with correct MAC address		
Condition:	In IP fabric scenario, virtual machine or the host moves from remote leaf to the local leaf with different mac.		

Parent Defect ID:	SLXOS-61937	Issue ID:	SLXOS-62241
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2b
Technology Group:	Monitoring	Technology:	Hardware Monitoring
Symptom:	IPv4 Flow based mirroring with VLAN as source does not work.		
Condition:	Configure IPv4 flow based mirroring with source as VLAN and then reload the Device.		

Parent Defect ID:	SLXOS-62268	Issue ID:	SLXOS-62268
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.3
Technology Group:	Other	Technology:	Other
Symptom:	On reload of the switch, sometimes the 100gig SR4 optic link may not come up.		
Condition:	On switch bootup.		

Parent Defect ID:	SLXOS-62311	Issue ID:	SLXOS-62323
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3e
Technology Group:	Management	Technology:	Software Installation & Upgrade
Symptom:	Firmware download and firmware download sanity NETCONF requests are failing.		
Condition:	Firmware host password has a special character '&' char in the password		

Parent Defect ID:	SLXOS-62111	Issue ID:	SLXOS-62364
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2b
Technology Group:	Management	Technology:	CLI - Command Line Interface
Symptom:	CLI command "show running-config snmp-server host <ip-address>" displays error for some specific host IP addresses.		
Condition:	When multiple host entries are configured, and if the numerically sorted order and lexicographically sorted order of host IP addresses are different.		

Parent Defect ID:	SLXOS-62334	Issue ID:	SLXOS-62386
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3g
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP session may get impacted due to internal BGP rate-limit in transient router on 9540/9640 devices.		
Condition:	BGP session may get impacted when high rate of BGP traffic is send via transient router 9540/9640.		

Parent Defect ID:	SLXOS-62526	Issue ID:	SLXOS-62526
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.3
Technology Group:	Layer 2 Switching	Technology:	VXLAN - Virtual Extensible LAN
Symptom:	Multicast traffic from remote leaf loops back to the source node and multi-home client receives duplicate traffic		
Condition:	When multicast traffic sent over the VxLAN tunnel to EVPN Multi-homing node, the traffic is not dropped at the non-DF multi-homing node. The traffic is looped back to the source node and multi-homed clients receives duplicate traffic.		

Parent Defect ID:	SLXOS-61207	Issue ID:	SLXOS-62595
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.2b
Technology Group:	Monitoring	Technology:	Syslog
Symptom:	The literal "BOM" is replaced with hexadecimal values "EF.BB.BF" as per RFC.		
Condition:	when the format "RFC-5424" is enabled for syslog-ng.		

Parent Defect ID:	SLXOS-62457	Issue ID:	SLXOS-62623
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2c
Technology Group:	Security	Technology:	ACLs - Access Control Lists
Symptom:	After switch reboot, user was not able to access the switch using ssh using management IP.		
Condition:	Upon switch reboot		

Parent Defect ID:	SLXOS-63022	Issue ID:	SLXOS-63055
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 flaps once in broader leaf .		
Condition:	Spine node is reloaded when SLX 9150/SLX9250/ Extreme 8720 / Extreme 8520 acts as a border leaf in Centralized IP fabric.		

Defects Closed without Code Changes

The following software defect was closed in 20.3.4a without code change as of **February 2022**.

Parent Defect ID:	SLXOS-62447	Issue ID:	SLXOS-62474
Reason Code:	Feature/Function Not Supported	Severity:	S2 - Major
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00j
Technology Group:	MPLS	Technology:	LDP - Label Distribution Protocol
Symptom:	Flow Label sync is not done after HA failover in SLX 9850		
Condition:	HA is not supported in 20.x release.		

Parent Defect ID:	SLXOS-64007	Issue ID:	SLXOS-64080
Reason Code:	Already Implemented	Severity:	S2 - Major

Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2b
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	Port-channel interfaces stay down		
Condition:	On a 8720 MCT, when one of the MCT leaf reloads, port-channel interfaces stay down on one end, as the LACP packets are not being received.		

The following software defect was closed in 20.3.4 without code change as of **December 2021**.

Parent Defect ID:	SLXOS-45474	Issue ID:	SLXOS-45474
Reason Code:	Will Not Fix	Severity:	S2 - Major
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Traffic Management	Technology:	Traffic Queueing and Scheduling
Symptom:	In some cases mcast drops are observed based on pkt size and number of replications.		
Condition:	Mcast drops will be observed when mcast traffic is sent with more replications along with unicast traffic.		
Workaround:	There is no traffic loss observed with following below numbers. 1 G link Egress (with 40% Unicast traffic) 48 OIFs (6 S,G's and 8 vlans (hosts) per S,G) without seeing loss. 10 G link Ingress/Egress (with 40% Unicast traffic) 54 vlan with 6 (S,G) Multicast groups per vlan 100G link Ingress/10G Egress (with 40% Unicast traffic) 42 vlan with 6 (S,G) Multicast groups per vlan		

Parent Defect ID:	SLXOS-51407	Issue ID:	SLXOS-51407
Reason Code:	Design Limitation	Severity:	S3 - Moderate
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.1
Technology Group:	MPLS	Technology:	MPLS VPLS - Virtual Private LAN Services
Symptom:	VPLS statistics will not be accounted in underlying MPLS tunnel statistics		
Condition:	When both Bridge-domain statistics and MPLS ingress-tunnel-account statistics are enabled, Traffic egress in VPLS PW under the bridge-domain will not be accounted in underlying MPLS tunnel statistics in which the VPLS PW is established.		

Parent Defect ID:	SLXOS-55185	Issue ID:	SLXOS-55185
Reason Code:	Working as Designed	Severity:	S3 - Moderate
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2c

Technology Group:	Monitoring	Technology:	RAS - Reliability, Availability, and Serviceability
Symptom:	Few RAS logs are missing		
Condition:	After reaching the higher value of sequence number in RAS logs. EX: [NSM-1020], 5610250(sequence number), DCE, INFO, SLX-R1, interface Ethernet 0/x is administratively down.		

Parent Defect ID:	SLXOS-55372	Issue ID:	SLXOS-55372
Reason Code:	Design Limitation	Severity:	S2 - Major
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.2a
Technology Group:	MPLS	Technology:	LDP - Label Distribution Protocol
Symptom:	"show mpls statistics ldp" command statistics will not increment on transit nodes for SLX9740 for transient session accounting.		
Condition:	MPLS XC statistics will not increment on transit nodes for SLX9740 if following transit-session-accounting config is enabled. -- router mpls policy transit-session-accounting		

Parent Defect ID:	SLXOS-57246	Issue ID:	SLXOS-57428
Reason Code:	Design Limitation	Severity:	S2 - Major
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3b
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BFD - BiDirectional Forwarding Detection
Symptom:	BFD session establishment will be delayed by 75-120 seconds in SLX 9740.		
Condition:	After MCT/ICL link comes UP .		

Parent Defect ID:	SLXOS-59114	Issue ID:	SLXOS-59114
Reason Code:	Not Reproducible	Severity:	S2 - Major
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BFD - BiDirectional Forwarding Detection
Symptom:	BFD sessions may flap in SLX-9740.		
Condition:	On shutting down the member interface of the port-channel .		

Parent Defect ID:	SLXOS-60738	Issue ID:	SLXOS-60796
Reason Code:	Already Implemented	Severity:	S3 - Moderate
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2a

Technology Group:	Security	Technology:	AAA - Authentication, Authorization, and Accounting
Symptom:	Removing secure LDAP server(configured for TPVM) changes secure LDAP server to non-secure LDAP server.		
Condition:	1. Configure LDAP server with "secure" parameter 2. Remove the LDAP server entry		

Parent Defect ID:	SLXOS-62156	Issue ID:	SLXOS-62156
Reason Code:	Design Limitation	Severity:	S2 - Major
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.3
Technology Group:	Layer 2 Switching	Technology:	Other
Symptom:	In EVPN Multi-homing environment, on repeated multiple triggers like node reload and clear-mac-dynamic operations, few macs may stuck as ES-Remote on one of the MH-node, and the same mac may be missing on peer MH-node.		
Condition:	Repeated execution of multiple triggers like MH node reload, ESI client port flag, and clear-mac-dynamic operations.		
Workaround:	ESI client port flap should clear macs on the interface.		

Parent Defect ID:	SLXOS-62153	Issue ID:	SLXOS-62192
Reason Code:	Cannot Fix	Severity:	S3 - Moderate
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2b
Technology Group:	Security	Technology:	User Accounts & Passwords
Symptom:	TPVM login is not working after upgrade from 20.3.2b to a later release		
Condition:	This happens when the TPVM login password string has a "\" character.		
Recovery:	Stop TPVM and reconfigure same password after upgrade		