

August 2020



Extreme SLX-OS 20.2.1a Release Notes

Supporting ExtremeRouting and ExtremeSwitching
SLX 9640, SLX 9540, SLX 9250, and SLX 9150

© 2020, Extreme Networks, Inc. All Rights Reserved.

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners. For additional information on Extreme Networks Trademarks, see www.extremenetworks.com/company/legal/trademarks/. The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Contents

Extreme SLX-OS 20.2.1a Release Notes	1
Contents	3
Document History	3
Preface	4
New Software Features	6
Behavior Changes	7
Commands	8
Hardware Support	9
Software Download and Upgrade	10
Limitations and Restrictions	12
Open Defects	12
Defects Closed with Code Changes	27
Defects Closed without Code Changes	41

Document History

Version	Summary of changes	Publication date
1.0	Initial version for 20.2.1a	August 2020

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 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.

New Software Features

The following key software features are added in the SLX-OS 20.2.1a release.

Feature Name	Supported SLX Platforms	Description
IP Fabric Multicast	All platforms	<p>IP Multicast Fabric is introduced to replace the current mechanism for sending BUM and customer multicast traffic in a fabric (ingress replication) with multicast trees.</p> <p>Ingress replication may send a packet over a link from leaf to spine, once for each ultimate destination (sent once over each unicast VxLAN tunnel).</p> <p>The overall mechanism uses Multicast Distribution Trees to deliver traffic effectively while minimizing packet replication in the fabric.</p>
Control Plane Policing	All platforms	Control Plane Policing (COPP) helps regulate the rate of control packets to the local processor at a predefined rate for control packets. The rate could be complete discard of packets.
MCT Multi-LIF (logical interface) support	All platforms	Traffic destined to host behind CCEP gets distributed to the corresponding LIF depending on the bridge domain ID, inner VLAN and outer VLAN. Earlier all the traffic was going on the first CCEP LIF, when more than one CCEP LIF from same client interface was configured on the Bridge domain.
DHCPv4 snooping	All platforms	DHCPv4 snooping mitigates the security risks posed by denial-of-service from rogue DHCP servers, which disrupt networks as they compete with legitimate DHCP servers that configure hosts on the network for communication.
Dynamic ARP inspection	All platforms	Dynamic ARP inspection feature ensures that only valid ARP requests and responses are relayed
IP source guard	All platforms	IP Source Guard feature provides source IP address filtering on a Layer 2 port. It prevents a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address.

Feature Name	Supported SLX Platforms	Description
IPv4 ICMP router discovery protocol	All platforms	Routers use the IPv4 ICMP Router Discovery Protocol to announce their presence to other systems in the subnet. Hosts use the protocol to dynamically discover IPv4 routers in the same subnet.
TLS server certificates and private keys with no trust point	All platforms	You can import a TLS server certificate and private key (in PKCS12 format) to an SLX device (with no trust point) and establish a secure connection.
OAuth2 authentication	All platforms	Support for OAuth2 authentication allows the processing of authentication requests from north-bound interfaces using an OAuth2 token.
Rebooting into maintenance mode	<p>'enable' parameter on all platforms</p> <p>'enable-on-reboot' parameter only on SLX 9250</p>	<p>The config-system-maintenance command provides two methods for you to access maintenance mode.</p> <ul style="list-style-type: none"> • Use the enable parameter, which puts the device into maintenance mode after a specified convergence time. • Use the enable-on-reboot parameter to enter maintenance mode upon reboot.
Support source-interface and VRF for all management functions	All platforms	Source IP option and a user defined VRF can be used now, apart from the earlier supported Mgmt-VRF.

Behavior Changes

System Feature	Behavior Change
Auto-persistence configuration	All configurations are automatically preserved across reboot. The copy running-config startup-config command is used to take a backup of the configuration. This backup configuration is used only if the running-config 'database' becomes unusable for any reason.
Static route with BFD	If BFD is configured for static route next hop, the corresponding prefixes are not installed in the routing table unless the BFD session comes up.
no logging CLI	Arguments are compulsory.
tpvm deploy CLI	The "mgmt/insight" options are mandatory.

Commands

New commands

- ip access-list extended; match icmp-type and icmp-code
- ip source-guard enable
- show ip source-guard binding entries [interface | all]
- ip irdp
- optimized-replication
- underlay-mdt-default-group
- underlay-mdt-group
- show ip pim mdt [detail]
- show ip pim mdt [group GROUP-IP-ADDRESS]
- clear ip pim mdt [group GROUP-IP-ADDRESS]
- crypto ca import-pkcs type pkcs12 cert-type https
- tpvm config dns add dns-server <IPv4 address> <IPv4 address> domain-name <string>
- tpvm config dns remove
- show tpvm config dns
- tpvm config ntp add server <IP address>
- tpvm config ntp remove server <IP address>
- tpvm config ntp default
- show tpvm config ntp
- tpvm config ldap add/remove host <ip address> port <port> secure
- tpvm config ldap add/remove basedn <domain name> rootdn <domain name> rootpw <password>
- tpvm config ldap ca-cert import protocol <SCP> host <hostname> user <username> password <password> directory <dirname> file <filename>
- show tpvm config ldap

Modified commands

- show bfd
- show bfd neighbors details
- storm-control ingress
- show ip pim mcache
- show ip dhcp snooping vlan
- show ip dhcp snooping brief
- copy running-config <scp|sftp>://<username>@<destination ip>//<file name> use-vrf <VRF name> source-ip <IPv4/IPv6 address>
- copy <scp|sftp>://<username>@<destination ip>//<file name> running-config use-vrf <VRF name> source-ip <IPv4/IPv6 address>
- copy support scp source-ip
- logging syslog-server <ip address> use-vrf <vrf name> [udp-port] <port number>
- password-attributes
- crypto import

- crypto ca authenticate
- crypto ca import
- aaa authentication login
- pki oosp
- ldap-server host
- logging syslog-server

Removed commands

- logging syslog-client (use **logging syslog-server** instead)

Hardware Support

Supported devices and software license

Supported devices	Description
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

Supported optics and cables

For a complete list of all supported optics, see **Extreme Optics** at optics.extremenetworks.com.

Software Download and Upgrade

For more information about the various methods of upgrading to SLX-OS 20.2.1a, see the *Extreme SLX-OS Software Upgrade Guide*.

Image files

Download the following images from www.extremenetworks.com.

Image file name	Description
slxos20.2.1a.tar.gz	SLX-OS 20.2.1a software
slxos20.2.1a_mibs.tar.gz	SLX-OS 20.2.a MIBS
slxos20.2.1a.md5	SLX-OS 20.2.1a md5 checksum
slxos20.2.1a-digests.tar.gz	SLX-OS 20.2.1a sha checksum
slxos-20.2.1a-releasenotes.pdf	Release Notes

SLX 9540 and SLX 9640

To	20.2.1a
From	
18r.2.00bc	For SLX 9540: 1. First move to 20.1.1 using fullinstall. 2. Then move to 20.2.1a using fullinstall. For SLX 9640: Use fullinstall.
20.1.1	For SLX 9540: Use fullinstall. For other platforms: Use the normal FWDL.
20.2.1a	N/A

Notes:

- From the 18r.1.00x and 18r.2.00a patches and earlier, upgrade to 18r.2.00bx and then to 20.2.1a, 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 baremetal device, use the fullinstall option to migrate between the SLX-OS 20.2.1a and SLX-OS 20.1.1 releases.
- Downgrade from 20.2.1a to 20.1.1 requires the fullinstall option for all platforms due to a change in glibc.

SLX 9150 and SLX 9250

To	20.2.1a
From	
20.1.1	Use the normal FWDL
20.2.1a	N/A

Limitations and Restrictions

FEC mode configuration

- Default FEC mode on 100G ports for all platforms is Disabled.
- Default FEC mode on 25G ports for the SLX 9250-32C is Enabled (FC-FEC).
- Default FEC mode on 25G ports for all other platforms is Disabled.
- Links will not come up if there is an FEC mismatch between local and peer ends (either FEC has to be Enabled or Disabled in both ends).
- The **no fec mode** and **fec mode auto-negotiation** configuration commands are not supported.
- The 100G link between SLX 9150-48Y and SLX 9150-48XT comes up ONLY with explicit FEC configuration of "Disabled-Disabled" (OR) RS-FEC and RS-FEC on both sides.

Other

- 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.

Open Defects

Parent Defect ID:	SLXOS-37598	Issue ID:	SLXOS-37598
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00
Technology Group:	Monitoring	Technology:	Hardware Monitoring
Symptom:	Unexpected BFD session flap may be experienced with 1 million IPv6 BGP routes on SLX 9640/SLX9540		
Condition:	Bringing down an interface cause other BFD session flap in scaled IPv6 Scenario		

Parent Defect ID:	SLXOS-41353	Issue ID:	SLXOS-41353
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Security	Technology:	TACACS & TACACS+
Symptom:	User role is not getting updated in audit logs for external users (Tacacs+/Radius/LDAP)		
Condition:	When login happens through NetConf and external (Tacacs+/Radius/LDAP) authentication has been configured		

Parent Defect ID:	SLXOS-42488	Issue ID:	SLXOS-42488
Severity:	S3 - Medium		
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 doesn't 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-42558	Issue ID:	SLXOS-42558
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Security	Technology:	AAA - Authentication, Authorization, and Accounting
Symptom:	Not able to login via telnet with radius credentials		
Condition:	On deleting vrf under ethernet interface which is configured as source-interface for Radius		
Workaround:	workaround is to remove/detach source interface config for RADIUS, Then, do the VRF related changes for the source interface and then re-attach it back to RADIUS.		

Parent Defect ID:	SLXOS-43141	Issue ID:	SLXOS-43141
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00a
Technology Group:	Other	Technology:	Other
Symptom:	TRCE-5006 RASLOG has been observed		
Condition:	During the reload		

Parent Defect ID:	SLXOS-43341	Issue ID:	SLXOS-43341
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Management	Technology:	Other
Symptom:	Rollback operation fails.		
Condition:	Rollback checkpoint has 'standard' ACL and running-config has 'extended' ACL (vice versa) with same name and applied to the same interfaces.		
Workaround:	Avoid using same name for standard and extended ACLs		

Parent Defect ID:	SLXOS-43354	Issue ID:	SLXOS-43354
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Other	Technology:	Other
Symptom:	show running-config route-map <route-map-name> on some specific route-map does give any output		
Condition:	issue is observed during highly scaled scale route-map configurations		
Workaround:	use 1. show running-config 2. show running-config route-map 3. show running-config route-map include <route-map-name>		

Parent Defect ID:	SLXOS-43409	Issue ID:	SLXOS-43409
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Security	Technology:	AAA - Authentication, Authorization, and Accounting
Symptom:	Certain REST operational queries may fail with "500 Internal Server Error" when TACACS+ command authorization is enabled.		
Condition:	This issue occurs when 'aaa authorization command tacacs+' is configured.		
Workaround:	Remove 'aaa authorization command tacacs+' configuration or use alternative methods like CLI/NETCONF (instead of REST) to retrieve the operational data that is having this issue.		

Parent Defect ID:	SLXOS-43527	Issue ID:	SLXOS-43527
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00
Technology Group:	Management	Technology:	CLI - Command Line Interface
Symptom:	"nssa no-redistribution" and "nssa translator-always" commands does not show up		
Condition:	When trying to configure "nssa no-redistribution" and "nssa translator-always"		

Parent Defect ID:	SLXOS-45474	Issue ID:	SLXOS-45474
Severity:	S2 - High		
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.		

Parent Defect ID:	SLXOS-45474	Issue ID:	SLXOS-45474
Workaround:	<p>There is no traffic loss observed with following below numbers.</p> <p>1 G link Egress (with 40% Unicast traffic) 48 OIFs (6 S,G's and 8 vlans (hosts) per S,G) without seeing loss.</p> <p>10 G link Ingress/Egress (with 40% Unicast traffic) 54 vlan with 6 (S,G) Multicast groups per vlan</p> <p>100G link Ingress/10G Egress (with 40% Unicast traffic) 42 vlan with 6 (S,G) Multicast groups per vlan</p>		

Parent Defect ID:	SLXOS-45634	Issue ID:	SLXOS-45634
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Management	Technology:	Other
Symptom:	In rare scenario, While doing (/restconf/data) datastore query for few REST commands , unwanted output is observed on console		
Condition:	issue is observed while executing top level REST query		

Parent Defect ID:	SLXOS-45991	Issue ID:	SLXOS-45991
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00a
Technology Group:	Layer 2 Switching	Technology:	xSTP - Spanning Tree Protocols
Symptom:	User will observe that STP BPDUs are getting flooded on VPLS Bridge domain like normal multicast traffic, even though user has enabled 'bpdu drop' feature using the CLI		
Condition:	'bpdu drop' configured on VPLS BD is not behaving as expected , where the BPDU should be dropped instead of flooding when 'bpdu drop ' is enabled on the VPLS bridge domain.		

Parent Defect ID:	SLXOS-46252	Issue ID:	SLXOS-46252
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	MPLS	Technology:	MPLS VPLS - Virtual Private LAN Services
Symptom:	PW preferential Status may not display the correct role and match with DF role of bridge-domain in MCT VPLS scenario on SLX9540 platform		
Condition:	This may occur when there are many flaps for VPLS and MCT		
Workaround:	Remove and re-add configuration of bridge-domain or Remove and re-add bridge-domain from MCT member bridge-domain configuration		

Parent Defect ID:	SLXOS-46276	Issue ID:	SLXOS-46276
Severity:	S2 - High		
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 - Medium		
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-46939	Issue ID:	SLXOS-46939
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	IP Multicast	Technology:	PIM - Protocol- Independent Multicast
Symptom:	PIMoMCT : traffic loss may be seen for some of the Outgoing interfaces (OIF's) when 126 pim OIFs are present		
Condition:	issue is seen with scaled deployment of PIM over MCT : traffic loss may be seen for some of the OIFs when 126 pim OIFs are present		
Workaround:	configure less than 126 outgoing interfaces while using PIM Multicast with MCT		

Parent Defect ID:	SLXOS-47226	Issue ID:	SLXOS-47226
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	Technology:	VLAN - Virtual LAN
Symptom:	A message "port_vlan_duplication_detected" may be seen on console session.		
Condition:	User was able to assign same VLAN to Logical-interface, and it's main interface.		

Parent Defect ID:	SLXOS-47395	Issue ID:	SLXOS-47395
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	Technology:	LAG - Link Aggregation Group
Symptom:	After a full install upgrade if a partner link speed mismatch is detected Port-channel member links will flap a couple of times and then transition to administrate down state		
Condition:	SLX LAG interface bundled with copper ports goes admin-down when the link detects a speed mismatch (auto negotiation enabled) as part of "auto err-disable" feature on the remote VDX box.		
Workaround:	perform "no shutdown" on LAG member to bring up online(assuming speed matches with partner link).		

Parent Defect ID:	SLXOS-47423	Issue ID:	SLXOS-47423
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Traffic Management	Technology:	Rate Limiting and Shaping
Symptom:	DHCP traffic rate limiting is not working in SLX9150/9250 when DHCP snooping and ACL RL is applied on the same hierarchical interface.		
Condition:	Issue seen when DHCP snooping and ACL RL is applied on the same hierarchical interface.		

Parent Defect ID:	SLXOS-47472	Issue ID:	SLXOS-47472
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	Technology:	VLAN - Virtual LAN
Symptom:	Mac addresses age out earlier than the configured mac aging time		
Condition:	Mac address ages out 20% earlier than the configured age time in the system.		
Workaround:	Configuring mac address aging time more than 20% of planned mac address age out time adjust the deviation of early aging cycle.		

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

Parent Defect ID:	SLXOS-48120	Issue ID:	SLXOS-48120
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2
Technology Group:	Layer 3 Routing/Network Layer	Technology:	Other
Symptom:	SLX9150/SLX9250 goes for unexpected reload after receiving huge routes beyond/w capabilities IPv4 or IPv6 unicast routes from routing protocol (like OSPF/BGP) neighbors with multicast routing enabled		
Condition:	Multicast Routing (PIM) enabled on the switch and system receives more than 128K IPv4 unicast routes or 32K IPv6 unicast routes or collectively (Multi-D) more than 64K IPv4 unicast routes and 16K IPv6 unicast routes.		
Workaround:	IPv4 and IPv6 route scale must be maintained as per the scale document route limits		

Parent Defect ID:	SLXOS-48195	Issue ID:	SLXOS-48195
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00
Technology Group:	Layer 2 Switching	Technology:	VLAN - Virtual LAN
Symptom:	VLAN 4091 to 4095 are reserved. so the configuration was not accepted.		
Condition:	Don't configure on VLAN 4091 to 4095		

Parent Defect ID:	SLXOS-48758	Issue ID:	SLXOS-48758
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00a
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	IP Load Sharing or BGP Multipathing not being performed.		
Condition:	BGP is configured with multiple ECMP paths.		

Parent Defect ID:	SLXOS-48868	Issue ID:	SLXOS-48868
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2
Technology Group:	Management	Technology:	CLI - Command Line Interface
Symptom:	Auditlog doesn't capture configuration failures.		
Condition:	When multiple VLANs are being configured using vlan-range command, the auditlog may not log the errors, if there are any failures for individual vlans.		

Parent Defect ID:	SLXOS-49371	Issue ID:	SLXOS-49371
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2
Technology Group:	Network Automation and Orchestration	Technology:	NETCONF - Network Configuration Protocol
Symptom:	In scaled scenario, querying for RPC get-ip-interface using NETCONF/REST returns error.		
Condition:	User will observe this behavior when more than 5000 VE/SVI interfaces are configured on the device.		

Parent Defect ID:	SLXOS-49399	Issue ID:	SLXOS-49399
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Monitoring	Technology:	OAM - Operations, Admin & Maintenance
Symptom:	"show media" command doesn't display optical encoding string for particular optics as per the IEEE standard		
Condition:	When QSFP28 optic has encoding index "5"		

Parent Defect ID:	SLXOS-49610	Issue ID:	SLXOS-49610
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2
Technology Group:	Layer 3 Routing/Network Layer	Technology:	DHCP - Dynamic Host Configuration Protocol
Symptom:	When a checkpoint is taken with "ipv6 dhcp relay source interface" configuration, and applied back at a later point of time, the "ipv6 dhcp relay source-interface" config throws an error.		
Condition:	Issue is seen when a checkpoint is taken and applied on the "dhcp relay source interface configuration". Not observed with manual addition/removal of the configuration.		
Workaround:	Apply/delete the dhcp relay source interface configuration manually.		

Parent Defect ID:	SLXOS-49668	Issue ID:	SLXOS-49668
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ca
Technology Group:	Monitoring	Technology:	RAS - Reliability, Availability, and Serviceability
Symptom:	show audit log displays single log		
Condition:	Rare scenario, when audit log file got corrupted		

Parent Defect ID:	SLXOS-49674	Issue ID:	SLXOS-49674
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00b
Technology Group:	Security	Technology:	ACLs - Access Control Lists
Symptom:	Invalid warning logs come on the console " Key type(Destination Port) is not supported".		
Condition:	If Ipv4 ACL rule has same destination and source port, warning log comes on console.		

Parent Defect ID:	SLXOS-50020	Issue ID:	SLXOS-50020
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	Some of the ND entries learned from normal leaf may have MACs unresolved on border leaf switches in Centralized routing deployments.		
Condition:	When a MAC is moved from EVPN to local MCT node, the mac is stuck as CCR on MCT and the mac didn't get advertised to BGP.		

Parent Defect ID:	SLXOS-50117	Issue ID:	SLXOS-50117
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2
Technology Group:	Layer 3 Routing/Network Layer	Technology:	OSPF - IPv4 Open Shortest Path First
Symptom:	When multiple summary addresses with same prefix but different subnets are configured and unconfigured, one summary route is not removed in the system		
Condition:	Multiple summary addresses with same prefix but different subnets should be configured. Check the aggregated summary routes. Then unconfigure all the summary routes, and user will observe One aggregate route is still present in the system.		

Parent Defect ID:	SLXOS-50130	Issue ID:	SLXOS-50130
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2
Technology Group:	Management	Technology:	Other
Symptom:	On rare occasion, "WaveManagementServer::connect : Error" trace message displayed on switch's console session during device bring up. No functionality impact observed because of this trace message as system retries, connect and recover internally.		
Condition:	The error message may appear on console during switch boot up.		

Parent Defect ID:	SLXOS-50693	Issue ID:	SLXOS-50693
Severity:	S2 - High		
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-48753	Issue ID:	SLXOS-50786
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2
Technology Group:	Layer 3 Routing/Network Layer	Technology:	Other
Symptom:	On SLX 9540/ SLX 9640, In scaled multicast deployments, traffic loss might be observed due to invalid next-hop entry in hardware after repeated interface disable/enable operation.		
Condition:	When disabling/enabling VE interfaces multiple times using a script over night with full Internet routes (~800K routes) and multicast routes (4000+ multicast cache entries) in the system.		
Workaround:	Disable and enable the interface with a delay of 10 sec for medium scale environment.		

Parent Defect ID:	SLXOS-50793	Issue ID:	SLXOS-50793
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Monitoring	Technology:	OAM - Operations, Admin & Maintenance
Symptom:	"show media" may display encoding string that doesn't comply with the IEEE standard for certain optics.		
Condition:	When 100G-LR4 QSFP28 optic has encoding value 5 Ex: show media interface ethernet x/y Encoding 5 IEEE 802.3ab		

Parent Defect ID:	SLXOS-50873	Issue ID:	SLXOS-50873
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2a
Technology Group:	Security	Technology:	AAA - Authentication, Authorization, and Accounting
Symptom:	Incorrect role name is displayed in "show users" command output and audit logs.		
Condition:	Issue is seen when, 1. OAuth2 mode of authentication is configured on SLX device. 2. SLX device is accessed by NETCONF clients.		

Parent Defect ID:	SLXOS-50980	Issue ID:	SLXOS-50980
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2a
Technology Group:	Security	Technology:	HTTP/HTTPS
Symptom:	Secure access to SLX device through Hypertext Transfer Protocol Secure (HTTPS) service generates duplicate Transport Layer Security(TLS) audit logs on SLX device.		
Condition:	<p>Issue is seen when,</p> <ol style="list-style-type: none"> 1. HTTPS is enabled on SLX device. 2. SLX device is accessed by HTTPS clients. <p>Example, RESTCONF connection request to SLX device to gain access.</p>		

Parent Defect ID:	SLXOS-51200	Issue ID:	SLXOS-51200
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00b
Technology Group:	Layer 3 Routing/Network Layer	Technology:	Static Routing (IPv4)
Symptom:	Ping traffic latency observed on the network		
Condition:	<ol style="list-style-type: none"> 1. Enabled the network with MCT cluster configuration. 2. IP MTU is configured with default value of 1500bytes CEP port(egress). 3.Ping traffic(1495-1500 bytes) should reach on CCEP interface(ingress). 		

Parent Defect ID:	SLXOS-51214	Issue ID:	SLXOS-51214
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00c
Technology Group:	Management	Technology:	Software Installation & Upgrade
Symptom:	The SLX device may possibly become unresponsive while connecting USB		
Condition:	It may occur if the USB is corrupted or not mounted properly due to some hardware glitches		
Workaround:	Power-cycle the chassis and mount the USB again		

Parent Defect ID:	SLXOS-50787	Issue ID:	SLXOS-51320
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2a
Technology Group:	Other	Technology:	Other
Symptom:	security auditlog indicates wrong role for admin user while importing/Deleting oauth2pki certificate		
Condition:	This issue occurs when user tries to import/delete oauth2pki certificate.		

Parent Defect ID:	SLXOS-51126	Issue ID:	SLXOS-51326
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2a
Technology Group:	Monitoring	Technology:	RAS - Reliability, Availability, and Serviceability
Symptom:	When the tpvm deploy command fails, error is not displayed under the accounting log in TACACs server.		
Condition:	When "tpvm deploy" command is executed while tpvm is already installed, it'll cause failure in "tpvm deploy", this information is not captured as part of account log.		

Parent Defect ID:	SLXOS-51474	Issue ID:	SLXOS-51474
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Layer 2 Switching	Technology:	VLAN - Virtual LAN
Symptom:	Packets may flood on the same port from where it is received.		
Condition:	On reception of packet with ethertype of 0x88e7(PBB)		

Parent Defect ID:	SLXOS-51586	Issue ID:	SLXOS-51586
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00bf
Technology Group:	Other	Technology:	Other
Symptom:	Show command for NTP not giving the proper o/p		
Condition:	When they are running with 18r.2.00bf version.		

Parent Defect ID:	SLXOS-49524	Issue ID:	SLXOS-51657
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.1
Technology Group:	Traffic Management	Technology:	Rate Limiting and Shaping
Symptom:	"show access-list receive IP" command is not displaying output even though the CoPP ACL RL is applied.		
Condition:	When using "show access-list receive ip" display command.		

Parent Defect ID:	SLXOS-51794	Issue ID:	SLXOS-51822
Severity:	S2 - High		
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 Chip are not incrementing for priority traffic class.		
Condition:	CLI command: Traffic manager cmd "show tm voq-stat" is executed.		

Parent Defect ID:	SLXOS-51548	Issue ID:	SLXOS-51902
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2
Technology Group:	Layer 3 Routing/Network Layer	Technology:	IP Addressing
Symptom:	Device goes into "unregistered_netdevice" error state and does not recover. For example - Following message continuously keep scrolling on the console. [772093.586512] unregister_netdevice: waiting for po64 to become free. Usage count = 1 [772103.842611] unregister_netdevice: waiting for po64 to become free. Usage count = 1		
Condition:	Deleting ICL L3 interface.		

Parent Defect ID:	SLXOS-52329	Issue ID:	SLXOS-52329
Severity:	S2 - High		
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:	<ol style="list-style-type: none"> 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-52124	Issue ID:	SLXOS-52354
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00a
Technology Group:	Layer 3 Routing/Network Layer	Technology:	MBGP - Multiprotocol Border Gateway Protocol
Symptom:	In certain conditions SLX device would reload unexpectedly		
Condition:	BGP Static-network is configured locally and BGP also learns the same static-network prefix from one or more Remote peers.		
Workaround:	Apply an inbound route-map or prefix list to deny static-network prefixes from Remote peers.		

Parent Defect ID:	SLXOS-52365	Issue ID:	SLXOS-52551
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2a
Technology Group:	Layer 2 Switching	Technology:	VXLAN - Virtual Extensible LAN
Symptom:	QinQ Packet goes out with inner tag at the Egress device.		
Condition:	QinQ packet over vxlan tunnel.		

Parent Defect ID:	SLXOS-52746	Issue ID:	SLXOS-52746
Severity:	S1 - Critical		
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-52792	Issue ID:	SLXOS-52792
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.1a
Technology Group:	IP Multicast	Technology:	IGMP - Internet Group Management Protocol
Symptom:	Multicast traffic loss can be seen for the receivers present on other leaf nodes.		
Condition:	<ol style="list-style-type: none"> 1. One of the MCT node learns IGMP groups on Multicast tunnel. 2. The MCT peer is receiving IGMP Queries and Multicast traffic for the learnt groups. So it has to forward the traffic to Multicast tunnel. 2. The spine node, through which the MDT is formed, is reloaded. When it boots up, the MDT convergence will happen through this node again. After this convergence the issue can be seen. 		
Recovery:	Clearing the IGMP group cache should recover from the issue and a fresh learning of snooping routes should happen.		

Defects Closed with Code Changes

Parent Defect ID:	SLXOS-38060	Issue ID:	SLXOS-38060
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00
Technology Group:	Layer 3 Routing/Network Layer	Technology:	Other
Symptom:	With certain conditions, configuring an ipv4 or ipv6 prefix list would result into a Command line error.		
Condition:	An ipv4 or ipv6 prefix list instance is configured with 1024 rules and a new rule is added to the instance.		

Parent Defect ID:	SLXOS-42324	Issue ID:	SLXOS-42324
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00
Technology Group:	Management	Technology:	SNMP - Simple Network Management Protocol
Symptom:	<p>For 1 combination of auth/priv/groupname, <cr> is wrongly being displayed.</p> <p>SLX(config)# snmp-server user user100 priv AES128 groupname group1</p> <p>Possible completions:</p> <p>auth Authentication protocol for username (Default=noauth)</p> <p>priv-password Privacy password associated with username <cr></p> <p>SLX(config)# snmp-server user user100 priv AES128 groupname group1 <<< Hit Enter and will cause error</p> <p>%Error: Invalid password length. String size must be between 1 and 32 and cannot be a pre-defined string</p>		
Condition:	When there is no auth config and priv-password is not entered immediately followed by priv option.		
Workaround:	<p>Auth has to be entered first before priv and priv-password can be entered immediately following the priv option in which case this issue is not seen.</p> <p>SLX(config)# snmp-server user user1 auth md5 auth-password password priv AES128 priv-password password</p> <p>SLX(config)#</p>		

Parent Defect ID:	SLXOS-45114	Issue ID:	SLXOS-45114
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP-EVPN-MAC Stale Entries are programmed on MAC address table.		
Condition:	In BGP dampening case , when mac-address age-out timer value is lesser than BGP-EVPN dampen reuse timer value of 5 minutes.		
Workaround:	Clear the BGP-EVPN Peer connection using "clear bgp evpn neighbor all"		

Parent Defect ID:	SLXOS-47142	Issue ID:	SLXOS-47142
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	Technology:	Other
Symptom:	BGP and BFD flap may be observed when system about million routes from one vrf are leaked to 3+ other user-defined vrfs using "match vrf" condition in route map		
Condition:	When a disruptive command like clear ip route all is executed in source vrf, BGP and BFD session flaps may be seen with aggressive time intervals.		

Parent Defect ID:	SLXOS-47492	Issue ID:	SLXOS-47492
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	MCT keep-alive flaps during longevity . There is no functional impact when ICL is up.		
Condition:	MCT keep-alive on management network (auto option) was seen flapping during 24hr longevity test - idle setup with traffic running. We see a hold-timer expiry possibly due to mgmt network congestion leading to a reset of keep-alive session.		

Parent Defect ID:	SLXOS-47531	Issue ID:	SLXOS-47531
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	Technology:	Other
Symptom:	On firmware upgrade from lower versions to 20.1.1 if L2 MTU configured as 1548 then it will get converted to 9216. This holds good for global as well as interface level L2 MTU. In 20.1.1 default value of L2 MTU is changed to 9216 from 1548 in lower versions.		
Condition:	Firmware upgrade from lower version to 20.1.1.		

Parent Defect ID:	SLXOS-47629	Issue ID:	SLXOS-47629
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 17r.1.01aj
Technology Group:	Monitoring	Technology:	Syslog
Symptom:	RASLOG for optical temperature may display alarm even though the values are within boundary		
Condition:	During Port Up events		

Parent Defect ID:	SLXOS-47777	Issue ID:	SLXOS-47777
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00b
Technology Group:	Layer 3 Routing/Network Layer	Technology:	ARP - Address Resolution Protocol
Symptom:	traffic loss in EVPN + MRP topology		
Condition:	Configure EVPN + MRP topology		

Parent Defect ID:	SLXOS-47946	Issue ID:	SLXOS-47946
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00a
Technology Group:	Layer 3 Routing/Network Layer	Technology:	ICMP - Internet Control Message Protocol
Symptom:	ICMP Redirect on /31 Network induces Stack Trace of random Daemon		
Condition:	Assign IP address with /31 network on an interface and enable ICMP redirect on interface.		

Parent Defect ID:	SLXOS-48011	Issue ID:	SLXOS-48011
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00db
Technology Group:	IP Multicast	Technology:	PIM - Protocol- Independent Multicast
Symptom:	Unexpected reload		
Condition:	On continuous execution of 'clear ip pim mcache' with multicast data traffic passing through		

Parent Defect ID:	SLXOS-48171	Issue ID:	SLXOS-48171
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00b
Technology Group:	Layer 3 Routing/Network Layer	Technology:	ARP - Address Resolution Protocol
Symptom:	ARP age out is not working as expected.		
Condition:	When "ip dhcp relay address" is configured.		

Parent Defect ID:	SLXOS-48294	Issue ID:	SLXOS-48294
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00a
Technology Group:	Layer 3 Routing/Network Layer	Technology:	IPv6 Addressing
Symptom:	IPv6 RACL and control plane policy with cir 0 do not drop packets when profile etcam ipv4-v6-route and tcam bgp_flowspec is configured.		
Condition:	when hardware etcam profile ipv4-v6-route and tcam profile bgp_flowspec is configuration, do not drop packets IPv6 RACL and control plane policy with cir 0.		

Parent Defect ID:	SLXOS-48501	Issue ID:	SLXOS-48501
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 17r.1.00a
Technology Group:	Security	Technology:	ACLs - Access Control Lists
Symptom:	Traffic may get permitted with hard-drop L2 ACL configured on device.		
Condition:	During configuration of log option in addition to hard-drop L2 ACL		

Parent Defect ID:	SLXOS-48918	Issue ID:	SLXOS-48918
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	Technology:	VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom:	on SLX 9540/9640, VRRP Virtual IP is not functioning when vlan Id and Ve Id are not same.		
Condition:	User will observe this issue on SLX 9540/9640, with VRRP Virtual IP when the vlan Id and the associated VE Id are not same.		

Parent Defect ID:	SLXOS-48938	Issue ID:	SLXOS-48938
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00b
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Routes showing incorrect next-hop		
Condition:	After changing OSPF costs		

Parent Defect ID:	SLXOS-49062	Issue ID:	SLXOS-49062
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	MPLS	Technology:	IP over MPLS
Symptom:	on SLX 9540/SLX 9640, IP control packets from the control plane with next hop as MPLS LSP will not egress out from the system. No issues will be seen with the Data traffic		
Condition:	With bypass protected MPLS LSP as Next hop, Control Packets get dropped in the system, when the MPLS LSP egressing traffic through its bypass protection path. i.e. When primary path is down.		

Parent Defect ID:	SLXOS-49230	Issue ID:	SLXOS-49230
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00db
Technology Group:	IP Multicast	Technology:	IGMP - Internet Group Management Protocol
Symptom:	Unexpected reload		
Condition:	While processing high rate of IGMP join and leave messages		

Parent Defect ID:	SLXOS-49290	Issue ID:	SLXOS-49290
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00a
Technology Group:	MPLS	Technology:	LDP - Label Distribution Protocol
Symptom:	LDP session in nonexistent state with Cisco box.		
Condition:	IP MTU on the network is higher than 4096. SLX node is the active side for the LDP Session.		
Workaround:	1. Configure lower IP MTU (or) 2. Make SLX the passive peer.		

Parent Defect ID:	SLXOS-49542	Issue ID:	SLXOS-49542
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Management	Technology:	Software Installation & Upgrade
Symptom:	User may observe that Hardware profiles are not activated.		
Condition:	This is specific to SLX 9640 platform. After downgrade from 20.2.1 release to pre-20.1.1 release trains.		

Parent Defect ID:	SLXOS-49550	Issue ID:	SLXOS-49550
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	IP Multicast	Technology:	IGMP - Internet Group Management Protocol
Symptom:	IGMP Snooping with VLL , Multicast traffic is not transmitted out		
Condition:	After upgrading PE2 to 20.1.1.1		

Parent Defect ID:	SLXOS-49650	Issue ID:	SLXOS-49650
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Other	Technology:	Other
Symptom:	ON SLX 9640, 100G/40G port LED displays the link status incorrectly		
Condition:	On SLX 9640 only.		

Parent Defect ID:	SLXOS-49787	Issue ID:	SLXOS-49787
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00bc
Technology Group:	Layer 3 Routing/Network Layer	Technology:	MBGP - Multiprotocol Border Gateway Protocol
Symptom:	In certain error scenarios where BGP is flooded with erroneous attributes, user may observe BGP not learning/advertising routes from/to peers after significant amount of time under this condition.		
Condition:	Remote BGP peer advertising route updates with invalid next-hop attribute or invalid as-path attribute can cause this condition. This can be checked by running SLX-OS CLI command "show [ip ipv6] bgp neighbors routes-summary"		

Parent Defect ID:	SLXOS-49827	Issue ID:	SLXOS-49827
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	Technology:	ICMP - Internet Control Message Protocol
Symptom:	<p>Ping to an IP address on a local interface succeeds even if the interface is down.</p> <p>Example:</p> <pre>SLX# show running-config interface Ethernet 0/1 interface Ethernet 0/1 ip address 10.1.1.1/24 shutdown ! SLX# ping 10.1.1.1 Type Control-c to abort PING 10.1.1.1 (10.1.1.1) from 10.1.1.1 56(84) bytes of data. 64 bytes from 10.1.1.1: icmp_seq=1 ttl=64 time=0.102 ms 64 bytes from 10.1.1.1: icmp_seq=2 ttl=64 time=0.134 ms</pre>		
Condition:	Ping was not checking if the interface was UP before sending out a reply.		

Parent Defect ID:	SLXOS-49910	Issue ID:	SLXOS-49910
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	In SLX 9540/9640, if BGP PIC feature is enabled and BGP has more than 900+ nexthops, administrator may experience Hardware FEC resource not available error on the console/syslogs.		
Condition:	BGP PIC feature needs to be enabled and BGP should have more than 900+ nexthops.		

Parent Defect ID:	SLXOS-49936	Issue ID:	SLXOS-49936
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00b
Technology Group:	Layer 2 Switching	Technology:	VLAN - Virtual LAN
Symptom:	Intermittent TCP connection failure		
Condition:	When the TCP ACK number starts from 0x2C70****. This we can verify from packet capture only. (Example: Acknowledgement number(raw):745552767 [0x2C703B7F]).		

Parent Defect ID:	SLXOS-50034	Issue ID:	SLXOS-50034
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00bb
Technology Group:	IP Multicast	Technology:	PIM - Protocol-Independent Multicast
Symptom:	SLX device is not forwarding the multicast traffic.		
Condition:	<ol style="list-style-type: none"> 1. SLX device is the first hop router and acting as RP. 2. When the source of stream is not directly connected and Next-hop towards source is not enabled with PIM. 		

Parent Defect ID:	SLXOS-50077	Issue ID:	SLXOS-50077
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Security	Technology:	User Accounts & Passwords
Symptom:	System level commands are accessible by non-admin users		
Condition:	when we have non-admin users		

Parent Defect ID:	SLXOS-50230	Issue ID:	SLXOS-50230
Severity:	S1 - Critical		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	Technology:	RIP - IPv4 Routing Information Protocol
Symptom:	On SLX-9540, with hw-opt profile enabled, Traffic to /32 v4 prefixes or Host routes can get mis-forwarded. Packets may also come to CPU in some scenario causing high CPU.		
Condition:	SLX-9540 with hw-opt profile enabled		

Parent Defect ID:	SLXOS-50340	Issue ID:	SLXOS-50340
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00d
Technology Group:	Layer 3 Routing/Network Layer	Technology:	IP Addressing
Symptom:	traceroute command may succeed for disabled loopback ip address from peer.		
Condition:	<ol style="list-style-type: none"> 1) Configure /32 mask ip address for loopback interface. 2) Disable loopback interface using shut. 		

Parent Defect ID:	SLXOS-50387	Issue ID:	SLXOS-50387
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Management	Technology:	CLI - Command Line Interface
Symptom:	show vlan brief doesn't display if vlan name .		
Condition:	When we configured the VLAN name with more than 15 characters.		

Parent Defect ID:	SLXOS-50569	Issue ID:	SLXOS-50569
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP reload might be observed.		
Condition:	Modifying the Listen Range (Dynamic Peers related configuration).		
Workaround:	Use static neighbor configuration.		

Parent Defect ID:	SLXOS-50653	Issue ID:	SLXOS-50653
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00bg
Technology Group:	Management	Technology:	Configuration Fundamentals
Symptom:	"no max-metric router-lsa all-lsas" would not delete all lsas in OSPF		
Condition:	Executing "no max-metric router-lsa all-lsas" under ospf		

Parent Defect ID:	SLXOS-50875	Issue ID:	SLXOS-50875
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2a
Technology Group:	Management	Technology:	Other
Symptom:	tacacs accounting log shows "Message Generic Error" when user deletes the imported oauth2 certificate.		
Condition:	User will observe this when oauth2 certificate is deleted using "no crypto import oauth2pkicert" cmd		
Workaround:	NA		

Parent Defect ID:	SLXOS-51206	Issue ID:	SLXOS-51206
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BFD - Bidirectional Forwarding Detection
Symptom:	BFD sessions state may flap or remain in DOWN state.		
Condition:	IP address re-used across different VRFs		

Parent Defect ID:	SLXOS-51230	Issue ID:	SLXOS-51309
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2a
Technology Group:	Management	Technology:	Configuration Fundamentals
Symptom:	On upgrading to SLX 20.1.2a with TPVM 3.0 and EFA 2.1, user will observe that the SLX CLI 'show efa status' is giving erroneous output		
Condition:	User will observe this issue on SLXOS 20.1.2a with TPVM 3.0 and EFA 2.1. Issue will not be observed with TPVM 4.0 and EFA 2.2.		
Workaround:	<p>User instead of using "show efa status" from SLX CLI, can execute below steps to avoid the issue</p> <ol style="list-style-type: none"> 1. login to TPVM 2. issue "efa version" from TPVM 3. Issue "k3s kubectl -n efa get all" from TPVM <p>Sample output</p> <pre> +++++++ admin@TPVM:~\$ efa version Version : 2.1.0 Build: GA Time Stamp: 20-01-31:15:11:36 --- Time Elapsed: 1.273838ms -- admin@TPVM:~\$ k3s kubectl -n efa get all NAME READY STATUS RESTARTS AGE pod/efa-api-docs-6bb5dbcc74-gxjf5 1/1 Running 2 24m pod/godb-service-5b4f9bbd6c-bm4ln 1/1 Running 2 24m pod/goopenstack-service-554c57548f-kxfnp 1/1 Running 8 24m pod/rabbitmq-0 1/1 Running 2 24m pod/gofabric-service-69d8995fc6-n976w 1/1 Running 7 24m pod/gotenant-service-55fd8889d8-xx5tg 1/1 Running 7 24m pod/goinventory-service-59d9b798d8-2zg48 1/1 Running 7 24m </pre>		

Parent Defect ID:	SLXOS-51230	Issue ID:	SLXOS-51309
	pod/govcenter-service-f6b49d9b9-ljthb	1/1	Running 13 24m
	pod/gohyperv-service-854654f6b9-zjqwc	1/1	Running 12 24m
	NAME	TYPE	CLUSTER-IP
	AGE	EXTERNAL-IP	PORT(S)
	service/gofabric-service	ClusterIP	10.43.24.224 <none>
	8081/TCP	24m	
	service/goinventory-service	ClusterIP	10.43.225.147 <none>
	8082/TCP	24m	
	service/gotenant-service	ClusterIP	10.43.177.177 <none>
	8083/TCP	24m	
	service/efa-api-docs	ClusterIP	10.43.37.1 <none> 80/TCP
	24m		
	service/rabbitmq	NodePort	10.43.0.52 <none>
	15672:31672/TCP,5672:30672/TCP	24m	
	service/db-service	NodePort	10.43.144.44 <none>
	5432:30432/TCP	24m	
	service/goopenstack-service	NodePort	10.43.206.251 <none>
	8085:30085/TCP	24m	
	service/govcenter-service	ClusterIP	10.43.144.146 <none>
	8086/TCP	24m	
	service/gohyperv-service	ClusterIP	10.43.43.183 <none>
	8087/TCP	24m	
	NAME	READY	UP-TO-DATE
	AVAILABLE	AGE	
	deployment.apps/efa-api-docs	1/1	1 1 24m
	deployment.apps/godb-service	1/1	1 1 24m
	deployment.apps/goopenstack-service	1/1	1 1 24m
	deployment.apps/gofabric-service	1/1	1 1 24m
	deployment.apps/gotenant-service	1/1	1 1 24m
	deployment.apps/goinventory-service	1/1	1 1 24m
	deployment.apps/govcenter-service	1/1	1 1 24m
	deployment.apps/gohyperv-service	1/1	1 1 24m
	NAME	DESIRED	CURRENT
	READY	AGE	
	replicaset.apps/efa-api-docs-6bb5dbcc74	1	1 1 24m
	replicaset.apps/godb-service-5b4f9bbd6c	1	1 1 24m
	replicaset.apps/goopenstack-service-554c57548f	1	1 1 24m
	replicaset.apps/gofabric-service-69d8995fc6	1	1 1 24m
	replicaset.apps/gotenant-service-55fd8889d8	1	1 1 24m
	replicaset.apps/goinventory-service-59d9b798d8	1	1 1 24m
	replicaset.apps/govcenter-service-f6b49d9b9	1	1 1 24m

Parent Defect ID:	SLXOS-51230	Issue ID:	SLXOS-51309
	24m replicaset.apps/gohyperv-service-854654f6b9 1 1 1 24m NAME READY AGE statefulset.apps/rabbitmq 1/1 24m admin@TPVM:~\$		

Parent Defect ID:	SLXOS-50076	Issue ID:	SLXOS-51328
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	In Centralized routing scenario, reloading one of the Border leaf nodes configured as MCT pairs, with scaled config may cause more than second delay in convergence once the node comes up		
Condition:	Reload of one of the Border leaf nodes in Centralized routing scenario, user will observe this behavior especially when the node is having scaled config (like 50 VRF, more than 2500 VE IP interfaces spread across these VRF and 1500 BD/Vlan VEs, more than 1500 IPV4 and 1500 IPV6 SAG interfaces etc.)		

Parent Defect ID:	SLXOS-51235	Issue ID:	SLXOS-51727
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2a
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BFD - Bidirectional Forwarding Detection
Symptom:	User will observe that Static route monitored by BFD are no longer reachable, when BFD hold down timer is configured, and BFD session is brought down by triggers like interface down		
Condition:	Static route's nexthop is monitored by BFD with holddown interval & BFD session goes down .		
Workaround:	NA		
Recovery:	Removing hold-down interval & flapping interface.		

Parent Defect ID:	SLXOS-22366	Issue ID:	SLXOS-51785
Severity:	S4 - Low		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00
Technology Group:	IP Multicast	Technology:	IGMP - Internet Group Management Protocol
Symptom:	IGMPv3 Vlan not learning the mrouter port on receiving IGMP v2 query.		
Condition:	Vlan configured with igmpv3 on the host side , does not learn the mrouter port, if the received query is igmpv2.		

Parent Defect ID:	SLXOS-51131	Issue ID:	SLXOS-51792
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00bd
Technology Group:	Layer 3 Routing/Network Layer	Technology:	VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom:	High CPU and protocol flapping.		
Condition:	When data IP traffic is sent with VRRP Protocol number then packets are trapped to CPU and may congest CPU protocol queue.		
Workaround:	<pre> Create policy map:- policy-map pip class cip police cir 0 ! ! class-map cip match access-group x20 ! ip access-list extended x20 seq 10 permit 112 any host 224.0.0.18 ! Apply on control plane:- control-plane service-policy in pip ! </pre>		

Parent Defect ID:	SLXOS-51086	Issue ID:	SLXOS-51809
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2a
Technology Group:	Security	Technology:	SSH - Secure Shell
Symptom:	User will observe that when outbound SSH connection is made on mgmt-vrf, a message "failed to write to known hosts file" occurs, even though the connection is established successfully.		
Condition:	User will observe this behavior when outbound SSH is executed on mgmt-vrf		
Workaround:	NA		

Defects Closed without Code Changes

Parent Defect ID:	SLXOS-50242	Issue ID:	SLXOS-50242
Reason Code:	Not Reproducible	Severity:	S3 - Medium
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2
Technology Group:	Other	Technology:	Other
Symptom:	Observing a trace "grep: support for the -P option is not compiled into this --disable-perl-regexp binary" under console while triggering firmware download. Issue has no functional impact		
Condition:	The trace is observed on the console during switch reboot after firmware download.		

Parent Defect ID:	SLXOS-51048	Issue ID:	SLXOS-51048
Reason Code:	Will Not Fix	Severity:	S3 - Medium
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2a
Technology Group:	Security	Technology:	AAA - Authentication, Authorization, and Accounting
Symptom:	User will observe that during downgrade procedure, using coldboot downgrade from 20.1.2a to 20.1.1 gets blocked with error.		
Condition:	After configuring the CLIs crypto pkcs12 import and aaa login outh2 the coldboot downgrade from 20.1.2a to 20.1.1 gets blocked. This forces user to remove these 2 commands before downgrade.		
Workaround:	User should remove the 'aaa login outh2' and 'crypto pkcs12 import' cmds using "no form" of these commands before downgrade.		

Parent Defect ID:	SLXOS-51046	Issue ID:	SLXOS-51311
Reason Code:	Already Reported	Severity:	S2 - High
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2a
Technology Group:	Management	Technology:	Other
Symptom:	While using TPVM, user will observe that sometimes SSH session from SLX CLI prompt to TPVM on the node is not connecting.		
Condition:	<p>In the following sequence of operations, step 5 will fail due to stale entry for TPVM IP Address in the /fabos/user/admin/.ssh/known_hosts.</p> <ol style="list-style-type: none"> 1. Install TPVM 2. SSH from SLX CLI to TPVM 3. Uninstall TPVM 4. Install TPVM 5. SSH from SLX CLI to TPVM 		
Workaround:	Delete the entry in the /fabos/user/admin/.ssh/known_hosts from bash prompt.		