June 2020

Extreme SLX-OS 20.2.1 Release Notes

Supporting ExtremeRouting and ExtremeSwitching SLX 9740, SLX 9640, SLX 9540, SLX 9150, and SLX 9250

9036654-00 Rev AA

Contents

Document History

Version	Summary of changes	Publication date
1.0	Initial version for 20.2.1	June 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.

Release Overview

Release SLX-OS 20.2.1 provides the following features:

- Support for two new hardware platforms: SLX-9740-40C and SLX-9740-80C
- Feature parity for the SLX 9740 with the 20.1.2a release software, with exceptions as described in Limitations and Restrictions
- Specific focus on Border Routing and IP Fabric Spine
- Additional new features as described in Software Features

Behavior Changes

System Feature	Behavior Change
Auto-persistence	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	Arguments are compulsory.
tpvm deploy	The “mgmt/insight" options are mandatory.

Software Features

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

Feature Name	Supported SLX Platforms	Description
IP Fabric Multicast	All platforms* (9740 as spine device only)	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. 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). The overall mechanism uses Multicast Distribution Trees to deliver traffic effectively while minimizing packet replication in the fabric.
COPP	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.

CLI 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 ocsp
- ldap-server host
- logging syslog-server

Removed commands

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

RFCs, Standards, and Scalability

RFC Compliance for SLX 9740

General Protocols

RFC	**RFC Name**	**SLX 9740**
RFC 768	User Datagram Protocol (UDP)	X
RFC 791	Internet Protocol (IP)	X
RFC 792	Internet Control Message Protocol (ICMP)	X
RFC 793	Transmission Control Protocol (TCP)	X
RFC 826	ARP	X
RFC 894	IP over Ethernet	X
RFC 903	RARP	X
RFC 906	TFTP Bootstrap	X
RFC 950	Subnet	X
RFC 951	BootP	X
RFC 1027	Proxy ARP	X
RFC 1042	Standard for The Transmission of IP	X
RFC 1166	Internet Numbers	X
RFC 1122	Requirements for Internet Hosts	X
RFC 1191	Path MTU Discovery	X
RFC 3232	Assigned Numbers	X
RFC 4632	Classless Interdomain Routing (CIDR)	X
RFC 1542	BootP Extensions	X
RFC 1591	DNS (client)	X
RFC 2819	RMON Groups 1, 2, 3, 9	X
RFC 1812	Requirements for IP Version 4 Routers	X
RFC 1858	Security Considerations for IP Fragment Filtering	X
RFC 2131	BootP/DHCP Helper	X
RFC 2784	Generic Routing Encapsulation (GRE)	X
RFC 3021	Using 31-Bit Prefixes on IPv4 Point-to- Point Links	X
RFC 3046	DHCP Relay Agent Information Option	X
RFC 3527	Link Selection Sub Option for the Relay Agent Information Option for DHCPv4	X
RFC 3768	Virtual Router Redundancy Protocol (VRRP)	X
RFC 4001	INET-ADDRESS-MIB	X

RFC	RFC Name	SLX 9740
RFC 5880	Bidirectional Forwarding Detection	X
RFC 5881	Bidirectional Forwarding Detection for IPv4 and IPv6 (Single Hop)	X
RFC 5882	Generic Application of Bidirectional Forwarding Detection	X
RFC 5883	Bidirectional Forwarding Detection for Multihop Paths	X

BGPv4

RFC	RFC Name	SLX 9740
RFC 1745	OSPF Interactions	X
RFC 1772	Application of BGP in the Internet	X
RFC 1997	Communities and Attributes	X
RFC 2385	BGP Session Protection via TCP MD5	X
RFC 2439	Route Flap Dampening	X
RFC 2918	Route Refresh Capability	X
RFC 3392	Capability Advertisement	X
RFC 3682	Generalized TT L Security Mechanism for eBGP Session Protection	X
RFC 4271	BGPv4	X
RFC 4364	BGP/MPLS IP Virtual Private Networks	X
RFC 4456	Route Reflection	X
RFC 4486	Sub codes for BGP Cease Notification Message	X
RFC 4724	Graceful Restart Mechanism for BGP	X
RFC 6198	Requirements for the Graceful Shutdown of BGP sessions	X
RFC 8326	Graceful BGP Session Shutdown	X
RFC 6793	BGP Support for Four-octet AS Number Space	X
RFC 5065	BGP4 Confederations	X
RFC 5291	Outbound Route Filtering Capability for BGP-4	X
RFC 5396	Textual Representation of Autonomous System (AS) Numbers	X
RFC 5668	4-Octet AS specific BGP Extended Community	X
Draft-ietf-rtgwg-bgp-pic-07.txt BGP Prefix Independent Convergence		X
RFC 5575	Dissemination of Flow Specification Rules (BGP Flow Spec)	X
RFC 8092	BGP Large Community Attribute	X
sFlow BGP AS path		X

Element Security

RFC	RFC Name	SLX 9740
AAA		X
Username/Password (Challenge and Response)		X
Bi-level Access Mode (Standard and EXEC Level)		X
Role-based Access Control (RBAC)		X
RFC 2865	RADIUS	X

RFC	RFC Name	SLX 9740
RFC 2866	RADIUS Accounting	X
RFC 3162	RADIUS and IPv6	X
RFC 6613	RADIUS over TCP	X
RFC 6614	Transport Layer Security (TLS) Encryption for RADIUS	X
TACACS/TACACS+		X
RFC 4510 thru 4519	LDAP	X
RFC 4510 thru 4519	LDAP over TLS	X
RFC 6749, 7515, 7519	OAuth2 - JSON Web Token (JWT)	X
RFC 5905	NTP Version 4	X
RFC 3986	Uniform Resource Identifier (URI): Generic Syntax	X
RFC 6241	NETCONF Configuration Protocol (Partial)	X
RFC 4742	"Using the NETCONF Configuration Protocol over Secure Shell (SSH)"	X
RFC 6020	"YANG – A Data Modeling Language for the Network Configuration Protocol (NETCONF)"	X
RFC 6021	"Common YANG Data Types"	X
NTP client and NTP server		X
RFC 5961	TCP Security	X
RFC 4251	Secure Shell (SSH) Protocol Architecture	X
RFC 4253	Secure Shell (SSH)	X
RFC 4346	TLS 1.1	X
RFC 5246	TLS 1.2	X
RFC 5280	Internet X.509 PKI Certificates	X
RFC 6960	Internet X.509 PKI OCSP	
Protection against Denial of Service (DoS) attacks such as TCP SYN or Smurf Attacks		X

OSPF

RFC	RFC Name	SLX 9740
RFC 1745	OSPF Interactions	X
RFC 1765	OSPF Database Overflow	X
RFC 2328	OSPF v2	X
RFC 3101	OSPF NSSA	X
RFC 3137	OSPF Stub Router Advertisement	X
RFC 3623	Graceful OSPF Restart	X
RFC 3630	TE Extensions to OSPF v2	X
RFC 4222	Prioritized Treatment of Specific OSPF Version 2	X
RFC 5250	OSPF Opaque LSA Option	X
RFC 5709	OSPFv2 HMAC-SHA Cryptographic Authentication	X
RFC 7166	Supporting Authentication Trailer for OSPFv3	X
RFC 7474	Security Extension for OSPFv2 When Using Manual Key Management	X

IS-IS

RFC	RFC Name	SLX 9740
RFC 1142	OSI IS-IS Intra-domain Routing Protocol	X
RFC 1195	Routing in TCP/IP and Dual Environments	X
RFC 3277	IS-IS Blackhole Avoidance	X
RFC 5120	IS-IS Multi-Topology Support	X
RFC 5301	Dynamic Host Name Exchange	X
RFC 5302	Domain-wide Prefix Distribution	X
RFC 5303	Three-Way Handshake for IS-IS Point-to-Point	X
RFC 5304	IS-IS Cryptographic Authentication (MD-5)	X
RFC 5306	Restart Signaling for ISIS (helper mode)	X
RFC 5309	Point-to-point operation over LAN in link state routing protocol	X

IPv4 Multicast

RFC	RFC Name	SLX 9740
RFC 1112	IGMP v1	X
RFC 2236	IGMP v2	X
RFC 3376	IGMP v3	X
RFC 4601	PIM-SM	X
RFC 4607	PIM-SSM	X
RFC 4610	Anycast RP using PIM	X
RFC 5059	BSR for PIM	X
PIM IPv4 MCT		

Quality of Service (QoS)

RFC	RFC Name	SLX 9740
RFC 2474	DiffServ Definition	X
RFC 2475	An Architecture for Differentiated Services	X
RFC 2597	Assured Forwarding PHB Group	X
RFC 2697	Single Rate Three-Color Marker	X
RFC 2698	A Two-Rate Three-Color Marker	X
RFC 3246	An Expedited Forwarding PHB	X

IPv6 Core

RFC	RFC Name	SLX 9740
RFC 1887	IPv6 unicast address allocation architecture	X
RFC 1981	IPv6 Path MTU Discovery	X
RFC 8201	IPv6 Path MTU Discovery	X
RFC 2375	IPv6 Multicast Address Assignments	X
RFC 2450	Proposed TLA and NLA Assignment Rules	X
RFC 2460	IPv6 Specification	X
RFC 8200	IPv6 Specification	X
RFC 4861	IPv6 Neighbor Discovery	X
RFC 4862	IPv6 Stateless Address Auto-configuration	X
RFC 2464	Transmission of IPv6 over Ethernet Networks	X

RFC	RFC Name	SLX 9740
RFC 2471	IPv6 Testing Address allocation	X
RFC 3701	IPv6 Testing Address allocation	X
RFC 2711	IPv6 Router Alert Option	X
RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	X
RFC 3587	IPv6 Global Unicast Address Format	X
RFC 4193	Unique Local IPv6 Unicast Addresses	X
RFC 4291	IPv6 Addressing architecture	X
RFC 4301	IP Security Architecture	X
RFC 4303	Encapsulating Security Payload (ESP)	X
RFC 4305	ESP and AH cryptography	X
RFC 4443	ICMPv6	X
RFC 4552	Auth for OSPFv3 using AH/ESP	X
RFC 4835	Cryptographic Alg. Req. for ESP	X
RFC 4861	Neighbor Discovery for IP version 6 (IPv6)	X
RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	X

IPv6 Routing

RFC	RFC Name	SLX 9740
RFC 5340	OSPFv3 for IPv6	X
RFC 5308	Routing IPv6 with IS-IS	X
RFC 2545	Use of BGP-MP for IPv6	X
RFC 8106	Support for IPv6 Router Advertisements with DNS Attributes	X
RFC 6164	Using 127-Bit IPv6 Prefixes on Inter-Router Links	X

MPLS

RFC	RFC Name	SLX 9740
RFC 2205	RSVP v1 Functional Specification	X
RFC 2209	RSVP v1 Message Processing Rules	X
RFC 2674	P-BRIDGE-MIB	X
RFC 2702	TE over MPLS	X
RFC 2961	RSVP Refresh Overhead Reduction Extensions	X
RFC 3031	MPLS Architecture	X
RFC 3032	MPLS Label Stack Encoding	X
RFC 3037	LDP Applicability	X
RFC 3097	RSVP Cryptographic Authentication	X
RFC 3209	RSVP-TE	X
RFC 3478	LDP Graceful Restart	X
RFC 3813	MPLS-LSR-STD-MIB	X
RFC 3815	MPLS-LDP-STD-MIB MPLS-LDP-GENERIC-STD-MIB	X
RFC 4090	Fast Re-Route for RSVP-TE for LSP Tunnels; partial support	X
RFC 4379	OAM	
RFC 4448	Encapsulation Methods for Transport of Ethernet over MPLS Networks	X
RFC 5036	LDP Specification	X

RFC	RFC Name	SLX 9740
RFC 5305	ISIS-TE	X
RFC 5443	LDP IGP Synchronization	X
RFC 5561	LDP Capabilities	X
RFC 5712	MPLS traffic Engineering Soft Preemption	X
RFC 5918	LDP "Typed Wildcard" FEC	X
RFC 5919	Signaling LDP Label Advertisement Completion	X

Layer 2 VPN and Pseudowire Emulation Edge to Edge PWE3

RFC	RFC Name	SLX 9740
RFC 3343	TTL Processing in MPLS Networks	X
RFC 3985	Pseudowire Emulation Edge to Edge (PWE3) Architecture	X
RFC 4265	VPN-TC-STD-MIB	X
RFC 4364	BGP/MPLS IP Virtual Private Networks4	X
RFC 4447	Pseudowire Setup and Maintenance using LDP	X
RFC 4448	Encapsulation Methods for Transport of Ethernet Frames Over IP/MPLS Networks	X
RFC 4664	Framework for Layer 2 Virtual Private Networks	X
RFC 4665	Service Requirements for Layer 2 Provider- Provisioned Virtual Private Networks	X
RFC 4762	Virtual Private LAN Service (VPLS) Using LDP Signaling	X
RFC 5542	PW-TC-STD-MIB	X
RFC 5601	IANA-PWE3-MIB PW-STD-MIB	X
RFC 6391	Flow-Aware Transport of Pseudowires	X
RFC 6870	PW Preferential Forwarding Status Bit3	X
RFC 7348	Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks (Partial – MPLS encap is not supported)	X
RFC 8365	A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN) (partial)	X
draft-sd-l2vpn-evpn-overlay-03		X
draft-ietf-bess-evpn-prefix-advertisement-11		X

Manageability and Visibility

RFC	RFC Name	SLX 9740
Integrated industry-standard Command Line Interface (CLI)		X
RFC 854	Telnet	X
RFC 1573	IANAifType-MIB	X
RFC 2068	HTTP	X
RFC 2571	SNMP-FRAMEWORK-MIB	X
RFC 2572	SNMP-MPD-MIB	X
RFC 2573	SNMP-TARGET-MIB SNMP-NOTIFICATION-MIB	X

RFC	RFC Name	SLX 9740
RFC 2574	SNMP-USER-BASED-SM-MIB	X
RFC 2575	SNMP-VIEW-BASED-ACM-MIB	X
RFC 2576	SNMP-COMMUNITY-MIB	X
RFC 2818	HTTPS	X
RFC 2665	Ethernet Interface MIB	X
RFC 2677	IANA-ADDRESS-FAMILY-NUMBERS-MIB	X
IANA ifType-MIB [https://www.iana.org/assignments/ianaiftype-mip/ianaiftype-mib		X
RFC 2790	HOST-RESOURCES-MIB	X
RFC 2856	HCNUM-TC	X
RFC 2863	IF-MIB	X
RFC 2932	IANA-RTPROTO-MIB	X
RFC 3176	sFlow	X
sFlow extension to VXLAN		X
RFC 3273	RMON2-MIB	X
RFC 3289	DIFFSERV-DSCP-TC INTEGRATED-SERVICES-MIB DIFFSERV-MIB	X
RFC 3418	SNMPv2-MIB	X
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	X
RFC 3419	TRANSPORT-ADDRESS-MIB	X
RFC 3593	PerfHist-TC-MIB	X
RFC 3705	HC-PerfHist-TC-MIB	X
sFLow Version 5 and sFLow VxLAN extensions		X
Secure Copy (SCP v2) SFTP		X
SFTP		X
RFC 8040	RESTCONF Protocol – PATCH, PUT, POST, DELETE support	X
RFC 4022	TCP-MIB	X
RFC 4087	IP Tunnel MIB	X
RFC 4113	UDP-MIB	X
RFC 4133	Entity MIB	X
RFC 4253	Secure Shell (SSH)	X
RFC 4254	Secure Shell (SSH) Connection Protocol	X
RFC 4344	SSH Transport Layer Encryption Modes	X
RFC 4419	Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol	X
RFC 6187	X.509v3 Certificates for Secure Shell Authentication	X
draft-ietf-secsh-filexfer-13.txt SSH File Transfer Protocol (SFTP)		X
Secure Copy (SCP v2)		X
RFC 4293	IP MIB	X
RFC 4741	NETCONF (Partial)	X
Chrome		X
Curl		X
Tcpdump		X

RFC	RFC Name	SLX 9740
Wireshark		X
SNMP v1/v2c/v3		X
RFC 1157	Simple Network Management Protocol	X
RFC 1908	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework	X
RFC 2578	Structure of Management Information Version 2	X
RFC 2579	Textual Conventions for SMIv2	X
RFC 2580	Conformance Statements for SMIv2	X
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework	X
RFC 3411	An Architecture for Describing SNMP Management Frameworks	X
RFC 3412	Message Processing and Dispatching	X
RFC 3413	SNMP Applications	X
RFC 3414	User-based Security Model	X
RFC 3415	View-based Access Control Model	X
RFC 3416	Version 2 of SNMP Protocol Operations	X
RFC 3417	Transport Mappings	X
RFC 2819	RMON Groups 1, 2, 3, 9	X
IEEE8021-PAE-MIB		X
IEEE802 LLDP MIB		X
IEEE8023-LAGMIB		X
RFC 1213	MIB-II	X
RFC 4292	IP-FORWARD-MIB	X
RFC 4188	BRIDGE-MIB	X
RFC 4750	OSPF-MIB	X
RFC 5643	OSPFv3 MIB	X
RFC 4363	Q-BRIDGE-MIB	X
RFC 3635	EtherLike-MIB	X
RFC 3811	MPLS TC STD MIB	X
RFC 3812	MPLS-TE-STD-MIB	X
RFC 3813	MPLS-LSR-STD-MIB	X
RFC 3826	SNMP-USM-AES MIB	X
RFC 4273	BGP4-MIB	X
draft-ietf-idr-bgp4-mibv2-15	BGP4v2 Draft 15 MIB	X
RFC 4318	RSTP-MIB	X
RFC 4444	ISIS-MIB	X
RFC 4878	DOT3-OAM-MIB	X
RFC 7257	VPLS-GENERIC-MIB VPLS-LDP-MIB VPLS-BGP-MIB	X
RFC 7330	BFD-TC-STD-MIB IANA-BFD-TC-STD-MIB	X

RFC	RFC Name	SLX 9740
RFC 7331	BFD-STD-MIB	X

SLX-OS IEEE Standards Compliance for SLX 9740

IEEE standard	IEEE standard name	SLX 9740
IEEE Std 802.1AB-2005	LLDP-MIB LLDP-EXT-DOT1-MIB LLDP-EXT-DOT3-MIB	X
IEEE P802.1AG D8.1	IEEE8021-CFM-MIB	X
IEEE 802.1AP	IEEE8021-CFM-V2-MIB	X
IEEE 802.3-2005	CSMA/CD Access Method and Physical Layer Specifications	X
IEEE 802.3AB	1000BASE-T	X
IEEE 802.3AE	10G Ethernet	X
IEEE 802.3U	100BASE-TX, 100BASE-T4 100BASE-FX Fast Ethernet at 100 Mbps with Auto-Negotiation	X
IEEE 802.3X	Flow Control	X
IEEE 802.3Z	1000BASE-X Gigabit Ethernet over fiber optic at 1 Gbps	X
IEEE 802.3AD	LAG-MIB	X
IEEE 802.1Q	Virtual Bridged VLANs	X
IEEE 802.1D	MAC Bridges	X
IEEE 802.1W	Rapid Spanning Tree Protocol	X
IEEE 802.1S	Multiple Spanning Trees	X
IEEE 802.1AG	Connectivity Fault Management (CFM)	X
IEEE 8023.BA	100 Gigabit Ethernet	X
IEEE 802.1AB	Link Layer Discovery Protocol	X
IEEE 802.1X	Port-Based Network Access Control	X
IEEE 802.3AH	Ethernet in the First Mile Link OAM3	X
IEEE 8021	PAE-MIB	X
ITU-T G.8013/Y.1731	OAM mechanisms for Ethernet4	Y.1731 not supported for DM. SLM supported.
ITU-T G.8032	Ethernet Ring Protection	50ms protection switching not supported
MEF	MEF-SOAM-TC-MIB	X
MEF	MEF-SOAM-PM-MIB	X

Scalability for SLX 9740

Function	SLX 9740
LAYER 2 SWITCHING	
Number of Trunk Groups supported	77 groups for 1U(1 to 256 ID's) 153 groups for 2U(1 to 256ID's) Tested: 44 Groups
Number of Ports per Trunk Group	64
Maximum LACP Trunk threshold	64

Maximum number of MAC Addresses per Switch	600K(Default Profile)
	190K(Route Profile)

Jumbo Frames	9216 bytes
Number of VLANs	4096
Maximum number of Spanning-Tree instances (RSTP)	RSTP is 1 instance only, RPVST/PVST 128, MSTP 32
Maximum number of bridge domains	4K
RSTP	
Max Number of Spanning-Tree instances (RSTP)	1 (RSTP is always 1 instance)
Maximum Number of physical ports supported with STP/RSTP	Max number of front end ports
MSTP	
Maximum Number of instances	32
Maximum Number of VLANs per instance	4090
Maximum Number of physical interfaces participating per instance	Max number of front end ports
Maximum Number of LAG interfaces participating per instance	Max number of allowed LAG Tested: 44 PO's
PVST	
Maximum number of VLANS	126
Maximum number of interfaces	Max number of front end ports (PORTS X VLANS <=2K)
Maximum number of instance	126
Max number of port-vlan associations	2048
Multicast	
Maximum IGMPv2/v3 L3 entries	16K
L2 Multicast Cache	16K
IPv4 Software Multicast Cache for PIM/SM	20K
IPv4 Hardware Multicast Entries	20K
Maximum IGMP snooping vlans	500
Maximum IGMP snooping vlans (MCT)	500
Maximum static entry (IGMPv2) with uplink - IPv4	1000

Function	SLX 9740
Maximum static entry (IGMPv3) with uplink - IPv4	1000
Snoop Multicast IGMP Join rate per port	1000
Snoop Multicast IGMP leave rate per port	1000
IGMP Join rate (with PIM-SM)	4000
IGMP Leave rate (with PIM-SM)	4000
PIM SM Maximum local receivers (IGMP)	4000
PIM SM Maximum OIF's per system	64000
PIM SM Maximum OIF's per S,G	128
Maximum number of vlan replication per entry	128
Maximum number of multicast VRFs	50
Maximum number of IGMP groups per system	16K
Maximum number of IGMP groups per interface	128
Maximum number of IGMP OIF per system	8000
Maximum number of Mcast Prefix advertised by a RP	250
Maximum number of BSR RP per mcast domain	56 Tested: 4
Maximum number of Static RP per system	56 Tested: 4
Maximum number of RPset x RP per system	56 Tested: 4
Maximum number of PIM Anycast RPs per system	56 Tested: 4
Maximum number of Anycast RP peers per system	8 Tested: 4
PIM Fast Hello	Min Hello : 1 Sec, Neighbor Removal : 3 Sec
Multicast ECMP Paths	32
LAYER 3 FEATURES - IPv4	
Maximum number of IP interfaces per system (ipv4, ipv6)	8K
Maximum number of Virtual Ethernet interfaces per system	8K
Maximum number of ARP entries	Default Profile: 102k Route Profile: 95K
Maximum number of ND entries	Default Profile: 102k Route Profile: 95K
Maximum number of Static ARP	Default Profile: 102k Route Profile: 95K
Maximum ARP/ND Suppression Scale	8K
Maximum number of directly connected host routes (or IP Next-hops)	64K Tested: 52K
Number of possible secondary IP Addresses	255
Maximum number of Loopback interfaces	255
Maximum number of OSPF areas (Per VRF)	200
Number of OSPF routers in a single area	200
Number of OSPF adjacencies (per VRF)	200

Function	SLX 9740
Maximum Number of OSPF Routes	100K
Maximum Number of Static Route Entries	32K
Maximum BGP Peer-Groups	250
Maximum BGP Routes in RIB	9M IN, 14M OUT
BGP Peers (IPv4 and IPv6 concurrent)	2400
Maximum Number of IS-IS Routes	25K
Number of ISIS adjacencies	Broadcast : 255
	P2P : 1024
Number of ISIS LSPs	255
Maximum Number of IPv4 Routes	Default Profile: 2M Route Profile: 3.5M
Maximum VE per system	8K
Maximum VRFs per system (BGP VRF IPv4/IPv6)	1024
Maximum VRFs per system (OSPF VRF IPv4/IPv6)	1024
Maximum VRFs per system (Static VRF IPv4/IPv6)	1024
Number of ISIS routers in a level	255
Max Paths in ECMP Group	64
ECMP(Next Hop)	32K
Number of VRRP/VRRPe Instances per system (IPv4, IPv6)	1K
Number of VRRP instances per IP interface	10
Number of VRRP/VRRPe instances with Time Scale	128
Maximum Number of GRE Tunnels	1024
Maximum ISIS interfaces	Broadcast : 255
	P2P : 1024
PBR Over GRE	NA
ICMP Error Message handling	5000
LAYER 3 FEATURES - IPv6	
Maximum Number of IPv6 Static Route Entries	32K
Maximum Number of IPv6 Routes	Default Profile: 2M Route Profile: 3.5M
Maximum Number of OSPFv3 Routes	64K
Maximum Number of OSPFv3 Interfaces	256
Maximum Number of OSPFv3 Neighbors	256
Maximum Number of OSPFv3 area	10
Maximum Number of BGPv6 Routes in the RIB	Same as Ipv4
Maximum Number of BGPv6 Neighbors	2400
BGP Flow Spec	
Maximum Number of Local Flowspec rules alone *	1K
Maximum Number of Remote Flow spec rules alone *	1K

Function	SLX 9740
Maximum Number of Local and remote Flow spec rules together *	1K
BGP large-community	
Maximum number of Large-community that can be added/replaced/deleted for incoming route updates(NLRI) using set directive.	32
Maximum number large-community standard/extended Acl type	1024 rules per list. Max Seq # is 65535
Maximum number of large-community ACL that can be matched in route-map	32
Maximum no of large community attributes that be received per route update (including in bound set large community)	64
MPLS	
Maximum MPLS labels	15K
Maximum Label stacking depth	3
Maximum Target LDP sessions	100
Maximum ingress	5K
Maximum transit LSPs	20K cross-connects
MPLS Tunnels	5K
Maximum VLLs per system (with MCT)	500
Maximum VPLSs per system (with MCT)	8K
Maximum endpoints per VLL per system	1K
VPLS/VLL PW	8K
Load-Balanced PWs (out of 8k)	Default Profile: 3K Route Profile: 1K
Maximum endpoints per VPLS per system (non MCT, MCT)	20K
Maximum VPLS MACs per system (max vpls mac table)	Default Profile: 600K Route Profile: 190K
Total VPLS VC labels per system	8K
Maximum Routes per VRF/VPN	Default Profile: 2M Route Profile: 3M
Maximum MPLS VPNs (IPv4) per system	512
Maximum MPLS VPNs (IPv6) per system	512
Maximum Adaptive LSP (ingress/egress)	5k
Maximum FRR instances	5K Facility or 2K 1-to-1 detour
Maximum number of VPLS LSP load balance	16
Maximum number of LDP ECMP path	16
RSVP LSP History support	Max 32 events per LSP at Ingress router
Maximum number of Auto-bandwidth templates	100
Maximum number of recorded samples per Auto-	1500
Single-hop LSP Accounting	5K

Function	SLX 9740
Maximum number of VPLS instance with IPv4/IPv6 VE VRF support (MCT)	8K
Maximum number of Bypass LSP per system	512
Maximum number of LDP session	100
Maximum number of LDP FEC	5K
RATE LIMITING AND TRAFFIC POLICING FEATURES	
Granularity	22kbps
Number of Rate-limiters/Traffic-policers Per System	1k/32k
ACL	
Ingress Ipv4 ACLs (ACLs, PBR, RACL, RL, RACL-RL, v4Broadcast ACL) per system	4K
Ingress Ipv6 ACLs (ACLs, PBR, RL, RACL, RACL-RL)	2K
Ingress MAC ACL	2K
Egress L2 ACL	1K
Egress L3 ACL	1K
Named L2 ACL statements	2k
Maximum number of IP receive ACLs	200
Maximum number of IPv6 receive ACLs	50
Policy Based Routing (PBR)	4K
IPv6 PBR	2K
Max Number of configurable PBR route maps	200
Max Number of configurable stanzas in PBR	1024
MULTI-CHASSIS TRUNKING (MCT support)	
Number of vPorts – (# of VLANs) times (# of ports)	100K

Maximum MCT Clients	72(1U) (72 x 25G/10G+ 4x100G possibility)
	144(2U) (144*25G/10G + 8x100G possibility)

Maximum of VLANs for ICL	All vlans
Maximum number of L2 / unified bridging instances (VPLS/EVPN, L2, VXLAN) with MCT and BUM RL	4k
Maximum number endpoint in MCT for L2/bridging (VPLS, EVPN, L2, VXLAN)	Breakdown for each endpoint types *100K AC LIFs
MCT VPLS	*8K PW instances total
	*8K total VNI (including 4K for vlan and 4K for BD)
	*100K for all types of services.
MCT VLL	500
Maximum number of MAC addr for MCT	Default Profile: 256K Route Profile: 190K Tested: 250K
SOFTWARE DEFINED NETWORKING/OpenFlow	
Maximum number of Flows per system	N/A - Not supported

Function	SLX 9740
Maximum number of L2 Mode Flows	N/A - Not supported
Maximum number of L3 Mode Flows	N/A - Not supported
Maximum number of L23 Mode Flows	N/A - Not supported
Maximum number of Flows with multi-point modification	N/A - Not supported
Maximum number of L2, L3, L23 Mode Flows with Flow statistic	N/A - Not supported
Max number of controller connections	N/A - Not supported
Maximum Flows with Wildcard match	N/A - Not supported
Maximum Protected Vlans per Hybrid Port	N/A - Not supported
Maximum Protected Vlans per system	N/A - Not supported
OAM	
BFD min timer	200ms
Max BFD Sessions	250(16 Multihop Sessions)
802.1ag sessions	4000
Y.1731 SLM/DM sessions	NA
EVPN-VXLAN Scaling (IP Fabric)	
VxLAN Tunnel (e.g. ToR, DCI, hybrid cloud)	1K
L2 VNI	8K
L3 VNI	1024
Maximum # VRF	1024
Layer 2	
Maximum # of MAC entries	Default Profile: 600K non-MCT(256K MCT/EVPN) Route Profile: 190K
Layer 3	
Maximum # of BGP peers (IPv4+IPv6)	256 (V4 only)
Max # of BD VE	4K
SAG per switch	8K
SAG address per interface	64
BGP EVPN IPv4 and IPv6 route (HW) and (SW)	HW: 2M SW: 5M
BGP EVPN macIP routes (HW) and (SW)	HW: 102K ARP/102K ND SW: 2M
BGP EVPN mac routes (SW)	HW:250K SW: 2M
MVRP	
Maximum no. of dynamic VLANs advertised over MVRP (with/without MCT)	Not Supported
Maximum no. of MACs on DUT on 2K dynamic VLANs (with/without MCT)	Not Supported
QoS	
Maximum Number of Traffic Classes	8

Function	SLX 9740
On chip buffers per ASIC (shared between ingress and egress)	Ingress OCB: 16MB per core (32MB total) Ingress DRAM Buffer: 8GB Egress OCB: 48MB per core (96MB total)
Max schedulers on SYSTEM	40
Max Shapers on System	40
POLICY-MAP MAX config on SYSTEM (Created in SW globally)	1K
CLASS-MAP MAX config per policy	4K
POLICY-MAP MAX config per interface	1
SERVICE-POLICY - per interface	1 per direction
CLASS-MAP MAX config on SYSTEM (Created in SW globally)	32k
DEFAULT CLASS-MAP per POLICY	1
MATCH ACL CLASS-MAP per POLICY	4k non default class map per policymap
PORT-BASED IN service-policy on SYSTEM	no of ports supported
MATCH ACL CLASS IN service-policy on SYSTEM	4K non default-class map per policy-map
PORT-BASED OUT service-policy on SYSTEM	no of ports supported
STORM-CONTROL (BUM traffic policy)	3
Maximum number of ACL table per CLASS	1
Number of Policers(HW supported)	16K
Maximum unique RED profiles configured (SW)	256
Maximum unique RED profiles configured (HW)	256
PCP->TC, DSCP->TC	400, 400
DSCP->DSCP	400
DSCP-> CoS, TC-> CoS	400, 1
TC->DSCP	NA
Maximum per-port priority pause level	Not Supported
QoS priority queues (per port)	8
SNMP	
Maximum communities	256
Maximum contexts	256
Maximum community maps	256
Maximum SNMP v3 users	10

Function	SLX 9740
Maximum groups	10
Maximum views	10
Maximum v1/v2c trap hosts	12
Maximum v3 trap hosts	6

Hardware Support

Supported devices and software license

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

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

Supported optics and cables

For a complete list of all supported optics for the SLX 9740, see **Extreme Optics** at optics.extremenetworks.com.

Software Download and Upgrade

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

Image file names

Download the following images from www.extremenetworks.com.

Image file name	Description
slxos20.2.1.tar.gz	SLX-OS 20.2.1 software
slxos20.2.1_all_mibs.tar.gz	SLX-OS 20.2.1 MIBS
slxos20.2.1.md5	SLX-OS 20.2.1 md5 checksum
slxos-20.2.1-releasenotes.pdf	Release Notes

SLX 9540 and SLX 9640

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

Notes:

- From the 18r.1.00x and 18r.2.00a patches and earlier, you must upgrade to 18r.2.00bx and then to 20.2.1, 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 moved to baremetal mode in 20.2.1, "fullinstall" must be used to migrate between the SLX-OS 20.2.1 and SLX-OS 20.1.1 releases.
- Also, downgrade from 20.2.1 to 20.1.1 requires fullinstall option for all platforms due to a change in glibc.

SLX 9150 and SLX 9250

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

Limitations and Restrictions

Known limitations for SLX 9740

- FEC mode is enabled by default on the 100G.
    - There is a restricted CLI to disable FEC mode for LR4 optics on an interface.
    - FEC mode disabled option will not be preserved across reloads.
    - When the peer side FEC mode is Disabled, on 9740 the links come up due to auto-neg.
    - When the peer side FEC mode is configured as RS-FEC, the links do not come up automatically. You must configure FEC mode as RS-FEC explicitly on 9740.
- FEC mode display issues for all platforms.
- PM (Port Macro) restriction on breakout port configuration:
    - A 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.
    - For any PM, 40g and 10g ports cannot coexist with 25g ports. The following configurations are not supported:
        - If any port in a PM is configured as 40g or 4x10g breakout, no 4x25g breakout is allowed in the PM unless the 40g ports will be removed as part of the breakout operation.
          Example:.
          Example: If 0/3 or 0/4 is 40g, you cannot configure 0/1 as 4x25g breakout.
          Example: If 0/1 is 4x10g breakout, you cannot configure 0/3 as 4x25g breakout.
          Example: If 0/3 is 4x10g breakout, you cannot configure 0/1 as 4x25g breakout.
          Example: 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.
          Example: 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 in a PM, no 40g or 4x10g is allowed in the PM.
          Example: If 0/1 is configured as 4x25g breakout, you cannot configure 0/3 or 0/4 as 40g.
          Example: If 0/1 is configured as 4x25g breakout, you cannot configure 0/3 as 4x10g breakout.
          Example: If 0/3 is configured as 4x25g breakout, you cannot configure 0/1 or 0/2 as 40g.
          Example: If 0/3 is configured as 4x25g breakout, you cannot configure 0/1 as 4x10g breakout.

    - Ports 5-8, 45-48 cannot be broken up, and only can be supported in 100G.
- Breakout port: Dynamic breakout ports may not work in some configurations.
- Increased CPU usage in steady state.
- Layer 3 fragmentation not supported. Layer 3 MTU is not checked on egress interfaces.
- Sflow is not supported on PO and PO member ports.
- Mirroring is not supported if the source is a PO member port.
- PCP remarking is not supported on 9740.

IPF Border Leaf and IXP

- Border Leaf and IXP use cases are not fully qualified.

Open Defects

Parent Defect ID:	SLXOS-45417	**Issue ID:**	SLXOS-45417
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	"show interface ethernet 0/x" CLI does not show updated (if any) FEC oper data but always show DISABLED.		
Condition:	If any "fec mode <newvalue>" is updated, it may not be updated correctly in the display.		

Parent Defect ID:	SLXOS-49200	**Issue ID:**	SLXOS-49200
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	IP Addressing
Symptom:	When L3 port-channel is deleted, bcm error message"hslagt_lif_brcm_create_lag_lif: bcm_vlan_port_create failed" is printed on console. There is no functionality issue.		
Condition:	When L3 port-channel is deleted.		

Parent Defect ID:	SLXOS-49524	**Issue ID:**	SLXOS-49524
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-49863	**Issue ID:**	SLXOS-49863
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD session over L2 Port-channel flaps once on SLX-9740-80C device.		
Condition:	When the primary member port of a Port-channel is shutdown.		

Parent Defect ID:	SLXOS-49992	**Issue ID:**	SLXOS-49992
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Routing traffic with L3 port-channel interface as the Nexthop interface gets black holed.		
Condition:	After removal followed by immediate addition of IPv4 address from L3 port-channel interface, Routing traffic with this L3 port-channel interface as the Nexthop interface, will get dropped.		
Workaround:	'clear ip bgp neighbor all' should resolve the problem		

Parent Defect ID:	SLXOS-50277	**Issue ID:**	SLXOS-50277
Severity:	S2 - High		

Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	OSPF protocol may flap when over-subscribed traffic is send to PO.		
Condition:	When more than 10G traffic is sent to PO with one 10G member port.		

Parent Defect ID:	SLXOS-50386	**Issue ID:**	SLXOS-50386
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Monitoring	**Technology:**	sFlow
Symptom:	Under specific conditions sflow samples might not carry Extended gateway data (BGP source AS, destination AS, and BGP next hop information)		
Condition:	sflow sampling is configured. BGP routing is also configured and BGP learned routes are installed in FIB. After a BGP peer flap and all the BGP learned routes in FIB are removed and re-installed. Sflow samples after the BGP peer flap might not have extended gateway data.		

Parent Defect ID:	SLXOS-50747	**Issue ID:**	SLXOS-50747
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Layer 2 Switching	**Technology:**	UDLD - Uni-Directional Link Detection
Symptom:	UDLD sessions don't get established		
Condition:	UDLD when enabled is not converging on SLX-9150/9250 platforms		

Parent Defect ID:	SLXOS-51137	**Issue ID:**	SLXOS-51137
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1

Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	DSCP to Traffic Class QoS Map applied in L3 Port-Channel does not work as expected.		
Condition:	This feature stops working after the system-reload.		
Workaround:	After the reload, remove the DSCP-TC QOS map on L3 Port-Channel and re-apply the same.		

Parent Defect ID:	SLXOS-51177	**Issue ID:**	SLXOS-51177
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Management	**Technology:**	NTP - Network Time Protocol
Symptom:	NTP packets switches from source IP to inband IP after 1 hour		
Condition:	COPP ACL bocks NTP response on scaled setup with lot of VE interfaces where route addition/deletion happens frequently.		
Workaround:	Avoid applying COPP ACL for long time like 1 hour or avoid adding/deleting routes very frequently.		

Parent Defect ID:	SLXOS-51210	**Issue ID:**	SLXOS-51210
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Traffic Management	**Technology:**	Rate Limiting and Shaping
Symptom:	TM Port shaper is not working as expected when shaper is configured on interface, traffic will not be rate-limited.		
Condition:	TM Port shaper is not working as expected when shaper is configured on interface.		

Parent Defect ID:	SLXOS-51256	**Issue ID:**	SLXOS-51256
Severity:	S2 - High		

Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	MBGP - Multiprotocol Border Gateway Protocol
Symptom:	Under certain conditions SLX might reload unexpectedly		
Condition:	BGP routing is enabled and configured with multiple peering sessions which learn/advertise routes from/to these peering sessions. Clear action is performed for all BGP peering sessions at the same time using SLX CLI command "clear ip bgp neighbor all soft out" or "clear ip bgp neighbor all"		

Parent Defect ID:	SLXOS-51264	**Issue ID:**	SLXOS-51264
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	IP Multicast	**Technology:**	IGMP - Internet Group Management Protocol
Symptom:	Traffic loss can be seen on the hosts attached to one or more leaf nodes which are interested and subscribed for the IGMP multicast group.		
Condition:	1. The Optimized replication feature should be enabled. 2. When Multicast Distribution Tree (MDT) for a group is not formed through same Spine. 3. Generally seen when link between Leaf and Spine is down OR PIM neighbor-ship is down OR PIM RPF towards source VTEP is different Spine when compared to other leaf nodes.		
Workaround:	Make sure that all leaf nodes are electing the same spine node for a given Multicast Distribution Tree. Make sure that PIM RPF for source VTEP is elected towards the same spine on all the leaf nodes.		

Parent Defect ID:	SLXOS-51384	**Issue ID:**	SLXOS-51384
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1

Technology Group:	Security	**Technology:**	DoS (Denial of Service) protection
Symptom:	ICMP-Type match based Control Plane Policing does not work.		
Condition:	An equivalent rule is created as RACL which matches the same packets and counter is enabled on that RACL rule.		
Workaround:	Disable the counters on RACL rule that matches the packets.		

Parent Defect ID:	SLXOS-51420	**Issue ID:**	SLXOS-51420
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD sessions may flap.		
Condition:	Start OSPF graceful-restart via "clear ipv6 ospf graceful" CLI.		

Parent Defect ID:	SLXOS-51469	**Issue ID:**	SLXOS-51469
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	Unexpected reload of system with BFD enabled in certain scenarios		
Condition:	Loopback interface flap may sometimes cause the issue.		

Parent Defect ID:	SLXOS-51486	**Issue ID:**	SLXOS-51486
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Other	**Technology:**	Other
Symptom:	DNS with source interface configuration is not working.		

Condition:	This issue occurs only when source interface is configured with DNS
Workaround:	Not to configure source interface with DNS since without source interface DNS is working as expected.

Parent Defect ID:	SLXOS-51494	**Issue ID:**	SLXOS-51494
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	Traffic-Class-CoS Map applied on one egress interface may effect all the ports.		
Condition:	Create Traffic-Class-CoS Map and apply on an egress interface.		

Parent Defect ID:	SLXOS-51547	**Issue ID:**	SLXOS-51547
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD Sessions may flap.		
Condition:	Number of BFD multihop session count exceeds 16.		

Parent Defect ID:	SLXOS-51569	**Issue ID:**	SLXOS-51569
Severity:	S2 - High		
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-51587	**Issue ID:**	SLXOS-51587
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	DSCP to CoS map does not work as expected.		
Condition:	Configure a DSCP-CoS map and apply it on VE interface. Traffic routed to this VE interface, egressing packets do not match CoS as configure in the Map.		

Parent Defect ID:	SLXOS-51776	**Issue ID:**	SLXOS-51776
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Security	**Technology:**	ACLs - Access Control Lists
Symptom:	512 cam entries are supported for egress Ipv4 ACL. ACL will not take effect if ACLs are applied after 512 cam entries are utilized.		
Condition:	If more than 512 cam entries for egress IPv4 ACL are used.		

Parent Defect ID:	SLXOS-51793	**Issue ID:**	SLXOS-51793
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Traffic Management	**Technology:**	Rate Limiting and Shaping
Symptom:	Storm control action not happening on Port channel interface		
Condition:	Apply storm control rate limit on the Port-channel. It is seen from the storm control output that the rate limit is happening and violation		

	counters are incrementing, but the mentioned action is not taking place(shutdown/monitor)

Parent Defect ID:	SLXOS-51794	**Issue ID:**	SLXOS-51794
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	VOQ Stats not incrementing for priority traffic class.		
Condition:	When TM VOQ cmd "show tm voq-stat" is executed.		

Parent Defect ID:	SLXOS-51804	**Issue ID:**	SLXOS-51804
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.2.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	VRRPv3 - Virtual Router Redundancy Protocol Version 3
Symptom:	Maximum number of VRRP sessions that are allowed to be configured are 255 in 9740, 9640 and 9540		
Condition:	When configuring more than 255 VRRP sessions.		

Defects Closed with Code Changes

Parent Defect ID:	SLXOS-29054	**Issue ID:**	SLXOS-29054
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.2.00
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	IS-IS - IPv4 Intermediate System to Intermediate System
Symptom:	In a scaled environment of IS-IS adjacency, User may observer IS-IS adjacency may not come up		

Condition:	User may observe this in a scaled system when IS-IS configuration is removed from an interface and enabled on a different interface when maximum IS-IS adjacency scale is reached
Workaround:	No

Parent Defect ID:	SLXOS-40489	**Issue ID:**	SLXOS-40489
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Network Automation and Orchestration	**Technology:**	NETCONF - Network Configuration Protocol
Symptom:	Few unwanted keypaths will be noticed in the output of the NETCONF RPC get-last-config-update-time.		
Condition:	User executed the NETCONF RPC get-last-config-update-time.		

Parent Defect ID:	SLXOS-44135	**Issue ID:**	SLXOS-44135
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	BUM traffic may be flooded back to source interface on one of the port-channel intermittently upon shut/no shut of CCEP interface on SLX 9640 Cluster nodes		
Condition:	BUM traffic may be flooded back to source interface on one of the port-channel intermittently upon shut/no shut of CCEP interface on SLX9640 Cluster nodes		

Parent Defect ID:	SLXOS-44598	**Issue ID:**	SLXOS-44598
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	VLAN - Virtual LAN

Symptom:	Possible VPLS packet corruption when untagged VE interface used as MPLS underlay interface on SLX 9540/9640 platform
Condition:	Following are the condition for the VPLS packet corruption. •Physical port configured as trunk-no-default-native, Bind with single untagged VLAN and one or more tagged VLANs •MPLS VE interface (used as underlay for VPLS traffic) created over the untagged VLAN configured on the physical port With the above configuration, Removing any of the tagged VLAN from the physical port will cause the problem.
Workaround:	Avoiding removing VLAN from a physical interface, when an untagged VLAN bound to the same interface with a MPLS VE interface configured over it.

Parent Defect ID:	SLXOS-45286	**Issue ID:**	SLXOS-45286
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	show cluster client-pw cli throws error “%Error: Client-pw not configured.” when client-pw config is not done.		
Condition:	when client-pw config is not configured and user tries to execute show cluster client-pw command. It will throw error “%Error: Client-pw not configured.”		
Workaround:	user need to make sure client-pw is configured under cluster before executing this cli.		

Parent Defect ID:	SLXOS-45483	**Issue ID:**	SLXOS-45483
Severity:	S4 - Low		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	'show ip igmp groups cluster' and 'show cluster client' CLIs throwing error instead of blank output		
Condition:	CLI Display commands to show IGMP groups on MCT cluster		

Workaround:	Returned correct code from backend

Parent Defect ID:	SLXOS-45564	**Issue ID:**	SLXOS-45564
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	IP Multicast	**Technology:**	Other
Symptom:	Traffic loss is seen on the host connected on a CEP port. The corresponding PIM OIFs of MCT peers will be entering the PIM Assert state. The receiver ports connected to Assert looser node will see the traffic loss.		
Condition:	When PIM SG-RPT prune is received on CCEP port and there are no other ports learnt as part of that PIM Snooping (S,G) entry, the issue can be seen.		

Parent Defect ID:	SLXOS-45626	**Issue ID:**	SLXOS-45626
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	The CLI for Peer IP under cluster configuration does not perform error checks and accepts any IP address like broadcast/multicast		
Condition:	Configuration of MCT Peer IP address accepts any IP address		

Parent Defect ID:	SLXOS-45953	**Issue ID:**	SLXOS-45953
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Thousands of mac across 100s of lifs are moving rapidly causing LIFs to be shut (mac-move-detect), a few macs might go out of sync with the network and traffic would flood for those destinations.		

Condition:	Traffic destined to missing macs will be flooded
Workaround:	clear mac address which is out of sync

Parent Defect ID:	SLXOS-46439	**Issue ID:**	SLXOS-46439
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	'Insight enable' configuration goes missing from Insight PO after fullinstall OR when the configuration is copied from file to running configuration on SLX9640 & SLX9540		
Condition:	When full-install is done or when configuration from the file is copied to running configuration with insight PO configured		
Workaround:	No		

Parent Defect ID:	SLXOS-46483	**Issue ID:**	SLXOS-46483
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	BFD IPv6 Session may flap and bring down associated clients sessions on scale setup on SLX9640/SLX9540 platforms		
Condition:	If user issues, Link/admin down the IPv6 interface which has more than 40K IPv6 routes associated with it, it may cause BFD flaps on these platforms		

Parent Defect ID:	SLXOS-47149	**Issue ID:**	SLXOS-47149
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	Under specific circumstances the "show ip dhcp snooping binding entries" command will not show any dhcp snooping binding entries.		
Condition:	Currently dhcp snooping entries are written to flash every 5 min. In case there are changes to any interface followed by reboot within 5 min, this change will not be persisted to flash. Post reboot, there could be some stale interface entry in the binding database while reading from flash. This will result in the "show ip dhcp snooping binding entries" not displaying any entries.		

Parent Defect ID:	SLXOS-47168	**Issue ID:**	SLXOS-47168
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Management	**Technology:**	Licensing
Symptom:	When license add command is used with the options FTP-URL or SCP-URL and if the operation fails, the TACACS+ account logs wrongly display the operation as Success.		
Condition:	Issue is seen only when license add command is issued with the FTP-URL or SCP-URL option and the operation fails for valid reasons (ex: invalid file path). license add using 'licStr' option results in the correct Accounting log.		
Workaround:	Ignore the operation status in the TACACS+ accounting logs when license add is done using FTP-URL or SCP-URL options (or) add/remove license via 'licStr' option instead of using the FTP-URL or SCP-URL options.		

Parent Defect ID:	SLXOS-47221	**Issue ID:**	SLXOS-47221
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking

Symptom:	In IPfabric configured node, the CCL type mac address are displayed as CCR type mac address until the mac address age out on the remote MCT peer node.
Condition:	When "shut" and "no shut" performed on one of the MCT cluster CCEP interface, the CCL mac address traffic stream moved from the peer MCT node to the local MCT node shows as CCR type until the macs are aged out on the peer node.

Parent Defect ID:	SLXOS-47247	**Issue ID:**	SLXOS-47247
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	In configuration mode, under 'router pim', 'route-precedence' has three arguments, 'none' , 'uc-default' and 'uc-non-default'. These three arguments must be assigned priority(1-3). By default 'none' has priority-3, 'uc-default' has priority-2 and 'uc-non-default' has priority-1. While configuring each of the arguments must be provided with one priority.		
Condition:	The error occurs when one argument is set to multiple priorities or vice-versa. E.g: SLX(config-router-pim-vrf-default-vrf)# route-precedence uc-default priority-1 <<<<< 'uc-default' has priority-2 by default, now assigning violates one to one relation between the arguments and priority. % Error: Invalid route precedence priority. The correct way to assign values: SLX(config-router-pim-vrf-default-vrf)# route-precedence uc-default priority-1 uc-non-default priority-2		

Parent Defect ID:	SLXOS-47272	**Issue ID:**	SLXOS-47272
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service

Symptom:	Wred profile scale on SLX-9150 /SLX 9250 platform is 32
Condition:	Wred profile configuration more than 32 will not work

Parent Defect ID:	SLXOS-47361	**Issue ID:**	SLXOS-47361
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	IP Multicast	**Technology:**	IGMP - Internet Group Management Protocol
Symptom:	System shows IGMPv2 entries when Host is configured in IGMP version-3. So IGMP version-2 entries are shown as part of "show ip multicast snooping mcache"		
Condition:	When a VLAN is upgraded to IGMP version-3 and Host is already configured to send IGMP version-3 reports, the issue can be seen.		
Workaround:	None		

Parent Defect ID:	SLXOS-47575	**Issue ID:**	SLXOS-47575
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	IPv6 BFD Session received Tx and Rx Timer interval will not get updated with new value on SLX 9540 & SLX 9640 platform		
Condition:	Issue is observed when user configure IPv6 BFD sessions		

Parent Defect ID:	SLXOS-47577	**Issue ID:**	SLXOS-47577
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Incorrect CLI help string is shown for the bridge domain CLI configuration command		
Condition:	While executing bridge domain configuration CLI for add and remove commands under EVPN instance		
Workaround:	No		

Parent Defect ID:	SLXOS-47578	**Issue ID:**	SLXOS-47578
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Traffic Management	**Technology:**	QoS - Quality of Service
Symptom:	Traffic running with 800G with 128B pkt size will see throughput of ~95.125%		
Condition:	Traffic running with 800G with 128B pkt size will see drops.		

Parent Defect ID:	SLXOS-47592	**Issue ID:**	SLXOS-47592
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Management	**Technology:**	NTP - Network Time Protocol
Symptom:	When trusted key is deleted a remote authenticated peer will continue to sync until the server DUT in which trusted key was deleted is rebooted.		
Condition:	When a DUT is synced with an auth key to an SLX as NTP server that adds the remote peer's auth key as trusted key		

Parent Defect ID:	SLXOS-47652	**Issue ID:**	SLXOS-47652
Severity:	S2 - High		

Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	MAC/ARP/ND can go out of sync between the two MCT nodes. This would impact traffic destined to these hosts.		
Condition:	As part of heavy triggers - in this case "no member vlan all + no member bridge-domain all" and config the same back again while traffic is running. When we remove member-vlan/member-bd, the client ports move from CCEP to CEP. Traffic causes us to learn mac/arp/nd during that window. When member vlan/bd is configured back again, depending on scale and timing, few entries might get out of sync.		
Workaround:	bring down the cluster/clients using "shutdown all or shutdown clients" before doing cluster management operations.		

Parent Defect ID:	SLXOS-47698	**Issue ID:**	SLXOS-47698
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	In a certain scenario, Flapping the ICL interface brings back the MCT session even when the cluster is shutdown		
Condition:	After a 'shutdown all' on cluster, a 'shutdown' followed by 'no shutdown' on the ICL interface brings up the MCT session up		
Workaround:	Perform 'no shutdown all' and then 'shutdown all' on cluster		

Parent Defect ID:	SLXOS-47714	**Issue ID:**	SLXOS-47714
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	On SLX 9540/ SLX 9640, ARP-Suppression status will be displayed as “Enabled” and ARP packets will be trapped to CPU, when the VE		

	associated to the VLAN (ARP Suppression enabled) is Administratively Down
Condition:	VE which is Administratively Down is binded to a VLAN which is ARP Suppression enabled and ARP packets are received on that VLAN.
Workaround:	Disable ARP Suppression configuration from the Vlan. No functional impact, as ARP-Suppression is applicable only for Vlan's that have a VE which is operationally UP.

Parent Defect ID:	SLXOS-47782	**Issue ID:**	SLXOS-47782
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Traffic Management	**Technology:**	Traffic Queueing and Scheduling
Symptom:	clear tm voq-stat slot-id 0 cpu-group all may not clear the voq-stats.		
Condition:	User executed "clear tm voq-stat slot-id 0 cpu-group all" command		
Workaround:	None		

Parent Defect ID:	SLXOS-47800	**Issue ID:**	SLXOS-47800
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	LAG - Link Aggregation Group
Symptom:	Local Port-channel shutdown will not result in peer Port-channel down immediately. LAG will be made down after LACP timeout.		
Condition:	On execution of 'shutdown' command on L3 Port-channel, all members of Port-channel goes down on local system, but at peer side link-down is not detected for some links.		
Workaround:	Shutdown port-channel member links also along with port-channel.		

Parent Defect ID:	SLXOS-47803	**Issue ID:**	SLXOS-47803
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 on configuring NTP server		
Condition:	When the clock is updated there is a jump in time, MCT assumes that the hold timer has expired if the system time moves beyond the hold timer.		
Workaround:	Configure NTP before MCT bringup		

Parent Defect ID:	SLXOS-47823	**Issue ID:**	SLXOS-47823
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	ARP - Address Resolution Protocol
Symptom:	sh ip arp suppression-statistics" & "sh ipv6 nd suppression-statistics" returns no output in some scenarios		
Condition:	sh ip arp suppression-statistics" & "sh ipv6 nd suppression-statistics" returns no output in some scenarios		
Workaround:	none		

Parent Defect ID:	SLXOS-48598	**Issue ID:**	SLXOS-48598
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.2
Technology Group:	IP Multicast	**Technology:**	IPv4 Multicast Routing
Symptom:	Traffic loss in L3 Multicast MCT scenario.		
Condition:	In Multicast MCT scenario, where the MCT nodes act as both First Hop & Last Hop router with Source connected to one CCEP switch, Vlan & Receivers on another CCEP switch, Vlan. PIM mcahe route OIFs might start Assert mechanism and go into Blocked state with triggers like Firmware upgrade or CCEP Port-		

	channel Up/Down events. This leads to traffic loss for few (S,G) entries.

Parent Defect ID:	SLXOS-49326	**Issue ID:**	SLXOS-49326
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.2
Technology Group:	IP Multicast	**Technology:**	IGMP - Internet Group Management Protocol
Symptom:	In Multicast MCT deployment scenario where IGMP & PIM snooping are enabled on both the MCT nodes, if IGMP Join report & PIM Join message are received simultaneously on one of the MCT nodes for given (S, G) or (*, G) on given VLAN/VE followed by a PIM prune & IGMP leave message then a stale entry for this route is left in the remote MCT node's IGMP cluster database causing extra/duplicate traffic.		
Condition:	In Multicast MCT deployment scenario where IGMP & PIM snooping are enabled on both the MCT nodes, CCEP/CEP configured as L2 switch connected to a PIM router or configured as PIM router, If IGMP Join report & PIM Join are received simultaneously on a MCT node for a given (*, G) or (S, G) on a given Vlan/VE and one of the CCEP ports or any CEP port then these (*, G) or (S, G) info along with the IGMP/PIM states is synced to the peer MCT node. Now if PIM prune is received first on the local MCT node for this (*, G) or (S, G), route sync delete is sent to the peer MCT node. However, the peer MCT node does not delete the route, but unchecks the PIM state only. Later, if IGMP leave is received on the local MCT node, a route delete cannot be sent (as it was already deleted from the transporting MCT module earlier); thus leaving a stale entry for (*, G) or (S, G) for given Vlan on the remote MCT peer node. This stale entry may cause extra/duplicate traffic and also multicast traffic flooding where expected may not happen as well depending on the deployment and configuration.		
Workaround:	"clear ip igmp group cluster" on the remote MCT node where the stale entries are present will flush and relearn all the routes.		

Parent Defect ID:	SLXOS-50055	**Issue ID:**	SLXOS-50055
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.2
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	VRRPv2 - Virtual Router Redundancy Protocol Version 2
Symptom:	For VRRP and VRRPe, the configuration CLI to change the advertisement interval value is rejected by the system and hence it will work with default value of 1 second.		
Condition:	User will observe this behavior only with CLI to change the advertisement-interval on VRRP/VRRPe protocol and rest of VRRP and VRRPe config CLI should work as desired.		

Parent Defect ID:	SLXOS-50164	**Issue ID:**	SLXOS-50878
Severity:	S2 - High		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.2
Technology Group:	Layer 2 Switching	**Technology:**	LAG - Link Aggregation Group
Symptom:	In MCT deployments, user may occasionally observe traffic loss of more than a second when CCEP Port-channel is disabled by executing CLI shut command on port-channel interface.		
Condition:	Disabling of the CCEP Port-channel on any one of the Cluster node using CLI shut command, will result in traffic loss. Issue is not seen when the link of physical member-port of Port-Channel goes down or member-ports are disabled using CLI.		
Workaround:	Disable all Port-channel member interfaces using range command instead of disabling Port-channel directly.		

Parent Defect ID:	SLXOS-49266	**Issue ID:**	SLXOS-51313
Severity:	S4 - Low		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.2
Technology Group:	Management	**Technology:**	CLI - Command Line Interface

Symptom:	If operational command "system maintenance turn-off" returns error on CLI the status of the command reflects as success on TACACS server.
Condition:	The issue is seen on execution of operational command "system maintenance turn-off" and switch has TACACS server configured.
Workaround:	No

Parent Defect ID:	SLXOS-50890	**Issue ID:**	SLXOS-51318
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.2a
Technology Group:	Security	**Technology:**	AAA - Authentication, Authorization, and Accounting
Symptom:	The 'admin-pwd' for the TPVM is displayed in clear text in the accounting log when configured through 'tpvm deploy'.		
Condition:	tpvm admin password is set as part of the command line argument in the 'tpvm deploy', user will observe the password in clear text in account log		
Workaround:	'tpvm password' command can be used as an alternative to set the password.		

Parent Defect ID:	SLXOS-50148	**Issue ID:**	SLXOS-51457
Severity:	S3 - Medium		
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.2
Technology Group:	Security	**Technology:**	TACACS & TACACS+
Symptom:	Error messages which are captured while doing tpvm configurations using the "tpvm config" command are not getting recorded under Account log.		
Condition:	The issue is observed when the "tpvm config" commands fails due to following issues: 1. Maximum server limit reached. 2. Trying to remove certificates when secure servers are configured. 3. Trying to remove a configuration that doesn't exist.		

	4. Trying to add an already existing configuration. 5. Failure in importing the certificates.

Defects Closed without Code Changes

Parent Defect ID:	SLXOS-22336	**Issue ID:**	SLXOS-22336
Reason Code:	Third Party Issue	**Severity:**	S3 - Medium
Product:	SLX-OS	**Reported in Release:**	SLXOS 17r.2.00
Technology Group:	Security	**Technology:**	ACLs - Access Control Lists
Symptom:	For "mac access-list" rules, providing 'count' option only works if provided before 'copy-sflow', 'mirror' and 'log' option.		
Condition:	Occurs when configuring rules under mac access list		
Workaround:	Workaround is to provide 'count' option before 'copy-sflow', 'mirror' and 'log' options.		

Parent Defect ID:	SLXOS-25106	**Issue ID:**	SLXOS-25106
Reason Code:	Third Party Issue	**Severity:**	S4 - Low
Product:	SLX-OS	**Reported in Release:**	SLXOS 18r.1.00
Technology Group:	Management	**Technology:**	Configuration Fundamentals
Symptom:	Minor cosmetic issue in help. When user enters '?' or '<TAB>' after command 'ip access-list extended <acl-name>', help does not show '<cr>'. The command works as expected if user hits '<ENTER>'. Issue is only with help string.		
Condition:	When using IP ACL.		

Parent Defect ID:	SLXOS-41318	**Issue ID:**	SLXOS-41318
Reason Code:	Working as Designed	**Severity:**	S2 - High
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Security	**Technology:**	SSH - Secure Shell
Symptom:	In TACACS+ accounting log, the session is identified as a Pseudo tty (ex:/dev/pts/1) for commands executed via SSH/Telnet sessions.		
Condition:	This issue is always seen in the Accounting logs for SSH/Telnet sessions.		

Workaround:	Interpret the “/dev/pts/<number>” as SSH/Telnet session in the accounting logs.

Parent Defect ID:	SLXOS-41800	**Issue ID:**	SLXOS-41800
Reason Code:	Cannot Fix	**Severity:**	S3 - Medium
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Management	**Technology:**	CLI - Command Line Interface
Symptom:	The command "aaa authentication login tacacs+ local" conflicts with " aaa authentication login tacacs+ local-auth-fallback" and thus, pressing tab doesn't render the help text defined under "tailf:info" in the yang model.		
Condition:	write in cli configuration mode, aaa authentication login tacacs+ local or aaa authentication login tacacs+ local-auth-fallback and press 'tab'		
Workaround:	.		

Parent Defect ID:	SLXOS-43539	**Issue ID:**	SLXOS-43539
Reason Code:	Not Reproducible	**Severity:**	S2 - High
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Management	**Technology:**	Other
Symptom:	copy config command times out with error.		
Condition:	When copy config command is used with IPv6 address along with TFTP protocol only.		
Workaround:	Issue is not observed when copy command is used with IPv6 address along with ftp/scp/sftp protocols.		

Parent Defect ID:	SLXOS-43576	**Issue ID:**	SLXOS-43576
Reason Code:	Working as Designed	**Severity:**	S3 - Medium
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	VLAN - Virtual LAN

Symptom:	Customer would get error thrown on the screen when a bridge domain ID is exceeded
Condition:	Bridge domain ID beyond the supported range can be given by the user
Workaround:	Reduce the scale

Parent Defect ID:	SLXOS-44276	**Issue ID:**	SLXOS-44276
Reason Code:	Already Reported	**Severity:**	S3 - Medium
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	IP Addressing
Symptom:	Message "cannot find ve interface" may be thrown on the console with scaled Ve interface config.		
Condition:	This issue can be seen with scaled Ve config, i.e when more than 1K Ves are created and configuration is saved and reloaded.		
Workaround:	none		

Parent Defect ID:	SLXOS-44337	**Issue ID:**	SLXOS-44337
Reason Code:	Already Reported	**Severity:**	S2 - High
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	Other
Symptom:	In scale route-map scenario , show running-config route-map <route-map-name> command doesn't fetch the specified route-map information		
Condition:	Issue is observed if "to" keyword is part of route-map name		
Workaround:	use any one of below commands : show running-config show running-config route-map | begin <route-map-name> show running-config route-map		

Parent Defect ID:	SLXOS-45020	**Issue ID:**	SLXOS-45020
Reason Code:	Feature/Function Not Supported	**Severity:**	S3 - Medium
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1

Technology Group:	Management	**Technology:**	Other
Symptom:	When user issue tpvm deploy or tpvm password command on SLX9540 , "block nbd0: Receive control failed" messages will display on the console		
Condition:	Issue tpvm deploy or tpvm password command on 9540		
Workaround:	N/A.		

Parent Defect ID:	SLXOS-46623	**Issue ID:**	SLXOS-46623
Reason Code:	Not Reproducible	**Severity:**	S2 - High
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Security	**Technology:**	DoS (Denial of Service) protection
Symptom:	Egress RL will not work as expected if QOS flow control is enabled.		
Condition:	When QOS flow control is enabled, egress RL will affect Rx and Tx traffic		
Workaround:	Workaround: Turn of the TX or disable QOS flow control.		

Parent Defect ID:	SLXOS-47184	**Issue ID:**	SLXOS-47184
Reason Code:	Not Reproducible	**Severity:**	S2 - High
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Executing certain disruptive triggers on a switch with scaled VLAN/MAC configuration will result in few seconds of traffic loss. Issue is rarely observed and not seen in recent releases		
Condition:	When the switch is configured with 4K VLANs and more than 40k MAC's, if user executes the command "clear mac dynamic", traffic loss will be observed for few seconds		

Parent Defect ID:	SLXOS-47363	**Issue ID:**	SLXOS-47363
Reason Code:	Insufficient Information	**Severity:**	S2 - High
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	IP Multicast	**Technology:**	IGMP - Internet Group Management Protocol

Symptom:	System does not show the IGMP version-3 entries for "show ip multicast snooping mcache" for around 100 seconds.
Condition:	If a host(Traffic Generator) is configured to send IGMP version-3 reports. Then IGMP version is upgraded to version-3 on a VLAN (connected to the host) which is acting as a querier.

Parent Defect ID:	SLXOS-47392	**Issue ID:**	SLXOS-47392
Reason Code:	Not Reproducible	**Severity:**	S2 - High
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:	VRRP error message will be displayed on the console and experiencing traffic forwarding issue only for the failed VSI		
Condition:	While deletion and addition of MCT cluster peer when the system is configured with 500 or more VRRP/E sessions.		
Workaround:	No		

Parent Defect ID:	SLXOS-47417	**Issue ID:**	SLXOS-47417
Reason Code:	Not Reproducible	**Severity:**	S2 - High
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Other	**Technology:**	Other
Symptom:	If user configured VLAN,BD and Tunnel scale goes beyond 8k , then we don’t get VLAN statistics for the LIF scale beyond 8k VLAN statistics continue to work for scale below 8k		
Condition:	If user configured VLAN,BD and Tunnel scale goes beyond 8k , then we don’t get VLAN statistics for the LIF scale beyond 8k VLAN statistics continue to work for scale below 8k		

Parent Defect ID:	SLXOS-47438	**Issue ID:**	SLXOS-47438
Reason Code:	Feature/Function Not Supported	**Severity:**	S2 - High
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1

Technology Group:	Layer 3 Routing/Network Layer	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	In MCT cluster topology, when cluster shutdown all is performed one of the MCT nodes, traffic drop of 19 secs is observed from host to CCEP client.		
Condition:	In MCT cluster topology, OSPF must be configured between MCT peers, MCT peer and CCEP client, MCT peers and host on another end forming ECMP paths towards CCEP Client. Cluster shutdown all must be performed on one of the MCT nodes.		
Workaround:	Before performing cluster shutdown, first bring down the link between MCT peer and CCEP client.		

Parent Defect ID:	SLXOS-47524	**Issue ID:**	SLXOS-47524
Reason Code:	Insufficient Information	**Severity:**	S2 - High
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Other	**Technology:**	Other
Symptom:	ZTP operation to boot up with an image that is already installed on SLX does not fail		
Condition:	ZTP is initiated with same image as the one installed and specified in the ztp.conf file		
Workaround:	Remove or comment out "fwdir" field from ztp.conf file.		

Parent Defect ID:	SLXOS-47641	**Issue ID:**	SLXOS-47641
Reason Code:	Configuration/User Error	**Severity:**	S2 - High
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	LAG - Link Aggregation Group
Symptom:	LAG will be down but LAG member interface stats will still showtraffic egressing.		
Condition:	When min-link is configured more than already UP LAG member, min-link is not affective		
Workaround:	configure min-link before binging UP LAG and LAG member links		

Parent Defect ID:	SLXOS-47701	**Issue ID:**	SLXOS-47701

Reason Code:	Insufficient Information	**Severity:**	S2 - High
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Other	**Technology:**	Other
Symptom:	During a firmware upgrade with fullinstall option, under rare timing conditions, few ports may not come up		
Condition:	The issue will be seen only during firmware upgrade with fullinstall option. Issue is not seen without fullinstall option		

Parent Defect ID:	SLXOS-47756	**Issue ID:**	SLXOS-47756
Reason Code:	Will Not Fix	**Severity:**	S2 - High
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	**Technology:**	VXLAN - Virtual Extensible LAN
Symptom:	Some of the L2VNI traffic is forwarded on the ICL link		
Condition:	1. Scaled config with 64 Vxlan tunnels and 25K mac's 2. L2VNI, Symmetric, and Asymmetric traffic 3. Delete and add the cluster config		

Parent Defect ID:	SLXOS-49879	**Issue ID:**	SLXOS-49879
Reason Code:	Cannot Fix	**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:	User will observe BFD flaps in some specific deployments when BFD session running over CEP interface, changes its path due to change in active/standby interface of remote server such that new path is over ICL and vice versa		
Condition:	BFD session flaps if the nexthop to the BFD neighbor moves from CEP interface to MCT ICL interface and vice versa.		

Parent Defect ID:	SLXOS-49323	**Issue ID:**	SLXOS-51314
Reason Code:	Working as Designed	**Severity:**	S2 - High
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.2
Technology Group:	Other	**Technology:**	Other

Symptom:	ON SLX 9540, While applying rate limiting, user might observe that for CPU destined traffic with TTL0/TTL1 , rate limiting is not precise. For a rate limiting of ~40Kbps, it might rate limit to ~40-120Kbps.
Condition:	on SLX 9540, Issue is observed only for CPU bound traffic (for packet whose TTL reaches 0 or 1),above symptom are observed when rate-limiting is applied on this specific traffic

Parent Defect ID:	SLXOS-50280	**Issue ID:**	SLXOS-51325
Reason Code:	Will Not Fix	**Severity:**	S2 - High
Product:	SLX-OS	**Reported in Release:**	SLXOS 20.1.2
Technology Group:	Layer 2 Switching	**Technology:**	Other
Symptom:	When system is stressed with frequent disruptive user driven operations, Interface flap is observed on the MCT ICL port-channel.		
Condition:	In a Scaled up MCT deployment when maintenance mode is enable and disable operations are performed in quick succession in a loop, user might observe link flap		
Workaround:	Issue could be avoid by giving a time gap of 30-40 second for such operations in medium scaled setup.		

Parent Defect ID:	SLXOS-28694	**Issue ID:**	SLXOS-51442
Reason Code:	Already Implemented	**Severity:**	S4 - Low
Product:	SLX-OS	**Reported in Release:**	SLXOS 17r.2.01
Technology Group:	Monitoring	**Technology:**	Hardware Monitoring
Symptom:	The output of "show media" command shows wrong calculation for Aggregate TX power. This issue do not have any impact to functionality.		
Condition:	The user issues the command "show media".		