June 2020

Extreme SLX-OS 20.1.2a Release Notes

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

9036654-00 Rev AA

© 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

Document History

Version	Summary of changes	Publication date
1.0	Initial version for 20.1.2a	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

SLX-OS 20.1.2a is a software-only release that targets data center use cases on the SLX 9150 and 9250 platforms. A few platform-independent features, such as the auto-persistence of SLX-OS configurations, are available on all the supported platforms: 9150, 9250, 9540, and 9640.

This release focuses on the following:

- Extending manageability and data center capabilities
- Extending BFD support for more use cases: static route, VxLAN, and MCT
- Improving scale and convergence numbers on the SLX 9250 platform for key strategic customer engagements
- Enhancing the user experience
- Qualifying newer optics
- Security enhancements

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.
Centralized routing (BGP EVPN SAG MAC)	• SAG MAC advertised by BGP-EVPN with "sticky Bit community" (in previous releases it was advertised with "Gateway community") • BGP-EVPN allows installing SAG MAC on a remote node to support "Centralized Routing Feature" (in previous release BGP-EVPN did not support installing SAG MAC)
FEC	Support for SLX 9640 and SLX 9540: • FEC was disabled on these platforms in SLX-OS 20.1.1 • CLI is enabled in 20.1.2a Behavior changes on SLX 9640 and SLX 9540: • RS-FEC: Supported on 100G interfaces only • FC-FEC: Supported on 25G/4x25G interfaces • Auto-neg: Based on media inserted • Disabled: FEC is disabled or removes FEC configurations on interfaces
TPVM	• TPVM default login changed to "extreme/password", earlier it was "admin/password" • Ubuntu 16.04 LTS to 18.04 LTS (no behavior change) • TPVM uses ifupdown rather than netplan (no behavior change to end user) • TPVM DNS uses resolver rather than system-resolved (no behavior change to end user)

Software Features

The following key software features are added in the SLX-OS 20.1.2a release.

Feature Name	Supported SLX Platforms	Description
Redundant Management Interface	9250	Provides fault tolerance for the Management path
Auto-persist configuration	9150, 9250, 9540, 9640	Allows any successfully executed configuration through any management interface (CLI, REST, NETCONF) to be automatically made persistent. This enables dynamic provisioning use cases.
Data Consistency- using Maintenance mode feature	9150, 9250	Ensures that SLX switches provisioned through EFA always have the right configuration and are synchronized with EFA before it starts to receive or forward traffic
Centralized Routing	9150, 9250	A deployment solution where all tenant routing-related Layer 3 configuration is enabled only on Border Leaves in an IP Fabric deployment. The other Leaf nodes perform Layer 2 switching only. This contrasts with a Distributed Routing solution, where in Layer 3 is enabled on all the Leaf nodes.
BGP Listen range	9150, 9250	Helps to simplify BGP neighbor configuration by consolidating the relevant config into few lines.
BFD on static route	9150, 9250	Extends BFD support for static routes to provide faster detection of failure in the forwarding path between the BFD peers, including interface and data links failures. Supports single- and multi-hop sessions.
BFD on VxLAN with MCT	9150, 9250	BFD is supported over VxLAN endpoints with MCT in the environment.
Default route behavior	9150, 9250	Allows routes reachable through default route to be installed in the route table.
Security Enhancements	9150, 9250	Following changes have been added: • HTTPS and SSH x509v3 host key and certificate import via PKCS#12 file format. • AAA: Added support for OAuth2 tokens in SSH, NETCONF, and RESTCONF using the **aaa authentication login oauth2** command • LDAP client packaged with TPVM (third party VM) on SLXSLX CLIs to set and show LDAP, NTP, and DNS on TPVM • New TPVM 4.0.0 based on Ubuntu 18.04.4 with 5.3 HWE kernel • Default TPVM login changed to “extreme/password” • Audit Log Enhancements

Feature Name	Supported SLX Platforms	Description
IP Fabric scale and convergence	9250	• Higher IP Fabric scale for static anycast gateway (SAG) instances, BFD sessions in hardware for IPv4 and IPv6. • Faster convergence for MCT operations.
Cluster-track	9150, 9250, 9540, 9640	This feature helps reduce convergence for planned reload cases by diverting traffic to alternate paths. The cluster tracked ports are brought down along with MCT clients especially in maintenance mode or cluster 'shutdown all ' cases for faster convergence.

CLI Commands

New commands

Exec mode commands:

- show tpvm config ldap
- show tpvm config ntp
- show tpvm config dns
- tpvm config ldap add {host <IPv4/v6/FQDN> [port <1-65535>] [secure] | [basedn <string>] [rootdn <string>] [rootdnpw <string>] [host <IPv4/v6/FQDN>] [port <1-65535>] [secure]}
- tpvm config ldap remove {host <IPv4/v6/FQDN> [port] [secure] | [basedn] [rootdn] [rootdnpw]}
- tpvm config ldap ca-cert import protocol <SCP> host <IPv4/v6/FQDN> user <string> password <string> directory <string> filename <string>
- tpvm config ldap ca-cert remove
- tpvm config ntp add server <IPv4/v6/FQDN>
- tpvm config ntp remove server <IPv4/v6/FQDN>
- tpvm config ntp default
- tpvm config dns add dns-server <IPv4>, [<IPv4>] [domain-name <string>]
- tpvm config dns remove
- clear {ip|ipv6} bgp neighbor dynamic [all] [vrf <vrf-name>]
- clear ip bgp {vpnv4|vpnv6} neighbor dynamic all
- clear bgp {ip|ipv6} flowspec neighbor dynamic

Configuration commands:

- system maintenance
  - [no] enable-on-reboot
- Interface ethernet 0/x
  - [no] redundant-management enable
  - [no] cluster-track
- Router bgp
  - [no] listen-limit [1-255]

    - [no] listen-range {<ipv4 prefix>|<ipv6 prefix>} peer-group <name> [limit <1-255>
    - [no] neighbor <peer-group-name> alternate-as {add|remove} <as-range>,[<as-range>, ….]
- af-ipv6-ucast-vrf:
    - [no] listen-range <Ipv6-Network/Length> peer-group <name> [limit <1-255>]

Modified commands

Modified options are highlighted.

- [no] crypto ca import-pkcs type pkcs12 cert-type [https | ssh-x509v3]
- [no] crypto import oauth2pkicert
- [no] aaa authentication login oauth2 [local | local-auth-fallback]

Removed commands

- show startup-database

RFCs, Standards, and Scalability

RFC Compliance

General Protocols

RFC number	RFC Name	SLX 9150	SLX9250	SLX 9640	SLX 9540
RFC 768	User Datagram Protocol (UDP)	X	X	X	X
RFC 791	Internet Protocol (IP)	X	X	X	X
RFC 792	Internet Control Message Protocol (ICMP)	X	X	X	X
RFC 793	Transmission Control Protocol (TCP)	X	X	X	X
RFC 826	ARP	X	X	X	X
RFC 894	IP over Ethernet	X	X	X	X
RFC 903	RARP	X	X	X	X
RFC 906	TFTP Bootstrap	X	X	X	X
RFC 950	Subnet	X	X	X	X
RFC 951	BootP	X	X	X	X
RFC 1027	Proxy ARP	X	X	X	X
RFC 1042	Standard for The Transmission of IP	X	X	X	X
RFC 1166	Internet Numbers	X	X	X	X
RFC 1122	Requirements for Internet Hosts	X	X	X	X
RFC 1191	Path MTU Discovery	X	X	X	X
RFC 3232	Assigned Numbers	X	X	X	X
RFC 4632	Classless Interdomain Routing (CIDR)	X	X	X	X
RFC 1542	BootP Extensions	X	X	X	X
RFC 1591	DNS (client)	X	X	X	X

RFC number	RFC Name	SLX 9150	SLX9250	SLX 9640	SLX 9540
RFC 2819	RMON Groups 1, 2, 3, 9	X	X	X	X
RFC 1812	Requirements for IP Version 4 Routers	X	X	X	X
RFC 1858	Security Considerations for IP Fragment Filtering	X	X	X	X
RFC 2131	BootP/DHCP Helper	X	X	X	X
RFC 2784	Generic Routing Encapsulation (GRE)	Not Supported	Not supported	X	X
RFC 3021	Using 31-Bit Prefixes on IPv4 Point-to- Point Links	X	X	X	X
RFC 3046	DHCP Relay Agent Information Option	X	X	X	X
RFC 3527	Link Selection Sub Option for the Relay Agent Information Option for DHCPv4	X	X	X	X
RFC 3768	Virtual Router Redundancy Protocol (VRRP)	X	X	X	X
RFC 4001	INET-ADDRESS-MIB	X	X	X	X
RFC 5880	Bidirectional Forwarding Detection	X	X	X	X
RFC 5881	Bidirectional Forwarding Detection for IPv4 and IPv6 (Single Hop)	X	X	X	X
RFC 5882	Generic Application of Bidirectional Forwarding Detection	X	X	X	X
RFC 5883	Bidirectional Forwarding Detection for Multihop Paths	X	X	X	X

BGPv4

RFC Number	RFC Name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
RFC 1745	OSPF Interactions	X	X	X	X
RFC 1772	Application of BGP in the Internet	X	X	X	X
RFC 1997	Communities and Attributes	X	X	X	X
RFC 2385	BGP Session Protection via TCP MD5	X	X	X	X
RFC 2439	Route Flap Dampening	X	X	X	X
RFC 2918	Route Refresh Capability	X	X	X	X
RFC 3392	Capability Advertisement	X	X	X	X
RFC 3682	Generalized TT L Security Mechanism for eBGP Session Protection	X	X	X	X
RFC 4271	BGPv4	X	X	X	X

RFC Number	RFC Name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
RFC 4364	BGP/MPLS IP Virtual Private Networks	Not Supported	Not supported	X	X
RFC 4456	Route Reflection	X	X	X	X
RFC 4486	Sub codes for BGP Cease Notification Message	X	X	X	X
RFC 4724	Graceful Restart Mechanism for BGP	X	X	X	X
RFC 6198	Requirements for the Graceful Shutdown of BGP sessions	X	X	X	X
RFC 8326	Graceful BGP Session Shutdown	X	X	X	X
RFC 6793	BGP Support for Four-octet AS Number Space	X	X	X	X
RFC 5065	BGP4 Confederations	X	X	X	X
RFC 5291	Outbound Route Filtering Capability for BGP-4	X	X	X	X
RFC 5396	Textual Representation of Autonomous System (AS) Numbers	X	X	X	X
RFC 5668	4-Octet AS specific BGP Extended Community	X	X	X	X
Draft-ietf-rtgwg-bgp-pic-07.txt BGP Prefix Independent Convergence		X		X	X
RFC 5575	Dissemination of Flow Specification Rules (BGP Flow Spec)	X	X	X	X
RFC 8092	BGP Large Community Attribute	X	X	X	X
sFlow BGP AS path		X	X	X	X

Element Security

RFC Number	RFC Name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
AAA		X	X	X	X
Username/Password (Challenge and Response)		X	X	X	X
Bi-level Access Mode (Standard and EXEC Level)		X	X	X	X
Role-based Access Control (RBAC)		X	X	X	X
RFC 2865	RADIUS	X	X	X	X
RFC 2866	RADIUS Accounting	X	X	X	X
RFC 3162	RADIUS and IPv6	X	X	X	X
RFC 6613	RADIUS over TCP	X	X	X	X
RFC 6614	Transport Layer Security (TLS) Encryption for RADIUS	X	X	X	X

RFC Number	RFC Name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
TACACS/TACACS+		X	X	X	X
RFC 4510 thru 4519	LDAP	X	X	X	X
RFC 4510 thru 4519	LDAP over TLS	X	X	X	X
RFC 6749, 7515, 7519	OAuth2 - JSON Web Token (JWT)	X	X	X	X
RFC 5905	NTP Version 4	X	X	X	X
RFC 3986	Uniform Resource Identifier (URI): Generic Syntax	X	X	X	X
RFC 6241	NETCONF Configuration Protocol (Partial)	X	X	X	X
RFC 4742	"Using the NETCONF Configuration Protocol over Secure Shell (SSH)"	X	X	X	X
RFC 6020	"YANG – A Data Modeling Language for the Network Configuration Protocol (NETCONF)"	X	X	X	X
RFC 6021	"Common YANG Data Types"	X	X	X	X
NTP client and NTP server		X	X	X	X
RFC 5961	TCP Security	X	X	X	X
RFC 4251	Secure Shell (SSH) Protocol Architecture	X	X	X	X
RFC 4253	Secure Shell (SSH)	X	X	X	X
RFC 4346	TLS 1.1	X	X	X	X
RFC 5246	TLS 1.2	X	X	X	X
RFC 5280	Internet X.509 PKI Certificates	X	X	X	X
RFC 6960	Internet X.509 PKI OCSP				
Protection against Denial of Service (DoS) attacks such as TCP SYN or Smurf Attacks		X	X	X	X

OSPF

RFC Number	RFC Name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
RFC 1745	OSPF Interactions	X	X	X	X
RFC 1765	OSPF Database Overflow	X	X	X	X
RFC 2328	OSPF v2	X	X	X	X
RFC 3101	OSPF NSSA	X	X	X	X
RFC 3137	OSPF Stub Router Advertisement	X	X	X	X
RFC 3623	Graceful OSPF Restart	X	X	X	X
RFC 3630	TE Extensions to OSPF v2	N/A	N/A	X	X

RFC 4222	Prioritized Treatment of Specific OSPF Version 2	X	X	X	X
RFC 5250	OSPF Opaque LSA Option	X	X	X	X
RFC 5709	OSPFv2 HMAC-SHA Cryptographic Authentication	X	X	X	X
RFC 7166	Supporting Authentication Trailer for OSPFv3	X	X	X	X
RFC 7474	Security Extension for OSPFv2 When Using Manual Key Management	X	X	X	X

IS-IS

RFC Number	RFC Name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
RFC 1142	OSI IS-IS Intra-domain Routing Protocol	X	X	X	X
RFC 1195	Routing in TCP/IP and Dual Environments	X	X	X	X
RFC 3277	IS-IS Blackhole Avoidance	X	X	X	X
RFC 5120	IS-IS Multi-Topology Support	X	X	X	X
RFC 5301	Dynamic Host Name Exchange	X	X	X	X
RFC 5302	Domain-wide Prefix Distribution	X	X	X	X
RFC 5303	Three-Way Handshake for IS-IS Point-to-Point	X	X	X	X
RFC 5304	IS-IS Cryptographic Authentication (MD-5)	X	X	X	X
RFC 5306	Restart Signaling for ISIS (helper mode)	X	X	X	X
RFC 5309	Point-to-point operation over LAN in link state routing protocol	X	X	X	X

IPv4 Multicast

RFC Number	RFC Name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
RFC 1112	IGMP v1	X	X	X	X
RFC 2236	IGMP v2	X	X	X	X
RFC 3376	IGMP v3	X	X	X	X
RFC 4601	PIM-SM	X	X	X	X
RFC 4607	PIM-SSM	X	X	X	X
RFC 4610	Anycast RP using PIM	X	X	X	X
RFC 5059	BSR for PIM	X	X	X	X
PIM IPv4 MCT		X	X	X	X

Quality of Service (QoS)

RFC Number	RFC Name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
RFC 2474	DiffServ Definition	X	X	X	X
RFC 2475	An Architecture for Differentiated Services	X	X	X	X
RFC 2597	Assured Forwarding PHB Group	X	X	X	X
RFC 2697	Single Rate Three-Color Marker	X	X	X	X
RFC 2698	A Two-Rate Three-Color Marker	X	X	X	X
RFC 3246	An Expedited Forwarding PHB	X	X	X	X

IPv6 Core

RFC Number	RFC Name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
RFC 1887	IPv6 unicast address allocation architecture	X	X	X	X
RFC 1981	IPv6 Path MTU Discovery	X	X	X	X
RFC 8201	IPv6 Path MTU Discovery	X	X	X	X
RFC 2375	IPv6 Multicast Address Assignments	X	X	X	X
RFC 2450	Proposed TLA and NLA Assignment Rules	X	X	X	X
RFC 2460	IPv6 Specification	X	X	X	X
RFC 8200	IPv6 Specification	X	X	X	X
RFC 4861	IPv6 Neighbor Discovery	X	X	X	X
RFC 4862	IPv6 Stateless Address Auto-configuration	X	X	X	X
RFC 2464	Transmission of IPv6 over Ethernet Networks	X	X	X	X
RFC 2471	IPv6 Testing Address allocation	X	X	X	X
RFC 3701	IPv6 Testing Address allocation	X	X	X	X
RFC 2711	IPv6 Router Alert Option	X	X	X	X
RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	X	X	X	X
RFC 3587	IPv6 Global Unicast Address Format	X	X	X	X
RFC 4193	Unique Local IPv6 Unicast Addresses	X	X	X	X
RFC 4291	IPv6 Addressing architecture	X	X	X	X
RFC 4301	IP Security Architecture	X	X	X	X
RFC 4303	Encapsulating Security Payload (ESP)	X	X	X	X

RFC Number	RFC Name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
RFC 4305	ESP and AH cryptography	X	X	X	X
RFC 4443	ICMPv6	X	X	X	X
RFC 4552	Auth for OSPFv3 using AH/ESP	X	X	X	X
RFC 4835	Cryptographic Alg. Req. for ESP	X	X	X	X
RFC 4861	Neighbor Discovery for IP version 6 (IPv6)	X	X	X	X
RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	X	X	X	X

IPv6 Routing

RFC Number	RFC Name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
RFC 5340	OSPFv3 for IPv6	X	X	X	X
RFC 5308	Routing IPv6 with IS-IS	X	X	X	X
RFC 2545	Use of BGP-MP for IPv6	X	X	X	X
RFC 8106	Support for IPv6 Router Advertisements with DNS Attributes	X	X	X	X
RFC 6164	Using 127-Bit IPv6 Prefixes on Inter-Router Links	X	X	X	X

MPLS

RFC Number	RFC Name	SLX 9150/9250	SLX 9640	SLX 9540
RFC 2205	RSVP v1 Functional Specification	N/A	X	X
RFC 2209	RSVP v1 Message Processing Rules	N/A	X	X
RFC 2674	P-BRIDGE-MIB	N/A	X	X
RFC 2702	TE over MPLS	N/A	X	X
RFC 2961	RSVP Refresh Overhead Reduction Extensions	N/A	X	X
RFC 3031	MPLS Architecture	N/A	X	X
RFC 3032	MPLS Label Stack Encoding	N/A	X	X
RFC 3037	LDP Applicability	N/A	X	X
RFC 3097	RSVP Cryptographic Authentication	N/A	X	X
RFC 3209	RSVP-TE	N/A	X	X
RFC 3478	LDP Graceful Restart	N/A	X	X
RFC 3813	MPLS-LSR-STD-MIB	N/A	X	X
RFC 3815	MPLS-LDP-STD-MIB MPLS-LDP-GENERIC-STD-MIB	N/A	X	X
RFC 4090	Fast Re-Route for RSVP-TE for LSP Tunnels; partial support	N/A	X	X
RFC 4379	OAM	N/A	X	X
RFC 4448	Encapsulation Methods for Transport of Ethernet over MPLS Networks	N/A	X	X

RFC 5036	LDP Specification	N/A	X	X
RFC 5305	ISIS-TE	N/A	X	X
RFC 5443	LDP IGP Synchronization	N/A	X	X
RFC 5561	LDP Capabilities	N/A	X	X
RFC 5712	MPLS traffic Engineering Soft Preemption	N/A	X	X
RFC 5918	LDP "Typed Wildcard" FEC	N/A	X	X
RFC 5919	Signaling LDP Label Advertisement Completion	N/A	X	X

Layer 2 VPN and Pseudowire Emulation Edge to Edge PWE3

RFC Number	RFC Name	SLX 9150/9250	SLX 9640	SLX 9540
RFC 3343	TTL Processing in MPLS Networks	N/A	X	X
RFC 3985	Pseudowire Emulation Edge to Edge (PWE3) Architecture	N/A	X	X
RFC 4265	VPN-TC-STD-MIB	N/A	X	X
RFC 4364	BGP/MPLS IP Virtual Private Networks4	N/A	X	X
RFC 4447	Pseudowire Setup and Maintenance using LDP	N/A	X	X
RFC 4448	Encapsulation Methods for Transport of Ethernet Frames Over IP/MPLS Networks	N/A	X	X
RFC 4664	Framework for Layer 2 Virtual Private Networks	N/A	X	X
RFC 4665	Service Requirements for Layer 2 Provider- Provisioned Virtual Private Networks	N/A	X	X
RFC 4762	Virtual Private LAN Service (VPLS) Using LDP Signaling	N/A	X	X
RFC 5542	PW-TC-STD-MIB	N/A	X	X
RFC 5601	IANA-PWE3-MIB PW-STD-MIB	N/A	X	X
RFC 6391	Flow-Aware Transport of Pseudowires	N/A	X	X
RFC 6870	PW Preferential Forwarding Status Bit3	N/A	X	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	X	X
RFC 8365	A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN) (partial)	X	X	X
draft-sd-l2vpn-evpn-overlay-03		x	X	x

RFC Number	RFC Name	SLX 9150/9250	SLX 9640	SLX 9540
draft-ietf-bess-evpn-prefix-advertisement-11		X	X	x

Manageability and Visibility

RFC Number	RFC Name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
Integrated industry-standard Command Line Interface (CLI)		X	X	X	X
RFC 854	Telnet	X	X	X	X
RFC 1573	IANAifType-MIB	X	X	X	X
RFC 2068	HTTP	X	X	X	X
RFC 2571	SNMP-FRAMEWORK-MIB	X	X	X	X
RFC 2572	SNMP-MPD-MIB	X	X	X	X
RFC 2573	SNMP-TARGET-MIB SNMP-NOTIFICATION-MIB	X	X	X	X
RFC 2574	SNMP-USER-BASED-SM-MIB	X	X	X	X
RFC 2575	SNMP-VIEW-BASED-ACM-MIB	X	X	X	X
RFC 2576	SNMP-COMMUNITY-MIB	X	X	X	X
RFC 2818	HTTPS	X	X	X	X
RFC 2665	Ethernet Interface MIB	X	X	X	X
RFC 2677	IANA-ADDRESS-FAMILY-NUMBERS-MIB	X	X	X	X
IANA ifType-MIB [https://www.iana.org/assignments/ianaiftype-mip/ianaiftype-mib		X	X	X	X
RFC 2790	HOST-RESOURCES-MIB	X	X	X	X
RFC 2856	HCNUM-TC	X	X	X	X
RFC 2863	IF-MIB	X	X	X	X
RFC 2932	IANA-RTPROTO-MIB	X	X	X	X
RFC 3176	sFlow	X	X	X	X
sFlow extension to VXLAN		X		X	X
RFC 3273	RMON2-MIB	X	X	X	X
RFC 3289	DIFFSERV-DSCP-TC INTEGRATED-SERVICES-MIB DIFFSERV-MIB	X	X	X	X
RFC 3418	SNMPv2-MIB	X	X	X	X
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	X	X	X	X
RFC 3419	TRANSPORT-ADDRESS-MIB	X	X	X	X
RFC 3593	PerfHist-TC-MIB	X	X	X	X
RFC 3705	HC-PerfHist-TC-MIB	X	X	X	X
sFLow Version 5 and sFLow VxLAN extensions		X	X	X	X
Secure Copy (SCP v2) SFTP		X	X	X	X
SFTP		X	X	X	X

RFC Number	RFC Name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
RFC 8040	RESTCONF Protocol – PATCH, PUT, POST, DELETE support	X	X	X	X
RFC 4022	TCP-MIB	X	X	X	X
RFC 4087	IP Tunnel MIB	X	X	X	X
RFC 4113	UDP-MIB	X	X	X	X
RFC 4133	Entity MIB	X	X	X	X
RFC 4253	Secure Shell (SSH)	X	X	X	X
RFC 4254	Secure Shell (SSH) Connection Protocol	X	X	X	X
RFC 4344	SSH Transport Layer Encryption Modes	X	X	X	X
RFC 4419	Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol	X	X	X	X
RFC 6187	X.509v3 Certificates for Secure Shell Authentication	X	X	X	X
draft-ietf-secsh-filexfer-13.txt SSH File Transfer Protocol (SFTP)		X	X	X	X
Secure Copy (SCP v2)		X	X	X	X
RFC 4293	IP MIB	X	X	X	X
RFC 4741	NETCONF (Partial)	X	X	X	X
Chrome		X	X	X	X
Curl		X	X	X	X
Tcpdump		X	X	X	X
Wireshark		X	X	X	X
SNMP v1/v2c/v3		X	X	X	X
RFC 1157	Simple Network Management Protocol	X	X	X	X
RFC 1908	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework	X	X	X	X
RFC 2578	Structure of Management Information Version 2	X	X	X	X
RFC 2579	Textual Conventions for SMIv2	X	X	X	X
RFC 2580	Conformance Statements for SMIv2	X	X	X	X
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework	X	X	X	X
RFC 3411	An Architecture for Describing SNMP Management Frameworks	X	X	X	X
RFC 3412	Message Processing and Dispatching	X	X	X	X
RFC 3413	SNMP Applications	X	X	X	X

RFC Number	RFC Name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
RFC 3414	User-based Security Model	X	X	X	X
RFC 3415	View-based Access Control Model	X	X	X	X
RFC 3416	Version 2 of SNMP Protocol Operations	X	X	X	X
RFC 3417	Transport Mappings	X	X	X	X
RFC 2819	RMON Groups 1, 2, 3, 9	X	X	X	X
IEEE8021-PAE-MIB		X	X	X	X
IEEE802 LLDP MIB		X	X	X	X
IEEE8023-LAGMIB		X	X	X	X
RFC 1213	MIB-II	X	X	X	X
RFC 4292	IP-FORWARD-MIB	X	X	X	X
RFC 4188	BRIDGE-MIB	X	X	X	X
RFC 4750	OSPF-MIB	X	X	X	X
RFC 5643	OSPFv3 MIB	X	X	X	X
RFC 4363	Q-BRIDGE-MIB	X	X	X	X
RFC 3635	EtherLike-MIB	X	X	X	X
RFC 3811	MPLS TC STD MIB	N/A	N/A	X	X
RFC 3812	MPLS-TE-STD-MIB	N/A	N/A	X	X
RFC 3813	MPLS-LSR-STD-MIB	N/A	N/A	X	X
RFC 3826	SNMP-USM-AES MIB	X	X	X	X
RFC 4273	BGP4-MIB	X	X	X	X
draft-ietf-idr-bgp4-mibv2-15	BGP4v2 Draft 15 MIB	X	X	X	X
RFC 4318	RSTP-MIB	X	X	X	X
RFC 4444	ISIS-MIB	X	X	X	X
RFC 4878	DOT3-OAM-MIB	X	X	X	X
RFC 7257	VPLS-GENERIC-MIB VPLS-LDP-MIB VPLS-BGP-MIB	X	X	X	X
RFC 7330	BFD-TC-STD-MIB IANA-BFD-TC-STD-MIB	X	X	X	X
RFC 7331	BFD-STD-MIB	X	X	X	X

SLX-OS IEEE Standards Compliance

IEEE standard number	IEEE standard name	SLX 9150	SLX 9250	SLX 9640	SLX 9540
IEEE Std 802.1AB-2005	LLDP-MIB LLDP-EXT-DOT1-MIB LLDP-EXT-DOT3-MIB	X	X	X	X
IEEE P802.1AG D8.1	IEEE8021-CFM-MIB	X	X	X	X
IEEE 802.1AP	IEEE8021-CFM-V2-MIB	X	X	X	X
IEEE 802.3-2005	CSMA/CD Access Method and Physical Layer Specifications	X	X	X	X
IEEE 802.3AB	1000BASE-T	X	X	X	X
IEEE 802.3AE	10G Ethernet	X	X	X	X
IEEE 802.3U	100BASE-TX, 100BASE-T4 100BASE-FX Fast Ethernet at 100 Mbps with Auto-Negotiation	X	X	X	X
IEEE 802.3X	Flow Control	X	X	X	X
IEEE 802.3Z	1000BASE-X Gigabit Ethernet over fiber optic at 1 Gbps	X	X	X	X
IEEE 802.3AD	LAG-MIB	X	X	X	X
IEEE 802.1Q	Virtual Bridged VLANs	X	X	X	X
IEEE 802.1D	MAC Bridges	X	X	X	X
IEEE 802.1W	Rapid Spanning Tree Protocol	X	X	X	X
IEEE 802.1S	Multiple Spanning Trees	X	X	X	X
IEEE 802.1AG	Connectivity Fault Management (CFM)	No Support	No Support	X	X
IEEE 8023.BA	100 Gigabit Ethernet	X	X	X	X
IEEE 802.1AB	Link Layer Discovery Protocol	X	X	X	X
IEEE 802.1X	Port-Based Network Access Control	X	X	X	X
IEEE 802.3AH	Ethernet in the First Mile Link OAM3	No Support	No Support	X	X
IEEE 8021	PAE-MIB	X	X	X	X
ITU-T G.8013/Y.1731	OAM mechanisms for Ethernet4	No Support	No Support	X	X
ITU-T G.8032	Ethernet Ring Protection	No Support	No Support	X	X
MEF	MEF-SOAM-TC-MIB	X	X	X	X
MEF	MEF-SOAM-PM-MIB	X	X	X	X

Scalability

		SLX 9150	SLX 9250
LAYER 2 SWITCHING			
	Number of Trunk Groups supported	Default profile - 80 groups(1 to 256 ID's)	Default profile - 128 groups(1 to 256 ID's)
	Number of Ports per Trunk Group	64	64
	Max LACP Trunk threshold	64	64
LAYER 2 SWITCHING			
	max. number of MAC Addresses per Switch	64K	64K
	Jumbo Frames	9216 bytes	9216 bytes
	Number of VLANs	4K	4K
	Max number of bridge domains	4K	4K
	Maximum Number of port-vlan associations	15.5K	15.5K
RSTP	Max Number of Spanning-Tree instances (RSTP)	RSTP is 1 instance only,	RSTP is 1 instance only,
	Maximum Number of physical ports supported with STP/RSTP	Equal to max number of front-end ports	Equal to max number of front-end ports
MSTP	Maximum Number of instances	32	32
	Maximum Number of VLANs per instance	4090	4090
	Maximum Number of physical interfaces participating per instance	Equal to max number of front-end ports	Equal to max number of front-end ports
	Maximum Number of LAG interfaces participating per instance	64	128
PVST	Maximum number of VLANS	254	254
	Maximum number of interfaces	Equal to max number of front-end ports	Equal to max number of front-end ports
	Maximum number of instances	254	254
	Max number of port-vlan associations	2032	2032
MULTICAST			
	IPv4 Software Multicast Cache for PIM/SM	8k	8K

		SLX 9150	SLX 9250
	IPv4 Hardware Multicast Entries	8K	8K
	Max (IGMP/MLD) snooping vlans	512	512
	Max (IGMP/MLD) snooping vlans (MCT)	512	512
	Max static entry (IGMPv2 and MLDv1) with uplink - IPv4	8K	8K
	Snoop Multicast IGMP Join rate per port	500/s	500/s
	Snoop Multicast IGMP leave rate per port	500/s	500/s
	PIM SM Max OIF's per system	15.5K(Max VLAN-Port Combination)	15.5K(Max VLAN-Port Combination)
	PIM SM Max OIF's per entry	128	128
	PIM Join/Prune Rate	1500/s	1500/s
	Max number of vlan replication per entry	128	128
	Max number of multicast VRFs	50	50
	Max number of IGMP/MLD groups per interface	No Restriction	No Restriction
	Max number of IGMP/MLD OIF per entry	128	128
	Max number of Mcast Prefix advertised by a RP	250	250
	Max number of BSR RP per mcast domain	56	56
	Max number of Static RP per system	56	56
	Max number of RPset x RP per system	56	56
	Max number of PIM Anycast RPs per system	56	56
	Max number of Anycast RP peers per system	8	8
	Multicast ECMP Paths	64	64
LAYER 3 FEATURES - IPv4			
	Max number of IP interfaces per system (ipv4, ipv6)	4K	4K

		SLX 9150	SLX 9250
	Max number of Virtual Ethernet interfaces per system	8K	8K
	Max number of ARP entries	47K	47K
	Max number of ND entries	33K	33K
	Max number of Static ARP entries	47K	47K
	Max number of IP Next-hops	48K	48K
	Number of possible secondary IP Addresses	254	254
	Max. number of Loopback interfaces	255	255
	Maximum number of OSPF areas (Per VRF)	200	200
	Number of OSPF routers in a single area	200	200
	Maximum Number of OSPF Routes	64K	64K
	Maximum Number of Static Route Entries	24K	24K
	Max BGP Peer-Groups	250	250
	Max BGP Routes in RIB	3.25M (in + out)	3.25M (in + out)
	BGP Peers (IPv4 and IPv6 concurrent)	512	512
	Maximum Number of IS-IS Routes	25K	25K
	Number of IS-IS adjacencies	Broadcast : 255 P2P : 1024	Broadcast : 255 P2P : 1024
	Number of IS-IS LSP's	255	255
	Number of IS-IS routers in a level	255	255
	Max IS-IS interfaces	Broadcast:255 P2P: 1024	Broadcast:255 P2P: 1024
	Maximum Number of IPv4 Routes	128K	128K
	Maximum number of routes in hardware (IPv4 and IPv6 concurrent)	80K v4 and 16K v6	80K v4 and 16K v6
	Max VRFs per system (BGP VRF IPv4/IPv6)	1K	1K

		SLX 9150	SLX 9250
	Max VRFs per system (OSPF VRF IPv4/IPv6)	1K	1K
	Max VRFs per system (Static VRF IPv4/IPv6)	1K	1K
	ECMP Support	16K	16K
	Max number of ECMP Paths	64	64
	ECMP adjacency	1K	1K
	Number of VRRP/VRRPe Instances per system (ipv4, ipv6)	255	255
	Number of VRRP instances per IP interface	16	16
	ICMP Error Message handling	Supported	Supported
LAYER 3 FEATURES - IPv6			
	Maximum Number of IPv6 Static Route Entries	10K	10K
	Maximum Number of IPv6 Routes	10K	10K
	Maximum Number of OSPFv3 Routes	64K	64K
	Maximum Number of OSPFv3 Interfaces	200	200
	Maximum number of OSPFv3 Neighbors	200	200
	Maximum number of OSPFv3 area per VRF	10	10
	Maximum Number of BGPv6 Routes in the RIB	Same as IPv4	Same as IPv4
	Maximum Number of BGPv6 Neighbors	512	512
RATE LIMITING AND TRAFFIC POLICING FEATURES			
	Granularity	1kbps	1kbps
	Number of Rate-limiters/Traffic-policers Per System	8k in SW	8k in SW
ACL			

		SLX 9150	SLX 9250
	Max shared IPv4 ACLs per system	2K ACL groups with 2K ACL statements each(SW) IPv4 ACL DB Standard Ingress Count :767/768, Egress Count 245/246 .Extended Ingress Count :767/768 Egress Count245/246. Note: Same DB is shared by PBR, ACL Ratelimiters and RACL)	2K ACL groups with 2K ACL statements each(SW) IPv4 ACL DB Standard Ingress Count :767/768, Egress Count 245/246 .Extended Ingress Count :767/768 Egress Count245/246. Note: Same DB is shared by PBR, ACL Ratelimiters and RACL)
	Max shared IPv6 ACLs per system	2K ACL groups with 2K ACL statements each(SW) IPv6 ACL DB Standard : 767/768. Extended :767/768 Note: (Same DB is shared by PBR, ACL Ratelimiters and RACL)	2K ACL groups with 2K ACL statements each(SW) IPv6 ACL DB Standard : 767/768. Extended :767/768 Note: (Same DB is shared by PBR, ACL Ratelimiters and RACL)
	Max shared L2 ACLs per system	2K ACL groups with 2K ACL statements each(SW) MAC ACL DB: Standard Ingress Count: 501/502, Egress Count: 245/246.Extended Ingress Count: 501/502, Egress Count245/246. Note: (L2 Rate limiter also shared same DB)	2K ACL groups with 2K ACL statements each(SW) MAC ACL DB: Standard Ingress Count: 501/502, Egress Count: 245/246.Extended Ingress Count: 501/502, Egress Count245/246. Note: (L2 Rate limiter also shared same DB)
	Max number of IP receive ACLs	Same as Ipv4 ACL	Same as Ipv4 ACL
	Max number of IPv6 receive ACLs	Same as Ipv6 ACL	Same as Ipv6 ACL
	Policy Based Routing (PBR)	767 (TCAM entries shared with v4 ACL)	767 (TCAM entries shared with v4 ACL)
	IPv6 PBR	767 (TCAM entries shared with v6 ACL)	767 (TCAM entries shared with v6 ACL)
	Max Number of configurable PBR route maps	200	200
	Max Number of configurable stanzas in PBR	1024	1024

		SLX 9150	SLX 9250
Multi-Chassis Trunking (vLAG support)			
	Number of vPorts - (# of VLANs) **times** (# of ports)	15.5K	15.5K
	Number of VLANs for logical port (single port or LAG)	4K (4K VLAN OR 2K BD)	4K (4K VLAN OR 2K BD)
	Max MCT Clients	62	126
	Max of VLANs for ICL	4K VLAN + 2K BD (VxLAN Tunnels)	4K VLAN + 2K BD (VxLAN Tunnels)
	Max number of L2 / unified bridging instances (VPLS, EVPN, L2, VXLAN) with MCT and BUM RL	4K VLAN + 1K BD(EVPN-VXLAN) VPLS not supported	4K VLAN + 1K BD(EVPN-VXLAN) VPLS not supported
	Max number endpoint in MCT for L2/bridging (VPLS, EVPN, L2, VXLAN)	VPLS not supported 6K VXLAN VNIs L2-15K	VPLS not supported 6K VXLAN VNIs L2-15K
	Max number of MAC addr for MCT	64K	64K
EVPN-VXLAN Scaling (IP Fabric)			
	VxLAN Tunnel (e.g ToR, DCI, hybrid cloud)	128	128
	L2 VNI (Bridge Domains)	4K VLAN+2K BD	4K VLAN+2K BD
	L3 VNI	128	128
Layer 2	Max # of VLAN's	4K	4K
	Max # of Bridge Domains	4K (* centralized routing)	4K (* centralized routing)
	Max # of MAC entries	64K	64K
	Max # of ARP entries	47K	47K
	Max # VNI	4K+2K+128	4K+2K+128
Layer 3	Max # of BGP peers (IPv4+IPv6)	1k	1k
	Max # of VE	8k	8k
	Max # of BD VE	4K	4K
	Max # of VRF	1K	1K
	ND entries	34k	34k
	SAG per switch	8K	8K
	SAG address per interface	64	64

		SLX 9150	SLX 9250
	BGP EVPN IPv4 and IPv6 route (HW) and (SW)	HW IPv4: 128k, HW IPV6: 10k SW: 2M	HW IPv4: 128k, HW IPV6: 10k SW: 2M
	BGP EVPN mac IP routes (HW) and (SW)	HW: 47k SW: 2M	HW: 47k SW: 2M
	BGP EVPN mac routes (SW)	HW: 47k SW: 2M	HW: 47k SW: 2M
QoS			
	Maximum Number of Traffic Classes	8	8
	On chip buffers per ASIC (shared between ingress and egress)	32MB	32MB
	Max schedulers on SYSTEM	80	128
	Max Shapers on System	80	128
	POLICY-MAP MAX config on SYSTEM (Created in SW globally)	1K	1K
	CLASS-MAP MAX config per policy	4K	4K
	POLICY-MAP MAX config per interface	1	1
	SERVICE-POLICY - per interface	1 per direction	1 per direction
	CLASS-MAP MAX config on SYSTEM (Created in SW globally)	32k	32k
	DEFAULT CLASS-MAP per POLICY	1	1
	MATCH ACL CLASS-MAP per POLICY	4k non default class map per policymap	4k non default class map per policymap
	PORT-BASED IN service-policy on SYSTEM	64	128
	MATCH ACL CLASS IN service-policy on SYSTEM	4K non default-class map per policy-map	4K non default-class map per policy-map
	PORT-BASED IN service-policy on SYSTEM	64	128
	STORM-CONTROL (BUM traffic policy)	3	3
	Maximum number of ACL table per CLASS	1	1
	Number of Policers	1024	1024

		SLX 9150	SLX 9250
	Maximum unique RED profiles configured (SW)	120	120
	Maximum unique RED profiles configured (HW)	128	128
	PCP->TC, DSCP->TC	61	61
	DSCP->DSCP	10	10
	DSCP->CoS, TC->CoS	12	12
	TC->DSCP	NA	NA
	Maximum per-port priority pause level	Pause and PFC N/A in 20.1.1	Pause and PFC N/A in 20.1.1
	QoS priority queues (per port)	8	8
SNMP			
	Maximum communities	256	256
	Maximum contexts	256	256
	Maximum community maps	256	256
	Maximum SNMP v3 users	10	10
	Maximum groups	10	10
	Maximum views	10	10
	Maximum v1/v2c trap hosts	12	12
	Maximum v3 trap hosts	6	6
Netconf			
	Max number of SSH concurrent sessions	16	16
Rest/Restconf			
	Max number of REST/Restconf sessions	30	30
BFD			
BFD for static routes			
	IPv4 static Hardware sessions	1000	1000
	IPv6 static Hardware sessions	600	600
	IPv4/IPv6 concurrent static Hardware sessions	850 v4 and 150 v6	850 v4 and 150 v6
	Static Software sessions Supported for IPv4 and IPv6	250	250
BFD for BGP/OSPF			
	IPv4/IPv6 Hardware sessions for single hop	250	250

		SLX 9150	SLX 9250
	IPv4/IPv6 Hardware sessions for multi hop	250	250

Hardware Support

Supported devices

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.

Supported power supplies

SLX 9150 and SLX 9250 power supplies share common parts with the VSP 7400.

XN-ACPWR-750W-F	750W AC PSU Front to Back airflow
XN-ACPWR-750W-R	750W AC PSU Back to Front airflow
XN-DCPWR-750W-F	750W DC PSU Front to Back airflow
XN-DCPWR-750W-R	750W DC PSU Back to Front airflow

Supported optics

These optics are supported on SLX 9150 and SLX 9250.

SKU	Description
10065	10/100/1000BASE-T SFP
10301	SR SFP+ module
10302	LR SFP+ module
10303	LRM SFP+ module
10304	1m SFP+ Cable
10305	3m SFP+ Cable
10310	ZR SFP+ module
10051H	1000BASE-SX SFP, Hi
10052H	1000BASE-LX SFP, Hi
10056H	1000BASE-BX-D BiDi SFP, Hi
10057H	1000BASE-BX-U BiDi SFP, Hi
10070H	10/100/1000BASE-T SFP, Hi
100G-4WDM-QSFP20KM	100G 4WDM-20 QSFP28 20km
100G-4WDM-QSFP40KM	100G 4WDM-40 QSFP28 40km
100G-AOC-QSFP10M-TA	100G AOC QSFP28 10m TAA
100G-CWDM4-QSFP2KM	100G CWDM4 QSFP28 2km
100G-DACP-QSFP1M	100G Passive DAC QSFP28 1m
100G-DACP-QSFP3M	100G Passive DAC QSFP28 3m
100G-DACP-QSFP4SFP1M	100G Passive DAC QSFP28 to 4xSFP28 1m
100G-DACP-QSFP4SFP3M	100G Passive DAC QSFP28 to 4xSFP28 3m
100G-DACP-QSFP5M	100G Passive DAC QSFP28 5m
100G-ER4LT-QSFP40KM	100G ER4-lite QSFP28 40km
100G-LR4-QSFP10KM	100G LR4 QSFP28 10km
100G-LR4-QSFP2KM	100G LR4 QSFP28 2km
100G-QSFP28-CWDM4-2KM	100GE QSFP28 CWDM
100G-QSFP28-LR4L-2KM	100GE QSFP28 LRL 2km
100G-QSFP28-LR4-LP-10KM	100GE QSFP28 LR4 (3.5W)
100G-QSFP28-SR4	100GE QSFP28 SR4

SKU	Description
100G-QSFP-QSFP-AOC-1001	100G QSFP28 Active Optical (10m)
100G-SR4-QSFP100M	100G SR4 QSFP28 100m
100G-SWDM4-QSFP100M	100G SWDM4 QSFP28 100m
10GB-BX10-D	10 GB, SINGLE FIBER SM, -D 10 KM
10GB-BX10-U	10 GB, SINGLE FIBER SM, -U 10 KM
10G-ER-SFP40KM-ET	10G ER SFP+ 40km Ext.Temp
10GE-SFP-AOC-0701	10GE AOC 7M
10GE-SFP-AOC-1001	10GE AOC 10M
10G-LR-SFP10KM-ET	10G LR SFP+ 10km Ext.Temp
10G-LR-SFP10KM-ET8PK	10G LR SFP+ 10km 8pack Ext.Temp
10G-SFP-ER	10GE ER 40km
10G-SFP-LR	10GE LR SFP+, 85C
10G-SFP-LR-S	10GE LR SFP+, 70C
10G-SFP-LR-SA	10GE LR SFP+, 70C TAA
10G-SFP-SR	10GE SR SFP+, 85C
10G-SFP-SR-S	10GE SR SFP+, 70C
10G-SFP-SR-SA	10GE SR SFP+, 70C TAA
10G-SFP-TWX-0101	10GE Direct Attach 1M Active
10G-SFP-TWX-P-0301	10GE Direct Attach 3M Passive
10G-SFP-TWX-P-0501	10GE Direct Attach 5M Passive
10G-SFP-USR	10GE USR SFP+
10G-SFP-USR-SA	10GE USR SFP+, 70C TAA
10G-SFP-ZR	10GE ZR SFP+ 80km
10G-SR-SFP300M-ET	10G SR SFP+ 300m Ext.Temp
10G-SR-SFP300M-ET8PK	10G SR SFP+ 300m 8pack Ext.Temp
10G-USR-SFP100M	10G USR SFP+ 100m Hight Rx Sens
1G-SFP-LX-OM	1000Base-LX
1G-SFP-SX-OM	1000Base-SX
1G-SFP-TX	1GE Copper SFP (Pseudo-Branded)
25G-DACP-SFP1M	25G Passive DAC SFP28 1m
25G-DACP-SFP3M	25G Passive DAC SFP28 3m
25G-LR-SFP10KM	25G LR SFP28 10km
25G-SR-SFP100M	25G SR SFP28 100m
40G-AOC-QSFP100M	40G AOC QSFP+ 100m
40G-AOC-QSFP10M	40G AOC QSFP+ 10m
40G-AOC-QSFP20M	40G AOC QSFP+ 20m
40G-AOC-QSFP3M	40G AOC QSFP+ 3m
40G-AOC-QSFP5M	40G AOC QSFP+ 5m
40G-BDSR-QSFP150M	40G BiDi SR QSFP+ 150m
40G-DACA-QSFP1M	40G Active DAC QSFP+ 1m

SKU	Description
40G-DACA-QSFP3M	40G Active DAC QSFP+ 3m
40G-DACA-QSFP4SFP1M	40G Active DAC QSFP+ to 4xSFP+ 1m
40G-DACA-QSFP4SFP3M	40G Active DAC QSFP+ to 4xSFP+ 3m
40G-DACA-QSFP4SFP5M	40G Active DAC QSFP+ to 4xSFP+ 5m
40G-DACA-QSFP5M	40G Active DAC QSFP+ 5m
40G-DACP-QSFP1M	40G Passive DAC QSFP+ 1m
40G-DACP-QSFP3M	40G Passive DAC QSFP+ 3m
40G-DACP-QSFP4SFP1M	40G Passive DAC QSFP+ to 4xSFP+ 1m
40G-DACP-QSFP4SFP2M	40G Passive DAC QSFP+ to 4xSFP+ 2m
40G-DACP-QSFP4SFP3M	40G Passive DAC QSFP+ to 4xSFP+ 3m
40G-DACP-QSFP4SFP5M	40G Passive DAC QSFP+ to 4xSFP+ 5m
40G-DACP-QSFP5M	40G Passive DAC QSFP+ 5m
40G-DACP-QSFPZ5M	40G Passive DAC QSFP+ 0.5m
40G-ESR4-QSFP400M-NT	40G ESR4 QSFP+ 400m 10G-SR interop.
40G-LM4-QSFP160M	40G LM4 QSFP+ 160m 160m MMF. 1km SMF
40G-LR4-QSFP10KM	40G LR4 QSFP+ 10km
40G-QSFP-4SFP-C-0101	4x10GE QSFP+ to 4 SFP+ Active copper cable - 1m
40G-QSFP-4SFP-C-0301	4x10GE QSFP+ to 4 SFP+ Active copper cable - 3m
40G-QSFP-4SFP-C-0501	4x10GE QSFP+ to 4 SFP+ Active copper cable - 5m
40G-QSFP-C-0101	40GE QSFP to QSFP 1M Cable(Passive)
40G-QSFP-C-0301	40GE QSFP to QSFP 3M Cable(Passive)
40G-QSFP-C-0501	40GE QSFP to QSFP 5M Cable(Passive)
40G-QSFP-LR4-1	40GE QSFP+ LR4, 10KM, 70C
40G-QSFP-LR4-INT	4x10GE QSFP+ LR4, 10km,
40G-QSFP-QSFP-AOC-1001	40GE QSFP to QSFP cable - 10m AOC
40G-QSFP-SR-BIDI	40GE BiDi QSFP+
40G-SR4-QSFP150M	40G SR4 QSFP+ 150m
40G-SR4-QSFP150M-NT	40G SR4 QSFP+ 150m 10G-SR interoperable
MGBIC-LC01-G	1GB SX MM, SFP, TAA
10504	25G LR SFP28 10km
10405	100Gb QSFP28 PSM4
10327	MPO to 4xLC breakout patch cable, SM 10m

Note: The 10GE LR SFP+, 85C multi-speed optic can operate on 10G and 1G.

DAC cables

- 40G-QSFP-QSFP-P-0X01: passive 40G direct attached copper cables (X = 1, 3, 5m reach)
- 40G-QSFP-QSFP-C-0X01: active 40G direct attached copper cables (X = 1, 3, 5m reach)
- 40G-QSFP-4SFP-C-0X01: active 40G direct attached breakout copper cables (X = 1, 3, 5m reach)
- 100G-QSFP-QSFP-P-0101: 100GE Direct Attached QSFP-28 to QSFP-28 Passive Copper cable, 1m
- 100G-QSFP-QSFP-P-0301: 100GE Direct Attached QSFP-28 to QSFP-28 Passive Copper cable, 3m
- 100G-QSFP-QSFP-P-0501: 100GE Direct Attached QSFP-28 to QSFP-28 Passive Copper cable, 5m

Redundant Management Interface (RME)

The Redundant Management Interface (RME) is new for this release for SLX 9250.

RME provides fault tolerance for Management path to reach the device. The device has only one physical RJ45 port available for management purposes. RME uses standard Linux Networking Bonding Interface in "Mode 1" (**Active-Standby**) to achieve fault tolerance.

With this feature, the front panel Management physical path by default is **always** available as **Active** as well as **Primary** path. You can configure *any switch front panel* port as **Standby** path.

- **Primary** path: Whenever healthy, it shall **only** be used. For example, eth0 Management port.
- **Active** path: Currently healthy and being used for both ingress and egress traffic. For example, port is active Management port eth0 or switch front panel port 0/15 based on link , the other port becomes Standby.
- **Standby** path: May be healthy but still not used, until the Active member goes bad. No egress traffic is pushed out, or duplicated, on this path and all ingress traffic on this path is dropped.

Limitation:

Though any user port with any native may be used, internally ingress traffic is rate-limited on standby path to low bandwidth from ASIC to CPU trapping. It is good for SSH and HTTP transactions. Even long file transfers will occur, although they will take some time. Firmware download works but may take 30 to 40 minutes.

Recommendation:

For SLX-9250, we recommend using the Mellanox QSA adaptor with 1GE Cu SFP.

Breakout mode 4x1G is required. For more information, see the *Extreme SLX-OS Management Configuration Guide*.

Only **one** member-port can be used.

The following examples configure any port (such as 0/15) as a standby member.

1) Simple example:

```
configure terminal
   interface ethernet 0/15
   redundant-management enable
   no shut
```

2) (SLX-9250) Breakout example for Mellanox Adaptor use:

```
SLX# conf t
SLX(config)# hardware
SLX(config-hardware)# connector 0/15
SLX(config-connector-0/15)# breakout mode 4x1G
SLX(config-connector-0/15)# end

SLX# conf t
SLX(config)# interface Ethernet 0/15:1
SLX(conf-if-eth-0/15:1)# redundant-management enable
SLX(conf-if-eth-0/15:1)# no shut
```

Internally, port 0/15 or 0/15:1 is converted to an inband port by moving to mgmt-vrf from default-vrf and made as a standby member (Eth0.15 or Eth0.15.1) to Linux bond0 interface.

The active primary member on the device is typically named eth3 and is by default member to bond0 at boot.

Zero Touch Provisioning (ZTP)

ZTP allows device configuration using DHCP Server, enabled with DHCP option 66 and 67, *viz.* for ftp server address and ZTP config file location respectively.

ZTP typically and optionally downloads the following three files from "ZTP (ftp) Server" to configure the device.

1. Firmware image – if any.
2. Switch Config File – Configuration to be set/replay at switch.
3. Python Script – Script which can be executed at switch.

On SLX switches from the factory, upon power-on, ZTP is enabled by default. Alternatively, it can be enforced by SLX CLI command **write erase**, which reboots the switch in ZTP mode.

On start of ZTP, the switch searches for DHCP Server on both management port (OOB) "eth0" as well as all front panel ports, which are moved to **inband** mode by moving them to mgmt-vrf, till ZTP finds DHCP Server and required downloads are completed.

If the DHCP Server is not found, ZTP keeps retrying with some timeout periods. If necessary, you can stop ZTP with the SLX CLI command **dhcp ztp cancel**.

You set up a standard DHCP server and a standard FTP server that is accessible to the device from any of its links.

The FTP Server should enable user **anonymous** access.

DHCP Server Configuration

A typical DHCP server configuration file (such as dhcpd.conf) allocates the IPv4 address, the default route gateway, the boot file, and the TFTP server.

```
option bootfile-name "/config/ztp.cfg";
option tftp-server-name "192.168.1.10";
subnet 192.168.1.0 netmask 255.255.255.0 {
  pool {
    range 192.168.1.100 192.168.1.200;
  }
  option routers 192.168.1.10;
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.1.255;
}
```

- bootfile-name (option 67) is used for ZTP configuration file path at ftp server.
- tftp-server-name (option 66) is used for FTP Server address

ZTP Configuration

A typical ZTP configuration file is shown below, but for a detailed explanation, see the *Extreme SLX-OS Management Configuration Guide*.

```
version=3
date=03/06/2018
supported_nos=18s.1.03 20.1.1
#proto=ftp

common_begin
  vcsmode=SA
  scriptcfgflag=2  #0-config file only, 1-script only, 2 both
  fullinstall=0
  startup=/config/switchCommonConfig.cfg
  script=/script/switchCommonScript.py
  fwdir=/fw/slxos20.1.1_bld18
common_end


#host_mac=00:05:33:E5:85:38
#host_sn=1907Q-20083
host_client_id=EXTREMENETWORKS##SLX9150-48Y##1907Q-20083
  defaultconfig=no
  scriptcfgflag=0
  startup=/config/switchSpecificConfig_20083.cfg
  fwdir=/fw/slxos20.1.1_bld69
  script=/script/switchSpecificScript_20083.py
host_end
```

Notes:

- Switch-specific settings override the common setting.
- “fwdir” is in the firmware image dist folder.
- “startup” is the typical switch configuration file.
- “script” is the Python script file

When ZTP is searching the DHCP server or downloading files, you can log in user ‘admin’. The ZTP dump progress logs on console and user may dump XTP ongoing logs by SLX CLI command **dhcp ztp log**. Also, you can use the SLX CLI command **show ztp status** to dump the previous ZTP history.

ZTP Logs

The following are sample progress logs of normal, successful ZTP operations. These captured logs are for downloading script, config, and firmware. For firmware download, the system is reloaded with a new image, then config is replayed, followed by script execution.

```
SLX# dhcp ztp log

ZTP, Mon Nov 18 12:18:36 2019, ========== ZTP start ==========

ZTP, Mon Nov 18 12:18:36 2019, disable raslog

ZTP, Mon Nov 18 12:18:36 2019, CLI is ready

ZTP, Mon Nov 18 12:18:49 2019, inband ports are enabled

ZTP, Mon Nov 18 12:18:49 2019, serial number = 1907Q-20083

ZTP, Mon Nov 18 12:18:49 2019, model name = SLX9150-48Y

ZTP, Mon Nov 18 12:18:49 2019, use both management interface and inband interfaces

ZTP, Mon Nov 18 12:18:49 2019, checking inband interfaces link status

ZTP, Mon Nov 18 12:19:40 2019, find link up on interfaces: eth0 Eth0.81 Eth0.56
Eth0.55 Eth0.54 Eth0.53 Eth0.52 Eth0.51 Eth0.50 Eth0.49 Eth0.48 Eth0.47 Eth0.46
Eth0.45 Eth0.44 Eth0.43 Eth0.42 Eth0.41 Eth0.40 Eth0.39 Eth0.38 Eth0.37 Eth0.36
Eth0.35 Eth0.34 Eth0.33 Eth0.32 Eth0.31 Eth0.30 Eth0.29 Eth0.28 Eth0.27 Eth0.26
Eth0.25 Eth0.24 Eth0.23 Eth0.22 Eth0.21 Eth0.20 Eth0.19 Eth0.18 Eth0.17 Eth0.16
Eth0.15 Eth0.14 Eth0.13 Eth0.12 Eth0.11 Eth0.10 Eth0.9 Eth0.8 Eth0.7 Eth0.6 Eth0.5
Eth0.4 Eth0.3 Eth0.2 Eth0.1

ZTP, Mon Nov 18 12:19:40 2019, start dhcp process on interfaces: eth0 Eth0.81 Eth0.56
Eth0.55 Eth0.54 Eth0.53 Eth0.52 Eth0.51 Eth0.50 Eth0.49 Eth0.48 Eth0.47 Eth0.46
Eth0.45 Eth0.44 Eth0.43 Eth0.42 Eth0.41 Eth0.40 Eth0.39 Eth0.38 Eth0.37 Eth0.36
Eth0.35 Eth0.34 Eth0.33 Eth0.32 Eth0.31 Eth0.30 Eth0.29 Eth0.28 Eth0.27 Eth0.26
Eth0.25 Eth0.24 Eth0.23 Eth0.22 Eth0.21 Eth0.20 Eth0.19 Eth0.18 Eth0.17 Eth0.16
Eth0.15 Eth0.14 Eth0.13 Eth0.12 Eth0.11 Eth0.10 Eth0.9 Eth0.8 Eth0.7 Eth0.6 Eth0.5
Eth0.4 Eth0.3 Eth0.2 Eth0.1

ZTP, Mon Nov 18 12:19:43 2019, interface eth0 receives dhcp response

ZTP, Mon Nov 18 12:19:43 2019, ping server 192.168.1.10

ZTP, Mon Nov 18 12:19:44 2019, ping succeed

ZTP, Mon Nov 18 12:19:44 2019, download ZTP config file from
https://192.168.1.10/config/ztp.cfg
```

```
ZTP, Mon Nov 18 12:19:44 2019, download ZTP config file from
http://192.168.1.10/config/ztp.cfg

ZTP, Mon Nov 18 12:19:44 2019, download ZTP config file from
ftp://192.168.1.10/config/ztp.cfg

ZTP, Mon Nov 18 12:19:44 2019, receive ZTP configuration file [ztp.cfg]

ZTP, Mon Nov 18 12:19:44 2019, interface eth0 connectivity test pass

ZTP, Mon Nov 18 12:19:46 2019, firmware upgrade sanity check passed

ZTP, Mon Nov 18 12:19:46 2019, download script file [switchSpecificScript_20083.py]

ZTP, Mon Nov 18 12:19:46 2019, download switch config file
[switchSpecificConfig_20083.cfg]

ZTP, Mon Nov 18 12:19:46 2019, ZTP configuration sanity check pass

ZTP, Mon Nov 18 12:19:46 2019, start firmware upgrade...

ZTP, Mon Nov 18 12:26:30 2019, ========== ZTP continue ==========

ZTP, Mon Nov 18 12:26:30 2019, disable raslog

ZTP, Mon Nov 18 12:26:30 2019, CLI is ready

ZTP, Mon Nov 18 12:26:40 2019, firmware upgrade succeed.

ZTP, Mon Nov 18 12:26:51 2019, replay config file...

ZTP, Mon Nov 18 12:27:01 2019, running configuration script
[switchSpecificScript_20083.py]

ZTP, Mon Nov 18 12:27:36 2019, commit configuration

ZTP, Mon Nov 18 12:27:36 2019, ZTP succeed

ZTP, Mon Nov 18 12:27:36 2019, enable raslog

ZTP, Mon Nov 18 12:27:36 2019, ========== ZTP completed ==========
```

The following are sample progress logs of a canceled ZTP operation:

```
SLX# dhcp ztp cancel

This command is terminating the existing ZTP session.


SLX# dhcp ztp log

ZTP, Mon Nov 18 12:06:21 2019, ========== ZTP start ==========

ZTP, Mon Nov 18 12:06:21 2019, disable raslog

ZTP, Mon Nov 18 12:06:21 2019, CLI is ready

ZTP, Mon Nov 18 12:06:34 2019, inband ports are enabled

ZTP, Mon Nov 18 12:06:34 2019, serial number = 1907Q-20083

ZTP, Mon Nov 18 12:06:34 2019, model name = SLX9150-48Y
```

```
ZTP, Mon Nov 18 12:06:34 2019, use both management interface and inband interfaces

ZTP, Mon Nov 18 12:06:34 2019, checking inband interfaces link status

ZTP, Mon Nov 18 12:06:46 2019, Sanity test canceled

ZTP, Mon Nov 18 12:06:46 2019, retry in 10 seconds

ZTP, Mon Nov 18 12:06:48 2019, ZTP is canceled

ZTP, Mon Nov 18 12:06:49 2019, enable raslog

ZTP, Mon Nov 18 12:06:49 2019, ========== ZTP completed ==========
```

Note: These logs also show up on the console.

The following are sample progress logs of a canceled ZTP operation:

```
SLX# dhcp ztp log

ZTP, Mon Nov 18 12:49:58 2019, ========== ZTP start ==========

ZTP, Mon Nov 18 12:49:58 2019, disable raslog

ZTP, Mon Nov 18 12:49:58 2019, CLI is ready

ZTP, Mon Nov 18 12:50:11 2019, inband ports are enabled

ZTP, Mon Nov 18 12:50:12 2019, serial number = 1907Q-20083

ZTP, Mon Nov 18 12:50:12 2019, model name = SLX9150-48Y

ZTP, Mon Nov 18 12:50:12 2019, use both management interface and inband interfaces

ZTP, Mon Nov 18 12:50:12 2019, checking inband interfaces link status

ZTP, Mon Nov 18 12:51:03 2019, find link up on interfaces: eth0 Eth0.81 Eth0.56
Eth0.55 Eth0.54 Eth0.53 Eth0.52 Eth0.51 Eth0.50 Eth0.49 Eth0.48 Eth0.47 Eth0.46
Eth0.45 Eth0.44 Eth0.43 Eth0.42 Eth0.41 Eth0.40 Eth0.39 Eth0.38 Eth0.37 Eth0.36
Eth0.35 Eth0.34 Eth0.33 Eth0.32 Eth0.31 Eth0.30 Eth0.29 Eth0.28 Eth0.27 Eth0.26
Eth0.25 Eth0.24 Eth0.23 Eth0.22 Eth0.21 Eth0.20 Eth0.19 Eth0.18 Eth0.17 Eth0.16
Eth0.15 Eth0.14 Eth0.13 Eth0.12 Eth0.11 Eth0.10 Eth0.9 Eth0.8 Eth0.7 Eth0.6 Eth0.5
Eth0.4 Eth0.3 Eth0.2 Eth0.1

ZTP, Mon Nov 18 12:51:03 2019, start dhcp process on interfaces: eth0 Eth0.81 Eth0.56
Eth0.55 Eth0.54 Eth0.53 Eth0.52 Eth0.51 Eth0.50 Eth0.49 Eth0.48 Eth0.47 Eth0.46
Eth0.45 Eth0.44 Eth0.43 Eth0.42 Eth0.41 Eth0.40 Eth0.39 Eth0.38 Eth0.37 Eth0.36
Eth0.35 Eth0.34 Eth0.33 Eth0.32 Eth0.31 Eth0.30 Eth0.29 Eth0.28 Eth0.27 Eth0.26
Eth0.25 Eth0.24 Eth0.23 Eth0.22 Eth0.21 Eth0.20 Eth0.19 Eth0.18 Eth0.17 Eth0.16
Eth0.15 Eth0.14 Eth0.13 Eth0.12 Eth0.11 Eth0.10 Eth0.9 Eth0.8 Eth0.7 Eth0.6 Eth0.5
Eth0.4 Eth0.3 Eth0.2 Eth0.1

ZTP, Mon Nov 18 12:51:13 2019, get no dhcp response from all interfaces

ZTP, Mon Nov 18 12:51:13 2019, retry in 10 seconds
```

```
ZTP, Mon Nov 18 12:51:23 2019, inband ports are enabled

ZTP, Mon Nov 18 13:06:25 2019, serial number = 1907Q-20083

ZTP, Mon Nov 18 13:06:25 2019, model name = SLX9150-48Y

ZTP, Mon Nov 18 13:06:25 2019, use both management interface and inband interfaces

ZTP, Mon Nov 18 13:06:25 2019, checking inband interfaces link status

ZTP, Mon Nov 18 13:06:26 2019, find link up on interfaces: eth0 Eth0.81 Eth0.56
Eth0.55 Eth0.54 Eth0.53 Eth0.52 Eth0.51 Eth0.50 Eth0.49 Eth0.48 Eth0.47 Eth0.46
Eth0.45 Eth0.44 Eth0.43 Eth0.42 Eth0.41 Eth0.40 Eth0.39 Eth0.38 Eth0.37 Eth0.36
Eth0.35 Eth0.34 Eth0.33 Eth0.32 Eth0.31 Eth0.30 Eth0.29 Eth0.28 Eth0.27 Eth0.26
Eth0.25 Eth0.24 Eth0.23 Eth0.22 Eth0.21 Eth0.20 Eth0.19 Eth0.18 Eth0.17 Eth0.16
Eth0.15 Eth0.14 Eth0.13 Eth0.12 Eth0.11 Eth0.10 Eth0.9 Eth0.8 Eth0.7 Eth0.6 Eth0.5
Eth0.4 Eth0.3 Eth0.2 Eth0.1

ZTP, Mon Nov 18 13:06:26 2019, start dhcp process on interfaces: eth0 Eth0.81 Eth0.56
Eth0.55 Eth0.54 Eth0.53 Eth0.52 Eth0.51 Eth0.50 Eth0.49 Eth0.48 Eth0.47 Eth0.46
Eth0.45 Eth0.44 Eth0.43 Eth0.42 Eth0.41 Eth0.40 Eth0.39 Eth0.38 Eth0.37 Eth0.36
Eth0.35 Eth0.34 Eth0.33 Eth0.32 Eth0.31 Eth0.30 Eth0.29 Eth0.28 Eth0.27 Eth0.26
Eth0.25 Eth0.24 Eth0.23 Eth0.22 Eth0.21 Eth0.20 Eth0.19 Eth0.18 Eth0.17 Eth0.16
Eth0.15 Eth0.14 Eth0.13 Eth0.12 Eth0.11 Eth0.10 Eth0.9 Eth0.8 Eth0.7 Eth0.6 Eth0.5
Eth0.4 Eth0.3 Eth0.2 Eth0.1

ZTP, Mon Nov 18 13:06:36 2019, get no dhcp response from all interfaces

ZTP, Mon Nov 18 13:06:36 2019, retry in 10 seconds

ZTP, Mon Nov 18 13:06:48 2019, ZTP is canceled

ZTP, Mon Nov 18 13:06:49 2019, enable raslog

ZTP, Mon Nov 18 13:06:49 2019, ========== ZTP completed ==========
```

Software Download and Upgrade

For complete information about the various methods of upgrading to SLX-OS 20.1.2a, see the *Extreme SLX-OS Software Upgrade Guide, 20.1.2a.*

Image file names

Download the following images from www.extremenetworks.com.

Image file name	Description
slxos20.1.2a.tar.gz	SLX-OS 20.1.2a software
slxos20.1.2a_all_mibs.tar.gz	SLX-OS 20.1.2a MIBS
slxos20.1.2a.md5	SLX-OS 20.1.2a md5 checksum
slxos-20.1.2a-releasenotes.pdf	Release Notes

Considerations for obtaining and decompressing software

- Download the software and transfer it to the server and location (such as the FTP server root directory that you will use for the software upgrade.
    - You can also download the software package from a USB drive using the **firmware download usb** command.
- Decompress the software package before using the **firmware download** command to upgrade the software.
- As a best practice, use 7zip to decompress the software tarball when you use a Microsoft Windows platform for software upgrade.
- The decompressed software package expands into a directory that is named according to the software version. When issued with the path to the directory where the software is stored, the **firmware download** command performs an automatic search for the package file type that is associated with the device.
- The following firmware download command options are available. For more information about the options, see the *Extreme SLX-OS Command Reference*.
    - **default-config**: Downloads new software and, after a forced cold reboot, cleans up the in-band configuration.
    - **fullinstall**: Downloads a larger file selection to cover the differences between 32-bit and 64-bit software or between 2.6 and 4.14 kernel software.
    - **noactivate**: Downloads the software without activating it, so the device is not automatically rebooted.
    - **nocommit**: Disables auto-commit mode so that the software is downloaded only to the primary partition.
    - **noreboot**: Disables auto-reboot mode.
    - **use-vrf**: Specifies the name of the VRF where the host is located. If this option is not specified, mgmt.-vrf is used.
- So that you can address the FTP or SCP server by its name, ensure that a Domain Name System (DNS) entry is established for the server.
- SLX-OS does not support the use of special characters (such as &, !, %, or #) in FTP, TFTP, SFTP, or SCP passwords. The software download fails if your password contains special characters.

SLX 9540 and SLX 9640

To From	18r.2.00bc	SLX 20.1.1	20.1.2a
18r.2.00bc	NA	Fullinstall	Fullinstall
20.1.1	Fullinstall	NA	FWDL-coldboot
20.1.2a	Fullinstall	FWDL-coldboot	NA

Notes:

- From the 18r.1.00x and 18r.2.00a patches and earlier, you must upgrade to 18r.2.00bx and then to 20.1.1 or 20.1.2a, a two-step upgrade procedure.
- The MCT upgrade procedure from 18r.2.00bc to 20.1.x is detailed in the *Extreme SLX-OS Software Upgrade Guide.*

SLX 9150 and SLX 9250

To From	SLX 20.1.1	20.1.2a
slxos20.1.1_bosch_bootloader_v5	Fullinstall	Fullinstall
20.1.1	NA	FWDL-coldboot
20.1.2a	FWDL-coldboot	NA

SLX TPVM Support Matrix for 9150 and 9250

SLX Build	**TPVM – Fresh Install Supported**	**EFA**
20.1.1	TPVM 3.0	EFA 2.1
20.1.2a	TPVM 3.0	EFA 2.1
20.1.2a	TPVM 4.0	EFA 2.2

Upgrading TPVM from 3.0. to 4.0

Consider the following when upgrading TPVM from 20.1.1 to 20.1.2a.

- SLX-OS 20.1.1 had TPVM 3.0.0, which is based on Ubuntu16. SLX-OS 20.1.2 variants have TPVM 4.0.0, which is based on Ubuntu18.
- To upgrade from TPVM 3.0.0 to TPVM 4.0.0, take the following steps:
    - Upgrade to SLX-OS 20.1.2a.
    - Remove TPVM 3.0.0 using the **tpvm stop** and **tpvm uninstall** commands.
    - Copy the new tpvm-4.0.0.amd64.deb to /tftpboot/SWBD2900 on the SLX device.

    - Install TPVM 4.0.0 using the **tpvm install** or **tpvm deploy** command.
    - Note that any additional TPVM disks, including vdb (implicitly created by TPVM 3.0.0), are preserved with data during the previous steps.
    - If you need to remove the disks and start clean, then use the **tpvm uninstall force** command in place of **tpvm uninstall** in these steps. Alternatively, you can use **tpvm disk remove name <disk name>** to remove each additional disk manually. For example, tpvm disk remove name vdb.

Note that with TPVM 4.0.0, the default login and password have changed to “extreme/password” rather than “admin/password” as in TPVM 3.0.0.

- If some application requires TPVM3.0 based on Ubuntu16 on SLX, take the following steps to downgrade TPVM from TPVM 4.0.0 to TPVM 3.0.0:
    - Check whether SLX is running SLX-OS 20.1.2/20.1.2a and TPVM4.0
    - Remove TPVM 4.0.0 using the **tpvm stop** and **tpvm uninstall** commands.
    - Copy the tpvm-3.0.0.amd64.deb to /tftpboot/SWBD2900 on the SLX device.
    - Install TPVM 3.0.0 using the **tpvm install** or **tpvm deploy** command. TPVM login user is “admin”.
    - Note that any additional TPVM disks, including vdb (implicitly created by TPVM 4.0.0), are preserved with data during the above steps.
    - If you need to remove the disks and start clean, then use the **tpvm uninstall force** command in place of **tpvm uninstall** in these steps. Alternatively, you can use **tpvm disk remove name <disk name>** to remove each additional disk manually. For example, tpvm disk remove name vdb.

Consider the following when you upgrade TPVM from releases earlier than SLX-OS 20.1.1 to SLX-OS 20.1.x:

- During startup, the latest TPVM creates an additional TPVM disk (named vdb) and creates an ext4 partition inside it (named vdb1).
- This additional disk partition is mounted at `/apps` inside TPVM.
- The disk uses all the free space available and reserved for TPVM (platform specific) TPVM disk quota.
- If you are running an older TPVM and have the additional TPVM disks already created, as a best practice make a backup and then delete the old disks. Use the **tpvm disk remove name <disk name>** command, which requires TPVM to be started if not already running.
- Uninstall the older TPVM using the **tpvm uninstall** command.
- Install the new TPVM package using the **tpvm install** command.

Alternatively, after the SLX has been upgraded, you can use one command, **tpvm uninstall force**, to uninstall the TPVM and delete all the disks in the TPVM disk pool.

Important: The **tpvm uninstall force** process is destructive and irreversible, causing all TPVM data to be lost. The process works only if the TPVM is installed on the system.

Upgrading SLX-OS and retaining TPVM 3.0

- Back up EFA2.1 before performing the SLX-OS upgrade and save it to /efaboot in SLX.
- Upgrade SLX-OS to 20.1.2a.
- Run the **show efa status** command from SLX. If there is any error, take the following steps.
    - Uninstall TPVM3.0 and install TPVM3.0 and EFA2.1.
    - Restore the backup up EFA2.1 configuration.

Limitations and Restrictions

Auto-persistence

While downgrading to releases earlier than 20.1.2a, you must run the **copy running-config startup-config** command before downgrade so that startup-database will be in sync with the backup file after downgrade.

OAuth2

- Setting “aaa authentication” mode to OAuth2 is applicable to SSH (NETCONF) and RESTCONF modes of login. Telnet login using OAuth2 token will always fail because it not secure for transferring the OAuth2 token. As a best practice, set the secondary source of authentication in the **aaa authentication** command to always fallback to local authentication.
- Unlike other remote server authentications of operation, OAuth2 with local or local-auth-fallback will always fall back to local mode of authentication if the primary source fails.
- Any role from OAuth2 token is by default mapped to admin role in the SLX device.
- Only an RS256-based OAuth2 token is supported.
- FIPS mode, expiration time, and map role are not supported in the OAuth2 feature.

Redundant Management Interface

- The front-end port used for RME may have limited bandwidth, irrespective of the actual port speed.
- Across reboot and power cycle, the RME port will be active after config-replay.
- While redundant management-enabled port is handling the management services, firmware download may take at least 40 minutes to complete.
- When OOB MGMT port is not reachable on the network, RME port may also be not reachable, such as when the system is undergoing a rolling reboot due some other issue in the system.

TPVM

- The TPVM OS can only cater 1Gbps of Insight Interface traffic.
- A maximum of two LDAP or LDAPS servers can be configured when LDAP replication is in use, which means the basedn, certificate, rootdn, and other command parameters are common for both servers.
- The **tpvm config remove host** command removes both LDAP host entries even if they have different port numbers.
- TPVM is not upgraded with SLX upgrade and the older TPVM remains. So when upgrading TPVM, a best practice is to take a backup of TPVM data and uninstall the existing TPVM before upgrading SLX-OS. You can install the TPVM can be installed after SLX-OS upgrade.

SPAN (SLX 9150 and SLX 9250)

- CPU-generated frames cannot be mirrored using a TX span. For example, ping generated from the switch and egressing on a physical Layer 3 routed port cannot be mirrored using TX span.
- The VLAN and TTL fields in the mirrored frames are not accurate for TX span.

802.1ag

While using CFM on port channel, CFM sessions toggle when CFM timeout value is configured as 3.3, 10, or 100 ms due to a hardware limitation. You will not see this behavior with higher timeout values.

G.8032

- Configuring the **fast-convergence** command under ERP configuration is mandatory to achieve sub-50msec convergence.
- When the config is downloaded from an external file to running-config, sub-50msec convergence is effective only after a reload.
- When the config is downloaded from an external file to startup-config, sub-50msec convergence is effective only after two reloads.
- Sub-50 msec convergence is achieved with 4-device Ring topology. If the number of nodes in the topology increases beyond this, there will be small linear increase in convergence time accordingly.

MCT

- Port-security is not supported on CCEP interfaces.
- As a best practice, use maintenance-mode instead of cluster-shut for upgrade or planned reload scenario.

PXE Boot

During the PXE boot process, if the host-facing node involved in PXE boot goes for reload, all links in PXE Pre-boot down state change to Admin up.

QoS and Rate Limiting

- If you try to bind a policer with a configured CIR/EIR value less than 22,000 bps, the operational CIR/EIR value is set to zero. You are notified by syslog message.
- IP subnet rate limit will rate-limit both IPv4 and IPv6 subnet trap frames in SLX 9640 and SLX 9540 and only IPv6 frames in SLX 9150 and SLX 9250.
- For Egress ACL Rate Limiting, the rate limit is blocked for CIR rates that are less than 1,000 bps.

QoS (9150 and 9250)

- Queue shaper may not achieve the desired level of accuracy for rates less than 10 Mbps.
- Port shaper may not achieve the desired level of accuracy for rates less than 10 Mbps.
- Only the schedulers at the CoS queue level are user configurable.

App Telemetry

- The app telemetry feature is validated for platform-side changes for SLX 9150, SLX 9250, and SLX 9540.
- XMC integration testing is scheduled for a future XMC release.

BGP PIC

- When you redistribute interface routes with BGPs using “redistribute connected or static” commands, the same routes are present in the BGP route table due to the BGP route updates. Using BGP to withdraw such routes can lead to traffic issues.
- As a best practice, redistribute only specific routes through "network" statements while using it with BGP PIC.

Unsupported Password Characters

The following characters are not supported in the passwords for firmware download, copy support, and copy config commands:

- Firmware download: **` “ ! ? ‘ ~ { }**
- Copy support and copy config: **` “ ! ? ‘ ~ **
- When the use-vrf option is used in these commands, the **$** character is also not allowed in passwords.

System

Config reply from file may take more than 20 minutes with a large config file. For example, a file containing more than 70,000 lines, or a file including more than 7,000 VEs in combination with additional config on VEs.

SSH

SLX admin user does not have write permission for its home directory (/fabos/users/admin) and write operations (such as saving SSH public keys) fail. Therefore, you must accept SSH keys for each operation.

Local-switching within Bridge Domain (BD)

Local-switching is the flooding of Broadcast, Multicast, or Unknown unicast (BUM) traffic received on an AC logical interface (LIF) to all the other AC LIFs within the BD. Local-switching is enabled by default and disabling of local-switching within the BD is no longer supported.

Open Defects

The following software defects are open as of **June 2020**.

Parent Defect ID:	SLXOS-48120	**Issue ID:**	SLXOS-48120
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.2	**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-48599	**Issue ID:**	SLXOS-48599
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.2	**Technology:**	LAG - Link Aggregation Group
Symptom:	L2 traffic convergence takes more than sub-second convergence time during CCEP Port Channel Shut/no shut scenario when CCEP is multi-port port-channel		
Condition:	This issue will be observed only when we have more than 3 member ports in a CCEP port-channel interface and user triggered events like Port-channel shut and no-shut are triggered.		

Parent Defect ID:	SLXOS-48868	**Issue ID:**	SLXOS-48868
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Management
Reported in Release:	SLXOS 20.1.2	**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-49266	**Issue ID:**	SLXOS-49266
Severity:	S4 - Low		
Product:	SLX-OS	**Technology Group:**	Management
Reported in Release:	SLXOS 20.1.2	**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.		

Parent Defect ID:	SLXOS-49323	**Issue ID:**	SLXOS-49323
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Other
Reported in Release:	SLXOS 20.1.2	**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-49371	**Issue ID:**	SLXOS-49371
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Network Automation and Orchestration
Reported in Release:	SLXOS 20.1.2	**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-49610	**Issue ID:**	SLXOS-49610
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.2	**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-49760	**Issue ID:**	SLXOS-49760
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.2	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	In MCT deployment, when executing certain disruptive CLI like 'cluster shut all' or 'no shut' on MCT node, user will observe that traffic takes few seconds to converge in scaled up configs.		
Condition:	In L3 MCT Deployment with scaled config of VE spread across large number of VRF, if cluster shut/no shut operation are executed for any purpose, use will observe traffic loss.		
Workaround:	User is recommended to use Maintenance mode, as it avoids significant traffic loss.		

Parent Defect ID:	SLXOS-50072	**Issue ID:**	SLXOS-50072
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.2	**Technology:**	VXLAN - Virtual Extensible LAN
Symptom:	When all the leaf-to-spine links in one of the MCT node towards the spine nodes are shutdown, it takes more than sub-seconds for convergence to move all the traffic towards the other MCT nodes		
Condition:	This will occur in IP Fabric deployments with SLX9150/9250, when all the links from one of MCT node towards all the spines are disconnected		

Parent Defect ID:	SLXOS-50076	**Issue ID:**	SLXOS-50076
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.2	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	In Centralized routing scenario, reloading one of the Border leaf node 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 node 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-50117	**Issue ID:**	SLXOS-50117
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.2	**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.		
Recovery:	unconfigure and reconfigure ospf will help recover		

Parent Defect ID:	SLXOS-50130	**Issue ID:**	SLXOS-50130
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Management
Reported in Release:	SLXOS 20.1.2	**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-50242	**Issue ID:**	SLXOS-50242
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Other
Reported in Release:	SLXOS 20.1.2	**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-50280	**Issue ID:**	SLXOS-50280
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.2	**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-50361	**Issue ID:**	SLXOS-50361
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.2	**Technology:**	VXLAN - Virtual Extensible LAN
Symptom:	When the Spine link used for sending BUM traffic is shut, there could be traffic loss of more than sub-second to divert all the BUM traffic to a different spine link. Similarly traffic loss is observed on reload of one of the MCT node.		
Condition:	Issue can happen during the spine link flap or node reload for BUM traffic only.		
Recovery:	traffic recovers by itself		

Parent Defect ID:	SLXOS-50734	**Issue ID:**	SLXOS-50734
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.2a	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	In MCT deployment, when mandatory configuration are missing from MCT, Reloading the switch in such config inconsistent state may causes all the CCEP clients to remain down after the reload.		
Condition:	Issue is only seen when cluster is in a shutdown/undeployed state - can only happen when some mandatory configuration (peer interface or IP) is missing under cluster config.		
Workaround:	Adding the complete cluster configurations will avoid the issue as partial config can lead to undefined behavior		

Parent Defect ID:	SLXOS-50787	**Issue ID:**	SLXOS-50787
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Other
Reported in Release:	SLXOS 20.1.2a	**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-47856	**Issue ID:**	SLXOS-50816
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Management
Reported in Release:	SLXOS 20.1.1	**Technology:**	Other
Symptom:	User might observe that on rare occasions TPVM installation fails during the TPVM deploy command.		
Condition:	The issue is observed rarely when TPVM is already installed and is present in an intermediate inconsistent state. As the current status of the installation cannot be retrieved, observe an error.		

Parent Defect ID:	SLXOS-50258	**Issue ID:**	SLXOS-50821
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Security
Reported in Release:	SLXOS 20.1.2	**Technology:**	HTTP/HTTPS
Symptom:	The syslog for successful import does not display IP address and role correctly for the current logged in user		
Condition:	User will observe this behavior when he Execute Crypto import pkcs12 command to import certificates		
Workaround:	This is not functional impact. The client IP can be known from another audit log where the user has successfully logged in into this terminal. The role can be known from username command in show run		

Parent Defect ID:	SLXOS-50870	**Issue ID:**	SLXOS-50870
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.2a	**Technology:**	Other
Symptom:	In case of MCT deployments with user induced kernel panic, traffic convergence takes more than a seconds delay		
Condition:	In MCT deployments, in case of user induced kernel panic to check convergence time, user may observe this behavior		

Parent Defect ID:	SLXOS-50873	**Issue ID:**	SLXOS-50873
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Security
Reported in Release:	SLXOS 20.1.2a	**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-50875	**Issue ID:**	SLXOS-50875
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Management
Reported in Release:	SLXOS 20.1.2a	**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		

Parent Defect ID:	SLXOS-50889	**Issue ID:**	SLXOS-50889
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.2a	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	In scaled BFD over Vxlan deployments, it sometimes observed that some of the BFD session may take longer time to come up after manual resetting of BFD session using 'clear bfd ' CLI command		
Condition:	User will observe this in BFD over VxLan or BFD over MCT scaled deployments, when BFD session are administratively brought down & up using 'clear bfd' CLI		
Recovery:	Remove BFD session configuration and re-apply help in faster recovery of such sessions.		

Parent Defect ID:	SLXOS-50890	**Issue ID:**	SLXOS-50890
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Security
Reported in Release:	SLXOS 20.1.2a	**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-50925	**Issue ID:**	SLXOS-50940
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.1	**Technology:**	MBGP - Multiprotocol Border Gateway Protocol
Symptom:	SLX reboots after an unexpected termination of BGP daemon		
Condition:	BGP peers are configured with inbound route-map with multiple permit instances. In some scenarios when one or more route-map instances are added/deleted to/from the route-map, an unexpected termination of the BGP daemon is observed causing the SLX to reboot warm		

Parent Defect ID:	SLXOS-50980	**Issue ID:**	SLXOS-50980
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Security
Reported in Release:	SLXOS 20.1.2a	**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:	Issue is seen when, 1. HTTPS is enabled on SLX device. 2. SLX device is accessed by HTTPS clients. Example, RESTCONF connection request to SLX device to gain access.		

Parent Defect ID:	SLXOS-51022	**Issue ID:**	SLXOS-51022
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.2a	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Cluster tracked interfaces are not displaying the exception reason string during the period when cluster bring-up is in progress		
Condition:	User will observe this issue when cluster-track feature is enabled and system is reloaded under planned maintenance-mode		

Parent Defect ID:	SLXOS-51046	**Issue ID:**	SLXOS-51046
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Management
Reported in Release:	SLXOS 20.1.2a	**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:	In the following sequence of operations, step 5 will fail due to stale entryfor TPVM IP Address in the /fabos/user/admin/.ssh/known_hosts. 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.		

Parent Defect ID:	SLXOS-51048	**Issue ID:**	SLXOS-51048
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Security
Reported in Release:	SLXOS 20.1.2a	**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 oauth2 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-51086	**Issue ID:**	SLXOS-51086
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Security
Reported in Release:	SLXOS 20.1.2a	**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:	The user will be prompted to continue with the session. User should Click Y on the prompt to continue.		

Parent Defect ID:	SLXOS-50968	**Issue ID:**	SLXOS-51113
Severity:	S1 - Critical		
Product:	SLX-OS	**Technology Group:**	Management
Reported in Release:	SLXOS 20.1.2	**Technology:**	Other
Symptom:	After Management port disable/enable, Glusterfs based partition is found corrupted, leading to EFA commands not working as expected in multi-node TPVM deployments		
Condition:	In a EFA/MCT setup, if management port is shut and then brought up by "no-shut, user will observe the EFA commands are not working as expected.		

Parent Defect ID:	SLXOS-51126	**Issue ID:**	SLXOS-51126
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Monitoring
Reported in Release:	SLXOS 20.1.2a	**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-51215	**Issue ID:**	SLXOS-51215
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.2a	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	User will observe that the MCT Cluster client interfaces are in shutdown state even when the device has come out of maintenance mode		
Condition:	The client interfaces are observed in down state only if the 'shutdown' was configured on MCT peer-interface, before bringing the node out of maintenance mode		
Workaround:	Bringing up the peer-interface before disabling the maintenance mode		
Recovery:	Re-enable and then disable maintenance mode after configuring 'no shutdown' on the peer-interface will help recover from the situation		

Parent Defect ID:	SLXOS-50579	**Issue ID:**	SLXOS-51225
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.1	**Technology:**	Other
Symptom:	On SLX 9540/SLX 9640, user will observe that Local-switching is enabled by default and disabling of local-switching within the Bridge domain is no longer supported.		
Condition:	On SLX 9540/SLX 9640, the CLI to disable Local switching is not available for Bridge Domain		

Parent Defect ID:	SLXOS-51230	**Issue ID:**	SLXOS-51230
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Management
Reported in Release:	SLXOS 20.1.2a	**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:	User instead of using "show efa status" from SLX CLI, can execute below steps to avoid the issue 1. login to TPVM 2. issue “efa version” from TPVM 3. Issue “k3s kubectl -n efa get all” from TPVM Sample output ++++++++++++ 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 pod/govcenter-service-f6b49d9b9-ljthb 1/1 Running 13 24m pod/gohyperv-service-854654f6b9-zjqwc 1/1 Running 12 24m NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE 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 replicaset.apps/gohyperv-service-854654f6b9 1 1 1 24m NAME READY AGE statefulset.apps/rabbitmq 1/1 24m admin@TPVM:~$

Parent Defect ID:	SLXOS-51235	**Issue ID:**	SLXOS-51235
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.2a	**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:	User can avoid the the issue by avoiding BFD holddown configuration.		
Recovery:	Removing hold-down interval & flapping interface.		

Defects Closed with Code Changes

The following software defects were closed with a code change as of **June 2020**.

Parent Defect ID:	SLXOS-47628	**Issue ID:**	SLXOS-47640
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.1	**Technology:**	ARP - Address Resolution Protocol
Symptom:	enable suppress-arp may not work once it has reached the system limit on SLX 9540		
Condition:	In a scaled environment with suppress-arp enabled on all the bridge domains, deletion and re-addition of BDs with suppress-arp enabled will fail on SLX9540		

Parent Defect ID:	SLXOS-47459	**Issue ID:**	SLXOS-47894
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.1	**Technology:**	LAG - Link Aggregation Group
Symptom:	In LACP Default-up enabled LAG, new Active link is not selected if selected Active link is Shutdown while PXE boot process is in progress		
Condition:	In LACP Default-up enabled LAG, all LAG links will remain UP and no new Active link is selected, if user manually Shutdown already selected Active link.		
Recovery:	User should remove and reconfigure 'lacp default-up' on all LAG member links to recover from this situation.		

Parent Defect ID:	SLXOS-47450	**Issue ID:**	SLXOS-48031
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.1	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Traffic loss will be seen if one of the ECMP path goes down in BGP PIC deployment scenario		
Condition:	With BGP PIC enabled and if the local BGP has also done 'redistribute static', with same Prefix and same nexthop IP as coming from remote BGP Peer, shutting down this path will result in traffic loss.		
Workaround:	Remove the conflicting 'redistribute static' configuration.		

Parent Defect ID:	SLXOS-47803	**Issue ID:**	SLXOS-48070
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.1	**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		
Recovery:	System reload		

Parent Defect ID:	SLXOS-45114	**Issue ID:**	SLXOS-48122
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.1	**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-47652	**Issue ID:**	SLXOS-48222
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.1	**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.		
Recovery:	Clearing impacted mac/arp/nd should cause them to re-learn and resolve the issue.		

Parent Defect ID:	SLXOS-48752	**Issue ID:**	SLXOS-48752
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.2	**Technology:**	LAG - Link Aggregation Group
Symptom:	User will observe occasional LACP flap when LACP is configured with short-timeout and system is under stress due to high CPU load		
Condition:	Issue is observed when LACP is configured with short timeout and CPU load is higher due to higher scale or higher CPU based packet processing		

Parent Defect ID:	SLXOS-48854	**Issue ID:**	SLXOS-48854
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Management
Reported in Release:	SLXOS 20.1.2	**Technology:**	CLI - Command Line Interface
Symptom:	For PBR based route map, user may observe Unexpected reload of the device while unconfiguring route-map.		
Condition:	Configure PBR route-map and apply it on port-channel interface. Unconfigure route-map without removing its association from the port-channel interface. On repeated application of above steps of configure/unconfigure, user may observe unexpected reload		
Workaround:	Before unconfiguring route-map, remove the route-map association from the port-channel interface.		

Parent Defect ID:	SLXOS-48686	**Issue ID:**	SLXOS-49105
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Management
Reported in Release:	SLXOS 20.1.1	**Technology:**	CLI - Command Line Interface
Symptom:	In SLX 9540/SLX 9640, FEC mode setting CLI is not available in 20.1.1. This impacts the FEC operations.		
Condition:	User will observe that FEC CLI are not available in 20.1.1 on SLX 9540/SLX9640		

Parent Defect ID:	SLXOS-49149	**Issue ID:**	SLXOS-49149
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Security
Reported in Release:	SLXOS 20.1.2	**Technology:**	User Accounts & Passwords
Symptom:	Admin user can get the root privileges		
Condition:	when user try to use start-shell, python, OSCMD from admin login		

Parent Defect ID:	SLXOS-47823	**Issue ID:**	SLXOS-49166
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.1	**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		
Recovery:	none		

Parent Defect ID:	SLXOS-46276	**Issue ID:**	SLXOS-49339
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.1	**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-50018	**Issue ID:**	SLXOS-50018
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Security
Reported in Release:	SLXOS 20.1.2	**Technology:**	SSH - Secure Shell
Symptom:	Security audit log indicates login happened via "ssh/CLI" instead of "ssh/netnonf" when login was successful via NETCONF session.		
Condition:	This audit log issue occurs when user tries to login via NETCONF session.		
Workaround:	User can observe the description portion of the same audit log to verify the correct value - (Successful login attempt via NETCONF).		

Parent Defect ID:	SLXOS-50073	**Issue ID:**	SLXOS-50073
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Security
Reported in Release:	SLXOS 20.1.2	**Technology:**	ACLs - Access Control Lists
Symptom:	On SLX 9540/SLX9640, user may experience unexpected reload when Broadcast ACL applied on VE interface is modified.		
Condition:	This issue may be observed while using VE and Broadcast ACL is applied on VE , followed by modification of ACL.		
Workaround:	If ACL is applied as broadcast ACL on VE interface, then broadcast ACL should be removed and then ACL should be modified.		

Parent Defect ID:	SLXOS-50074	**Issue ID:**	SLXOS-50074
Severity:	S4 - Low		
Product:	SLX-OS	**Technology Group:**	Security
Reported in Release:	SLXOS 20.1.2	**Technology:**	AAA - Authentication, Authorization, and Accounting
Symptom:	While trying to delete a non-existent LDAP server on TPVM, the CLI command returns success instead of showing an error that the server doesn't exist in the configuration database.		
Condition:	This issue is seen when trying to remove an LDAP server which was not configured in the TPVM.		
Workaround:	None		

Parent Defect ID:	SLXOS-50090	**Issue ID:**	SLXOS-50090
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.2	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Reload delay configured on CEP port-channels gets activated as soon as config gets replayed on the switch after reload. This makes switch to go to operational before it is completely ready. (Note : It is recommended to configure proper reload delay with CEP port-channels).		
Condition:	This condition will occur when CEP port-channels are configured with reload delay on MCT node and the node reload operation is performed		
Workaround:	Reload delay should be configured based on time taken for config replay. This delay will ensure that when the MCT node goes for reload, the switch is completely operational before bringing the CEP port-channels up. For a moderate config size, reload delay can be configured as 300 sec		
Recovery:	.		

Parent Defect ID:	SLXOS-50148	**Issue ID:**	SLXOS-50148
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Security
Reported in Release:	SLXOS 20.1.2	**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.		

Parent Defect ID:	SLXOS-50162	**Issue ID:**	SLXOS-50162
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.2	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	When IP address and IP anycast address is configured with the same subnet on vlan interface and BGP neighbor is created for the same subnet, customer might experience session not being formed.		
Condition:	Only when IP anycast address and IP address is configured with same subnet on Vlan interface and if BGP neighbor is added for user-vrf, session might not come up due to source IP being ip anycast IP, instead of primary IP address.		
Workaround:	IP anycast and IP address should be configured in different subnet range for BGP session to be established.		

Parent Defect ID:	SLXOS-50164	**Issue ID:**	SLXOS-50164
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.2	**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-50172	**Issue ID:**	SLXOS-50172
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 20.1.2	**Technology:**	BFD - BiDirectional Forwarding Detection
Symptom:	ON SLX 9540/SLX9640, BFD session uses default BFD interval values instead of configured values.		
Condition:	After reload of device, BFD sessions enabled over L3 port-channel uses default BFD transmit interval,receive interval and multiplier values instead of configured values.		
Workaround:	After reload of device re-configure new transmit interval,receive interval and multiplier values.		

Parent Defect ID:	SLXOS-50174	**Issue ID:**	SLXOS-50174
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.2	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Client ports are not coming up after maintenance mode 'no enable',if ICL is made admin down on peer MCT node.		
Condition:	After 'no enable' under maintenance mode, MCT client ports are not brought back online if the ICL interface on the remote peer are down.		
Workaround:	Bring the ICL interface online on the remote MCT node which is not under maintenance in the case of a 2 node MCT deployment.		

Parent Defect ID:	SLXOS-50175	**Issue ID:**	SLXOS-50175
Severity:	S2 - High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.2	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	While enabling maintenance mode, User may observe sub-second traffic loss for the streams running across the CCEP ports in MCT deployments, where the number of CCEP port is substantially large.		
Condition:	User will experience the traffic loss condition while executing "Enable" under system maintenance configuration mode.		

Parent Defect ID:	SLXOS-50177	**Issue ID:**	SLXOS-50177
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 20.1.2	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	In rare scenario, MCT keep-alive session may flap, when cluster shut all or maintenance mode is disabled. There is no functional impact with the flap (doesn't cause the clients to flap or traffic loss).		
Condition:	Issue may be observed when user execute 'cluster 'no shutdown all'' or Under the system maintenance CLI configuration context, 'no enable' is performed.		

Defects Closed without Code Changes

The following software defects were closed without a code change as of **June 2020**.

Parent Defect ID:	SLXOS-48439	**Issue ID:**	SLXOS-48439
Reason Code:	Will Not Fix	**Severity:**	S2 - High
Product:	SLX-OS	**Technology Group:**	Network Automation and Orchestration
Reported in Release:	SLXOS 20.1.2	**Technology:**	NETCONF - Network Configuration Protocol
Symptom:	NETCONF query for SSH client configuration may fail with "expected type string, got uint32." error.		
Condition:	This issue occurs when "ssh client source-interface" is configured.		
Workaround:	use alternative methods like CLI or REST(instead of NETCONF) to retrieve the operational data (SSH client configuration) that is having this issue.		

Parent Defect ID:	SLXOS-49979	**Issue ID:**	SLXOS-49979
Reason Code:	Design Limitation	**Severity:**	S2 - High
Product:	SLX-OS	**Technology Group:**	Other
Reported in Release:	SLXOS 20.1.2	**Technology:**	Other
Symptom:	When two LDAP servers with same IP address but different port was configured on TPVM, trying to remove the port alone leaves the configuration with two LDAP server entries of same IP and same port (duplicate entries).		
Condition:	This issue is seen when two LDAP server with same IP but one with default port and another one with non-default port is configured in TPVM.		
Workaround:	In the specified use case, to make any changes to the existing TPVM LDAP server configuration, first remove both the LDAP servers using 'remove' command and then add the LDAP server address with the required ports again.		

Parent Defect ID:	SLXOS-50061	**Issue ID:**	SLXOS-50061
Reason Code:	Will Not Fix	**Severity:**	S2 - High
Product:	SLX-OS	**Technology Group:**	Other
Reported in Release:	SLXOS 20.1.2	**Technology:**	Other
Symptom:	When an LDAP server address with 'secure' option (LDAP over TLS) is configured, removing the 'secure' mode modifies the LDAP over TLS server to plain LDAP server (using the same IP address). However, it does not reset the port number to default LDAP port (i.e 389).		
Condition:	This issue is seen when 'secure' mode alone is removed, keeping the LDAP server IP address as is.		
Workaround:	In the issue scenario, if you want the port to reset back to default port, please run the following command for that LDAP server IP address. SLX# tpvm config ldap remove host <IP address> port		