19 November 2018

SLX-OS 18x.1.00 for SLX 9030-48S and SLX 9030-48T

Release Notes v1.0

© 2018, Extreme Networks, Inc. All Rights Reserved.

Contents

Document history

Version	Summary of changes	Publication date
1.0	Initial Release	November 19, 2018

Preface

- ## Contacting Extreme Technical Support

- As an Extreme customer, you can contact Extreme Technical Support using one of the following methods: 24x7 online or by telephone. OEM customers should contact their OEM/solution provider.
- If you require assistance, contact Extreme Networks using one of the following methods:
- GTAC (Global Technical Assistance Center) for immediate support
- Phone: 1-800-998-2408 (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.
- Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge - Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub - A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal - Manage cases, downloads, service contracts, product licensing, and training and certifications.
- Before contacting Extreme Networks for technical support, have the following information ready:
- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) 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

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

Quality is our first concern at Extreme, and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you.

You can provide feedback in two ways:

• Use our short online feedback form at http://www.extremenetworks.com/documentation-feedback-pdf/

• Email us at internalinfodev@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.

Overview

Supported Platforms

SLX-OS 18x.1.00 release supports the following SLX platforms:

- SLX 9030-48S: 48 x 10/1G + 4 x 100/40G
- SLX 9030-48T: 48 x 10/1G/100M + 4 x 100/40G

Supported Modes

Standalone bare-metal mode

SLX 9030-48S and SLX 9030-48T are fixed 1U switches that are used as the datacenter leaf switches. SLX 9030-48S provides 48x10/1G fiber ports for server connectivity along with 4x100/40G uplink ports. SLX 9030-48T provides 48x10/1G/100M copper ports for server connectivity along with 4x100/40G uplink ports. These switches are released as a part of SLX-OS 18x.1.00.

- High density 40G/100G spine-leaf connection
- Native 10/G/1G/100M server connectivity at the leaf
- High performance VXLAN routing
- Port-to-port Latency: 1us

Software Features

New software features in 18x.1.00

The following software features are supported in 18x.1.00:

- Layer 2/Layer 3 Forwarding, VLAN, LLDP, ARP/NDP, STP/MSTP, OSPF, BGP, VRRP, and Default VRF only

- Layer 2 and Layer 3 ACL

- LAG

- SPAN/SFlow

- Zero Touch Provisioning (ZTP) (No reboot required after ZTP)

- SNMP/REST

- Telemetry Streaming for CPU/Memory/Interface Statistics

- Shaper/Scheduler, COS/DSCP Remark – Port and Flow based

- QoS – Policers

- ACL on LAG

- Thermal Policy

- Layer 3 Scale (Host Routes only)

- Platform
    - All basic platform features
    - Breakout
    - Interface LED (new)

- VxLAN
    - Layer 2 Gateway
    - Router port and untagged VLAN VW

- User defined VRF

- Static Anycast Gateway (SAG)/Unnumbered Interface

- MCT

- Operational Diag

- ARP Suppression

- Conversational ARP

- ICMP Rate-limiting (IP Stack)

- Layer 3 MCT

- Layer 3 VxLAN

- DHCP Relay

- Multicast IGMPv1v2v3 Snooping Control plane and Data Path support

- QoS – WRED

- LVTEP

- Source Suppression with LVTEP and ARP Suppression

Unsupported features in the 18x.1.00 release:

- BFD
- MPLS
- VPLD (VLL)
- MVRP
- ISIS
- GuestVM
- UDLD

The following solution is supported in SLX-OS 18x.1.00:

- EVPN VxLAN based Network Virtualization Overlay

1. BGP-EVPN (VxLAN) – EVPN VxLAN based Network Virtualization Overlay

BGP eVPN Network Virtualization is a controller-less architecture that simplifies data center operations by leveraging open, standards-based protocols to abstract network control plane, data plane, and automation functions from the underlying physical platforms. As an integral part of the Extreme open data center design stack elements, BGP eVPN Network Virtualization builds upon underlying infrastructure platforms, fabrics, and automation to deliver simplified and secure network operations.

The following table lists the set of new features coming in SLX-OS 18x.1.00

Feature Name	Feature Description
BGP eVPN	Standards based, Controller-less Network Virtualization Overlays with VxLAN encapsulation. Provides automatic VxLAN tunnel end point discovery, end host MAC and MAC-IP learning over the control plane.
ARP Suppression	Suppress/reduce the ARP broadcast traffic in an IP fabric.
Static Anycast Gateway	Static Anycast Gateway allows configuring Static Anycast MAC as gateway for multiple tenant systems in a virtualized data center fabric. Same Gateway address is configured across all TORs for a given Tenant/VLAN combination, thus enabling seamless VM mobility across the leaf switches in an IP Fabric deployment without any need for host gateway configuration changes.
Conversational ARP	ARP entries for active conversations only (helps optimize ARP table size)
IP Unnumbered Interfaces	Reduces consumption of IP Address space. Leaf to spine inter-switch point-to-point L3 links are configured as ip unnumbered (/31 subnets) to conserve IP addresses and optimize hardware resources.
L2 VNI capability	The L2VNI is the MAC/NVE mapping table
L3 VNI	The L3VNI is IP prefix/NVE mapping table
Dynamic tunnel (VxLAN) discovery	Supports Dynamic Tunnel discovery using BGP EVPN.
Cluster Management	Configuration management between MCT nodes for logical VTEP is supported.
Manageability, Monitoring, Debugging	NetConf, RESTful API provisioning, VRF support for Telnet/SNMP/SSH,

	VxLAN tunnel traffic statistics, Show/debug commands

Consolidated Features in SLX-OS 18x.1.00

Following table lists the features present in SLX-OS 18x.1.00.

Layer 2 Switching

- Layer 2 Access Control Lists (ACLs)
- Address Resolution Protocol (ARP) RFC 826
- IGMP v1/v2/v3 Snooping
- MAC Learning and Aging
- Link Aggregation Control Protocol (LACP) IEEE 802.3ad/802.1AX
- Virtual Local Area Networks (VLANs)
- VLAN Encapsulation 802.1Q
- BD Support
- Per-VLAN Spanning Tree (PVST+/PVRST+)
- Rapid Spanning Tree Protocol (RSTP) 802.1w
- Multiple Spanning Tree Protocol (MSTP) 802.1s

- Pause Frames 802.3x
- Static MAC Configuration
- Multi-Chassis Trunking (MCT)
- VXLAN extenstion tunnels
- Overlay services: overlay gateway instances, overlay transit instances (on spine nodes)

Layer 3 Routing

- Border Gateway Protocol (BGP4+)
- DHCP Helper
- OSPF v2/v3
- Static routes
- IPv4/v6 ACL
- Route Policies
- 32-Way ECMP
- VRF Lite
- VRF-aware OSPF, BGP, VRRP, static routes
- VRRP v2 and v3
- Anycast Gateway over VxLAN

- IPv4/IPv6 dual stack
- ICMPv6 Route-Advertisement Guard IPv6 ACL packet filtering
- BGP-Allow AS
- IPv6 routing
- Multi-VRF
- L3 over Bridge Domains (BD)

Automation and Programmability

- gRPC Streaming protocol and API
- REST API with YANG data model
- Python

- DHCP automatic provisioning
- NETCONF API

Quality of Service

- ACL-based QoS
- Two Lossless priority levels for QoS

- Random Early Discard
- Per-port QoS configuration

• Class of Service (CoS) IEEE 802.1p • DSCP Trust • DSCP to Traffic Class Mutation • DSCP to CoS Mutation • DSCP to DSCP Mutation • CoPP (Control Plane Policing)	• ACL-based Rate Limit • Dual-rate, three-color token bucket • ACL-based remarking of CoS/DSCP/Precedence • ACL-based sFlow • Scheduling: Strict Priority (SP), Deficit Weighted Round-Robin (DWRR)

Management and Monitoring

• Zero-Touch Provisioning (ZTP) • IPv4/IPv6 management • Industry-standard Command Line Interface (CLI) • NETCONF API • REST API with YANG data model • SSH/SSHv2 • Link Layer Discovery Protocol (LLDP) IEEE 802.1AB • MIB II RFC 1213 MIB • Syslog (RASlog, AuditLog) • Management VRF • Switched Port Analyzer (SPAN) • Telnet	• SNMP v1, v2C, v3 • sFlow version 5 • Out-of-band management • RMON-1, RMON-2 • NTP • Management Access Control Lists (ACLs) • Role-Based Access Control (RBAC) • Range CLI support • Python • DHCP Relay • SLX-OS and Linux Shell Interoperability

Security

• RADIUS – Authentication and Authorization • AAA • TACACS+ • Secure Shell (SSHv2) • TLS 1.1, 1.2 • HTTP/HTTPS	• BPDU Drop • Secure Copy Protocol • Control Plane Protection • SFTP

IP Fabric

• Controllerless Network Virtualization (BGP-EVPN) • ARP surpression • Conversational ARP • Static Anycast Gateway	• Logical VTEP (Static and EVPN) • IP Un-numbered interface • RIOT (Routing In and Out of Tunnel) (v4 and v6)

Platform

• 1G/10G/40G/100G Auto speed detection • Multi Speed(1G/10G) Optic Support	40G 4x10G /100G 4x25 Breakout Support

Important Notes

Zero Touch Provisioning (ZTP)

- ZTP is enabled by default on SLX switches from factory or by "write erase". Upon switch power-on or reboot by "write erase", it will automatically connect to DHCP server through both management interface and inband ports with connection for firmware to download and configuring the switch based on the DHCP configuration.

- If the switch does not have a DHCP server connected or the DHCP server is not configured for ZTP, the switch will keep searching the DHCP server for ZTP.

  The serial console of the switch will display ZTP message as following:

  ZTP, Sat Nov 17 07:55:37 2018, ========== ZTP start ==========

  ZTP, Sat Nov 17 07:55:37 2018, disable raslog

  ZTP, Sat Nov 17 07:55:37 2018, CLI is ready

  ZTP, Sat Nov 17 07:55:49 2018, inband ports are enabled

  ZTP, Sat Nov 17 07:55:49 2018, serial number = 1818N-41522

  ZTP, Sat Nov 17 07:55:49 2018, model name = EN-SLX-9030-48S

  ZTP, Sat Nov 17 07:55:49 2018, use both management interface and inband interfaces

  ZTP, Sat Nov 17 07:55:49 2018, checking inband interfaces link status

  ZTP, Sat Nov 17 07:56:43 2018, find link up on interfaces: eth0 Eth0.1 Eth0.9 Eth0.10 Eth0.11

  ZTP, Sat Nov 17 07:56:43 2018, start dhcp process on interfaces: eth0 Eth0.1 Eth0.9 Eth0.10 Eth0.11

  ZTP, Sat Nov 17 07:56:53 2018, get no dhcp response from all interfaces

  ZTP, Sat Nov 17 07:56:53 2018, retry in 10 seconds

  ZTP, Sat Nov 17 07:57:03 2018, inband ports are enabled

  ZTP, Sat Nov 17 07:57:03 2018, serial number = 1818N-41522

  ZTP, Sat Nov 17 07:57:03 2018, model name = EN-SLX-9030-48S

  ZTP, Sat Nov 17 07:57:03 2018, use both management interface and inband interfaces

  ZTP, Sat Nov 17 07:57:03 2018, checking inband interfaces link status

  ZTP, Sat Nov 17 07:57:04 2018, find link up on interfaces: eth0 Eth0.1 Eth0.6 Eth0.9 Eth0.10 Eth0.11

ZTP, Sat Nov 17 07:57:04 2018, start dhcp process on interfaces: eth0 Eth0.1 Eth0.6 Eth0.9 Eth0.10 Eth0.11

ZTP, Sat Nov 17 07:57:14 2018, get no dhcp response from all interfaces

ZTP, Sat Nov 17 07:57:14 2018, retry in 10 seconds

You need to login onto the serial console, wait for the above message to show up to confirm ZTP has been triggered, and then run "dhcp ztp cancel" and "reload system" to cancel the ZTP operation.

SLX# dhcp ztp cancel

ZTP is canceled.

SLX#

SLX#

SLX# dhcp ztp cancel

ZTP is not enabled.

SLX#

After dhcp ztp cancel, reload is not required.

SLX# SLX# reload system

Warning: This operation will cause the chassis to reboot and

requires all existing telnet, secure telnet and SSH sessions to be

restarted.

Unsaved configuration will be lost. Please run `copy running-config startup-config` to save the current configuration if not done already.

Are you sure you want to reboot the chassis [y/n]? y

[940.360081] VBLADE: vblade_control: FEPORTS_DISABLE

xpDma::quiesce:307 devId=0

xpDriverWrapper::quiesce:146 devId=0

FABOS_BLADE_MSG_BL_DISABLE received in HSLUA for chip 0

2017/03/27-21:14:13, [RAS-1007], 567,, INFO, SLX9030, System is about to reload.

Platform:

O   "Error:soc_reg_above_64_field32_read(IQM_OCCUPIED_BD_COUNTERr) failed for unit 0 core 0 " is seeing on console when collecting SS

O   Console is flooded with "ifStats: get_if_utilization failsifStats" when collecting supportsave

O   ssh source interface as ethernet packet capture is not worknig after removing the source-intf ip address

O   Custom RPC call "show-ntp" is providing empty output instead of the active NTP server

O   Account log is showing SSH instead of unique tty identifier while login through SSH; after login, it's behaving correct

O   Login message says " admin connected using console" instead of "telnet" when accessing the switch via telnet

O   NTP is using wrong ip as source ip to send ntp packet out of OOB mgmt-interface after sh/no shut of mgmt.

O   Switches are taking default option as 'y', instead of 'no input' for 'y/n' prompt for 'reload system', 'firmware" etc commands.

o   Issues with special-characters in password.
- Dollar sign ($), double-quote sign ("), and single-quote (') are not supported by the firmware download command.
- Double-quote (") is not supported the copy support command.
- Single-quote (') is not supported by the copy config command.

o   The "copy <file> running-config" will always return success if you only specify the configuration file path but not the file name.

RFCs and Standards

For RFCs, standards, and scale numbers supported in 18x.1.00, refer to the [Extreme SLX-OS Scale and Standards Matrix for SLX 9030](#)

Hardware support

SLX 9030 Hardware and License SKUs

SKU	Description
EN-SLX-9030-48S-4C-AC-F	Extreme SLX 9030-48S Switch AC with Front to Back Airflow, Supports 48x10GE/1GE + 4x100GE/40GE
EN-SLX-9030-48S-4C-AC-R	Extreme SLX 9030-48S Switch AC with Back to Front Airflow, Supports 48x10GE/1GE + 4x100GE/40GE
EN-SLX-9030-48S-4C	Extreme SLX 9030-48S Switch with No Power supplies, no fans, Supports 48x10GE/1GE + 4x100GE/40GE
EN-SLX-9030-48T-4C-AC-F	Extreme SLX 9030-48T 10GBaseT Switch AC with Front to Back Airflow, Supports 48x10GE/1GE + 4x100GE/40GE
EN-SLX-9030-48T-4C-AC-R	Extreme SLX 9030-48T 10GBaseT Switch AC with Back to Front Airflow, Supports 48x10GE/1GE + 4x100GE/40GE
EN-SLX-9030-48T-4C	Extreme SLX 9030-48T 10GBaseT Switch with No Power supplies, no fans, Supports 48x10GE/1GE + 4x100GE/40GE
EN-SLX-9030-ADV-LIC-P	SLX 9030 Advanced Feature License for BGP-EVPN, gRPC

Supported Power supplies

The following table lists the power supplies that are available for the devices supported in this release:

SKU	Description
17115	Fan module, Front to Back airflow
17116	Fan module, Back to Front airflow
10960	770W AC power supply, Front -to-Back airflow
10961	770W AC power supply, Back-to-Front airflow
10962	1100W DC power supply, Front -to-Back airflow
10963	1100W DC power supply, Back-to-Front airflow

Supported Optics

For a list of supported fiber-optic transceivers that are available from Extreme Networks, refer to the latest version of the Extreme Netowrks Optics Family Data Sheet available online at www.extremenetworks.com.

Description	SKU	MFG Part Number
1000Base-SX SFP optic, MMF, LC connector, Optical Monitoring Capable	1G-SFP-SX-OM	33210-100
1000Base-LX SFP optic, SMF, LC connector, Optical Monitoring Capable	1G-SFP-LX-OM	33211-100
1000BASE-TX SFP Copper, RJ-45 Connector	1G-SFP-TX	33002-100
1GE COPPER SFP,1-PK, ROHS	1G-SFP-000190	57-1000042-02
10GBASE-USR, SFP+ optic (LC), target range 100m over MMF,	10G-SFP-USR	57-1000130-01
10GBASE-USR, SFP+ optic (LC), target range 100m over MMF 70C TAA COMPLIANT	10G-SFP- USR-SA	57-1000343-01
10GBASE-SR, SFP+ optic (LC), target range 300m over MMF , 80C	10G-SFP-SR	57-0000075-01
10GBASE-SR,SFP+ MMF LC CONNECTOR , 70C	10G-SFP-SR-S	57-1000340-01
10GBASE-SR, SFP+ optic (LC), target range 300m over MMF 70C-TAA COMPLIANT	10G-SFP-SR-SA	57-1000344-01
10GBASE-LR, SFP+ optic (LC), for up to 10km over SMF	10G-SFP-LR	57-0000076-01
10GBASE-LR,SFP+ SMF LC CONNECTOR (No TAA), 70C	10G-SFP-LR-S	57-1000341-01
10GBASE-LR, SFP+ optic (LC), for up to 10km over SMF 70C - TAA COMPLIANT	10G-SFP-LR-SA	57-1000345-01
10GBASE-ER SFP+ optic (LC), for up to 40km over SMF	10G-SFP-ER	57-0000058-01
10GBASE-ZR SFP+ optic (LC), for up to 80km over SMF	10G-SFP-ZR	57-1000180-01
10GBASE-ZRD SFP+ optic (LC), for up to 80km over SMF	10G-SFP-ZRD-T	57-1000266-01
ACTIVE DIRECT ATTACHED SFP+ COPPER, 1MTR, 1-PK	10G-SFP-TWX-0101	58-1000026-01
ACTIVE DIRECT ATTACHED SFP+ COPPER, 3MTR,1-PK	10G-SFP-TWX-0301	58-1000027-01
ACTIVE DIRECT ATTACHED SFP+ COPPER, 5MTR,1-PK	10G-SFP-TWX-0501	58-1000023-01
PASSIVE DIRECT ATTACHED SFP+ COPPER, 1MTR, 1-PK	10G-SFP-TWX-P-0101	58-1000024-01
PASSIVE DIRECT ATTACHED SFP+ COPPER, 3MTR,1-PK	10G-SFP-TWX-P-0301	58-1000025-01
PASSIVE DIRECT ATTACHED SFP+ COPPER, 5MTR,1-PK	10G-SFP-TWX-P-0501	58-1000019-01
10GE SFP+ Direct Attached Active Optical Cable, 7m, 1-pack	10G-SFP-AOC-0701	57-1000273-01
10GE SFP+ Direct Attached Active Optical Cable, 10m, 1-pack	10G-SFP-AOC-1001	57-1000274-01
10GBASE-T SFP+	10338	908711-10
40GBASE-SR4 QSFP+ optic (MTP 1x8 or 1x12), 100m over MMF, 1-pack	40G-QSFP-SR4-1	57-1000128-01
40GBASE-SR4 QSFP+ optic (MTP 1x8 or 1x12), 100m over MMF, compatible with 10GBASE-SR, 10G breakout-capable, 1-pack	40G-QSFP-SR4-INT	57-1000129-01
40GBase-LR4 QSFP+ optic (LC), for up to 10km over SMF, 1-pack	40G-QSFP-LR4-1	57-1000263-01
40GBase-LR4 QSFP+ to 4 SFP+ optic (LC), for up to 10km over SMF, 1-pack	40G-QSFP-LR4-INT	57-1000477-01
40GBASE-LM4 QSFP+, 1310nm, 160m over duplex LC OM4 MMF, 2km over duplex LC SMF	40G-QSFP-LM4	57-1000325-01
40GBase-ER4 QSFP+ optic (LC), for up to 40km over SMF	40G-QSFP-ER4-1	57-1000327-01
40GE SR QSFP+ optic (LC), Bidirectional, 100m over OM3 MMF	40G-QSFP-SR-BIDI	57-1000339-01

4x10GE QSFP+ to 4 SFP+ Active Copper Cable 1 M	40G-QSFP-4SFP-C-0101	58-0000051-01
4x10GE QSFP+ to 4 SFP+ Active Copper Cable 3 M	40G-QSFP-4SFP-C-0301	58-0000052-01
4x10GE QSFP+ to 4 SFP+ Active Copper Cable 3 M	40G-QSFP-4SFP-C-0501	58-0000053-01
40GE Direct Attached QSFP+ to QSFP+ Active Copper cable, 1m, 1-pack	40G-QSFP-QSFP-C-0101	58-0000041-01
40GE Direct Attached QSFP+ to QSFP+ Active Copper cable, 3m, 1-pack	40G-QSFP-QSFP-C-0301	58-0000042-01
40GE Direct Attached QSFP+ to QSFP+ Active Copper cable, 5m, 1-pack	40G-QSFP-QSFP-C-0501	58-0000043-01
40GE QSFP Direct Attached Passive Copper Cable, 1m, 1-pack	40G-QSFP-QSFP-P-0101	58-0000033-01
40GE QSFP Direct Attached Passive Copper Cable, 5m, 1-pack	40G-QSFP-QSFP-P-0501	58-0000035-01
40GE Direct Attached QSFP+ to QSFP+ Active Optical Cable, 10m, 1-pack	40G-QSFP-QSFP-AOC-1001	57-1000306-01
100 GbE QSFP28 optic (LC), LR4 low power, for distances up to 10 km over SMF	100G-QSFP28-LR4-LP-10KM	57-1000338-01
100 GbE QSFP28 optic (LC), LR4-lite, for distances up to 2 km over SMF	100G-QSFP28-LR4L-2KM	57-1000329-01
100 GbE QSFP28 optic (MTP 1x12), SR4, for distances up to 100 m over MMF	100G-QSFP28-SR4	57-1000326-01
100GBASE-ESR4 QSFP+ optic (MTP 1x8 or 1x12), eSR4, for distances up to 300 m over MMF	100G-QSFP-ESR4	57-1000352-01
100 GbE QSFP28 optic (LC), CWDM4, for distances up to 2 km over SMF	100G-QSFP28-CWDM4-2KM	57-1000336-01
100GE Direct Attached QSFP+ to QSFP+ Active Optical Cable, 10m, 1-pack	100G-QSFP-QSFP-AOC-1001-10m	57-1000347-01
100GE Direct Attached QSFP-28 to QSFP-28 Passive Copper cable, 1m	100G-QSFP-QSFP-P-0101	58-0000044-01
100GE Direct Attached QSFP-28 to QSFP-28 Passive Copper cable, 3m	100G-QSFP-QSFP-P-0301	58-0000045-01

Software upgrade and downgrade

Image file names

Download the following images from www.extremenetworks.com.

Image file name	Description
slxos18x.1.00.tar.gz	SLX-OS 18x.1.00 software
slxos18x.1.00_all_mibs.tar.gz	SLX-OS 18x.1.00 MIBS
slxos18x.1.00.md5	SLX-OS 18x.1.00 md5 checksum

Migration path

Recommended upgrade/downgrade migration path.

To From	SLX 18x.1.00_CR	SLX 18x.1.00
SLX 18x.1.00_CR	NA	Default - config
SLX 18x.1.00	Default - config	NA

Limitations and restrictions

- **IGMPv2 snooping**
  - Unknown multicast packets on IGMP snooping enabled vlans are dropped
  - In IGMPv3, only Include mode is supported

- **IP Fabric**
  - MCT cluster may not form or remote CCEP down, if router-id is toggled.
  - A few IP Anycast gateways are not active after save and reload of the system.
  - Removing and adding loopback interface or rebooting local MCT node causes client interface to go down on remote node
  - 'show mac-address-table evpn' also retrieves "Dynamic-CCL" MACs.
  - Logical VTEP flaps after node reboot or flapping underlay interfaces.
  - Sometimes moving L3VNI from Vlan to BD impacts traffic forwarding
  - Some mac-address learnt via ICL tunnel in "show mac-address" shows as unresolved.
  - SAG scale is supported for 256 VE interfaces.
  - Stale mac/arp entries exists after cluster config is removed.
  - "'clear bgp evpn neighbor dynamic all' reports error, as the command is not implemented
  - Traffic Convergence takes time on MCT scale (61k IPv4 prefix routes)
  - IPv6 Type5 remote prefix is not installed in h/w after delete and re-create VRF
  - Sometimes, switch not recovering from tunnel ID conflict causing tunnel flap.
  - Vlans are not getting extended to ICL tunnel resulting in traffic drop when manual vlan vni mapping is used
  - LVTEP to LVTEP L3 VNI Traffic is failing for some Hosts when cluster gateway is enabled.
  - Management cluster not forming after overlay-gateway deactivate/re-activate
  - Some config under 'overlay-gateway' is missing after replaying the config from remote
  - "show tunnel brief" displays wrong vrf name when tunnels are admin up and operation down.
  - Sometimes tunnel status not synchronized between LVTEP nodes.
  - MAC description of CCluster Local MAC' and Cluster Remote MAC not correct.
  - "show mac-address" table displays mac are active on CCEP Port-channel interface even though all the ports are down
  - After "clear bgp evpn neighbor all" trigger, cluster is not converging.

- **Layer 2**:
  - **System supports maximum scale of 2k mac-addresses on the system.**
  - Few MAC addresseses are not learnt when traffic is sent at scale (64K mac addresses) due to hash collisions.
  - Packets gets transiently duplicated when member interface in port channel is toggled.
  - Sometimes forwarding traffic on port-channel interface is disrupted (interface is going to blocking state in h/w - even though its in forwarding state in software)
  - Traffic not load balanced on LAG when destination IP gets incremented and hashing is set only for dst-ip.
  - Bridge-domain command does not accept range

- o "show system internal vxlan" command are working.
- o show mac-address count interface port-channe <>" is showing wrong "remote address count"

- **Layer3:**
  - o **VRRP**
    - ▪ Unable to configure virtual IP with VRRP v3 if the ipv4 prefix length is /31

  - o **IP**
    - ▪ Sometimes, IPv6 Asymmetric traffic are software forwarded.
    - ▪ "show interface loopback <>" displays incorrect mtu value.
    - ▪ "Duplicate IP addess with null mac messages detected for static arp configured while enabling STP
    - ▪ With combination of triggers (add/remote/reboot) Switch does not display management interface network in ipv6 routing table when management interface get-detail not returning all VE interfaces
    - ▪
  - o **BGP:**
    - ▪ Under vrf AF, "no export map" is accepted eventhough there is no <cr>,
    - ▪ Under vrf AF, "no export map", the 'no' operation of 'export map' command does not work
    - ▪ On removing Rd under VRF, Static routes persists in the system- leading to error message on static route reconfiguration
    - ▪ When the max-route limit for v4/v6 prefixes in a VRF is removed, it is not dynamically updating the route limit, nor it is asking user to clear the route table for the config to take effect
    - ▪ 'show ip bgp nexthop' is displays multicast flag for unnumbered nexthops.
    - ▪
  - o **OSPF:**
    - ▪ OSPFV3 neighborship is not forming with MD5 Authentication
    - ▪ Connected, OSPF routes exported to BGP EVPN are not working with export-map
    - ▪ "hsl_bridge_get_ivid_from_vsi: Unexpected VSI received for IVID conversion - VSI: 4018" are noticed on the console sometimes.

- **MCT**
  - o Traffic flooding after cluster deploy/no-deploy on high scale.
  - o After clear mac dynamic - Mac learning is very slow and also causes MAC still present in HW.

- **NetConf**
  - o When "clear ip bgp nei all" executed multiple times may cause process instability.

- **BFD**:
  - o BFD not supported

- **Platform**:
    - "Error:soc_reg_above_64_field32_read(IQM_OCCUPIED_BD_COUNTERr) failed for unit 0 core 0 " is seeing on console when collecting SS
    - Console is flooded with "ifStats: get_if_utilization failsifStats" when collecting supportsave
    - ssh source interface as ethernet packet capture is not worknig after removing the source-intf ip address
    - Custom RPC call "show-ntp" is providing empty output instead of the active NTP server
    - Account log is showing SSH instead of unique tty identifier while login through SSH; after login, it's behaving correct
    - Login message says " admin connected using console" instead of "telnet" when accessing the switch via telnet
    - NTP is using wrong ip as source ip to send ntp packet out of OOB mgmt-interface after sh/no shut of mgmt.
    - Switches are taking default option as 'y', instead of 'no input' for 'y/n' prompt for 'reload system', 'firmware" etc commands.

- **Port Mirroring (SPAN)**
    - " sflow-profile" command under policy-map is not supported.
- **QOS:**
    - "show qos flow-control interface all" shows port-channel member interfaces two times in the output.
    - L2 QOS egress maps not supported.
    - Flow Control not supported.

- **REST API**
    - Account log is showing wrong hostname while login through REST (HTTP)
- **Telemetry Streaming**
    - Unreachable GRPC Client causes in stability in the system.

Defects

TSBs—Critical issues to consider prior to installing this release

TSB issues resolved in SLX-OS 18x.1.00

None

Closed with code changes for SLX-OS 18x.1.00

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of November 19, 2018 in SLX-OS 18x.1.00.

None

Closed without code changes for SLX-OS 18x.1.00

This section lists software defects with Critical, High, and Medium Technical Severity closed without a code change as of November 19, 2018 in SLX-OS 18x.1.00.

None.

Known issues for SLX-OS 18x.1.00

This section lists open software defects with Critical, High, and Medium Technical Severity closed with a code change as of November 19, 2018 in SLX-OS 18x.1.00.

Defect ID:	DEFECT000663118		
Technical Severity:	High	Probability:	Medium
Product:	Brocade SLX-OS	Technology Group:	Management
Reported In Release:	SLXOS 18x.1.00	Technology:	CLI - Command Line Interface
Symptom:	Account log shows host ip as "127.0.0.1" , while logging in through SSH or RESTAPI.		
Condition:	Login through RESTAPI and NETCONF		
Workaround:	correct host ip shown if logged in through telnet.		

Defect ID:	DEFECT000664311		
Technical Severity:	High	Probability:	High
Product:	Brocade SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18x.1.00	Technology:	Static Routing (IPv4)
Symptom:	Continuous BGP, EVPN, and Tunnel flapping when VXLAN underlay VLAN added to EVPN instance		
Condition:	Adding VXLAN underlay VLAN to EVPN instance		

Defect ID:	DEFECT000664387		
Technical Severity:	High	Probability:	Medium
Product:	Brocade SLX-OS	Technology Group:	Monitoring
Reported In Release:	SLXOS 18x.1.00	Technology:	RAS - Reliability, Availability, and Serviceability
Symptom:	raslog filter in backend is not defaulted after "copy default startup" followed by "reload system"		
Condition:	copy default startup" followed by "reload system"		
Workaround:	configure and remove the suppress command again after defaulting the config to recover		

Defect ID:	DEFECT000664749		
Technical Severity:	High	Probability:	Medium
Product:	Brocade SLX-OS	Technology Group:	Layer 2 Switching
Reported In Release:	SLXOS 18x.1.00	Technology:	xSTP - Spanning Tree Protocols
Symptom:	Spanning tree MSTP stuck in " RTPT WAIT_FWD " state and could flap		
Condition:	scaled mstp configuration		
Workaround:	Need to configure mstp to vlan mapping with delay inbetween or re-configure flapping instance to fix issue when the issue already seen.		

Defect ID:	DEFECT000665514		
Technical Severity:	High	Probability:	High
Product:	Brocade SLX-OS	Technology Group:	Layer 2 Switching
Reported In Release:	SLXOS 18x.1.00	Technology:	LAG - Link Aggregation Group
Symptom:	Packets get duplicated on port channel member ports for a short duration		
Condition:	The transient defect is seen only while member interface of port channel is coming up		

Defect ID:	DEFECT000666271		
Technical Severity:	Medium	Probability:	High
Product:	Brocade SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18x.1.00	Technology:	Static Routing (IPv4)
Symptom:	The command "show system internal bgp evpn neighbor <neighbor IP>" is not working		
Condition:	Running BGP-EVPN for IP Fabric applications		

Defect ID:	DEFECT000667032		
Technical Severity:	High	Probability:	Low
Product:	Brocade SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18x.1.00	Technology:	Static Routing (IPv4)
Symptom:	MCDS cluster could flap post reboot		
Condition:	MCDS cluster config		
Workaround:	mcds packets not getting priorotised, reduce competing traffic or reconfigure to that effect		

Defect ID:	DEFECT000667271		
Technical Severity:	High	Probability:	High
Product:	Brocade SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18x.1.00	Technology:	BFD - BiDirectional Forwarding Detection
Symptom:	BFD flaps could be observed configuring switchport config on another interface		
Condition:	Configure BFD		
Workaround:	increase timer, reduces bfd sessions		

Defect ID:	DEFECT000667362		
Technical Severity:	High	Probability:	Low
Product:	Brocade SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18x.1.00	Technology:	Static Routing (IPv4)
Symptom:	Connected, OSPF routes exported to BGP EVPN do not work with export-map		
Condition:	Using export maps		

Defect ID:	DEFECT000668087		
Technical Severity:	High	Probability:	Medium
Product:	Brocade SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18x.1.00	Technology:	ARP - Address Resolution Protocol
Symptom:	Arp entry for few IP addresses show "L2 interface" as "Unresolved" when these entries have been learnt over an ICL tunnel		
Condition:	Layer 3 traffic in a cluster (MCT) environment		

Defect ID:	DEFECT000668376		
Technical Severity:	High	Probability:	High
Product:	Brocade SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18x.1.00	Technology:	Static Routing (IPv4)
Symptom:	Management cluster could flap continuously during underlay flap		
Condition:	management cluster config and underlay flap		
Workaround:	none		

Defect ID:	DEFECT000668481		
Technical Severity:	High	Probability:	High
Product:	Brocade SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18x.1.00	Technology:	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	IPv6 Type5 remote prefix not installed in forwarding plane after delet/re-create VRF		
Condition:	Running BGP_EVPN		

Defect ID:	DEFECT000668493		
Technical Severity:	Medium	Probability:	Low
Product:	Brocade SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18x.1.00	Technology:	Static Routing (IPv4)
Symptom:	Console could see "ifStats" releated error messages		
Condition:	The issue is seen when SNMP is trying to get utilization for port channel interface		
Workaround:	none		

Defect ID:	DEFECT000668594		
Technical Severity:	High	Probability:	Low
Product:	Brocade SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18x.1.00	Technology:	Static Routing (IPv4)
Symptom:	L3vni traffic fails when ARP is not resolved for hosts connected beyond LVTEP nodes and when cluster_gateway is enabled.		
Condition:	only when cluster_gateway is enabled.		
Workaround:	ARP resolution for hosts must be done before sending traffic.		

Defect ID:	DEFECT000668645		
Technical Severity:	High	Probability:	Low
Product:	Brocade SLX-OS	Technology Group:	Layer 2 Switching
Reported In Release:	SLXOS 18x.1.00	Technology:	VXLAN - Virtual Extensible LAN
Symptom:	MCDS cluster could flap		
Condition:	Management cluster not forming after overlay-gateway deactivate/re-activate		
Workaround:	stabilise overlay and reconfigure		

Defect ID:	DEFECT000668659		
Technical Severity:	Medium	Probability:	Low
Product:	Brocade SLX-OS	Technology Group:	Layer 2 Switching
Reported In Release:	SLXOS 18x.1.00	Technology:	LAG - Link Aggregation Group
Symptom:	Loadsharing on LAG will not happen for Destination IP incrementing traffic when the hashing is based only on dst ip as set below' no load-balance hash ipload-balance hash ip dst-ip'		
Condition:	when we have IP traffic with destination IP incrementing, and the hashing is set only based on dst-ip then load sharing is not happening on LAG interface		
Workaround:	Enable hash for L4-port		