SLX-OS 18s.1.01a Release for the ExtremeSwitching SLX 9140 and SLX 9240 Platforms, Release Notes v1.0

11 March 2019

9036079-00

Copyright Statement and Legal Notices

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

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, please see:

www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:

www.extremenetworks.com/support/policies/software-licensing

Contents

Document History

Version	Summary of changes	Publication date
1.0	Initial Release	11 March 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.

Software Features

This section addresses features introduced in the current release as well as those introduced in the previous release.

SLX-OS 18s.1.01a

SLX-OS 18s.1.0.1a release is the fourth release in a series for SLX platforms – the SLX 9140 is the focus of the new features in this release, while the SLX 9240 remains supported as in the previous release. No new hardware platform is added in this release, and only software features are added.

NOTE. This document includes information that is supported in previous release.

The key features for SLX-OS 18s.1.01a are focused on enhancing manageability and user experience on SLX.

The new features are as follows:

- **Endpoint tracking**: MAC authentication using RADIUS protocol on SLX 9140
- **Embedded Fabric Automation (EFA)**: Application support on the SLX 9140 and SLX 9240, interoperating with the SLX 9030 as a leaf and the SLX 9540 as a leaf and border leaf

  This release supports the EFA bring-up of **Clos topology** networks with SLX 9030 and SLX 9540 as leaf nodes, in addition to the bring-up of the SLX 9140 as a leaf as supported in the previous release. This release introduces support for the EFA bring-up of **non-Clos topology** networks with the SLX 9140 as a rack platform.

  NOTE: It is recommended that EFA run on one of the rack SLX 9140 platforms, as well as on one of the spine SLX 9240 platforms.

The SLX 9140/SLX 9240 are fixed 1-RU switching platforms based on programmable ASICs that enable the adoption of new protocols and technologies. These switches were released as a part of SLX-OS 17s.1.00, SLX-OS 18s.1.00, and SLX-OS 18s.1.01 to support enhanced Network Packet Broker (NPB) pipeline and SLX switching and routing feature. The features introduced in 18s.1.01 are as follows:

- High-density 40G/100G spine-leaf connection
- SLX 9140 native 1G/10G/25G server connectivity at the leaf
- High performance VXLAN routing
- Payload timestamping to enable accurate measurement of performance SLAs
- Port-to-port latency: ~2.5 microseconds
- Architecture: store and forward
- Enhanced NPB Pipeline
- Support for 4x10G and 4x25G with dynamic breakout

The major focus of this SLX-OS release is on the feature enhancements supporting End Point Tracking (EPT) and Data Center, with Embedded Fabric Automation (EFA) for DC Fabric use cases.

Endpoint tracking – MAC authentication using RADIUS protocol

Endpoint tracking (EPT) for SLX-OS product lines helps to authenticate the MACs and assign VLANs dynamically by using RADIUS/XMC-NAC (Extreme Management Center – Network Access Control).

In order to minimize configuration and management of VLANs on switches in the data center, SLX-OS needs to have the following:

- A method to associate MACs to specific VLANs
- Once a MAC is authorized and the VLAN is not already provisioned on the switch, the ability to dynamically create the VLAN to which this MAC is associated, configure the tag, and add the feature enabled port on which the MAC was detected
- Once the last MAC using the VLAN is deleted or aged out, deletion of the VLAN and associated resources on the switch

When a MAC is authorized, SLX-OS dynamically creates the VLAN that is required for the VM to send traffic. If a VM shuts down or is moved, its VLAN is pruned to preserve bandwidth. This feature creates an adaptive infrastructure in which the network responds to changes in the virtual machine network.

Embedded Fabric Automation non-CLOS support on SLX 9140

EFA is an application that can be installed on the TPVM (Third Party Virtual Machine) on the SLX 9240 (spine). The application is bundled as part of the SLX-OS firmware and can be used to configure an IP Fabric on the SLX 9240 and SLX 9140. EFA is documented in the "Embedded Fabric Automation" chapter of the *Extreme SLX-OS IP Fabrics Configuration Guide*. The following platform roles are supported: SLX 9140 as a leaf, and SLX 9240 as a spine and leaf.

NOTE: Before upgrading SLX-OS firmware on SLX9140/9240 it is recommended to save the configurations on the switch through the **copy running-config startup-config** command.

EFA application is bundled as part of the SLX firmware and can be used to configure an IP Fabric on the SLX 9240 and SLX 9140. **NOTE**: See "Upgrading to EFA 2.0.0 with TPVM Ubuntu version 16.04" later in this document	• The EFA application runs on the SLX TPVM to manage the IP Fabric. • EFA provides simplified mechanism to configure IP Fabric, once the IP addresses of the devices are provided. • Support for SLX 9030 as a leaf and SLX 9540 as a leaf and border leaf is added.

SLX-OS 18s.1.01

The following are the major features added in SLX-OS 18s.1.01 release.

Feature Name	Use case
IGMPv2 snooping with MCT	DC
SNMP Enhancements	DC
Management ACL to block ICMP timestamp in response packet	DC
Internal loopback support	NPB
On-board packet capture	NPB
EFA with additional support for SLX 9240 as a leaf	DC
New Optics Qualification 25G-LR Media	ALL
Qualify SLX 9240 as a high-density leaf	DC

SLX 9140 and SLX 9240 as Network Packet Broker

SLX HW can be used as standard switching/routing or in NPB-only mode. NPB features are enabled only in NPB mode with the following enhance header stripping and Flex ACL features with advance NPB scale. The following table summarizes the NPB features introduced with SLX-OS 18s.1.00.

Feature Name	Feature Description
NPB Parser	The ability to parse new set of protocol on existing hardware. **VXLAN, NVGRE, ERSPAN, IP-GTP-IP, IP-GRE-IP, IP-IP, EoMPLS, IPoMPLS, IPv4/IPv6/ARP**. Offset agnostic parsing up to inner L4/payload parsing. Payload (4/8/16/32) bytes follow the last possible parsed header.
Header Stripping	The ability to strip the header, for example, tunnel encapsulation and BR/VN tags for customer tools to analyze traffic that may or may not be able handle some of the tags or packet encapsulations during traffic analysis.
Flex/UDA Match ACL	The ability to filter based on deep packet inspection (DPI) or combination of MAC, IP fields using user-defined **Flex ACLs** (new for SLX 9240 and SLX 9140 platforms). Parses relatively deep into the packet. In MLX and SLX 95430 the UDA is based on offset/pattern match.

Consolidated Features in SLX-OS 18s.1.01

The following table lists the features introduced in SLX-OS 18s.1.01.

NPB Mode Features

Header Stripping	
802.1BR VN-Tag MPLS Label (EoMPLS & IPoMPLS) GTP -U-v1 VXLAN Encap ERSPAN-II NVGRE Encap	• Per port support of header stripping, enabled or disabled via CLI • Tag stripping: 802.1BR or VN-ag (either one is supported) • Tunnel encapsulations stripping VXLAN, NVGRE, ERSPAN-II/GTP-U-v1/MPLS • Filter traffic using policy engine, based on values of fields in the tags/encapsulations in addition to standard L2/L3/L4 fields (outer and/or inner) • Multiple stripping configurations per port.
Transparent VLAN	
• Aggregation • Replication • VLAN filtering • VLAN tag add • VLAN tag delete • Combination of VLAN delete and VLAN add with header stripping. • Max TVF domains	• Aggregate flows from multiple taps to a single egress interface. • Replicate flows from a single tap to multiple egress interfaces • Filter flows from tap to forward or drop based on route map policies • Outermost VLAN tag in the forwarded frame will be deleted • New VLAN tag will be added in standard canonical format • Route maps to be applied on ports or port-channels. • Maximum supported TVF domains is 4096
Flex ACLs	
Super ACL capability Limited deep packet inspection (DPI)	• Deep packet inspection of tunneled traffic to filter specific flows, especially traffic that cannot be filtered using standard or extended MAC/IP ACLs. • Uses **Flex ACLs** (new for SLX 9240 and SLX 9140 platforms). Dictionary format CLI

	• Super ACL capability for traffic (tunneled or not) to match packet fields spanning across well-known layers.
Scale Improvements	
L3 L2 Flex Per Core (2 core per switch)	• IP policy-based forwarding entries (IPACL): 2048 (IPV4+IPV6) • MAC policy-based forwarding entries (L2ACL): 2048 • Flex policy-based forwarding entries (Flex): 1024 • Ports per LAG: 64 • TVF domains: 4096
NPB enhancements	
Onboard packet capture Internal loopback support	• Onboard packet capture - capture ingress/egress data frames in PCAP format for a given port in NPB mode only, one port at a time. Auto stop after capturing designated number of frames • Internal loopback - service chaining in NPB operations. Deep packet header inspection.
New optics Qualified	
25G SFP28 LR	• 10504

Misc Features	
Port Breakout Support	Support for 4x25G
Dynamic Breakout Support	Eliminates the need to reload the system when breakout or non-breakout on ports.

Data Center Solutions

IGMPv2 Snooping with MCT	
	• IGMPv2 snooping support on MCT. • BGP EVPN based IGMP state syncing. • IGMP VLAN and Group Based DF election for traffic forwarding to MCT clients. **Note:-** Bridge Domain (BD) case is not supported.
SNMP Enhancements	
	• Support to disable SNMP traps for interface link status change events for Ethernet, Loopback, VE, and port-channel interfaces. • Allow SNMP server to be disabled/enabled for specific VRFs or for all the VRFs.
Mgmt ACL to block ICMP timestamp in response packet	
	• Allows ICMP timestamp requests and responses to be dropped, by default, as a security policy. • If an ACL with a "*permit icmp any any*" rule is applied to the management interface, such a rule permits ICMP timestamp requests but ICMP timestamp response is blocked.
Qualify SLX 9240 as a high-density leaf	
	• Allows to deploy SLX 9240 as a high-density leaf node in an IP fabric environment, similar to SLX 9140. • Routing in and out of Tunnel (RIOT) is not supported with IPv6. • Reduced scale numbers compared to 9140.

Embedded Fabric Automation

EFA is an application that can be installed on the TPVM (Third Party Virtual Machine) on the SLX 9240 (spine). The application is bundled as part of the SLX-OS firmware and can be used to configure an IP Fabric on the SLX 9240 and SLX 9140. EFA is documented in the "Embedded Fabric Automation" chapter of the *Extreme SLX-OS IP Fabrics Configuration Guide*. The following platform roles are supported: SLX 9140 as a leaf, and SLX 9240 as a spine and leaf.

Embedded Fabric Automation (EFA)	
EFA application is bundled as part of the SLX firmware and can be used to configure an IP Fabric on the SLX 9240 and SLX 9140. **NOTE**: See "Upgrading to EFA 2.2.0 with TPVM Ubuntu version 16.04" later in this document	• The EFA application runs on the SLX TPVM to manage the IP Fabric. • EFA provides simplified mechanism to configure IP Fabric, once the IP addresses of the devices are provided. • Support for SLX 9240 as a leaf is added.

RFCs, Standards, and Scalability

For RFCs, standards, and scale numbers supported in this release, refer to the Extreme SLX-OS Scale and Standards Matrix for SLX 9140 and SLX 9240.

Supported Optics

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

Description	Orderable PN	P/N
1000Base-SX	1G-SFP-SX-OM	33210-100
1000Base-LX	1G-SFP-LX-OM	33211-100
1GE Copper SFP (Pseudo-Branded)	1G-SFP-TX	33002-100
1GE Copper SFP (BR-Branded)	1G-SFP-000190	57-1000042-02
10GE USR SFP+	10G-SFP-USR	57-1000130-01
10GE USR SFP+, 70C TAA	10G-SFP-USR-SA	57-1000343-01
10GE SR SFP+, 85C	10G-SFP-SR	57-0000075-01
10GE SR SFP+, 70C	10G-SFP-SR-S	57-1000340-01
10GE SR SFP+, 70C TAA	10G-SFP-SR-SA	57-1000344-01
10GE LR SFP+, 85C	10G-SFP-LR	57-0000076-01
10GE LR SFP+, 70C	10G-SFP-LR-S	57-1000341-01
10GE LR SFP+, 70C TAA	10G-SFP-LR-SA	57-1000345-01
10GE AOC 7M	10GE-SFP-AOC-0701	57-1000273-01
10GE AOC 10M	10GE-SFP-AOC-1001	57-1000274-01
10GE Direct Attach 5M Active	10G-SFP-TWX-0501	58-1000023-01
10GE Direct Attach 1M Active	10G-SFP-TWX-0101	58-1000026-01
10GE Direct Attach 3M Passive	10G-SFP-TWX-P-0301	58-1000025-01
10GE Direct Attach 5M Passive	10G-SFP-TWX-P-0501	58-1000019-01
25G SR	25G-SFP28-SR	57-1000342-01
25GE Direct Attach 01M Passive	25G-SFP28-TWX-P-0101	58-0000064-01
25GE Direct Attach 03M Passive	25G-SFP28-TWX-P-0301	58-0000065-01
40GE QSFP+ SR4	40G-QSFP-SR4-1	57-1000128-01
4x10GE QSFP+ LR4, 10km,	40G-QSFP-LR4-INT	57-1000477-01
40GE BiDi QSFP+	40G-QSFP-SR-BIDI	57-1000339-01
40GE QSFP+ LR4, 10KM, 70C	40G-QSFP-LR4-1	57-1000263-01

40GE QSFP+ SR4 to 10G-SR SFP+	40G-QSFP-SR4-INT	57-1000129-01
40GE QSFP to QSFP 1M Cable(Passive)	40G-QSFP-C-0101	58-0000033-01
40GE QSFP to QSFP 3M Cable(Passive)	40G-QSFP-C-0301	58-0000034-01
40GE QSFP to QSFP 5M Cable(Passive)	40G-QSFP-C-0501	58-0000035-01
4x10GE QSFP+ to 4 SFP+ Active copper cable - 1m	40G-QSFP-4SFP-C-0101	58-0000051-01
4x10GE QSFP+ to 4 SFP+ Active copper cable - 3m	40G-QSFP-4SFP-C-0301	58-0000052-01
4x10GE QSFP+ to 4 SFP+ Active copper cable - 5m	40G-QSFP-4SFP-C-0501	58-0000053-01
40GE QSFP to QSFP cable - 10m AOC	40G-QSFP-QSFP-AOC-1001	57-1000306-01
100GE QSFP28 SR4	100G-QSFP28-SR4	57-1000326-01
100GE QSFP28 LR4 (3.5W)	100G-QSFP28-LR4-LP-10KM	57-1000338-01
100GE QSFP28 CWDM	100G-QSFP28-CWDM4-2KM	57-1000336-01
100G QSFP28 Active Optical (10m)	100G-QSFP-QSFP-AOC-1001	57-1000347-01
100GE QSFP28 LRL 2km	100G-QSFP28-LR4L-2KM	57-1000329-01

Note: 10GE LR SFP+, 85C multi speed optic can operate on 10G as well as 1G.

New optics supported starting with SLX18s.1.01

25G SFP28 LR (10km), Single Mode, LC-connector, 70degC	25G-SFP28-LR	10504

Mellanox supports the following 10G optics:

- 10G USR SFP+
- 10G SR SFP+
- 10G LR SFP+ in RC2

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

Documentation Supporting SLX-OS

SLX-OS 18s.1.01a

For documents supporting the new features, see the following:

https://www.extremenetworks.com/support/documentation/slx-s-series-software-18s-1-01a/

SLX-OS 18s.1.01

For additional documentation support for the previous release, see the following:

https://www.extremenetworks.com/support/documentation/slx-s-series-software-18s-1-01/

Software Upgrade and Downgrade

This section includes information that supports both the current and previous release.

SLX-OS 18s.1.01a

Image file names

Download the following images from www.extremenetworks.com.

Image file name	Description
slxos18s.1.01a.tar.gz	SLX-OS 18s.1.01a_ software
slxos18s.1.01a_all_mibs.tar.gz	SLX-OS 18s.1.01a_ MIBS
slxos18s.1.01a.md5	SLX-OS md5 checksum

To Install SLX-OS 18s.1.01a from the network:

Run command: **firmware download scp host** <*ip-address*> <*directory*>

Where: <directory> is where the image is downloaded.

To Install SLX-OS 18s.1.01a from a USB device, follow the steps below:

Step 1: Copy unzipped SLX-OS firmware to the USB device under the firmware directory.

Step 2: Plug the USB device into the switch on which you want to download the firmware.

Step 3: Execute the **usb on** command from the CLI prompt.

Step 4: Execute the following: **firmware download usb** <*full path of the firmware*>

Migration path

Recommended upgrade/downgrade migration paths in default mode:

NOTE: Only if upgrading to **SLX 18s.1.01 or SLX 18s.1.01a** with "default-config" option, then "app-tele-l2-l3-iacl" HW profile is activated.

To From	SLX17s.1.00a	SLX17s.1.01	SLX17s.1.02	SLX17s.1.02x	SLX 18s.1.00	SLX 18s.1.01	SLX 18s.1.01a
SLX 17s.1.00a	NA	FWDL coldboot	FWDL coldboot	FWDL coldboot	*	*	*
SLX 17s.1.01	Default – config	NA	FWDL coldboot	Default-config	*	*	*
SLX 17s.1.02	Default – config	FWDL coldboot	NA	FWDL coldboot	FWD coldboot	FWD coldboot	FWD coldboot
SLX 17s.1.02x	Default – config	Default-config	FWDL coldboot	NA	FWD coldboot	FWD coldboot	FWD coldboot
18s.1.00	*	*	Default - config	Default - config	NA	FWD coldboot	FWD coldboot
18s.1.01	*	*	Default - config	Default - config	FWD coldboot	NA	FWD coldboot
SLX 18s.1.01a	*	*	Default - config	Default - config	FWD coldboot	FWD coldboot	NA

***NOTE:** For SLX 17s.1.00/a/1, the recommended path is first to install the SLX17s.1.02x release, and then the SLX 18s.1.01 release. For an MCT cluster, it recommended that only one node be upgraded at a time. Wait for the first node to come up completely before upgrading the second node.

Recommendations

Upgrading to EFA 2.0.0 with TPVM Ubuntu version 16.04

Do the following to upgrade the EFA application.

In the previous version used TPVM Ubuntu version 14.04 on an SLX-9240. This task upgrades the version to 16.04.

1. Log in to TPVM with the TPVM IP address.
   $ ssh -l root *<TPVM_IP>*

2. Copy the EFA database and logs backup to an external server.
   $ service efa-server stop

   $ scp /var/efa/efa.db *<server_EFA_DB_Location>*
   $ scp /var/log/efa/efa.log *<server_EFA_Log_Location>*

3. Stop and uninstall TPVM.
   $ tpvm stop
   $ tpvm uninstall

4. With the device upgraded to 18s.1.01a, execute the **efa deploy** command.
   $ efa deploy

5. Log in to TPVM and verify the TPVM version.
   $ ssh -l admin *<TPVM_IP>*

6. Restore the EFA database and logs.
   $ sudo su **<-- Provide TPVM root password**
   $ systemctl stop efa-server
   $ mv /var/efa/efa.db /tmp/
   $ mv /var/log/efa/efa.log /tmp/
   $ scp <server_EFA_DB_Location> /var/efa/
   $ scp <server_EFA_Log_Location> /var/log/efa/
   $ systemctl start efa-server

7. Verify that EFA is running and verify the version.
   $ ps -ef | grep -i efa

The EFA version should be 2.0.0.

8. Before executing the **efa deconfigure** command, execute the **efa configure** command at least once following the upgrade.

SLX-OS 18s.1.01

Migration path

Recommended upgrade/downgrade migration paths in NPB mode:

NOTE: Starting with SLX 17s.1.01 NPB feature is supported only with "Advanced feature" license.

- **SLX 17s.1.02/x/ab/18s.1.00 to SLX 18s.1.01 Upgrade**
  - Save running-config to startup-config
  - Make sure SLX 9240 / 9140 is in NPB mode
  - Make sure ADVANCED FEATURES license is present
  - Firmware Upgrade to SLX 18s.1.01

- **SLX 18s.1.01 to SLX 17s.1.02/x/ab/18s.1.00 Downgrade**
  - Save running-config to startup-config
  - Take back-up of the config
  - Firmware downgrade with default-config option
  - Restore the config

To From	SLX 17s.1.00	SLX 17s.1.00a	SLX17s.1.01	SLX17s.1.02	SLX17s.1.02x	SLX 18s.1.00	SLX 18s.1.01
SLX 17s.1.00	NA	Default - config	Default - config	Default - config	Default - config	*	*
SLX 17s.1.00a	Default - config	NA	Default - config	Default - config	Default - config	*	*
SLX 17s.1.01	Default- config	Default - Config	NA	FWD coldboot	Default - config	*	*
SLX 17s.1.02	Default- config	Default - Config	FWDL coldboot	NA	FWD coldboot	FWD coldboot	FWD coldboot
SLX17s.1.02x	Default- config	Default - Config	Default - Config	FWD coldboot	NA	FWD coldboot	FWD coldboot

SLX 18s.1.00	*	*	*	Default - config	Default - config	NA	FWD coldboot
SLX 18s.1.01	*	*	*	Default - config	Default - config	FWD coldboot	NA

NOTE: * For SLX 17s.1.00/a/1, the recommended path is first to install the SLX17s.1.02x release, and then the SLX 18s.1.01 release.

Upgrading to EFA 1.1.0 with TPVM Ubuntu version 16.04

Do the following to upgrade the EFA application.

In the previous version, SLX-OS 17s.1.02b used TPVM Ubuntu version 14.04 on an SLX-9240. This task upgrades the version to
16.04.

1. Log in to TPVM with the TPVM IP address.
   $ ssh -l root *<TPVM_IP>*

2. Copy the EFA database and logs backup to an external server.
   $ service efa-server stop

   $ scp /var/efa/efa.db *<server_EFA_DB_Location>*
   $ scp /var/log/efa/efa.log *<server_EFA_Log_Location>*

3. Stop and uninstall TPVM.
   $ tpvm stop
   $ tpvm uninstall

4. With the device upgraded to 18s.1.01, execute the **efa deploy** command.
   $ efa deploy

5. Log in to TPVM and verify the TPVM version.
   $ ssh -l admin *<TPVM_IP>*

6. Restore the EFA database and logs.
   $ sudo su **<-- Provide TPVM root password**
   $ systemctl stop efa-server
   $ mv /var/efa/efa.db /tmp/
   $ mv /var/log/efa/efa.log /tmp/
   $ scp <server_EFA_DB_Location> /var/efa/
   $ scp <server_EFA_Log_Location> /var/log/efa/
   $ systemctl start efa-server

7. Verify that EFA is running and verify the version.
   $ ps -ef | grep -i efa

The EFA version should be 1.1.0.

8. Before executing the **efa deconfigure** command, execute the **efa configure** command at least once following the upgrade.

Limitations and Restrictions

This section applies to 18s.1.01.

NPB limitations and restrictions

a. When switching from NPB to default mode, the user should un-configure the following and reload the system:
    a. TVF domains, NPB policy route-map, and route-map set next-hop-tvf-domain
b. When switching from default to NPB mode, the user should revert the system to default-configuration and reload the system.
c. To achieve the maximum L2/L3 ACL rules, the ACLs must be applied equally among the following two port groups:
    a. 9140
    b. Port Group 0: eth0/1-36
    c. Port Group 1: eth0/37-54
    d. 9240
    e. Port group0: eth 0/1-0/16
    f. Port group1: eth 0/17-0/32
d. With 4K TVF/route-maps scale, the system takes longer to load on config replay.
e. IPv6 GTP packets are not supported for NPB L3 ACL filtering or GTP HTTPS filtering.

NPB Header stripping

a. 802.1BR and VN tag are mutually exclusive on an interface.
    - Allowed only in the outer ETH.
b. MPLS labels can number up to maximum of 4.
c. ERSPAN stripping – Type 2 is supported. Type 1 is obsolete.
d. Parser block can parse only up to 128 bytes of ingress frame.
e. When both 802.1BR/VN-tag and GTP stripping are enabled, only 802.1BR/VN-tag is stripped
f. When both 802.1BR/VN-tag and MPLS label stripping are enabled, only MPLS labels are stripped
g. IPv6 SIP and DIP are only 64 bits each (upper or lower).
    - Needs appropriate profile
h. VLAN Delete will always remove the first tag.
    C in C-tag frames
    C1 in C1+C2 tag frames
    S in S+C tag frames
i. VLAN add can only add C-VLAN tag.
j. VLAN add/delete is ignored when GTP strip is enabled.

NPB Flex ACLs

a. Up to 8 headers in layer stack can be accessed.

b. Each flex word can be up to 4 bytes (with mask).

c. Payload bytes (if available) can be 4/8/16/32 bytes.

Onboard packet capture

a. Captured frames are rate limited to 256 PPS from hardware.

b. Frames are truncated to 256 bytes.

c. Auto stop occurs after capturing designated number of frames.

d. The PCAP file is deleted automatically upon reboot.

e. PCAP is supported only on one port at a time – ingress or egress and not both.

Internal loopback

a. No frames will go out of the service port, even if it is connected to an external device. Hence it is suggested that the user configure only unused ports as loopback ports.

b. A shut/no shut is required on a member port to bring it up, both while attaching it to a port-channel and detaching it from a port-channel.

c. It is suggested, not to have sfp present in ports, configured in loopback mode. In case, sfp is present, the sequence to configure port in loopback mode, is to shut it first, configure loopback phy, change speed if required, and then do a no shut.

Non-NPB limitations and restrictions

This section applies to 18s.1.01a.

End Point Tracking:

It is not suggested to enable spanning tree protocol on the EPT enabled port.

ACL is not supported on the EPT enabled port.

Defects

Defects 18s.1.01a

TSBs—Critical issues to consider prior to installing this release

Technical Support Bulletins (TSBs) provide detailed information about high priority defects or issues present in a release. The following sections specify all current TSBs that have been identified as being a risk to or resolved with this specific release. Please review carefully and refer to the complete TSB for relevant issues prior to migrating to this version of code. Refer to "Contacting Extreme Technical Support" at the beginning of this document."

TSB issues resolved in SLX-OS 18s.1.01a

TSB	Summary
None	

TSB issues outstanding in SLX-OS 18s.1.01a

TSB	Summary
None	

Closed with code changes for SLX-OS 18s.1.01a

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of March 5, 2019.

NOTE: Parent Defect ID is the customer found Defect ID. The Issue ID is the tracking number uniquely used to check in the fix for each major release.

Parent Defect ID:	SLXOS-28689	**Issue ID:**	SLXOS-39197
Severity:	S3 - Medium		
Product:	SLX-OS	**Technology Group:**	Management
Reported in Release:	SLXOS 17r.2.01	**Technology:**	Configuration Fundamentals
Symptom:	Symptom 1) Unable to configure large number of VLANs under an EVPN instance Symptom 2) Unable to restore a startup-config file containing a large number of VLANs under an EVPN instance.		
Condition:	Condition 1) When a vlan configuration, more than 253 characters long, is attempted when configuring an EVPN instance a length validation error is noticed. Condition 2) A vlan configuration, more than 253 characters long, when split and configured under an EVPN instance is saved in the startup-config file and restored the system may not accept the configuration.		
Workaround:	Workaround 1) Split the VLAN configuration into multiple lines. Workaround 2) Reconfigure the VLANs		

Parent Defect ID:	SLXOS-38942	**Issue ID:**	SLXOS-39012
Severity:	S2 – High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 18s.1.01	**Technology:**	LAG - Link Aggregation Group
Symptom:	Traffic ingressing on a Tunnel and egressing out of interface 0/9 and 0/9:1 on SLX 9240s can get dropped.		
Condition:	The issue happens when all these conditions are true, 1. It's SLX 9240 2. Ingress is a VXLAN tunnel or the ICL interface (NSH tunnel) 3. Egress interface is 0/9 or 0/9:1		

Closed without code changes for SLX-OS 18s.1.01a

This section lists software defects with Critical, High, and Medium Technical Severity closed without a code change as of 5 March 2019.

- None

Open defects for SLX-OS 18s.1.01a

This section lists open software defects with Critical, High, and Medium Technical as of 5 March 2019.

NOTE: Parent Defect ID is the customer found Defect ID. The Issue ID is the tracking number uniquely used to check in the fix for each major release.

Parent Defect ID:	SLXOS-38816	**Issue ID:**	SLXOS-38816
Severity:	S2 – High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 18s.1.01a	**Technology:**	VLAN - Virtual LAN
Symptom:	Dynamic VLANs provisioned through End Point Tracking (EPT) are not getting added in Total No. of VLANs configured.		
Condition:	show VLAN brief command executed		
Workaround:	None		
Recovery:	None		

Parent Defect ID:	SLXOS-39065	**Issue ID:**	SLXOS-39065
Severity:	S2 – High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 18s.1.01a	**Technology:**	Other
Symptom:	Mac authentication not happening for untagged native VLAN after reload or interface shut/no-shut.		
Condition:	System is reloaded with native VLAN and tagged VLAN present on port-channel. Also seen with shut/no-shut is done on port-channel interface.		
Workaround:	disable/enable native VLAN to make it work.		

Parent Defect ID:	SLXOS-39182	**Issue ID:**	SLXOS-39339
Severity:	S2 – High		
Product:	SLX-OS	**Technology Group:**	Layer 2 Switching
Reported in Release:	SLXOS 18s.1.01a	**Technology:**	Other
Symptom:	When MAC moves between EPT CEP port to remote EPT CCEP port few times mac is not learnt.		
Condition:	Under MCT and EPT deployment		
Recovery:	Add port statistically to that VLAN and remove the configuration again.		

EFA open defects

Defect ID:	SIPF-599		
Technical Severity:	High	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	NA
Reported In Release:	SLXOS 18s.1.01a	**Technology:**	NA
Symptom:	Heavy traffic from a port is causing not to form MCT cluster for long time		
Condition:	Management Cluster is not operational, and polling timed out. As a work around shut down server facing ports.		

Defect ID:	SIPF-586		
Technical Severity:	High	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	NA
Reported In Release:	SLXOS 18s.1.01a	**Technology:**	NA
Symptom:	BFD configuration under interface/single hop is not supported. Only multi-hop BFD configuration is supported.		
Condition:	BFD configuration change		

Defect ID:	SIPF-607		
Technical Severity:	High	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	NA
Reported In Release:	SLXOS 18s.1.01a	**Technology:**	NA
Symptom:	MCT Port Channel members should be of the same speed. Here there are multiple ports of differing speed (10G,40G) present.		
Condition:	User setup error. MCT with different port speed links is not supported		

Defect ID:	SIPF-608		
Technical Severity:	High	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	NA
Reported In Release:	SLXOS 18s.1.01a	**Technology:**	NA
Symptom:	Seeing an individual message when MCT links and L3 backup links are not interconnected.		
Condition:	MCT and L3 back up links are not interconnected		

Defect ID:	SIPF-606		
Technical Severity:	High	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	NA
Reported In Release:	SLXOS 18s.1.01a	**Technology:**	NA
Symptom:	Validation errors are missing.		
Condition:	Enable links between racks and disable port 46 at the same time		

Closed with code changes for SLX-OS 18s.1.01

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 12/11/2018.

Defect ID:	DEFECT000643147		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Software Installation & Upgrade
Symptom:	Observe "N O T A K N O W N R e s o u r c e I d" error message		
Condition:	Making configuration updates before ZTP process is complete.		
Workaround:	Do not perform configuration changes until "ZTP Complete" message is seen.		
Recovery:	Disable ZTP with "dhcp ztp cancel" and reboot the switch.		

Defect ID:	DEFECT000644467		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Monitoring
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Telemetry
Symptom:	GRPC Streaming application daemon goes down after continuous streaming of data for an extended period of time of more than 12 hours.		
Condition:	Concurrent processing of streams to GRPC clients on a periodic basis interferes with processing of client disconnect notifications when streaming was done for an extended period of time.		
Workaround:	For extended periods of streaming use-case, Setup collector mode for clients to collect streaming data instead of Grpc client interface.		

Defect ID:	DEFECT000645352		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 17s.1.02	**Technology:**	VXLAN - Virtual Extensible LAN
Symptom:	When the command "clear counters all" is executed sflow statistics will not reset.		
Condition:	For the command "clear counters all" ,reset of sflow statistics is not yet implemented.		
Workaround:	The command "clear sflow statistics interface <type><name>" resets sflow statistics.		

Defect ID:	DEFECT000646017		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Network Automation and Orchestration
Reported In Release:	SLXOS 17s.1.02	**Technology:**	NETCONF - Network Configuration Protocol
Symptom:	"Time logged in " information is not displayed in proper format under "show user"		
Condition:	User logged into the switch using NETCONF		

Defect ID:	DEFECT000646026		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 17s.1.02	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	Error message for ENTITY-MIB while loading SNMP MIBs in SNMP MIB browser		
Condition:	Observed while loading Extreme MIBs on the management station.		

Defect ID:	DEFECT000646440		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	DHCP option 82 Circuit-ID and Remote-ID displayed without any space between them.		
Condition:	The circuit ID is the combination of Interface index and description, the display command is not accounting for size of index while calculating the length of the circuit ID string. This issue happens only when the circuit ID is more than 60 characters.		
Workaround:	Configure IP DHCP Relay option with Circuit ID size less than 60 characters.		

Defect ID:	DEFECT000646799		
Technical Severity:	High	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	DHCP client relay frames are dropped in the switch.		
Condition:	When both DHCP L2 relay and L3 relay is configured on the switch.		
Workaround:	Configure only L2 DHCP relay or L3 DHCP relay on the switch. If accidentally both are configured, remove one of the configuration and reload the switch.		
Recovery:	Remove one of the DHCP Relay (L2 or L3) configuration and reload the switch.		

Defect ID:	DEFECT000651882		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 17s.1.02	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Unexpected reload due to HSLAgtd software daemon termination.		
Condition:	Too many MAC add/delete events continuously happening.		

Defect ID:	DEFECT000652922		
Technical Severity:	High	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 17s.1.02	**Technology:**	VLAN - Virtual LAN
Symptom:	REST/Netconf for bridge-domain-mac-state is not working		
Condition:	When REST API bridge-domain-mac-state executed.		
Workaround:	Use CLI "show bridge-domain"		

Defect ID:	DEFECT000652986		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Security
Reported In Release:	SLXOS 17s.1.02	**Technology:**	ACLs - Access Control Lists
Symptom:	"deny inner-gtp-https" configuration not restricted on individual member-ports of a Port-channel.		
Condition:	"deny inner-gtp-https" configuration.		

Defect ID:	DEFECT000653111		
Technical Severity:	Low	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 17s.1.02	**Technology:**	CLI - Command Line Interface
Symptom:	Confusion between DAD and ZTP		
Condition:	No conditions, removing CLI "show dadstatus" and "dhcp auto-deployment enable" from SLX to avoid confusion		

Defect ID:	DEFECT000653286		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 17s.1.02	**Technology:**	VLAN - Virtual LAN
Symptom:	A UDP/IP Packet with UDP Destination Port = 2152 (0x868) which is reserved for GTP Header can not be matched with UDP Source or Destination Port in L3 ACL.		
Condition:	L3 ACL Entry to match for UDP Source or Destination Port = 2152, will not be matched by GTP Packets (Packets with UDP Dest Port = 2152). No Issue with non-GTP packets.		

Defect ID:	DEFECT000653903		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 17s.1.02	**Technology:**	LAG - Link Aggregation Group
Symptom:	Switch experiences unexpected reload due to software module hslagtd daemon termination.		
Condition:	This issue may be seen when time-stamping feature enabled on MCT links, and one of the MCT peer is rebooted for any other reason.		

Defect ID:	DEFECT000654107		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 17s.1.02	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Traffic flooding observed on the Tunnel interface.		
Condition:	When the Tunnel interface is associated to both MCT and non-MCT member vlans and the last non-MCT member vlan of the tunnel interface is deleted.		

Defect ID:	DEFECT000654906		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	ARP - Address Resolution Protocol
Symptom:	ARP suppression-cache entries gets cleared inadvertently.		
Condition:	'clear arp' CLI command inadvertently clears the ARP suppression-cache entries.		

Defect ID:	DEFECT000659607		
Technical Severity:	High	**Probability:**	High
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	GTP - GPRS Tunneling Protocol
Symptom:	Load balancing and symmetric load balancing are not achieved with GTP.		
Condition:	This issue is seen for GTP packets with same inner IP addresses but varying L4 addresses.		

Defect ID:	DEFECT000660196		
Technical Severity:	Critical	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Monitoring
Reported In Release:	SLXOS 17r.2.01	**Technology:**	sFlow
Symptom:	sFlow collector IPv4 address configuration in 23.x.x.x range are rejected with the error "Given IP is Invalid for Sflow collector".		
Condition:	The issue occurs since there was an error in deciding if it's a multicast address (224.x.x.x. through 239.x.x.x). Note that, multicast addresses can not be used as sFlow collector address.		

Defect ID:	DEFECT000660903		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 17s.1.02	**Technology:**	CLI - Command Line Interface
Symptom:	Public ip was getting mismatched in the output of show cluster management rpc.		
Condition:	When REST query done for show-cluster-management in MCT		

Defect ID:	DEFECT000661098		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Configuration Fundamentals
Symptom:	The configuration of virtual-mac for IPv6 VRRP extended group for Ve interface is not working via REST.		
Condition:	Issue is seen only through REST interface. CLI is working fine.		
Workaround:	CLI can be used for configuration of virtual-mac for IPv6 VRRP extended group.		

Defect ID:	DEFECT000661218		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Traffic Management
Reported In Release:	SLXOS 18s.1.00	**Technology:**	Rate Limiting and Shaping
Symptom:	Unexpected reload of SLX 9240 after reboot.		
Condition:	Unexpected reload o SLX 9240 after save and reload with QoS configuration.		
Workaround:	Save QoS configuration on interface to seprate file, instead of startup-config. After reboot, copy qos configuration to running-config.		
Recovery:	Remove qos configuration on physical interface, save the configuration to startup-configuration and reload.		

Defect ID:	DEFECT000661483		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 17s.1.02	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	L2agtd daemon may terminate unexpectedly causing a reload during the boot-up process.		
Condition:	When a SLX switch is acting as a MCT node, the L2agtd daemon may terminate unexpectedly during boot up.		

Defect ID:	DEFECT000662177		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Monitoring
Reported In Release:	SLXOS 18s.1.00	**Technology:**	Port Mirroring
Symptom:	Have port mirroring configuration as a part of running configuration. Reloading the system, try to remove port mirroring configuration. Now we see error in removing port mirroring configuration.		
Condition:	Port mirroring configuration with reload and then remove span configuration.		
Workaround:	Reconfigure mirroring.		

Defect ID:	DEFECT000662513		
Technical Severity:	High	**Probability:**	High
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18s.1.00	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Issue seen when same MAC is received by both leaf nodes at the same time. Duplication of mac not detected.		
Condition:	Same as above.		
Workaround:	Clear bgp evpn neighbor all		

Defect ID:	DEFECT000662716		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 17s.1.02	**Technology:**	VLAN - Virtual LAN
Symptom:	Not all MACs are (re)learnt on an interface when checking the CLI "show mac-address-table" for learnt MACs.		
Condition:	When an interface is shutdown and brought up immediately not all MACs are shown as learnt under the "show mac-address-table" for that interface.		

Defect ID:	DEFECT000662736		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 18s.1.00	**Technology:**	CLI - Command Line Interface
Symptom:	The FEC mode CLI is not enabled for interfaces in 4x25G breakout mode.		
Condition:	The 4x25G breakout feature is introduced in Picasso release.		
Workaround:	The default FEC mode for the 4x25G breakout interfaces is 'auto'. Set the FEC mode for the link peer interface in 'auto' FEC mode for the link to come up.		
Recovery:	The default FEC mode for the 4x25G breakout interfaces is 'auto'. Set the FEC mode for the link peer interface in 'auto' FEC mode for the link to come up.		

Defect ID:	DEFECT000662980		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 18s.1.00	**Technology:**	VLAN - Virtual LAN
Symptom:	Unexpected reload seen under certain config combinations. The box has to be reloaded with the following config- < file config1> After box reboots, configure evpn default vlan 5 Box reload when this CLI is issued after reload.		
Condition:	Node reloads when VLAN is added to EVPN under certain configuration combinations.		
Workaround:	Avoid adding VLAN to EVPN default after reload. Add it as a part of reload config.		
Recovery:	reload the node.		

Defect ID:	DEFECT000664464		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18s.1.00	**Technology:**	ARP - Address Resolution Protocol
Symptom:	Adding a vlan to EVPN default configuration led to an unsual restart of an internal process		
Condition:	Configuring EVPN		

Defect ID:	DEFECT000664625		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	Unexpected hslagt daemon termination		
Condition:	When insight port is enabled via the CLI command "insight port enable" and an unexpected hslagt daemon termination is noticed.		
Workaround:	Disable the "insight port enable" CLI command.		

Closed without code changes for SLX-OS 18s.1.01

This section lists software defects with Critical, High, and Medium Technical Severity closed without a code change as of 12/11/2018.

Defect ID:	DEFECT000650222	**Technical Severity:**	High
Reason Code:	Design Limitation	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	ARP - Address Resolution Protocol
Symptom:	Under conditions of scale, arp daemon displays high cpu utilization after disruptive operations like "clear arp no-refresh" on remote leaf node.		
Condition:	Disruptive triggers executed in high scale IP Fabric deployments.		

Defect ID:	DEFECT000663149	**Technical Severity:**	Medium
Reason Code:	Design Limitation	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 18s.1.00	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	mac database may not be in sync across MCT nodes		
Condition:	when mac are scaled to maximum and hash collision is seen in platform hardware		

Open defects for SLX-OS 18s.1.01

This section lists opoen software defects with Critical, High, and Medium Technical as of 12/11/2018.

Defect ID:	DEFECT000627390		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	IPv6 Addressing
Symptom:	IPv6 ND address may not get suppressed by using this command.		
Condition:	The issue is seen only when ipv6 ND address <address> suppress command is used.		

Defect ID:	DEFECT000627724		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	IP Addressing
Symptom:	REST API with PUT request results in "404 Not Found"		
Condition:	When URI contains elements from multiple yang modules (for example common-def, extreme-interface, intf-loopback and then again extreme-interface) in below example: http://<device-ip>/rest/config/running/common-def:routing-system/extreme-interface:interface/intf-loopback:loopback/100/extreme-interface:vrf/forwarding		

Defect ID:	DEFECT000631251		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Security
Reported In Release:	SLXOS 17s.1.02	**Technology:**	ACLs - Access Control Lists
Symptom:	With large number of rules in IPv4 and IPv6 ACLs, boot up of switch could take up to two hours.		
Condition:	Seen in scenarios where there are large number of rules configured in IPv4 and IPv6 ACL's.		

Defect ID:	DEFECT000635596		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	OSPF neighbor-ship will not formed after changing authentication wait time to 0		
Condition:	Un-configure authentication key after changing the waiting interval to 0		
Workaround:	Configure authentication waiting interval back to 300		
Recovery:	Configure authentication waiting interval back to 300 and shut / no-shut on the interface.		

Defect ID:	DEFECT000635635		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	User might see an error message: "%%Error: OSPF encountered an internal error" when issuing the command "clear ip ospf nei <neighbor address>"		
Condition:	When clear ip ospf neighbor with an unknown IP address.		
Workaround:	clear ip ospf neighbor with a valid neighbor IP address.		

Defect ID:	DEFECT000639874		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Security
Reported In Release:	SLXOS 17s.1.02	**Technology:**	ACLs - Access Control Lists
Symptom:	Security violation RASLog message is not displayed.		
Condition:	On Management port, when ACL applied is changed from ACL with permit rule to an ACL with deny rule.		
Recovery:	No functional impact, only missing RASlog		

Defect ID:	DEFECT000642939		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 17s.1.02	**Technology:**	SNMP - Simple Network Management Protocol
Symptom:	Security violation RASLog message is not displayed.		
Condition:	IPv6 ACL with deny rule is configured on the management interface.		
Recovery:	No functional impact, only missing RASlog		

Defect ID:	DEFECT000643184		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Security
Reported In Release:	SLXOS 17s.1.02	**Technology:**	RADIUS
Symptom:	After reload, the user role mapped with RADIUS of the existing users can't be modified.		
Condition:	Modifying user role is not allowed after switch reload.		
Workaround:	Remove user and reconfigure.		

Defect ID:	DEFECT000643267		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 17s.1.02	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Mac Addresses are not learnt as expected on MCT CCEP/LAG interface.		
Condition:	With large scale configuration and after cluster reload, Mac learning issue observed upon stp disable/enable of an MCT Client interface.		
Recovery:	Perform shut/ no-shut on both nodes of MCT client interface to recover the traffic.		

Defect ID:	DEFECT000644362		
Technical Severity:	Low	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	ASBR status is printed No, when a switch is ABR in NSSR area.		
Condition:	When switch is configured ABR in NSSA area , ASBR status still shows No.		
Workaround:	This is show command print issue and no impact on functionality. As per functionality the switch does act as ASBR		
Recovery:	This is show command print issue and no impact on functionality.As per functionality the switch does act as ASBR		

Defect ID:	DEFECT000645964		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Configuration Fundamentals
Symptom:	When configuring timestamp on a range of interfaces, only the first interface in the range is being configured.		
Condition:	Configure timestamp configuration on a range of interfaces		
Workaround:	Configure timestamp on an individual port basis.		
Recovery:	Configure timestamp on an individual port basis.		

Defect ID:	DEFECT000647174		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	DHCP client packets are dropped by relay agent.		
Condition:	When local subnet broadcast address is configured as relay address.		
Workaround:	Use local DHCP server address as relay address instead of local subnet broadcast address.		

Defect ID:	DEFECT000647572		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	After clear ip bgp neighbor all command is executed, BGP routing table will be empty until user executes the same command after some time.		
Condition:	When Route-maps, Prefix-list or other policies are changed, if user executes clear command before the filter update delay is expired (default 10s), all routes are cleared and not updated until the filter change update delay is expired.		
Workaround:	Use clear ip bgp neighbor all command one more time after the filter change notification delay is complete. The default value for filter change update delay is 10 seconds		
Recovery:	Use clear ip bgp neighbor all command one more time after the filter change notification delay is complete. The default value for filter change update delay is 10 seconds.		

Defect ID:	DEFECT000647939		
Technical Severity:	Medium	**Probability:**	High
Product:	Extreme SLX-OS	**Technology Group:**	Monitoring
Reported In Release:	SLXOS 17r.1.01	**Technology:**	OAM - Operations, Admin & Maintenance
Symptom:	Optical monitoring OIDs are not reporting the aggregate values for RX/TX power on 100G optics. CLI displays aggregate and the MIB displays average values.		
Condition:	snmpwalk on bcsioptMonInfoTable.		

Defect ID:	DEFECT000648466		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	IP Multicast
Reported In Release:	SLXOS 17s.1.02	**Technology:**	IGMP - Internet Group Management Protocol
Symptom:	Upgrading SLX OS from older releases(slxos17s.1.00 or prior) will have Multicast Vlan IGMP and MLD startup query interval value set to 100.		
Condition:	During upgrade the old configuration is restored and the startup query interval value is set to 100.		
Recovery:	Configure "ip igmp snooping startup-query-interval" as 31 under the Vlan.		

Defect ID:	DEFECT000648537		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Monitoring
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Hardware Monitoring
Symptom:	Any port in auto detect mode and the optic is not at default speed, the port will be admin down.		
Condition:	Downgrade from 17s.1.01/02 to 17s.1.00/00a		

Defect ID:	DEFECT000649259		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 17s.1.02	**Technology:**	VXLAN - Virtual Extensible LAN
Symptom:	IPv6 Flow Based ACLs applied under Overlay Gateway services(VXLAN), may not filter traffic.		
Condition:	IPv6 acl with mask greater than 64 for SIP.		
Workaround:	Use "IP address/mask" format with mask less than or equal to 64.		

Defect ID:	DEFECT000650700		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 17s.1.02	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	MCT (Multi-Chassis Trunking) cluster may reset with data traffic loss.		
Condition:	On toggle of MCT client interface with "shutdown" and "no shutdown" commands under stressed scaled configuration.		

Defect ID:	DEFECT000650990		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Provisioned Global MTU not applied on Port-channel interface.		
Condition:	Global MTU configuration applied on port-channel interface.		
Workaround:	Apply MTU configuration on port-channel interface locally		
Recovery:	Remove global MTU configuration and re-provision it.		

Defect ID:	DEFECT000651393		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	OSPFv3 - IPv6 Open Shortest Path First
Symptom:	256 OSPFv3 interfaces are supported on default VRF and in non-default 1000+ OSPFv3 interfaces can be configured.		
Condition:	OSPFv3 interface scale above 256 interfaces in default VRF.		

Defect ID:	DEFECT000652626		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	"show bgp evpn routes rd" does not display all IPV4 routes advertised.		
Condition:	"show bgp evpn routes rd" does not display all IPV4 routes advertised.		
Workaround:	Use alternate CLI - "show bgp evpn routes type ipv4-prefix brief"		

Defect ID:	DEFECT000653005		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	IPv6 Addressing
Symptom:	IPv6 gateway address is not reachable via Ping on Management interface.		
Condition:	Performing shut and no shut after 30 seconds on Management port.		
Workaround:	Initiate a ping to host/gateway from switch or remove/re-add the IPv6 address on the Management port.		

Defect ID:	DEFECT000653273		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	DHCP - Dynamic Host Configuration Protocol
Symptom:	DHCP client on MCT-CCEP ports, may receive inconsistent (option-82 tagged and untagged) OFFER/ACK packets.		
Condition:	DHCP Relay with Option 82 with MCT configuration		

Defect ID:	DEFECT000653384		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 17s.1.02	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	"Show mac-address-table interface" doesn't display learnt Mac-Address on Logical interface.		
Condition:	Execute ?clear mac-address-table dynamic logical-interface <name>? command instead of "clear mac-address-table dynamic".		
Workaround:	Execute `clear mac-address-table dynamic bridge-domain <id>?		

Defect ID:	DEFECT000657587		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Monitoring
Reported In Release:	SLXOS 17s.1.00	**Technology:**	Hardware Monitoring
Symptom:	The status light on the switch blinks from Amber to Green even though one FAN is missing.		
Condition:	A missing fan causes the switch status LED to blink.		

Defect ID:	DEFECT000660054		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Monitoring
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Hardware Monitoring
Symptom:	10GE SFP+ optics used with Mellanox QSA Adapter may not link up.		
Condition:	When 10GE SFP+ optic is used with Mellanox QSA Adapter the port may not link up and "Unqualified SFP transceiver" logs would be reported on the console.		

Defect ID:	DEFECT000660185		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 17s.1.02	**Technology:**	RFN - Remote Fault Notification
Symptom:	Ports with 100G QSFP LR4 Lite optics may experience link down issues.		
Condition:	When using 100G QSFP LR4 Lite optics, part # 57-1000329-01, link instabilities may be noticed with link fault condition.		

Defect ID:	DEFECT000661993		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Monitoring
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Telemetry
Symptom:	Random link down issues noticed with 100G optics		
Condition:	Even after configuring both Tx and Rx link fault signaling to off, random link (remaining) down issues noticed with 100G optics.		
Workaround:	Configure link fault signaling "rx off tx on" as a workaround		

Defect ID:	DEFECT000662124		
Technical Severity:	Medium	**Probability:**	High
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18s.1.00	**Technology:**	Static Routing (IPv4)
Symptom:	Static Anycast Gateway warning message is not printing Virtual interface Id in raslog message in case of mismatch of Virtual IP configured across leaf nodes.		
Condition:	IP Fabric, Satic Anycast Gateway IP configure with different Virtual IP across leaf nodes and configure Vlan entries manual mapping under overlay gateway.		

Defect ID:	DEFECT000662129		
Technical Severity:	High	**Probability:**	High
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18s.1.00	**Technology:**	Static Routing (IPv4)
Symptom:	Static Anycast Gateway warning message is not notified to user in case of different Virtual Mac mapped to same Virtual IP.		
Condition:	IP Fabric, Satic Anycast Gateway configured with different Virtual MAC mapped to same Virtual IP across leaf nodes.		

Defect ID:	DEFECT000662276		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Monitoring
Reported In Release:	SLXOS 17s.1.02	**Technology:**	OAM - Operations, Admin & Maintenance
Symptom:	Customer application cannot read interface power values as the mibs are displaying in microwatts/ dbm format		
Condition:	TX (1.3.6.1.4.1.1588.3.1.8.1.1.1.4) and RX power (1.3.6.1.4.1.1588.3.1.8.1.1.1.7) mibs reporting microwatts/dbm instead of dbm value only		

Defect ID:	DEFECT000662458		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18s.1.00	**Technology:**	GTP - GPRS Tunneling Protocol
Symptom:	Flow header matching option for payload is missing in User Defined ACL for IPv6_GTP_IPv4_L4_Payload packets.		
Condition:	For IPv6 underlay in GTP, only the following frame formats may be matched in ACL: ETH-IPv6-UDP-GTP-IPv4-payload16 ETH-IPv6-UDP-GTP-payload32		

Defect ID:	DEFECT000662477		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Monitoring
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Hardware Monitoring
Symptom:	Unable to get TX/RX Power values for an optic/transceiver through SNMP for the first 3 channels.		
Condition:	TX/RX power is supported for particular SFP/QSFP.		

Defect ID:	DEFECT000663194		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 18s.1.00	**Technology:**	VXLAN - Virtual Extensible LAN
Symptom:	In stress scenario, few MACs can be seen as EVPN though they originated on the same node.		
Condition:	Due to shut on LAG interfaces, in show mac-address-table, fews MACs are shown as EVPN		

Defect ID:	DEFECT000663298		
Technical Severity:	High	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	Monitoring
Reported In Release:	SLXOS 18r.1.00	**Technology:**	Hardware Monitoring
Symptom:	Fan failure will not be displayed in 'show system monitor'.		
Condition:	Fan monitor state in 'show system monitor' will not change from healthy to marginal in case of any fan failure.		

Defect ID:	DEFECT000663724		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18s.1.01	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	User will observe that BGP peer-group cannot be used to de-activate a neighbors under EVPN address-family		
Condition:	when user is using BGP EVPN with peer group configuration, user might observe this behavior.		
Workaround:	Individual neighor can be deactivated under address-family ipv4 unicast.		

Defect ID:	DEFECT000664394		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 18s.1.00	**Technology:**	Software Installation & Upgrade
Symptom:	Default high threshold value for "Current mA" field shown in the output of CLI command "show default threshold" is incorrect.		
Condition:	For SFP type 40GSRINT, the CLI output of "show defaults threshold sfp type 40GSRINT" displays incorrect high threshold for the "Current mA" field.		

Defect ID:	DEFECT000665355		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 18s.1.01	**Technology:**	VLAN - Virtual LAN
Symptom:	This issue is seen only when CLIs "link-error-disable" and "link-fault-signaling" are being configured for an interface first time		
Condition:	when CLI "loopback phy" is not configured.		
Workaround:	Unconfigure the "link-error-disable" and "link-fault-signaling", by running “no link-error-disable” and “no link-fault-signaling” commands.		

Defect ID:	DEFECT000665565		
Technical Severity:	Low	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 18s.1.01	**Technology:**	VLAN - Virtual LAN
Symptom:	SFP boundary check warning messages may appear for current, tx power and rx power, on the console and in the syslog when physical loopback is enabled for physical interfaces. Ex: QSFP28 RX power for port <slot/port>, is below low boundary(High=2188, Low=40). Current value is 0 uW. QSFP28 TX power for port <slot/port>, is below low boundary(High=3162, Low=100). Current value is 0 uW. QSFP28 Current for port <slot/port>, is below low boundary(High=13, Low=3). Current value is 0 mA.		
Condition:	When physical loopback is enabled via "loopback phy" command for SFP ports, current, tx power and rx power related boundary check warning messages may appear on the console and in the syslog.		
Workaround:	Ignore the warning messages or disable the physical loopback after debugging/verification tests are completed.		

Defect ID:	DEFECT000666116		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18s.1.01	**Technology:**	Multi-VRF
Symptom:	Changing the VRF from one format to another format- resulted in RD configured as False in 'show bgp evpn l3vni vrf' command		
Condition:	Same as above		
Workaround:	Remove vrf instance and reconfigure.		

Defect ID:	DEFECT000666289		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18s.1.00	**Technology:**	OSPF - IPv4 Open Shortest Path First
Symptom:	OSPFv2 incorrectly advertises multiple external summary LSAs when overlapping external address ranges are present		
Condition:	Issue will happen only when overlapping external summary ranges are configured		

Defect ID:	DEFECT000666377		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18s.1.01	**Technology:**	BGP4 - IPv4 Border Gateway Protocol
Symptom:	User might observe that the REST API for BGP EVPN IP Fabric is giving some discrepancies for operational data.		
Condition:	User is using REST to query BGP EVPN IP Fabric Operational DB		

Defect ID:	DEFECT000668019		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 18s.1.01	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	CCEP receivers receive double multicast traffic when server is CEP and receivers are on CCEP		
Condition:	Issue seen intermittently on reload		
Workaround:	'shutdown/no shutdown' of the MCT Client followed by 'clear ip igmp group' on both of the MCT cluster nodes.		

Defect ID:	DEFECT000668209		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 18s.1.01	**Technology:**	CLI - Command Line Interface
Symptom:	Should show "Copyright (c) 2017-2018 Extreme Networks Inc."		
Condition:	only when show verison command is executed through rest api		

Defect ID:	DEFECT000668298		
Technical Severity:	High	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 18s.1.01	**Technology:**	CLI - Command Line Interface
Symptom:	"Security Violation: Login failure - Public key Authentication failed" may appear in audit log although the login is successful.		
Condition:	When logged in to the device via SSH or Netconf, "Security Violation: Login failure - Public key Authentication failed" may appear in the audit log, followed by "Successful login" message.		
Workaround:	Ignore the erroneous "Login failure" message in the audit log.		

Defect ID:	DEFECT000668405		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 18s.1.01	**Technology:**	CLI - Command Line Interface
Symptom:	SNMP query for dot1qTpFdbPort object doesn't yield the correct output.		
Condition:	When SNMP query is performed on the MIB object dot1qTpFdbPort, it always returns "-1". Avoid using the query output		

Defect ID:	DEFECT000668408		
Technical Severity:	High	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 18s.1.01	**Technology:**	CLI - Command Line Interface
Symptom:	Radius local-auth-fallback configuration may not reflect correctly in running config.		
Condition:	When AAA authentication configuration is modified from "tacacs+ local-auth-fallback" to "radius local-auth-fallback" in one step, the "local-auth-fallback" option may not reflect in the running config.		
Workaround:	Remove the existing authentication configuration (ex:"tacacs+ local-auth-fallback") and then add the new configuration (ex: "radius local-auth-fallback") instead of attempting modification in one step.		

Defect ID:	DEFECT000668412		
Technical Severity:	High	**Probability:**	High
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 18s.1.01	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Additional traffic (known traffic) is forwarded to CCEP client		
Condition:	no deploy / deploy of CCEP client		

Defect ID:	DEFECT000668446		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 18s.1.01	**Technology:**	Multi-VRF
Symptom:	In EVPN Type-5 Route import into multiple vrf table use-case. while deleting import RT on one of the vrf , cleanup TYPE-5 EVPN routes happens on all vrf table.		
Condition:	Importing EVPN Type-5 L3 Prefix Route into more than one VRF table.		
Workaround:	when Route Target is deleted under vrf configuration, User trigger the clear command "clear bgp evpn neighbor <peer-ip> soft in"		

Defect ID:	DEFECT000668450		
Technical Severity:	High	**Probability:**	High
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 18s.1.01	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	Redundant traffic is sent from both MCT peers		
Condition:	no deploy / deploy the cluster		

Defect ID:	DEFECT000668458		
Technical Severity:	High	**Probability:**	High
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 18s.1.01	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	After "clear ip bgp neighbor all" on MCT cluster, traffic drop observed while forwarding multicast traffic		
Condition:	Execution of clear ip bgp neighbor all		

Defect ID:	DEFECT000668466		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 18s.1.01	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	static groups configured on a vlan shows the physical ports but not the CCEP PO ports		
Condition:	sh ip igmp groups for static groups		

Defect ID:	DEFECT000668477		
Technical Severity:	Medium	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 18s.1.01	**Technology:**	CLI - Command Line Interface
Symptom:	After firmware upgrade, when issue "usb on" for the first time, the command could fail with error "Fail to enable USB storage device. Error: The device directory structure is not formatted"		
Condition:	After firmware upgrade		
Workaround:	Wait for several minutes and issue the "usn on" again		

Defect ID:	DEFECT000668553		
Technical Severity:	High	**Probability:**	Low
Product:	Extreme SLX-OS	**Technology Group:**	Layer 2 Switching
Reported In Release:	SLXOS 18s.1.01	**Technology:**	MCT - Multi-Chassis Trunking
Symptom:	When MCT node is reloaded the Multicast traffic is stabilized/forwarded after few seconds on the MCT node that is up, but after some time some groups have the member ports removed from the group table on the currently up MCT node		
Condition:	MCT node is reloaded in scaled configuration.		

Defect ID:	DEFECT000668034		
Technical Severity:	High	**Probability:**	Med
Product:	Extreme SLX-OS	**Technology Group:**	Management
Reported In Release:	SLXOS 18s.1.01	**Technology:**	CLI - Command Line Interface
Symptom:	When the special character single code (') is used in password, "copy config" command will fail, as it is not supported.		
Condition:	password contains special character as single code (')		
Workaround:	Avoid using single code (') in password		

EFA open defects

Defect ID:		SIPF-471	
Technical Severity:	Medium	**Probability:**	Medium
Product:	Extreme SLX-OS	**Technology Group:**	NA
Reported In Release:	SLXOS 18s.1.01	**Technology:**	NA
Symptom:		Seeing a warning message to clear any warnings/errors with the TPVM startup.	
Condition:		First iteration of "efa deploy" failed with warnings.	

Defect ID:		SIPF-477	
Technical Severity:	High	**Probability:**	High
Product:	Extreme SLX-OS	**Technology Group:**	NA
Reported In Release:	SLXOS 18s.1.01	**Technology:**	NA
Symptom:		Failed to discover MCT links during ad devices to fabric.	
Condition:		MCT configuration failed between SLX 9140 over 25G links.	

Defect ID:		SIPF-479	
Technical Severity:	Low	**Probability:**	High
Product:	Extreme SLX-OS	**Technology Group:**	NA
Reported In Release:	SLXOS 18s.1.01	**Technology:**	NA
Symptom:		Configuring IPv4 Static Anycast MAC Address on spine.	
Condition:		IPv4 Static Anycast MAC Address is configured on spines.	