

May 2022



SLX-OS 18r.1.00m for SLX 9850 and SLX 9540

Release Notes

Copyright © 2022 Extreme Networks, Inc. All Rights Reserved.

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

Release Notes.....	1
Contents	3
Document history.....	5
Preface	6
Contacting Extreme Technical Support.....	6
Extreme resources	6
Document feedback	7
Overview	8
New SKUs	9
Behavior changes	10
Behavior changes in release 18r.1.00m	10
No system behavior changes were made in this release	10
Behavior changes in release 18r.1.00k	10
The following system behavior have changed in this release.....	10
Behavior changes in release 18r.1.00j	10
Software Features	11
New software features in 18r.1.00m	11
New software features in 18r.1.00k	11
New Software features in 18r.1.00j	12
CLI commands	16
CLI commands introduced in R18r.1.00m	16
CLI commands introduced in R18r.1.00k	16
CLI commands introduced in R18r.1.00j	16
RFCs, Standards, and Scalability.....	17
Hardware support	18
Supported devices.....	18
Supported power supplies	19
Supported optics	19
Supported Extreme optics in SLX-OS 18r.1.00d	21
Software upgrade and downgrade	22
Image file names	22
Upgrade and downgrade considerations.....	22
MCT Upgrade Process	25
Limitations and restrictions.....	29
Defects	34
Defects closed in 18r.1.00m.....	34
Defects closed in 18r.1.00k	35
Defects closed in 18r.1.00j.....	41
Defects closed in 18r.1.00h.....	48
Defects closed in 18r.1.00g	50
Defects closed in 18r.1.00f.....	52
Defects closed in 18r.1.00e	56
Defects closed in 18r.1.00d.....	61
Defects closed in 18r.1.00c	67

Document history

Version	Summary of changes	Publication date
1.0	Initial Release Removed versions older than 18r.1.00h	May 2022

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 <https://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 <https://www.extremenetworks.com/documentation-feedback/>
- Email us at documentation@extremenetworks.com

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Overview

SLX-OS 18r.1.00m supports multiple customer found defect solutions.

SLX-OS 18r.1.00k supports the following solutions and features:

- Source interface support for Tacacs server
- Disable Default Implicit Deny Rule for RACL

SLX-OS 18r.1.00j supports the following solutions and features:

- Import TLS Server Certificate and Private key without any Trust Point
- MPLS XC Scale increase 64K
- Mgmt vrf support for TFTP/SCP

SLX-OS 18r.1.00e adds Password Encryption Policy: SHA-512 Support .

SLX-OS 18r.1.00d supports multiple customer found defect solutions.

SLX-OS 18r.1.00a supports the following solutions and features:

- L2 Exchange
 - Egress ACL rate-limiting: This is a key feature for IXP customers to flexibly rate-limit ACL filtered traffic on port/VLAN/BD
- vSLX
 - IP fabric BGP EVPN VXLAN control plane
 - L2 Exchange control plane

Note:

vSLX is community supported in the Extreme “The Hub” Community pages for Switching and Routing Data Center products.

https://community.extremenetworks.com/extreme/categories/extreme_switchingrouting

Details of support process for vSLX is available in the vSLX guide and release note.

New SKUs

No new SKUs are introduced in this release.

Behavior changes

For information about 18r.1.00h and earlier releases, please refer to the [SLX-OS 18r.1.00h Release Notes](#).

Behavior changes in release 18r.1.00m

No system behavior changes were made in this release

Behavior changes in release 18r.1.00k

The following system behavior have changed in this release

- Source interface support for Tacacs server
- Disable Default Implicit Deny Rule for RACL

Behavior changes in release 18r.1.00j

The following system behaviors have changed in this release

- Import TLS Server Certificate and Private key without any Trust Point
- MPLS XC Scale increase 64K
- Mgmt vrf support for TFTP/SCP

Software Features

For information about 18r.1.00h and earlier releases, please refer to the [SLX-OS 18r.1.00h Release Notes](#).

New software features in 18r.1.00m

No new software features were added in this release.

New software features in 18r.1.00k

The following behaviors have changed in this release:

Source interface support for Tacacs server

“Source Interface support for tacacs server” feature implies that, use the IP address of the specified source interface in the ‘Source IP’ field of the IP header of the Tacacs packet.

In SLX 18r.1.00k release , options for ‘source-interface’ command to the Tacacs client. *Management Module IP address, physical interface, VE and Loopback* interfaces are all supported. *Chassis IP* is not supported under source-interface.

‘Source IP’ of IP header is used to recognize and reach back to a device using one IP address irrespective of the interface (in-band/data) of the device through which the packet has egressed.

One Source IP for all the packets transmitted from the device will help in cases such as:

1. Configuring the ACLs in firewalls with one IP address for a given device instead of using multiple in-band interface IP addresses of the device.
2. Maintaining connectivity with the device through an alternative path (for example, when Loopback interface is used for the Source IP) even when one of the in-band ports of the device goes down through which active communication was going through.

CLI Interface

```
dutA(config)# tacacs-server host <host-IPV4/IPV6> ?
```

Possible completions:

```
use-vrf    VRF to choose for server connection: mgmt-vrf(default), default-  
vrf, <user VRF>  
<cr>
```

With user defined VRF:

```
SLX(config)# tacacs-server host <IPV4/IPV6> use-vrf <vrf-name>  
SLX(config-host-IP/red)# source-interface
```

Possible completions:

```
ethernet          Ethernet interface  
loopback          loopback interface  
management-options 1 Active-MM-IP 0 Chassis-IP  
ve                ve interface
```

Note:- when use-vrf is not mentioned, mgmt-vrf is used by default.

Limitation:- Chassis IP is not supported as source-interface.

Disable Default rule for RACL

This feature is to provide a CLI option to disable programming of the default rule for receive ACL during binding operation.

With this feature, for IPV4 and IPV6 ACLs, while binding as receive ACL, users have the option to disable the default rule “Implicit deny” by configuring the “Implicit permit” option.
If “Implicit permit” option is not selected while binding the RACL, the default rule of “Implicit deny” will be enabled.

CLI Commands

To disable the default rule of “implicit deny any” during binding operation the below option `implicit_permit` needs to be selected.

To apply an IPV4 RACL:

```
ip receive access-group <acl_name>?
```

Possible completions:

```
Implicit_permit    -> will not program implicit deny rule by default.  
<cr>              -> Will program implicit deny rule by default.
```

To apply an IPV6 RACL:

```
Ipv6 receive access-group <acl_name>?
```

Possible completions:

```
Implicit_permit    -> will not program implicit deny rule by default.  
<cr>              -> Will program implicit deny rule by default.
```

If the default rule is already disabled and if we need to enable it, we just need to rebind without `implicit_permit` option.

Config examples:

```
sw0(config)# ip access-list extended test-racl  
sw0(conf-ipacl-ext)# deny ip 2.2.2.2/32 1.1.1.1/32  
sw0(conf-ipacl-ext)# permit ip 2.2.2.2/32 any  
sw0(conf-ipacl-ext)# exit  
sw0(config)#
```

To disable implicit deny:

```
SLX2(config)# ip receive access-group test_racl Implicit_permit
```

To enable implicit deny (Default behaviour):

```
SLX2(config)# ip receive access-group test_racl
```

If the default rule is already disabled and if we need to enable:

Remove the binding.

```
SLX2(config)# no ip receive access-group test_racl  
Re apply without selecting implicit_permit option.  
SLX2(config)# ip receive access-group test_racl
```

Limitations:

Only default Tcam profile is supported for RACL

New Software features in 18r.1.00j

The following behaviors have changed in this release:

Import TLS Server Certificate and Private Key Without any Trust Point

- System administrator will be able to import TLS server certificate and private key directly to SLX device

(without any trust point association) and use these two to establish secure connection.

- System administrator must use the new `crypto ca import-pkcs` command to import server certificate and private key in PKCS12 format from external server.

```
SLX# crypto ca import-pkcs type <pkcs12> directory <dir-name> file <file-name> host
<host-name/ip> protocol <SCP|FTP> user <user-name> password <scp-password> [pkcs-
passphrase <pkcs export password>]
```

- System administrator must perform the following configurations for the changes to take effect.

Restart the *https server* using `http server use-vrf <VRF Name> shutdown, no http server use-vrf <VRF Name> shutdown` or by rebooting the SLX device.

- System administrator must ensure that TLS server certificate being imported is well formed. That is, the certificate is a valid signing certificate, that has not expired, and not been tampered with.

Note:- System administrator can check the certificate's creation time using the `openssl x509 -noout -text -in tlscert.pem | grep 'Not Before'` command. The time on the device must be later than this time, or the installation will not work.

- Imported server certificate will be validated on some parameters to ensure that it is a valid certificate. Error message will be thrown when the certificate is not valid.

For example: The server certificate will be validated based on the 'not before' and 'not after time'. The time on the device must be within this time range, otherwise, validation will fail and a generic error message will be thrown.

- Only `crypto ca import` and `crypto ca import-pkcs` commands are mutually exclusive. You will be able to authenticate and enroll when PKCS based server certificate is present in device.
- If any pre-configured server certificate and key are present in the device (configured using the crypto CLI commands or imported using pkcs12), the System Administrator needs to remove the installed server certificate and its key using the 'no' equivalent of crypto commands before importing the new server certificate and private key using import pkcs12 command. The following example shows this process:

```
SLX# no crypto ca import <trustpoint-name> certificate
SLX# no crypto ca authenticate <trustpoint-name>
SLX# config
Entering configuration mode terminal
SLX(config)# crypto ca trustpoint <trustpoint-name>
SLX(config-ca-tl)# no keypair
SLX(config-ca-tl)# exit
SLX(config)# no crypto ca trustpoint <trustpoint-name>
SLX(config)# no crypto key label <key-name>
SLX(config)# end
SLX#
```

Note:

- The enrolled certificate from DUT cannot be converted into a *pfx* file since there will be a mismatch in the private key for the enroll process.
- TLS certificate will be deleted when `perform full-install upgrade`

MPLS XC Scale increased to 64K

- Increased the MPLS cross connections to 64K.

Note: 32K XC supported for FRR and 64K supported for non-FRR.

Mgmt vrf support for TFTP/SCP

- System administrator will be able to copy configurations using SCP and TFTP protocols with user-vrf

support.

```
SLX# copy startup-config scp://<username>:<Password>@<Host/IP>/ <File Path>
Possible completions:
  use-vrf      Valid Vrf Name
  |            Output modifiers
  <cr>
```

- Copy config using mgmt- vrf through SCP protocol

```
SLX# copy running-config scp://<username>:<password>@hostname/<filepath>
use-vrf mgmt-vrf
```

- Copy config using default- vrf through SCP protocol

```
SLX# copy running config scp://<username>:<password>@hostname/<filepath>
```

- Copy config using user- vrf through SCP protocol

```
SLX# copy running-config scp://<username>:<password>@hostname/<filepath>
user-vrf
```

- Copy config using mgmt- vrf support through TFTP protocol

```
SLX# copy running-config tftp://<username>:<password>@hostname/<filepath>
use-vrf mgmt-vrf
```

- Copy config using default- vrf support through TFTP protocol

```
SLX# copy running config tftp://<username>:<password>@hostname/<filepath>
```

- Copy config using user- vrf support through TFTP protocol

```
SLX#copy running-config tftp://<username>:<password>@hostname/<filepath>
user-vrf
```

- Ensure that Interface which configured as user defined vrf, should be connected to in-band server interface and reachable via user defined vrf.

```
SLX (config)# vrf <user defined vrf>
Eg: Configuring user -vrf as green-vrf
SLX (config)# vrf user-vrf
SLX (config-vrf-green-vrf) # address-family ipv4 unicast
SLX (config-vrf-green-vrf-ipv4-unicast) # address-family ipv6 unicast
SLX (config-vrf-green-vrf-ipv6-unicast) # end
```

- Assign IP for interface using user defined vrf and enable forwarding via this user defined vrf

```
SLX# conf t
SLX (config)# int eth slot/port
SLX (conf-if-eth-slot/port) # vrf forwarding <user defined vrf>
SLX (conf-if-eth-slot/port) # ip add <ip>
SLX (conf-if-eth-slot/port) # no shut
SLX (conf-if-eth-slot/port) # end
```

Note: The interface on in-band server should be on same subnet which connected to user -vrf interface having IP.

CLI commands

For information about 18r.1.00h and earlier releases, please refer to the [SLX-OS 18r.1.00h Release Notes](#).

CLI commands introduced in R18r.1.00m

No commands were introduced in this release.

CLI commands introduced in R18r.1.00k

The following commands were introduced in this release:

```
ip receive access-group <acl_name>?
```

Possible completions:

```
Implicit_permit    -> will not program implicit deny rule by default.
```

```
<cr>              -> Will program implicit deny rule by default.
```

```
Ipv6 receive access-group <acl_name>?
```

Possible completions:

```
Implicit_permit    -> will not program implicit deny rule by default.
```

```
<cr>              -> Will program implicit deny rule by default.
```

```
SLX(config)# tacacs-server host <IPV4/IPV6> use-vrf <vrf-name>
```

```
SLX(config-host-IP/red)# source-interface
```

CLI commands introduced in R18r.1.00j

The following command was introduced in this release:

```
SLX# crypto ca ?
```

Possible completions:

```
authenticate      Authenticate the certificate authority certificate
```

```
enroll            Create and export Certificate request
```

```
import            Import Certificate
```

```
import-pkcs       Import Host Certificate and Private key bundled in PKCS#12
```

```
format
```


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 9850 and SLX 9540](#).

Hardware support

Supported devices

The following devices are supported in this release:

Supported Hardware	Description
BR-SLX9850-4-BND-AC	Extreme SLX 9850 4-slot chassis with 1 management module, 5 switch fabric modules, 2 3000W AC power supplies, 3 fan modules, and accessory kit. Power cord not included.
BR-SLX9850-4-BND-DC	Extreme SLX 9850 4-slot chassis with 1 management module, 5 switch fabric modules, 2 3000W DC power supplies, 3 fan modules, and accessory kit. Power cord not included.
BR-SLX9850-8-BND-AC	Extreme SLX 9850 8-slot chassis with 1 management module, 5 switch fabric modules, 4 3000W AC power supplies, 3 fan modules, and accessory kit. Power cord not included.
BR-SLX9850-8-BND-DC	Extreme SLX 9850 8-slot chassis with 1 management module, 5 switch fabric modules, 4 3000W DC power supplies, and 3 fan modules, and accessory kit. Power cord not included.
BR-SLX9850-10GX72S-M	Extreme SLX 9850 72-port 10 GbE/1 GbE dual-speed (M) interface module with IPv4/IPv6/MPLS hardware support. Requires SFP+ optics for 10 GbE connectivity and SFP optics for 1 GbE connectivity. Supports up to 750,000 MAC. Supports up to 1,500,000 IPv4 routes, 140,000 IPv6 routes with OptiScale™ Internet Routing.
BR-SLX9850-100GX36CQ-M	Extreme SLX 9850 36-port 100 GbE, 60-port 40 GbE, or 240-port 10 GbE flex-speed (M) interface module with IPv4/IPv6/MPLS hardware support. Requires QSFP28 optics for 100 GbE, QSFP+ optics for 40 GbE, and 40 GbE to 10 GbE breakout for 10 GbE connectivity. Supports up to 750,000 MAC. Supports up to 1,500,000 IPv4 routes, 140,000 IPv6 routes with OptiScale™ Internet Routing.
BR-SLX9850-10GX72S-D	Extreme SLX985072-port 10GbE/1GbE (D) interface module with IPv4/IPv6 hardware support. Requires SFP+ optics for 10GbE connectivity and SFP optics for 10GbE connectivity. Supports 750K MAC, 256K IPv4 routes and 64K IPv6 routes with up to 8GB packet buffers
BR-SLX9850-100GX36CQ-D	Extreme SLX 9850 36-port 100GbE, 60-port 40GbE, or 240-port 10GbE flex-speed (D) interface module with IPv4/IPv6 hardware support. Requires QSFP28, QSFP+ optics & 40GbE to 10GbE
BR-SLX9850-100GX12CQ-M	Extreme SLX 9850 12-port 100 GbE, 20-port 40GbE, or 80-port 10GbE flex-speed (M) interface module with IPv4/IPv6/MPLS hardware support. Requires QSFP28, QSFP+ optics & 40GbE to 10GbE breakout (for 10 GbE) connectivity. Supports up to 750,000 MAC. Supports up to 1,500,000 IPv4 routes, 140,000 IPv6 routes with OptiScale™ Internet Routing.
BR-SLX9850-100GX6CQ-M-UPG	6x100G POD SW license to be used with SLX9850-100Gx12CQ-M 100G blade only
XBR-SLX9850-4-S	Extreme SLX9850 Spare 4-slot chassis
XBR-SLX9850-8-S	Extreme SLX9850 Spare 8-slot chassis
BR-SLX9850-MM	Extreme SLX 9850 management module for 4-slot and 8-slot systems, includes 16GB RAM, 2 internal Solid State Drives, 4-Core Intel CPU, 2 USB 3.0 ports, 2 RJ-45 console ports, and 10GbE Services port
BR-SLX9850-4-SFM	Extreme SLX 9850 switch fabric module for 4-slot chassis
BR-SLX9850-8-SFM	Extreme SLX 9850 switch fabric module for 8-slot chassis
XBR-SLX9850-ACPWR-3000	Extreme SLX 9850 AC 3000W power supply for 4- and 8-slot chassis, 90-270V AC input
XBR-SLX9850-DCPWR-3000	Extreme SLX 9850 DC 3000W power supply for 4- and 8-slot chassis
XBR-SLX9850-4-FANM	Extreme SLX 9850 fan module for 4-slot chassis. Fan module has 2 fans
XBR-SLX9850-8-FANM	Extreme SLX 9850 fan module for 8-slot chassis. Fan module has 4 fans
XBR-SLX9850-4-CAB	Extreme SLX 9850 Cable Combo Kit for 4-slot chassis
XBR-SLX9850-8-CAB	Extreme SLX 9850 Cable Combo Kit for 8-slot chassis
XBR-SLX9850-4-SFMPNL	Extreme SLX 9850 switch fabric module blank panel for 4-slot chassis
XBR-SLX9850-8-SFMPNL	Extreme SLX 9850 switch fabric module blank panel for 8-slot chassis
XBR-SLX9850-PWRPNL	Extreme SLX 9850 power supply blank panel for 4-slot and 8-slot chassis
XBR-SLX9850-IMPNL	Extreme SLX 9850 interface module blank panel for 4-slot and 8-slot chassis
XBR-SLX9850-MMPNL	Extreme SLX 9850 management module blank panel for 4-slot and 8-slot chassis
XBR-SLX9850-4-4PRM-KIT	Extreme SLX 9850 four-post rack mounting kit for 4-slot chassis. Include 27-31" flush and recessed Mounting
XBR-SLX9850-4-2PRM-KIT	Extreme SLX 9850 two-post rack mounting kit for 4-slot chassis. Include telco flush and midplane mounting
XBR-SLX9850-8-4PRM-KIT	Extreme SLX 9850 four-post rack mounting kit for 8-slot chassis. Include flush and recessed mounting
XBR-SLX9850-8-2PRM-KIT	Extreme SLX 9850 two-post rack mounting kit for 8-slot chassis. Include telco flush and midplane Mounting
BR-SLX-9540-24S-AC-F	Extreme SLX 9540-24S Switch AC with Front to Back airflow. Supports 24x10GE/1GE + 24x1GE ports
BR-SLX-9540-24S-DC-F	Extreme SLX 9540-48S Switch DC with Front to Back airflow. Supports 48x10GE/1GE + 6x100GE/40GE

BR-SLX-9540-24S-AC-R	Extreme SLX 9540-24S Switch AC with Back to Front airflow. Supports 24x10GE/1GE + 24x1GE ports
BR-SLX-9540-24S-DC-R	Extreme SLX 9540-24S Switch DC with Back to Front airflow. Supports 24x10GE/1GE + 24x1GE ports
BR-SLX-9540-48S-AC-F	Extreme SLX 9540-48S Switch AC with Front to Back airflow. Supports 48x10GE/1GE + 6x100GE/40GE
BR-SLX-9540-48S-DC-F	Extreme SLX 9540-48S Switch DC with Front to Back airflow. Supports 48x10GE/1GE + 6x100GE/40GE
BR-SLX-9540-48S-AC-R	Extreme SLX 9540-48S Switch AC with Back to Front airflow. Supports 48x10GE/1GE + 6x100GE/40GE
BR-SLX-9540-48S-DC-R	Extreme SLX 9540-48S Switch DC with Back to Front airflow. Supports 48x10GE/1GE + 6x100GE/40GE
BR-SLX-9540-24S-COD	Upgrade 24x1GE to 24x10GE/1GE
BR-SLX-9540-2C-POD	Ports on Demand for 2x100GE/40GE Uplinks
BR-SLX-9540-ADV-LIC-P	Advanced Feature License for MPLS, BGP-EVPN, CE2.0, NSX, OptiScale™ Internet Routing (for Extreme SLX 9540-24S and 9540-48S)

Supported power supplies

- Extreme SLX 9850 AC 3000W power supply for 4- and 8-slot chassis, 90-270V AC input
- Extreme SLX 9850 DC 3000W power supply for 4- and 8-slot chassis, 48V DC input

Supported optics

Part Number	Description
10065	10/100/1000BASE-T SFP
10301	ASSY, SR SFP+ SHIPPING
10302	ASSY, LR SFP+ SHIPPING
10303	LRM SFP+ Module
10304	1m SFP+ Cable
10305	3m SFP+ Cable
10306	5m SFP+ Cable
10310	ZR SFP+ module
10319	40g QSFP+ SR\$ 850nm
10338	10Gb SFP+ 10GBASE-T
10401	100Gb QSFP28 SR4 MMF
10405	100Gb QSFP28 PSM4
10504	25G LR SFP28 10km
10052H	1000BASE-LX SFP, Hi
10056H	1000BASE-BX-D BiDi SFP, Hi
10057H	1000BASE-BX-U BiDi SFP, Hi
10070H	10/100/1000BASE-T SFP, Hi
100G-4WDM-QSFP10KM	100G 4WDM-10 QSFP28 10km
100G-4WDM-QSFP20KM	100G 4WDM-20 QSFP28 20km
100G-4WDM-QSFP40KM	100G 4WDM-40 QSFP28 40km
100G-AOC-QSFP10M-TA	100G AOC QSFP28 10m TAA
100G-CWDM4-QSFP2KM	100G CWDM4 QSFP28 2km
100G-DACP-QSFP1M	100G Passive DAC QSFP28 1m
100G-DACP-QSFP3M	100G Passive DAC QSFP28 3m
100G-DACP-QSFP4SFP1M	100G Passive DAC QSFP28 to 4xSFP28 1m
100G-DACP-QSFP4SFP3M	100G Passive DAC QSFP28 to 4xSFP28 3m
100G-DACP-QSFP4SFP5M	100G Passive DAC QSFP28 to 4xSFP28 5m
100G-DACP-QSFP5M	100G Passive DAC QSFP28 5m
100G-ER4LT-QSFP40KM	100G ER4-lite QSFP28 40km
100G-ESR4-QSFP300M	100G ESR4 QSFP28 300m
100G-LR4-QSFP10KM	100G LR4 QSFP28 10km

Part Number	Description
100G-LR4-QSFP2KM	100G LR4 QSFP28 2km
100G-SR4-QSFP100M	100G SR4 QSFP28 100m
100G-SWDM4-QSFP100M	100G SWDM4 QSFP28 100m
10G-AOC-SFP10M	10G AOC SFP+ 10m
10G-AOC-SFP7M	10G AOC SFP+ 7m
10GB-BX10-D	10 GB, SINGLE FIBER SM, -D 10 KM
10GB-BX10-U	10 GB, SINGLE FIBER SM, -U 10 KM
10G-DACA-SFP1M	10G Active DAC SFP+ 1m
10G-DACA-SFP3M	10G Active DAC SFP+ 3m
10G-DACA-SFP5M	10G Active DAC SFP+ 5m
10G-ER-SFP40KM-ET	10G ER SFP+ 40km Ext.Temp
10G-LR-SFP10KM-ET	10G LR SFP+ 10km Ext.Temp
10G-SR-SFP300M-ET	10G SR SFP+ 300m Ext.Temp
10G-USR-SFP100M	10G USR SFP+ 100m Hight Rx Sens
25G-DACP-SFP1M	25G Passive DAC SFP28 1m
25G-DACP-SFP3M	25G Passive DAC SFP28 3m
25G-LR-SFP10KM	25G LR SFP28 10km
40G-AOC-QSFP100M	40G AOC QSFP+ 100m
40G-AOC-QSFP10M	40G AOC QSFP+ 10m
40G-AOC-QSFP20M	40G AOC QSFP+ 20m
40G-AOC-QSFP3M	40G AOC QSFP+ 3m
40G-AOC-QSFP5M	40G AOC QSFP+ 5m
40G-BDSR-QSFP150M	40G BiDi SR QSFP+ 150m
40G-DACA-QSFP1M	40G Active DAC QSFP+ 1m
40G-DACA-QSFP3M	40G Active DAC QSFP+ 3m
40G-DACA-QSFP4SFP1M	40G Active DAC QSFP+ to 4xSFP+ 1m
40G-DACA-QSFP4SFP5M	40G Active DAC QSFP+ to 4xSFP+ 5m
40G-DACA-QSFP5M	40G Active DAC QSFP+ 5m
40G-DACP-QSFP1M	40G Passive DAC QSFP+ 1m
40G-DACP-QSFP3M	40G Passive DAC QSFP+ 3m
40G-DACP-QSFP4SFP1M	40G Passive DAC QSFP+ to 4xSFP+ 1m
40G-DACP-QSFP4SFP2M	40G Passive DAC QSFP+ to 4xSFP+ 2m
40G-DACP-QSFP4SFP3M	40G Passive DAC QSFP+ to 4xSFP+ 3m
40G-DACP-QSFP4SFP5M	40G Passive DAC QSFP+ to 4xSFP+ 5m
40G-DACP-QSFP5M	40G Passive DAC QSFP+ 5m
40G-DACP-QSFPZ5M	40G Passive DAC QSFP+ 0.5m
40G-ESR4-QSFP400M-NT	40G ESR4 QSFP+ 400m 10G-SR interop.
40G-LM4-QSFP160M	40G LM4 QSFP+ 160m 160m MMF. 1km SMF
40G-LR4-QSFP10KM	40G LR4 QSFP+ 10km
40G-SR4-QSFP150M	40G SR4 QSFP+ 150m
MGBIC-LC01-G	1GB SX MM, SFP, TAA

*Optics reference qualified and should be purchased from the respective vendors. Extreme does not sell these directly.

Supported Extreme optics in SLX-OS 18r.1.00d

The following orderable Extreme optics are supported in release SLX-OS 18r.1.00d:

Orderable Optic SKUs	Description
100G-CWDM4-QSFP2KM	100G CWDM4 QSFP28 2km
10301	ASSY, SR SFP+ SHIPPING
10302	ASSY, LR SFP+ SHIPPING
10070H	10/100/1000BASE-T SFP, Hi
10052H	1000BASE-LX SFP, Hi
100G-LR4-QSFP10KM	100G LR4 QSFP28 10km
40G-SR4-QSFP150M	40G SR4 QSFP+ 150m

Software upgrade and downgrade

Image file names

Download the following images from www.extremenetworks.com.

Image file name	Description
SLX-OS_18r.1.00m.tar.gz	SLX-OS 18r.1.00m software
SLX-OS_18r.1.00_mib.tar.gz	SLX-OS 18r.1.00m MIBS
SLX-OS_18r.1.00m.md5	SLX-OS 18r.1.00m md5 checksum

Upgrade/downgrade considerations using firmware download CLI through fullinstall

The fullinstall CLI option is supported through the firmware download when upgrading from release SLX- OS 17r.1.01a to SLX-OS 17r.2.01. The fullinstall CLI option is NOT supported with USB.

Upgrade and downgrade considerations

- Upgrade from a 32-bit to 32-bit SLX-OS is performed using 'coldboot' option
- Upgrade from a 32-bit to 64-bit SLX-OS is a two-step sequential process as shown below:
 - 1) Upgrade using 'coldboot' to 17r.1.01a
 - 2) Upgrade using 'fullinstall' to 64-bit SLX OS
- Upgrade/Downgrade using 'fullinstall' takes up to 60 minutes for completion as compared to 25 minutes for 'coldboot'
- Upgrade from a 64-bit to 64-bit SLX-OS is performed using 'coldboot' option
- It is recommended to use 7zip or WinRAR to Un-compress the SLXOS tarfile
- When firmware upgrade or downgrade is performed, following matrix can be used as a reference.

To	16r.1.00 17r.1.00 17r.1.01 (32-bit)	17r.1.01b (32-bit)	17r.2.00a (64-bit)	18r.1.00 18r.1.00a to 18r.1.00k (64-bit)	18r.1.00m
From					
16r.1.00 17r.1.00 17r.1.01 (32-bit)	Coldboot	coldboot	Two Step Process: 1. Upgrade to 17r.1.01b 2. Upgrade to 17r.2.00a	Two Step Process: 1. Upgrade to 17r.1.01b 2. Upgrade to 18r.1.00,18r.1.00a to 18r.1.00j	Two Step Process: 1. Upgrade to 17r.1.01b 2. Upgrade to 18r.1.00k
17r.1.01b (32-bit)	Coldboot	coldboot	fullinstall	fullinstall	fullinstall
17r.2.00a (64-bit)	Two Step Process: 1. Downgrade to 17r.1.01b 2. coldboot to 16r.1.00	fullinstall	coldboot	coldboot	coldboot
18r.1.00 18r.1.00a to 18r.1.00k (64-bit)	Two Step Process: 1. Downgrade to 17r.1.01b 2. coldboot to 16r.1.00	fullinstall	coldboot	coldboot	coldboot
18r.1.00m	Two Step Process: 1. Downgrade to 17r.1.01b 2. coldboot to 16r.1.00	Fullinstall	Coldboot	coldboot	NA

Upgrade Steps from 32-bit to 64-bit SLX-OS

1. Make sure the device is running SLXOS 17r.1.01a or later, if not, please see the 17r.1.01 documentation on how to upgrade to that release.
2. Upgrade to SLX-OS 18r.1.00 using fullinstall
3. Save Configuration

To save the config, run

```
copy running-config startup-config
```

4. Firmware download with “fullinstall” option from source directory

```
device# firmware download fullinstall ftp user releaseuser password releaseuser file release.plist  
directory <path> host <host_ip>
```

Notes:

Firmware download with the “fullinstall” option will retain the startup configuration file, and upon auto reboot of the device, it will replay the startup configuration file automatically.

Firmware [download] upgrade support from SLXOS 18r.1.00b [Linux Kernel 2.6] to SLXOS 19.1.0 [Linux Kernel 4.14] is available from SLXOS 18r.1.00b onwards using "fullinstall" additional keyword

Upgrade/downgrade using firmware download CLI through USB:

- Upgrade from SLX-SLX 17r.1.01a to SLX-OS 17r.2.01 is supported via firmware download CLI with “fullinstall” option.
- Upgrade from SLX 17r.1.01b to SLX-OS 17r.2.01a or later is supported via firmware download CLI with “fullinstall” option.
- USB based FWD upgrade from SLX-OS 17r.1.01a (32-bit) to SLX-OS 17r.2.01 (64-bit) or later is supported with “fullinstall” option.
- USB3.0 used for firmware download can be in VFAT or EXT4 format.

Instruction to check and upgrade FPGAs/CPLDs:

Refer to the *SLX-OS Upgrade Guide* for all variations on upgrading SLX-OS.

FPGA/CPLD versions:

SLX-9850	Release Date
MM sys FPGA	08/25/2016
LC sys FPGA	08/30/2016
SFM sys FPGA	08/04/2016
SLX-9540	Release Date
Sys FPGA	02/09/2017
CPLD 0	02/09/2017
CPLD 1	02/09/2017

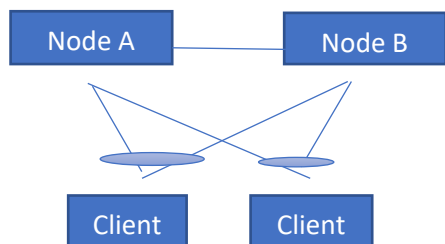
MCT Upgrade Process

This section describes the process to upgrade MCT cluster nodes with minimum traffic loss disruption.

The MCT upgrade process is divided into the following sections:

1. MCT upgrade process from SLX-OS 17r.1.01x to SLX-OS 18r.1.00d (32-bit OS to 64-bit OS)
2. MCT upgrade process from SLX-OS 18r.1.00 to SLX-OS 18r.1.00d (64-bit OS to 64-bit OS)

The steps in the MCT upgrade process use the following nomenclature for MCT nodes: Node A and Node B.



MCT upgrade process from SLX-OS 17r.1.01x to SLX-OS 18r.1.00d:

This section describes the procedure to upgrade MCT cluster nodes from SLX-OS 17r.1.01x to SLX-OS 18r.1.00d and later releases with minimal traffic loss disruption.

This is a 32-bit OS to 64-bit OS upgrade and hence uses the firmware download command with **fullinstall** option in order to perform the upgrade.

1. Configure client isolation mode under the cluster to be loose on Node A and on Node B respectively using the `client-isolation loose` command. For example:
Device(config)# cluster <Name of the cluster> <cluster-id> Device(config-cluster-1)# client-isolation loose
2. Isolate Node A from the network using the following steps:
 - a. Disable the MCT client-interfaces on Node A using `client-interfaces-shutdown` command under cluster configuration section.
Device-A(config-cluster-1)# client-interfaces-shutdown
 - b. Disable the link connected to MCT peer node and uplink to the core network.
This would result in all CCEP traffic to switch to Node B within 30 seconds depending on scale and other parameters.
3. Copy running-configuration to startup-configuration on node A.
4. Upgrade Node A to the 18r.1.00d release using the **firmware download fullinstall** command. While the upgrade on node A is in progress, the traffic would continue to pass through node B.
5. Verify that once the node comes UP, the member-vlan configuration under the cluster section is removed.
6. Create an evpn template and add to the existing configuration on Node A. For example:

```
Device(config)# evpn <evpn-instance-name> route-target both auto ignore-asrd auto  
vlan add <NUMBER: 1-4090> (If VLAN config is present) bridge-domain add <NUMBER: 1-4090> (If L2VPN config is present)
```

7. Isolate Node B from the network using the following steps. Please note that there is complete traffic loss at this step.

- a. Disable the MCT clients from the Node B using **client-interfaces-shutdown** command under cluster configuration section.

```
Device-B(config-cluster-1)# client-interfaces-shutdown
```

- b. Disable the link connected to MCT peer node and uplink to the core.

Note: This step is suggested at this stage to avoid traffic duplication if L2VPN configuration is present. If L2VPN config is not present, enter the **no client-interfaces-shutdown** command on Node A before isolating Node B to minimize traffic loss. (Swap Step 7 and 9)

8. Copy running-configuration to startup-configuration on Node B.
9. Enable the interface towards the peer MCT node (ICL interface) and the uplink to the core network on Node A. (The ICL link would still be down since Node-B is isolated before this step. This is performed so that after Node B gets upgraded, the ICL link will come up once no shut is performed on the ICL link on Node-B.)
10. Bring Node A back to the network by entering the **no client-interfaces-shutdown** command under cluster configuration.

```
Device-A(config-cluster-1)# no client-interfaces-shutdown
```

This would result in all CCEP traffic to switch to Node A within 30 seconds depending on scale and other parameters.

11. Upgrade Node B to the 18r.1.00d release using the **firmware download fullinstall** command. While the upgrade on node B is in progress, the traffic would continue to pass through node A.
12. Verify that once the Node B comes UP, the member-vlan configuration under the cluster section is removed.
13. Create an evpn template and add to the existing configuration on Node B. For example:

```
Device-B(config)# evpn <evpn-instance-name> route-target both auto ignore-as  
rd auto
```

```
vlan add <NUMBER: 1-4090> (If VLAN config is present) bridge-domain add <NUMBER: 1-  
4090> (If L2VPN config is present)
```

14. Enable the interface towards the peer MCT node (ICL) and the uplink to the core network on Node B.
15. Verify if the BGP session between the MCT peers is established and the cluster is up.
16. Bring Node B back to the network by entering the **no client-interfaces-shutdown** command under cluster configuration.

```
Device-B(config-cluster-1)# no client-interfaces-shutdown
```

17. Copy running-config to startup-config on both the nodes.

Additional upgrade considerations for upgrading SLX9850 from 17r.1.01a or 17r.1.01b to 18r.1.00d

When upgrading a SLX9850 from 17r.1.01a or 17r.1.01b to 18r.1.00d, if TPVM is installed in the system, you must un-install it by running the “`tpvm uninstall`” command before starting firmware download. Otherwise, it will cause system initialization issue. After the system is upgraded, you can install the TPVM image from 18r.1.00 by running the “`tpvm install`” command.

MCT upgrade process from SLX-OS 18r.1.00 to SLX-OS 18r.1.00d:

This section describes the procedure to upgrade MCT cluster nodes from SLX-OS 18r.1.00 or 18r.1.00ax patch or 18r.1.00b patch to SLX-OS 18r.1.00d patch and later releases with minimal traffic loss disruption.

This is a 64-bit OS to 64-bit OS upgrade and hence uses the firmware download command with **coldboot** option to perform the upgrade.

1. Configure client isolation mode under the cluster to be loose on Node A and Node B respectively using the client-isolation loose command. For example:

```
Device(config)# cluster <Name of the cluster> <cluster-id>
```

```
Device(config-cluster-1)# client-isolation loose
```

2. Isolate Node A from the network using the following steps:

- a. Disable the MCT client-interfaces on Node A using **client-interfaces-shutdown** command under cluster configuration section.

```
Device-A(config-cluster-1)# client-interfaces-shutdown
```

- b. Interface connected to MCT peer node (ICL interface) must be left in **no shut** state.
- c. Disable uplink to the core network.

This causes all CCEP traffic to switch to Node B within 30 seconds depending on the scale and other parameters.

3. Copy running-config to startup-config on node A.
4. Upgrade Node A using **firmware download** command with **coldboot** option to the 18r.1.00c image. While the upgrade on node A is in progress, the traffic would continue to pass through node B.
5. Verify if Node A is back online after the upgrade and has completed initialization.
6. Isolate Node B from the network using the following steps.

Note: There is complete traffic loss at this step.

- a. Disable the MCT client-interfaces on Node B using **client-interfaces-shutdown** command under cluster configuration section.

```
Device-B(config-cluster-1)# client-interfaces-shutdown
```

- b. Interface connected to MCT peer node (ICL interface) must be left in **no shut** state.
- c. Disable uplink to the core network.

Note: This step is suggested at this stage in order to avoid traffic duplication if L2VPN configuration is present. If L2VPN configuration is not present, perform **no client- interfaces-shutdown** on Node A before isolating Node B in order to minimize traffic loss. (Swap Step-6 and Step-9)

7. Copy running-configuration to startup-configuration on Node B.
8. Enable the uplink to the core network on Node A. (The ICL interface would be up by now since we did

not shut it prior to upgrade.)

9. Bring Node A back to the network by configuring the **no client-interfaces-shutdown** command under cluster configuration on Node A. This would result in all CCEP traffic to switch to Node A within 30 seconds depending on the scale and other parameters.

```
Device-A(config-cluster-1)# no client-interfaces-shutdown
```

10. Upgrade Node B to 18r.1.00d release using the **firmware download** command with **coldboot** option. While the upgrade on node B is in progress, the traffic would continue to pass through node A.
11. Verify that once the Node B comes UP, the uplink to the CORE network on Node B is configured to come up.
12. Verify if BGP session between MCT peers is established and the cluster is up.
13. Bring Node B back to the network by bringing the client-interfaces UP using the following command under cluster configuration.

```
Device-B(config-cluster-1)# no client-interfaces-shutdown
```
14. Copy running-config to startup-config on both the nodes.

Limitations and restrictions

- Raslog and ACL buffered logging as denied packet observed for ACL permit rules when ACL applied or removed for interface.
- QoS flowcontrol tx **on** is not recommended.
- Restricted mac learning observed on remote node with PMS applied for ingress traffic.
- Conform byte size is more than packet byte size in egress RL counters.
- In lag-profile-1, the maximum number of class-maps supported on port-channel is 64 class-maps.
- When a user egress ACL rule is configured with a VLAN keyword, 100% traffic drop is observed.
- Users will notice LACP port-channel flap while doing shutdown/no shutdown on the port channel. This flapping will occur a few times (between 2-8 times). Only those port-channels with LACP short timer will experience this behavior. Port channel with LACP long timer configuration (the default configuration) will not see extra flaps. This is due to the HW programming. We recommend using default timer (LACP long).
- Traffic drop will be seen on bridge domains when configuring and removing service policy under the port-channel. This issue occurs when the system is configured with 60 plus service policies and with 4 or more members in the port-channel. Traffic will automatically recover and becomes stable after 1-1.5 minutes.
- Egress BUM rate limiting is not supported.
- Ingress BUM rate limiting cannot be applied on port channels.
- The qos flowcontrol command on service-policy enabled interface is not supported.
- QoS rx flowcontrol is disabled by default.
- The policer receive rate improves with larger packet sizes (for example, larger than 1500 bytes for rate-limit values).
- VLAN match based RL supported only for L2 VLANs (No VPLS). BD RL to be used instead.
- Rate limit counters (conform/violate) are not supported for BD based ingress Rate limiting.
- Statistics (for example, counters) are not supported for Port, BUM, VLAN, BD rate-limiting in COUNTERS-PROFILE-5 profile due to hardware limitation. The shutdown/monitor operations are performed using counters that are impacted and may not work as expected.
- Under certain circumstances, counters for BUM storm control may not be accurate, resulting in the following:
 - With the monitor command, a log message may not reflect data accurately.
 - With the shutdown command, the "exceeded" rate limit may be inaccurate.
- With *layer2-ratelimit* tcam profile, the **lag-profile-1** LAG profile supports a maximum of 256 LAGs and Default LAG profile supports 128 LAGs. In the example below, when the **interface port-channel** command is configured with a value greater than 256, the following error message is displayed:

```
(config)# interface Port-channel 307
%%Error: PO ID greater than 256 is not allowed in profile tcam
Layer2-ratelimit with lag-profile-1 LAG profile
```

The default LAG profile supports 64 members on a LAG. The lag-profile-1 option under the **profile lag** command only supports 32 members on a LAG.
- When Ingress ACL RL and BUM RL are applied on same interface and if traffic hits both ingress ACL RL and BUM RL, then ACL RL will take place.

Egress ACL-based Rate Limiting:

- Support in *layer2-ratelimit* TCAM profile only.
- Support CE ports only (that is, not support for MPLS uplinks).

- Broadcast, multicast and unknown unicast packets not supported.
- Added EACL stats polling optimization in the slxos-18r.1.00ce.
As part of this optimization, user has to issue the show command `show policy-map` more frequently (greater than 3 time within a minute) to get fast stats update.
Earlier releases stats update took 400sec for fusion and 80 sec for avalanche, with current fix, this stats display delay has reduced to less than 180 sec for fusion and less than 20sec for avalanche. In order to make this optimization work, user has to run `Show policy-map` command more frequently (greater than 3 times within a min).

Limitations for Layer-2 Rate-limiting Tcam Profile :

- Sflow sampling is not supported on MPLS interfaces
- IPV6 ACL is not supported
- MPLS LAG hashing is not supported
- Vlan pcp and DSCP match is not supported in ACLs
- Statistics for BUM rate limiting, Port rate limiting, Vlan rate limiting, and BD rate limiting is not supported.

Limitation for Layer-2 Optimized Tcam Profile :

- Sflow sampling is not supported on MPLS interfaces

Additional Limitations

- If multiple VLANs on the same ingress port belong to the same BD, and the egress ACL rate limiting is configured to rate limit one of the VLANs, all VLAN traffic is rate limited. A workaround is to add matching source or destination MAC address along with the VLAN in the ACL.
- When Ingress ACL and Ingress ACL RL are applied on same interface, If traffic matches both ingress ACL and Ingress ACL RL, then Ingress ACL will apply.
- For Egress RL, the packet header is stripped out or added at egress PP block where the packet already passed rate limiting block. So, in the case if incoming packet header and outgoing packet header are not the same, the rate seen at the port are different from the configured rate.
- For Egress Rate-limiting, the configuration command `no switchport trunk tag native-vlan` is not supported. Use the `switchport mode trunk-no-default-native` command instead.
- Per design, though the user binded the policy and egress bit the ACL is at ingress and therefore there is no display for egress ACL.
- The packet count for “`show policy-map interface <eth/po>`” is not supported. Byte count can be used instead.
- Egress ACL RL with policer value "0" is not supported. Minimum supported policer value is 400kbps.
- ACL-based, storm-control, and port-based rate limiting can coexist on the same interface. ACL-based rate limiting has the highest priority, followed by storm-control rate limiting, and then port-based rate limiting.
- **Symptom:** Traffic loss seen after line card (LC) reload on 9850 when egress ACL RL is configured
Conditions: in 9850 chassis with at least two line cards, reload of line card can potentially cause traffic drop if egress ACL RL is applied to multiple interfaces with at least one port channel (PO). When LC is reloaded, system replays all eRL policies to that line card internal programming sequentially and exits in case of PO. Depending on the bounding sequence of eRL, reload of LC can potentially cause traffic drop.
Workaround:
Remove and add back egress ACL RL

CLI configuration design considerations for Rate limiting:

SLX 9850 (4 slots)

- 156 class maps per tower if bind to interface (VOQ limitation).
- 2k class maps per system (Supported hardware entry).
- 128 class maps for port-channel in default LAG profile, 128 LAG total (LAG hardware entry).
- 256 class map for port-channel in profile-1 LAG profile, 256 LAG total (LAG hardware entry).
- 1k policy maps per system (Software scaling).
- 32K class-maps per system (Software scaling).

Note: For SLX 9850 (8 slots), the VOQ limitation per tower is cut in half.

SLX 9540

- 64 class maps for port-channel in default LAG profile, 128 LAG total. (Support hardware entry).
- 128 class maps for port-channel in LAG profile-1, 128 LAG total. (Support hardware entry).
- 2k class maps per tower or system (Supported hardware entry).
- 1k policy maps per system (Software scaling).
- 32K class-maps per system (Software scaling).

QOS resource can be running out in following cases:

1. Out of resource when user bind the policy to a port or channel, in this case SW shall fail the command with error message.
2. Out of resource when user add new class to existing policy. SW shall fail the command to add new class with error message.
3. Out of resource when user add a new port to a LAG. In this case SW can't fail the command due to design limitation. Instead, it will send raslog to inform the user (the user need to check raslog and remove the config if resource running out).

sFlow

sFlow packet samples that are collected are inaccurate based on probability and low rate-limit.

With *layer2-ratelimit* or *layer2-optimised-1* tcam profile , Sflow over mpls interfaces are not supported in the version earlier than 20.1.1.

L2 ACL: Unintentional traffic leaking can occur in a short period time (within 10 ms) during the adding of an L2 and L3 ACL.

Cos to TC mapping

- “qos map cos-traffic-class cosTC” command has known issue in this release and not taking effect for port channel.

VPLS VC

- In certain situations, VC peer flaps can happen in the VPLS network due to excessive amount of multicast traffic. To protect the control plane protocols, the following configuration is recommended on all ingress interfaces.

- Apply BUM rate limit per interface

```
storm-control ingress broadcast limit-bps <rate in bps> storm-control ingress
multicast limit-bps <rate in bps>
```

```
storm-control ingress unknown-unicast limit-bps <rate in bps>
```

Rate limit values should be calculated based on amount of multicast traffic expected on the interface. Unknown-unicast should be as low as possible.

- Apply MCAST rate limit per forwarding ASIC

```
qos rx-queue multicast best-effort-rate <rate in kbps>
```

Command must be configured on one interface per ASIC. Actual rate depends of amount of expected MCAST traffic per forwarding ASIC.

BFD:

- Sessions with less than 300ms timer may flap in scale conditions
- Known issues with BFD when BFD is configured over multi-slot LAG, or multi-hop session over ECMP paths

L3VPN:

- Known issues with Peer-group, RR-group and Prefix-list ORF

FRR facility backup:

- VPLS/VLL Bypass traffic will not work when router/untagged VE interfaces configured as MPLS uplink ports

MCT

- L3 cases are not supported when ICL interface is configured as router/untagged VE. It is required for all MPLS uplinks to be tagged interfaces to use FRR bypass for VLL/VPLS/L3VPN applications.

Routing over VPLS

- pw-profile must be configured with tagged mode only under the bridge-domain instance for routing with VPLS.
- It is required for all MPLS uplinks to be tagged VE interfaces to support VEOVPLS.

Internet Routes Scaling

- It is recommended that the internet routes scaling features be enabled with internet peering configurations, as qualified by Extreme
- Feature is supported with default VRF only; default VRF and non-default VRF should not be co-existing when default VRF is configured with Internet routes scaling feature

L3VPN jumbo limitation

- The IPMTU value configured in CLI is applicable, if outgoing routing interface is an undelay IP interface (VE or L3 port); the IPMTU value configured in CLI is not applicable if the outgoing interface is uplink for IPoMPLS, L3VPN traffic, or ICL for MCT peers. Jumbo frames over MPLS/L3VPN tunnels can be accepted based the port L2MTU values.

EVPN IP Fabric

- IPv6 Static Anycast Gateway is not supported.

Storm-control

- The counter for Broadcast and Multicast storm-control are not supported in layer2-optimized-1 profile.

Increase scale support for class-maps under the service policy

- The ACL/VLAN/BD Rate Limiting scale numbers are dependent on tcam profile configured. Basically, based on the tcam entries reserved for the feature, user can scale number of policers/stats for appropriate application.

Consider below example with tcam profile "layer2-optimised-1".

- Create 2K Vlan/BD based class-maps and 2K ACL based class-maps associate those with policy-map pmap1.
- Configure 1k distinct policer attributes (cir/cbs/eir/ebs) for all the policy- map/class-map combination and bind the policy-map pmap1 to any interface.
- Now overall there will be 4K policers active for that interface with 4k distinct class-maps (match criteria).
- Note: The 4K policers (class-maps) scale will not be applicable to port-channel. There are only 1,215 policers are reserved for port-channels.
- Based on the requirement user must set the tcam profile and must reboot the box for activating the same.

MPLS XC Scale increase 64K

- 32k XC supported for FRR and 64k supported for non-FRR

Import TLS Server Certificate and Private key without any Trust Point

- TLS certificate will be deleted when perform full-install upgrade

Dynamic Route Leaking Behavior

Decision to leak is made at the time of route install by checking route policy that are configured. This is why the routes that are installed prior to configuring the import route-map are not leaked.

For this feature to be effective in SLX,

1. Configure the route-map command `ip import routes <vrf> route-map <>` first and then configure the static routes to be imported.
2. Do a `clear ip route` on the source once the route-map is applied.

Source interface support for Tacacs server

- *Chassis IP* is not supported as a *source-interface*.

Disable Default rule for RACL

- Only default Tcam profile is supported for RACL

Defects

Defects closed in 18r.1.00m

This section lists software defects with Critical, High, and Medium Technical Severity closed with code changes as on May 2022 in 18r.1.00m

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-65427	Issue ID:	SLXOS-65427
Severity:	S2 – Major		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00j
Technology Group:	VPLS/VLL/PWM	Technology:	VPLS Data Path-LP
Symptom:	When we have VPLS configured with flow label on SLX9850 with two management cards, and the active card goes to switchover with standby there is traffic interruption for approximately for 20sec to recover.		
Condition:	We have VPLS configured with flow label on SLX9850 with two management cards. With this configuration when active card goes to switchover with standby and the configurations are synced along with flow label, UP notification was missed and hence the traffic interruption for approximately for 20sec to recover.		
Recovery	If no flow label configurations, the problem won't be seen when switchover happens.		

Parent Defect ID:	SLXOS-64255	Issue ID:	SLXOS-64255
Severity:	S3 – Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00j
Technology Group:	Management	Technology:	CLI - Command Line Interface
Symptom:	ARP not resolved for the peer entry		
Condition:	When link fault is cleared.		

Parent Defect ID:	SLXOS-61254	Issue ID:	SLXOS-61254
Severity:	S3 – Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ca
Technology Group:	MPLS	Technology:	LDP - Label Distribution Protocol
Symptom:	Duplicate LDP Address Withdraw Message sent from LDP for each VC-Peer.		
Condition:	Issue is seen when we do "clear mac-address" under a bridge domain.		

Parent Defect ID:	SLXOS-61035	Issue ID:	SLXOS-61035
Severity:	S4 – Minor		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00e

Technology Group:	MPLS	Technology:	LDP - Label Distribution Protocol
Symptom:	Target LDP session crashes when VPLS address withdraw message is received during interop testing		
Condition:	This issue is encountered when address withdraw message with empty TLV is received from other vendor		
Recovery	When empty TLV message is received instead of processing it system will ignore.		

Defects closed in 18r.1.00k

This section lists software defects with Critical, High, and Medium Technical Severity closed with code changes as of February 2022 in 18r.1.00k

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-46618	Issue ID:	SLXOS-46622
Severity:	S3 – Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ce
Technology Group:	Traffic Management	Technology:	Traffic Queueing and Scheduling
Symptom:	Traffic loss observed.		
Condition:	When unicast traffic with less than 256 bytes, flows from 100G interface to 10G interface.		

Parent Defect ID:	SLXOS-48171	Issue ID:	SLXOS-48172
Severity:	S3 – Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00b
Technology Group:	Layer 3 Routing/Network Layer	Technology:	ARP - Address Resolution Protocol
Symptom:	ARP age out is not working as expected.		
Condition:	When "ip dhcp relay address" is configured.		

Parent Defect ID:	SLXOS-48938	Issue ID:	SLXOS-48939
Severity:	S2 – Major		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00b
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Routes showing incorrect next-hop		
Condition:	After changing OSPF costs		

Parent Defect ID:	SLXOS-50653	Issue ID:	SLXOS-50660
--------------------------	-------------	------------------	-------------

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

Parent Defect ID:	SLXOS-51764	Issue ID:	SLXOS-52414
Severity:	S3 – Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00bc
Technology Group:	Layer 2 Switching	Technology:	LAG - Link Aggregation Group
Symptom:	Port-channel flaps were seen on customer network		
Condition:	Port-channel configured uplink-interfaces on one side and other side there is no LACP enabled interface (earlier it is part of Port-channel), non-enabled interfaces are started allowing the LACP PDU's.		

Parent Defect ID:	SLXOS-52561	Issue ID:	SLXOS-54880
Severity:	S3 – Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00cg
Technology Group:	Other	Technology:	Other
Symptom:	SLX9540 stopped responding		
Condition:	HW failure		

Parent Defect ID:	SLXOS-55203	Issue ID:	SLXOS-55218
Severity:	S2 – Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2d
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	"show ip bgp neighbors <ip_address> advertised-routes" displays additional AS number along with local AS number. This is a non-functional issue.		
Condition:	If "neighbor <ip> remove-private-as" is configured under "SLX(config-bgp-router)#" Ex: SLX(config-bgp-router)# neighbor 10.1.1.1 remove-private-as		

Parent Defect ID:	SLXOS-57023	Issue ID:	SLXOS-57503
Severity:	S2 – Major		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00g
Technology Group:	MPLS	Technology:	MPLS VPLS - Virtual Private LAN Services
Symptom:	May notice VC peers moves to DOWN by itself.		
Condition:	Issue may be seen when a SLX device is connected to Cisco nexus device.		

Parent Defect ID:	SLXOS-56743	Issue ID:	SLXOS-56913
Severity:	S3 – Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.2b
Technology Group:	Management	Technology:	SNMP - Simple Network Management Protocol
Symptom:	SNMP dot1qTpFdbPort is showing as "0" on a dynamically learnt mac address. instead of the port number.		
Condition:	SNMP walk to OID dot1qTpFdbPort		

Parent Defect ID:	SLXOS-57276	Issue ID:	SLXOS-57812
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00b
Technology Group:	Monitoring	Technology:	sFlow
Symptom:	In sflow sample outgoing interface will be reported as - 1[4294967295]		
Condition:	Unknown VPLS traffic is sflow sampled on VPLS endpoint		

Parent Defect ID:	SLXOS-55311	Issue ID:	SLXOS-58706
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2c
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	No Functional impact.bgp_nexthop_delete_as_path_entry print messages are seen when terminal monitor is enabled		
Condition:	Received continuous LL nexthop prefixes from peer		

Parent Defect ID:	SLXOS-55553	Issue ID:	SLXOS-58714
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00ca
Technology Group:	MPLS	Technology:	LDP - Label Distribution Protocol
Symptom:	On SLX 9640 and SLX 9540, LDP Protocol packets will be trapped to CPU in the transient router.		
Condition:	LDP Protocol packets will be trapped to CPU in transient router even though they are not destined to the device's IP address.		

Parent Defect ID:	SLXOS-58443	Issue ID:	SLXOS-58728
Severity:	S2 – Major		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ga
Technology Group:	MPLS	Technology:	MPLS VPLS - Virtual Private LAN Services

Symptom:	LSP state is down when 'show mpls lsp' executed in new Active
Condition:	When ha failover is triggered in old Active
Workaround:	"clear mpls lsp name <>" brings the lsp to UP state

Parent Defect ID:	SLXOS-55587	Issue ID:	SLXOS-58746
Severity:	S2 – Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2e
Technology Group:	Management	Technology:	Other
Symptom:	Unexpected reload		
Condition:	Rare scenario . When the CLI stuck for long time.		

Parent Defect ID:	SLXOS-59458	Issue ID:	SLXOS-59524
Severity:	S3 – Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.1
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4+ - IPv6 Border Gateway Protocol
Symptom:	BGPd reload while executing show command		
Condition:	In scaled environment, while executing "show ip[v6] bgp neighbors all-vrfs", BGPd reload was seen.		

Parent Defect ID:	SLXOS-60296	Issue ID:	SLXOS-60296
Severity:	S3 – Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00h
Technology Group:	Layer 2 Switching	Technology:	Other
Symptom:	Crash is observed in eld daemon		
Condition:	When the port-channel interface is shut and no shut		

Parent Defect ID:	SLXOS-58858	Issue ID:	SLXOS-60434
Severity:	S3 – Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3b
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	VxLAN tunnels do not come up after continuous reboots.		
Condition:	After 500 reboots of SLXOS, BGP/EVPN VxLAN tunnel did not come up.		

Parent Defect ID:	SLXOS-60392	Issue ID:	SLXOS-60545
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.3.2
Technology Group:	Layer 3 Routing/Network Layer	Technology:	ARP - Address Resolution Protocol
Symptom:	In SLX 9250 BFD Sessions gets stuck in INIT state.		

Condition:	Reloading of BFD configured neighbor device and it comes up with different mac-address.
-------------------	---

Parent Defect ID:	SLXOS-60590	Issue ID:	SLXOS-60594
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3f
Technology Group:	Layer 3 Routing/Network Layer	Technology:	Static Routing (IPv4)
Symptom:	Layer 3 traffic will get dropped as ARP entries are missing from the hardware routing table.		
Condition:	During border leaf reload scenario, routing table manager data may go to a invalid state, which results in ARP resolution to be ignored.		

Parent Defect ID:	SLXOS-60674	Issue ID:	SLXOS-60674
Severity:	S3 – Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ca
Technology Group:	MPLS	Technology:	IP over MPLS
Symptom:	Primary LSP path is not UP and Active		
Condition:	Configured Strict LSP path is getting programmed with reverse/not-specified order		

Parent Defect ID:	SLXOS-60840	Issue ID:	SLXOS-60840
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00gb
Technology Group:	Management	Technology:	High Availability
Symptom:	MM may experiences Kernel panic.		
Condition:	It can be simulated sometime during re-insertion of MM into chassis.		

Parent Defect ID:	SLXOS-60868	Issue ID:	SLXOS-60997
Severity:	S2 - Major		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2h
Technology Group:	Layer 3 Routing/Network Layer	Technology:	OSPFv3 - IPv6 Open Shortest Path First
Symptom:	IPv6 OSPF session does not come up when IP Sec option is used.		
Condition:	OSPFv3 authentication with IPSEC and LSA is larger than interface MTU.		

Parent Defect ID:	SLXOS-61193	Issue ID:	SLXOS-61193
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ca
Technology Group:	Layer 2 Switching	Technology:	Other
Symptom:	After specific MAC cleared, MAC withdraw message is not triggered		
Condition:	MAC table should have the valid MAC entries.		

	Perform the cli command "clear mac-address-table dynamic address <mac>"
--	---

Parent Defect ID:	SLXOS-60721	Issue ID:	SLXOS-61358
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3d
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Unable to assign a BGP update source interface with a /31 IP address		
Condition:	This issue is observed only for the update-source IP which ends with 255 (example: 10.145.199.255)		

Parent Defect ID:	SLXOS-61382	Issue ID:	SLXOS-61382
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00gb
Technology Group:	Management	Technology:	High Availability
Symptom:	Few CLI commands may stuck with no response.		
Condition:	Repeated removal and re-insertion of management module.		

Parent Defect ID:	SLXOS-62135	Issue ID:	SLXOS-62135
Severity:	S3 - Moderate		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00b
Technology Group:	Monitoring	Technology:	RAS - Reliability, Availability, and Serviceability
Symptom:	Logs indicating flash size usage crossing high boundary		
Condition:	/var/log/hasm.log file size is large, with no impact on functionality		

Parent Defect ID:	SLXOS-62447	Issue ID:	SLXOS-62447
Severity:	S2 – Major		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00j
Technology Group:	MPLS	Technology:	LDP - Label Distribution Protocol
Symptom:	Flow Label sync is not done after HA failover in SLX 9850		
Condition:	HA is not supported in 20.x release.		

Parent Defect ID:	SLXOS-62528	Issue ID:	SLXOS-62528
Severity:	S2 – Major		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00h
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGPd module reset is observed which triggers MM failover.		
Condition:	BGPd module reset happens when received AS path entry is added		

	into routing table.
--	---------------------

Defects closed in 18r.1.00j

This section lists software defects with Critical, High, and Medium Technical Severity closed with code changes as of August 2021 in 18r.1.00j

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-49674	Issue ID:	SLXOS-49675
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00b
Technology Group:	Security	Technology:	ACLs - Access Control Lists
Symptom:	Invalid warning logs come on the console " Key type(Destination Port) is not supported".		
Condition:	While applying the Ipv4 access-list on VE interfaces, we are seeing the [SSMD-1440] warning message.		

Parent Defect ID:	SLXOS-49787	Issue ID:	SLXOS-49788
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00bc
Technology Group:	Layer 3 Routing/Network Layer	Technology:	MBGP - Multiprotocol Border Gateway Protocol
Symptom:	In certain error scenarios where BGP is flooded with erroneous attributes, user may observe BGP not learning/advertising routes from/to peers after significant amount of time under this condition.		
Condition:	Remote BGP peer advertising route updates with invalid next-hop attribute or invalid as-path attribute can cause this condition. This can be checked by running SLX-OS CLI command "show [ip ipv6] bgp neighbors routes-summary"		

Parent Defect ID:	SLXOS-51906	Issue ID:	SLXOS-52214
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00b
Technology Group:	Other	Technology:	Other
Symptom:	Unexpected reload		
Condition:	When we use the "ip prefix-list name" more than 32 character.		

Parent Defect ID:	SLXOS-52124	Issue ID:	SLXOS-52352
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00a
Technology Group:	Layer 3 Routing/Network Layer	Technology:	MBGP - Multiprotocol Border Gateway Protocol

Symptom:	In certain conditions SLX device would reload unexpectedly.
Condition:	BGP Static-network is configured locally and BGP also learns the same static-network prefix from one or more BGP peers.

Parent Defect ID:	SLXOS-53724	Issue ID:	SLXOS-54182
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00bc
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP route regex match is not working as expected		
Condition:	"show ipv6 & ipv4 bgp route reg<string>" is not giving the proper output when the CLI search string length exceeds the 15 characters.		

Parent Defect ID:	SLXOS-54306	Issue ID:	SLXOS-54361
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2c
Technology Group:	Layer 2 Switching	Technology:	QinQ - IEEE 802.1Q
Symptom:	End to end QinQ customer traffic loss seen when it passes through a VPLS tunnel.		
Condition:	Issue seen with following combination of configuration and traffic. In a bridge-domain, 1) Customer AC interface is configured as single tag 2) VC-Mode is set to tagged 3) Customer traffic is QinQ with outer vlan matched to the AC interface vlan tag		

Parent Defect ID:	SLXOS-54321	Issue ID:	SLXOS-54599
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ca
Technology Group:	Layer 2 Switching	Technology:	Other
Symptom:	Unexpected reload of Line card		
Condition:	Not specific from the user. It can happen due to corruption.		

Parent Defect ID:	SLXOS-54161	Issue ID:	SLXOS-54689
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2a
Technology Group:	Layer 3 Routing/Network Layer	Technology:	OSPF - IPv4 Open Shortest Path First
Symptom:	"show ip ospf database external-link-state link-state-id 0.0.0.0 vrf external-vrf" shows the default metric value (10) not the configured value.		
Condition:	Configure "default-information-originate metric <>" and advertise the default route.		

Parent Defect ID:	SLXOS-52211	Issue ID:	SLXOS-54792
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00bc
Technology Group:	Other	Technology:	Other
Symptom:	Unexpected reload.		
Condition:	When we create max. supported VRF(i.e.,1024) and perform some operations on last VRF(i.e., delete/create multiple times). This is a corner scenario and rare to hit.		

Parent Defect ID:	SLXOS-53818	Issue ID:	SLXOS-54907
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00e
Technology Group:	Layer 2 Switching	Technology:	MCT - Multi-Chassis Trunking
Symptom:	Ping fails when it comes from CCEP client and passing through MCT cluster.		
Condition:	When static VLANs configured locally and also learned through MVRP		

Parent Defect ID:	SLXOS-54078	Issue ID:	SLXOS-54952
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ca
Technology Group:	Layer 2 Switching	Technology:	Other
Symptom:	Unable to learn VPLS MAC address on the MPLS uplink		
Condition:	MLX & SLX are PEs and peer's to each other. MLX has VPLS config and SLX has bridge-domain config.		

Parent Defect ID:	SLXOS-55058	Issue ID:	SLXOS-55157
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.1a
Technology Group:	Monitoring	Technology:	Hardware Monitoring
Symptom:	10G SR SFP+ gives warning FW-1046 with 10G LR threshold values.		
Condition:	This will occur only on interfaces where already inserted 10G `LR'SFP+. are replaced with a 10G `SR' SFP+ and the link is up.		

Parent Defect ID:	SLXOS-55224	Issue ID:	SLXOS-55261
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2c
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Unexpected Reload.		
Condition:	BGP peers are configured without route-map. Making changes to the out route-map for one or more BGP peers.		

Parent Defect ID:	SLXOS-55051	Issue ID:	SLXOS-55286
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00c
Technology Group:	Monitoring	Technology:	sFlow
Symptom:	A number of fields such as Header Length, IP Size and Subnet Masks are reported incorrectly in the sflow samples		
Condition:	collecting sflow samples with a sflow collector		

Parent Defect ID:	SLXOS-55963	Issue ID:	SLXOS-56007
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2a
Technology Group:	Layer 3 Routing/Network Layer	Technology:	Multi-VRF
Symptom:	Inter VRF route leak doesn't work		
Condition:	Inter VRF route leak doesn't work if the used route-map uses 'match tag' as the match criteria.		

Parent Defect ID:	SLXOS-55949	Issue ID:	SLXOS-56028
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.2a
Technology Group:	Layer 2 Switching	Technology:	LAG - Link Aggregation Group
Symptom:	Connected LAG member dis-aggregates		
Condition:	Some LAG member of SLX gets dis-aggregated when one or more ports connected to Juniper switch and part of any LAG		

Parent Defect ID:	SLXOS-56043	Issue ID:	SLXOS-56118
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00f
Technology Group:	IP Multicast	Technology:	IGMP - Internet Group Management Protocol
Symptom:	Unexpected reload		
Condition:	When Layer 2 IGMP entries are aging out continuously.		

Parent Defect ID:	SLXOS-56062	Issue ID:	SLXOS-56274
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Layer 2 Switching	Technology:	VLAN - Virtual LAN
Symptom:	MAC address is missing in show mac table for few seconds		
Condition:	When MAC move between the Port channel interface and physical interface		

Parent Defect ID:	SLXOS-55862	Issue ID:	SLXOS-56294
--------------------------	-------------	------------------	-------------

Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00b
Technology Group:	Layer 3 Routing/Network Layer	Technology:	Other
Symptom:	SNMP walk output showing interface index of "null0" interface as 0		
Condition:	SNMP walk		

Parent Defect ID:	SLXOS-56418	Issue ID:	SLXOS-56504
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00e
Technology Group:	IP Multicast	Technology:	IGMP - Internet Group Management Protocol
Symptom:	May experience crash on execution of CLI command "show ip igmp interface port-channel" on mc_hsmc module.		
Condition:	IGMP snooping enabled on bridge domain where port-channel as logical interface.		

Parent Defect ID:	SLXOS-56657	Issue ID:	SLXOS-56786
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Layer 2 Switching	Technology:	VLAN - Virtual LAN
Symptom:	Mac address is not aged out in show mac.		
Condition:	When LC is powered down		

Parent Defect ID:	SLXOS-56949	Issue ID:	SLXOS-56985
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Management	Technology:	CLI - Command Line Interface
Symptom:	Unable to remove/configure-auto speed on 100G/40G interfaces.		
Condition:	Configure speed capability on 40G/100G interfaces.		

Parent Defect ID:	SLXOS-56732	Issue ID:	SLXOS-57044
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Traffic Management	Technology:	QoS - Quality of Service
Symptom:	Unicast flows stop completely with some traffic patterns under traffic congestion when multicast high priority traffic is sent with high rate along with Unicast traffic during over-subscription .		
Condition:	When multicast high priority traffic is sent with high rate along with Unicast traffic with over-subscription than Unicast traffic may get impacted.		

Parent Defect ID:	SLXOS-57176	Issue ID:	SLXOS-57206
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Layer 2 Switching	Technology:	LAG - Link Aggregation Group
Symptom:	No functional impact to the end user. There is mismatch in interface id at debug trace.		
Condition:	When the user dump the debug trace where he configured LACP. Not a customer use case.		

Parent Defect ID:	SLXOS-56962	Issue ID:	SLXOS-57523
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00bd
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	"show ip bgp summary" shows negative values for bytes counters.		
Condition:	In scaled BGP scenario, when traffic is send to all routes "show ip bgp summary".		

Parent Defect ID:	SLXOS-55076	Issue ID:	SLXOS-57550
Severity:	S1 - Critical		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00e
Technology Group:	MPLS	Technology:	MPLS VPLS - Virtual Private LAN Services
Symptom:	Unexpected reload of Line card		
Condition:	Can be observed in the presence of 180 RSVP signaled LSP with 511 cross-connect on VPLS service		

Parent Defect ID:	SLXOS-56996	Issue ID:	SLXOS-57635
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Network Automation and Orchestration	Technology:	YANG
Symptom:	Copy configuration to TFTP server with REST API commands hangs forever . All Subsequence copy command fails.		
Condition:	This issue happens when tftp server is not reachable OR is in off state		

Parent Defect ID:	SLXOS-57233	Issue ID:	SLXOS-57840
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00
Technology Group:	Layer 3 Routing/Network	Technology:	Other

	Layer		
Symptom:	Receive ACL (RACL) deny is working but its logging feature is not working		
Condition:	RACL deny packets are dropped but not logged in RASLOG		

Parent Defect ID:	SLXOS-58001	Issue ID:	SLXOS-58132
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.2e
Technology Group:	Layer 3 Routing/Network Layer	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Unexpected reload of SLX		
Condition:	When "show ip bgp neighbor" CLI is executed		

Parent Defect ID:	SLXOS-57970	Issue ID:	SLXOS-58347
Severity:	S4 - Low		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Management	Technology:	CLI - Command Line Interface
Symptom:	CLI "show mac-address-table dynamic bridge-domain <BD ID>" is not displaying mac address output		
Condition:	When we try to execute show command to fetch the specific BD ID details. Ex: "show mac-address-table dynamic bridge-domain <BD ID>" CLI in the noscli mode.		

Parent Defect ID:	SLXOS-58146	Issue ID:	SLXOS-58553
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Layer 2 Switching	Technology:	Other
Symptom:	Unexpected reload of Line card		
Condition:	Corner case .Due to slow Drain at message queue.		

Parent Defect ID:	SLXOS-58577	Issue ID:	SLXOS-58577
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00gb
Technology Group:	Layer 2 Switching	Technology:	LAG - Link Aggregation Group
Symptom:	Unexpected reload		
Condition:	When the MAX number of LAG ports data got corrupted.		

Parent Defect ID:	SLXOS-58580	Issue ID:	SLXOS-58580
Severity:	S3 – Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00j
Technology Group:	Other	Technology:	Other

Symptom:	TLS Certificates installed with trust point will get remove after upgrade
Condition:	After upgrading the device from 18r.1.00j to 20.1.2h & higher version through fullinstall

Parent Defect ID:	SLXOS-59987	Issue ID:	SLXOS-59995
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.2.3b
Technology Group:	Management	Technology:	Software Installation & Upgrade
Symptom:	Firmware download may fail.		
Condition:	If the hostkey is changed at the server side or the device connected to a new server (i.e upgrade/downgrade via new server)		

Parent Defect ID:	SLXOS-60246	Issue ID:	SLXOS-60246
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00h
Technology Group:	Layer 2 Switching	Technology:	LAG - Link Aggregation Group
Symptom:	Member ports are not able to remove from Port channel.		
Condition:	When we use the Insight interface(i.e., x/125,x/126) as member ports.This issue is specific to 9850(Fusion) Platform.		

Parent Defect ID:	SLXOS-60292	Issue ID:	SLXOS-60693
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00bd
Technology Group:	Layer 3 Routing/Network Layer	Technology:	Other
Symptom:	Unexpected reload.		
Condition:	In IP as-path access list config, when Regular expression token exceed the char limit config.		

Defects closed in 18r.1.00h

This section lists software defects with Critical, High, and Medium Technical Severity closed with code changes as of April 2021 in 18r.1.00h.

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-56443	Issue ID:	SLXOS-56496
Severity:	S1 – Critical		
Product:	Extreme SLX-OS	Technology Group:	MPLS
Reported in Release:	SLXOS 18r.1.00e	Technology:	MPLS VPLS - Virtual Private LAN Services

Symptom:	Unexpected restart of MPLSd with core file (without System reload)
Condition:	When peer interface is flapping carrying the LDP sessions.

Parent Defect ID:	SLXOS-54078	Issue ID:	SLX-54952
Severity:	S3 – Medium		
Product:	Extreme SLX-OS	Technology Group:	Layer 2 Switching
Reported in Release:	SLXOS 18r.1.00ca	Technology:	Other
Symptom:	Unable to learn VPLS MAC address on the MPLS uplink		
Condition:	MLX & SLX are PEs and peer's to each other. MLX has VPLS config and SLX has bridge-domain config		

Defects closed in 18r.1.00g

This section lists software defects with Critical, High, and Medium Technical Severity closed with code changes as of January 2021 in 18r.1.00g.

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-55370	Issue ID:	SLXOS-55681
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Security	Technology:	MACsec - Media Access Control security
Symptom:	Few MAC entries may get missed from software MAC table (L2Mgr) "show mac-address-table" after detection of mac move and not gets retrieved once after reception of traffic.		
Condition:	a) Port-security should be enabled on port. b) Send traffic with already learned mac (mac-move detection) and violate port-security mac count configured on port to make default action of port shut.		

Parent Defect ID:	SLXOS-55278	Issue ID:	SLXOS-55748
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Security	Technology:	RADIUS
Symptom:	SLX may ignore RADIUS server response for REST API authentication		
Condition:	1.Configure one or more radius servers with "aaa authentication login radius local-auth-fallback" 2.Send REST query to SLX from any linux device (SLX chooses lower source UDP port numbers, hence it ignores such responses)		

Parent Defect ID:	SLXOS-55742	Issue ID:	SLXOS-55914
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Layer 2 Switching	Technology:	Other
Symptom:	May notice MAC miss (address not learned) on "show mac-address-table" output once after receiving traffic with expected(missed) MAC.		
Condition:	a) Node should experience multiple mac-movements (between two interfaces). b) Introduce random manual shut in between mac-movement.		

Parent Defect ID:	SLXOS-55510	Issue ID:	SLXOS-56060
Severity:	S1 - Critical		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ca
Technology Group:	Management	Technology:	Software Installation & Upgrade
Symptom:	Unexpected reload		
Condition:	There is no specific operation to hit this case as it related to CPU kernel scheduling.		

Defects closed in 18r.1.00f

This section lists software defects with Critical, High, and Medium Technical Severity closed with code changes as of October 2020 in 18r.1.00f.

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-42283	Issue ID:	SLXOS-43665
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00a
Technology Group:	MPLS	Technology:	MPLS VPLS - Virtual Private LAN Services
Symptom:	MAC learning may not be happening after Management Module switchover		
Condition:	In the presence of 'spanning-tree shutdown' configuration applied on Bridge Domain interfaces		
Recovery:	Remove and re-apply the 'spanning-tree shutdown' configuration		

Parent Defect ID:	SLXOS-45991	Issue ID:	SLXOS-45992
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00a
Technology Group:	Layer 2 Switching	Technology:	xSTP - Spanning Tree Protocols
Symptom:	User will observe that STP BPDUs are getting flooded on VPLS Bridge domain like normal multicast traffic, even though user has enabled 'bpdu drop' feature using the CLI		
Condition:	'bpdu drop' configured on VPLS BD is not behaving as expected , where the BPDU should be dropped instead of flooding when 'bpdu drop ' is enabled on the VPLS bridge domain.		
Workaround:	None		

Parent Defect ID:	SLXOS-49410	Issue ID:	SLXOS-49411
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 17r.1.01aj
Technology Group:	Management	Technology:	High Availability
Symptom:	Standby Management may not reach Synchronized State		
Condition:	In the presence of 72x10G Line cards alone, on a SLX9850 8 slot chassis		
Workaround:	Shouldn't be observed if 36x100G is also present		

Parent Defect ID:	SLXOS-50077	Issue ID:	SLXOS-50078
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Security	Technology:	User Accounts & Passwords
Symptom:	System level commands are accessible by non-admin users		

Condition:	when we have non-admin users
-------------------	------------------------------

Parent Defect ID:	SLXOS-50419	Issue ID:	SLXOS-50420
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18x.1.00
Technology Group:	Management	Technology:	Other
Symptom:	Unexpected reload		
Condition:	It can happen when there is CPU intensive workload		

Parent Defect ID:	SLXOS-50340	Issue ID:	SLXOS-50588
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00d
Technology Group:	Layer 3 Routing/Network Layer	Technology:	IP Addressing
Symptom:	traceroute command may succeeds for disabled loopback IP address from peer		
Condition:	1) Configure /32 mask IP address for loopback interface. 2) Disable loopback interface using shut.		

Parent Defect ID:	SLXOS-50515	Issue ID:	SLXOS-50674
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.2.00a
Technology Group:	Layer 3 Routing/Network Layer	Technology:	IP Addressing
Symptom:	Notices duplicate IP address message on other Vendor device with SLX connected to it.		
Condition:	1) Back-to-back connection b/w SLX and other Vendor device 2) Configuration of IP address with mask /31 on other Vendor device followed by SLX.		

Parent Defect ID:	SLXOS-51201	Issue ID:	SLXOS-51365
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00d
Technology Group:	IP Multicast	Technology:	IPv4 Multicast Routing
Symptom:	SLX may unexpectedly reload in hslagtd daemon		
Condition:	Requires processing of the high scale of timed out (S,G) entries		

Parent Defect ID:	SLXOS-51474	Issue ID:	SLXOS-51477
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Layer 2 Switching	Technology:	VLAN - Virtual LAN
Symptom:	Packets may flood on the same port from where it is received		

Condition:	On reception of packet with ethertype of 0x88e7(PBB)
-------------------	--

Parent Defect ID:	SLXOS-51154	Issue ID:	SLXOS-51497
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00d
Technology Group:	Management	Technology:	SNMP - Simple Network Management Protocol
Symptom:	IP MTU configuration allows configuring sizes of interface MTU bounds		
Condition:	Configuring the IP MTU from SNMP		

Parent Defect ID:	SLXOS-50793	Issue ID:	SLXOS-52243
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ch
Technology Group:	Monitoring	Technology:	OAM - Operations, Admin & Maintenance
Symptom:	"show media" may display encoding string that doesn't comply with the IEEE standard for certain optics.		
Condition:	When 100G-LR4 QSFP28 optic has encoding value 5 Ex: show media interface ethernet x/y Encoding 5 IEEE 802.3ab		

Parent Defect ID:	SLXOS-50376	Issue ID:	SLXOS-52597
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ca
Technology Group:	Management	Technology:	Software Installation & Upgrade
Symptom:	Very rarely Management Module may fail to come up and enter into rolling reboot with Kernel Panic		
Condition:	Observed during module reset in the presence of CFM		

Parent Defect ID:	SLXOS-51831	Issue ID:	SLXOS-53563
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ca
Technology Group:	MPLS	Technology:	MPLS VPLS - Virtual Private LAN Services
Symptom:	SLX fails to learn VPLS MAC from remote PE		
Condition:	MPLS is configured with primary & bypass-path and can be observed with the flaps only in this following sequence (a) Flap on the primary path interface (b) Flap on the bypass-path interface		

	(c) Flap on the current primary path interface
--	--

Parent Defect ID:	SLXOS-50677	Issue ID:	SLXOS-53737
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00e
Technology Group:	Layer 3 Routing/Network Layer	Technology:	ARP - Address Resolution Protocol
Symptom:	Duplicate IP address SYSLOG message may be seen on the neighboring device console with no functional impact		
Condition:	When /31 subnet is configured on SLX to other Vendor devices as point-to-point links		

Parent Defect ID:	SLXOS-52104	Issue ID:	SLXOS-53873
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00e
Technology Group:	MPLS	Technology:	MPLS VPLS - Virtual Private LAN Services
Symptom:	Sometimes Line card may reload unexpectedly during the execution of support save		
Condition:	Can be observed in the presence of 180 RSVP signaled LSP with 511 cross-connect on VPLS service		

Parent Defect ID:	SLXOS-51453	Issue ID:	SLXOS-54229
Severity:	S3 - Medium		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Layer 3 Routing/Network Layer	Technology:	DHCP - Dynamic Host Configuration Protocol
Symptom:	Unexpected reload		
Condition:	DHCP malformed packet is received		

Parent Defect ID:	SLXOS-47656	Issue ID:	SLXOS-54270
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 20.1.1
Technology Group:	Layer 2 Switching	Technology:	VLAN - Virtual LAN
Symptom:	NETCONF configuration for bulk Bridge-domain LIF configuration will not succeed		
Condition:	By using NETCONF, user tries to configure multiple LIFs at once, in a single NETCONF request.		
Workaround:	None		

Defects closed in 18r.1.00e

This section lists software defects with Critical, High, and Medium Technical Severity closed with and without a code change as of May 2020 in 18r.1.00e.

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-38855	Issue ID:	SLXOS-42469
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 18r.1.00aa	Technology:	ICMP - Internet Control Message Protocol
Symptom:	Not able to ping the Broadcast address.		
Condition:	When pinging the broadcast address from both mgmt-vrf and default-vrf interfaces.		

Parent Defect ID:	SLXOS-25680	Issue ID:	SLXOS-42650
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Monitoring
Reported in Release:	SLXOS 17r.1.01b	Technology:	OAM - Operations, Admin & Maintenance
Symptom:	100g link with FEC enabled does not come back after a dwdm link switch over between lanes sometimes		
Condition:	Requiring a fast switchover using an equipment linking a DWDM or fast hand that removes / inserts the optic rapidly without damaging the cable / optic		
Workaround:	Shut/no-shut		

Parent Defect ID:	SLXOS-43173	Issue ID:	SLXOS-43715
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Monitoring
Reported in Release:	SLXOS 18r.2.00a	Technology:	Hardware Monitoring
Symptom:	"show media optical-monitoring" command is taking close to 1 minute to refresh the smart data values.		
Condition:	Observed after shutdown/no shutdown of physical interfaces.		

Parent Defect ID:	SLXOS-43371	Issue ID:	SLXOS-44088
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Monitoring
Reported in Release:	SLXOS 18r.1.00ca	Technology:	Sysmon
Symptom:	The output of "show system monitor" is not showing correct values sometimes with respect to the power supplies.		
Condition:	When the number of sensors in SLX9850-8 setup is more than 90		

Parent Defect ID:	SLXOS-44562	Issue ID:	SLXOS-44563
Severity:	S2 - High		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.1.00c	Technology:	CLI - Command Line Interface
Symptom:	High_free memory observed as OKB		

Condition:	In the output of “show process memory”		
Parent Defect ID:	SLXOS-42743	Issue ID:	SLXOS-45017
Severity:	S2 - High		
Product:	SLX-OS	Technology Group:	IP Multicast
Reported in Release:	SLXOS 18r.2.00	Technology:	PIM - Protocol-Independent Multicast
Symptom:	Unexpected MM reload		
Condition:	1. When Multicast (PIM) is enabled on multiple ports under single VLAN. 2. Any of the port receives the PIM(S,G) prune packet.		

Parent Defect ID:	SLXOS-45433	Issue ID:	SLXOS-45434
Severity:	S2 - High		
Product:	SLX-OS	Technology Group:	IP Multicast
Reported in Release:	SLXOS 18r.1.00c	Technology:	PIM - Protocol-Independent Multicast
Symptom:	Unexpected Management Module reload in mcagtd		
Condition:	1. Multicast (PIM) is enabled on multiple ports under same VLAN 2. Any of the port receives the PIM(S,G) prune packet		

Parent Defect ID:	SLXOS-45920	Issue ID:	SLXOS-45921
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.2.00a	Technology:	SNMP - Simple Network Management Protocol
Symptom:	Snmpwalk from a linux server works to the first hop router but not beyond		
Condition:	MPLS L3VPN configured on in-band custom Management VRF		

Parent Defect ID:	SLXOS-46308	Issue ID:	SLXOS-46312
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Monitoring
Reported in Release:	SLXOS 18r.2.00ac	Technology:	OAM - Operations, Admin & Maintenance
Symptom:	1G Copper SFP interface becomes link down after reload		
Condition:	When speed 100 is configured on 1G copper SFP and system reload is performed.		
Workaround:	Speed reconfiguration on the ports will recover the issue.		

Parent Defect ID:	SLXOS-46646	Issue ID:	SLXOS-46650
Severity:	S2 - High		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.2.00ac	Technology:	SNMP - Simple Network Management Protocol
Symptom:	Unexpected reload.		
Condition:	When SLX has MPLS tunnels configured and snmpbulkwalks are continuously run for ifTable/ifXTable.		

Parent Defect ID:	SLXOS-46770	Issue ID:	SLXOS-46774
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 17r.2.01	Technology:	Other
Symptom:	Unexpected reload with reason as Software Fault:Kernel Panic may be observed		
Condition:	It can happen with a long-running process where its low 32-bit of total process utime is '0' in do_div().		

Parent Defect ID:	SLXOS-46855	Issue ID:	SLXOS-46859
Severity:	S2 - High		
Product:	SLX-OS	Reported in Release:	SLXOS 18r.1.00ca
Technology Group:	Security	Technology:	ACLs - Access Control Lists
Symptom:	Unexpected reload.		
Condition:	When raslog logging is enabled globally and log keyword is used in ingress ACL rule		
Workaround:	Remove acl raslog command globally or do not use log keyword in any rule in ingress ACL policy		

Parent Defect ID:	SLXOS-47229	Issue ID:	SLXOS-47232
Severity:	S1 - Critical		
Product:	SLX-OS	Technology Group:	MPLS
Reported in Release:	SLXOS 18r.1.00c	Technology:	LDP - Label Distribution Protocol
Symptom:	Few MPLS Targeted LDP peers may stay in Non-existent state.		
Condition:	During multiple fiber flaps on LDP LSP's.		

Parent Defect ID:	SLXOS-47234	Issue ID:	SLXOS-47364
Severity:	S1 - Critical		
Product:	SLX-OS	Technology Group:	MPLS
Reported in Release:	SLXOS 18r.1.00d	Technology:	LDP - Label Distribution Protocol
Symptom:	Few MPLS Targeted LDP peers may stay in non-existent state.		
Condition:	1. Multiple fiber flaps observed on the Targeted-LDP LSP 2. With parallel programming enabled in the configuration		

Parent Defect ID:	SLXOS-47538	Issue ID:	SLXOS-47540
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 17r.1.01aj	Technology:	Other
Symptom:	REST runcmd operation fails with HTTP status code 406 or 502		
Condition:	Whenever upgrade and HA failover has been performed		

Parent Defect ID:	SLXOS-47629	Issue ID:	SLXOS-47631
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Monitoring
Reported in Release:	SLXOS 17r.1.01aj	Technology:	Syslog
Symptom:	RASLOG for optical temperature may display alarm even though the values are within boundary		

Condition:	During Port Up events
-------------------	-----------------------

Parent Defect ID:	SLXOS-47988	Issue ID:	SLXOS-47989
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.1.00ca	Technology:	Other
Symptom:	/fabos/libexec/ethmode may be missed on standby Management Module.		
Condition:	During /fabos/cliexec/ifmodeshow command run from active Management Module.		

Parent Defect ID:	SLXOS-48011	Issue ID:	SLXOS-48012
Severity:	S2 - High		
Product:	SLX-OS	Technology Group:	IP Multicast
Reported in Release:	SLXOS 18r.1.00db	Technology:	PIM - Protocol-Independent Multicast
Symptom:	Memory leak and unexpected reload may be observed in mcagtd daemon.		
Condition:	On continuous execution of 'clear ip pim mcache' with multicast data traffic passing through		

Parent Defect ID:	SLXOS-48040	Issue ID:	SLXOS-48040
Severity:	S1 - Critical		
Product:	SLX-OS	Technology Group:	MPLS
Reported in Release:	SLXOS 18r.1.00e	Technology:	LDP - Label Distribution Protocol
Symptom:	Few MPLS LDP peers may stay in LDP non-existent state		
Condition:	Occurs very rarely during multiple link flap events		

Parent Defect ID:	SLXOS-48075	Issue ID:	SLXOS-48076
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.1.00ch	Technology:	Software Installation & Upgrade
Symptom:	Very rarely Management Module may fail to come up and enter into rolling reboot with Kernel Panic		
Condition:	Observed during bring up of new Chassis		

Parent Defect ID:	SLXOS-37572	Issue ID:	SLXOS-48093
Severity:	S1 - Critical		
Product:	SLX-OS	Technology Group:	MPLS
Reported in Release:	SLXOS 18r.2.00	Technology:	IP over MPLS
Symptom:	After an MPLS RSVP LSP fails over to bypass, an MPLS ping initiated for the LSP causes unexpected reload of MPLS daemon		
Condition:	Issue will be seen only when the FRR failover happens for an RSVP LSP. Prior to failover, in protected path, MPLS ping works fine.		
Workaround:	No		

Parent Defect ID:	SLXOS-48501	Issue ID:	SLXOS-48502
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Security

Reported in Release:	SLXOS 17r.1.00a	Technology:	ACLs - Access Control Lists
Symptom:	May traffic gets permitted with hard-drop L2 ACL configured.		
Condition:	During configuration of log option in addition to hard-drop L2 ACL		

Parent Defect ID:	SLXOS-49209	Issue ID:	SLXOS-49210
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Monitoring
Reported in Release:	SLXOS 18r.1.00ch	Technology:	Hardware Monitoring
Symptom:	May observe following message in RASLOG for 1G SFP Optics like below:- "Optic inserted... is not compatible and laser is disabled"		
Condition:	Observed after Reload with speed configured as 1000		

Parent Defect ID:	SLXOS-49230	Issue ID:	SLXOS-49231
Severity:	S2 - High		
Product:	SLX-OS	Technology Group:	IP Multicast
Reported in Release:	SLXOS 18r.1.00db	Technology:	IGMP - Internet Group Management Protocol
Symptom:	Management Module may unexpectedly reload in NSM daemon		
Condition:	While processing high rate of IGMP join and leave messages		
Workaround:	None		

Parent Defect ID:	SLXOS-49149	Issue ID:	SLXOS-50007
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Security
Reported in Release:	SLXOS 20.1.2	Technology:	User Accounts & Passwords
Symptom:	Admin user can get the root privileges		
Condition:	when user try to use start-shell, python, OSCMD from admin login		

Defects closed in 18r.1.00d

This section lists software defects with Critical, High, and Medium Technical Severity closed with and without a code change as of October 2019 in 18r.1.00d.

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-39952	Issue ID:	SLXOS-39952
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.1.00c	Technology:	SNMP - Simple Network Management Protocol
Symptom:	SNMP config fails when it tries to map the community-map to context.		
Condition:	When used CLI "snmp-server mib community-map <map-name> context <context-name>"		

Parent Defect ID:	SLXOS-22414	Issue ID:	SLXOS-41496
Severity:	S2 - High		
Product:	SLX-OS	Technology Group:	Security
Reported in Release:	SLXOS 18r.2.00	Technology:	User Accounts & Passwords
Symptom:	Unexpected reload		
Condition:	When REST query is send with username same as role name		

Parent Defect ID:	SLXOS-40610	Issue ID:	SLXOS-41804
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.1.00b	Technology:	SNMP - Simple Network Management Protocol
Symptom:	SNMP walk output is not showing for OID 1.3.6.1.4.1.1588.2.1.2.1.7.1.1 for active MM index on 18r.1 release, but works on 17r.2x and 18r.2x.		
Condition:	When SNMP query is hit for OID 1.3.6.1.4.1.1588.2.1.2.1.7.1.1 the output doesn't contain result for active MM index.		

Parent Defect ID:	SLXOS-39522	Issue ID:	SLXOS-41962
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	IP Multicast
Reported in Release:	SLXOS 18r.2.00	Technology:	PIM - Protocol-Independent Multicast
Symptom:	Unexpected reload		
Condition:	When PIM debug (ip pim packet)enable and shut/no shut on some interfaces		

Parent Defect ID:	SLXOS-41629	Issue ID:	SLXOS-41987
Severity:	S3 - Medium		
Product:	SLX-OS	Technology Group:	Security
Reported in Release:	SLXOS 18r.1.00a	Technology:	User Accounts & Passwords
Symptom:	Unexpected reload		
Condition:	When REST query is send with username same as role name		

Parent Defect ID:	SLXOS-42310	Issue ID:	SLXOS-42472
Severity:	S2 - High		
Product:	SLX-OS	Technology Group:	Layer 2 Switching
Reported in Release:	SLXOS 18r.2.00	Technology:	MCT - Multi-Chassis Trunking
Symptom:	Unexpected reload of device		
Condition:	When “cluster <>” config is done followed by 'undeploy' and peer IP change without SRC IP and then 'deploy'.		

Parent Defect ID:	SLXOS-39856	Issue ID:	SLXOS-42500
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 18r.1.00a	Technology:	Static Routing (IPv4)
Symptom:	Route is not withdrawn on interface shut post HA failover		
Condition:	Ha failover performed and interface which is a next hop for the static route is shut		

Parent Defect ID:	SLXOS-42342	Issue ID:	SLXOS-42585
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 18r.2.00a	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	BGP peering may go down, when ‘no router mpls’ is issued, and when there are following routes under VRF: a) when learnt route is not selected b) when learnt route is re originated with network command		
Condition:	When learnt route is not selected or when learnt route is re-originated with ‘network’ command and when ‘no router mpls’ is issued.		
Workaround:	1) Shutdown BGP neighbors under VRF, remove network command. 2) Remove ‘router mpls’. 3) Issue ‘no shutdown’ of BGP neighbors under VRF and add ‘network’ command.		

Parent Defect ID:	SLXOS-42673	Issue ID:	SLXOS-42676
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Layer 2 Switching
Reported in Release:	SLXOS 18x.1.00a	Technology:	MCT - Multi-Chassis Trunking
Symptom:	Unexpected reload		
Condition:	When the management cluster is down.		

Parent Defect ID:	SLXOS-42503	Issue ID:	SLXOS-42686
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.1.00b	Technology:	Software Installation & Upgrade
Symptom:	1. Sysfpga image upgrading on SFM failed, sometimes. 2. FPGA image version checking and printing is too frequently.		
Condition:	SLX9850 platform		

Parent Defect ID:	SLXOS-42282	Issue ID:	SLXOS-42707
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 17r.1.01_CVR	Technology:	ARP - Address Resolution Protocol

Symptom:	Intermittent ping loss between the hosts via MCT cluster node.
Condition:	When the MCT networks is seeing excessive MAC movement on the cluster node

Parent Defect ID:	SLXOS-42441	Issue ID:	SLXOS-42762
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.2.00a	Technology:	CLI - Command Line Interface
Symptom:	"continue 100" under route-map does not persists after reload.		
Condition:	When "continue 100" is configured under route-map		

Parent Defect ID:	SLXOS-41226	Issue ID:	SLXOS-42782
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Traffic Management
Reported in Release:	SLXOS 18r.1.00aa	Technology:	QoS - Quality of Service
Symptom:	NetConf/REST response payload was returning with unsupported value 4. So that payload was not able to use for Netconf/REST request.		
Condition:	If Traffic-class to CoS mapping configured without DP value, Netconf/REST query returning with unsupported DP value 4. It fails in the Netconf/REST config with same payload.		
Workaround:	To make the same configuration through Netconf/REST, Make separate requests for each Dp values (0-3)		

Parent Defect ID:	SLXOS-42225	Issue ID:	SLXOS-42785
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 18r.2.00	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	Unexpected reload of the device		
Condition:	When “no cluster <>” MCT config is executed		
Workaround:	None		

Parent Defect ID:	SLXOS-42728	Issue ID:	SLXOS-42844
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.1.00c	Technology:	CLI - Command Line Interface
Symptom:	"show vlan brief" and "show vlan <N>" display member interfaces in random order.		

Condition:	When we use the "show vlan brief" and "show vlan <N>" command in CLI.
-------------------	---

Parent Defect ID:	SLXOS-41137	Issue ID:	SLXOS-43000
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	MPLS
Reported in Release:	SLXOS 18r.1.00b	Technology:	LDP - Label Distribution Protocol
Symptom:	LDP session was stuck because of an incorrect state.		
Condition:	LDP sessions flapping and being re-established. This state made it seem that the expected connection had already been established; causing the new connection setup to fail.		

Parent Defect ID:	SLXOS-42874	Issue ID:	SLXOS-43181
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Layer 2 Switching
Reported in Release:	SLXOS 18r.1.00b	Technology:	VLAN - Virtual LAN
Symptom:	When traffic is flowing between two endpoint tracking enabled port , unauthenticated traffic is not dropped.		
Condition:	When traffic is flowing between two endpoint tracking enabled port.		

Parent Defect ID:	SLXOS-43195	Issue ID:	SLXOS-43299
Severity:	S1 – Critical		
Product:	SLX-OS	Technology Group:	Layer 2 Switching
Reported in Release:	SLXOS 18r.1.00c	Technology:	MCT - Multi-Chassis Trunking
Symptom:	Unexpected LC reload		
Condition:	When MCT MAC CCR to CCL conversion		
Workaround:	None		

Parent Defect ID:	SLXOS-42649	Issue ID:	SLXOS-43308
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Layer 2 Switching
Reported in Release:	SLXOS 17r.1.00	Technology:	VLAN - Virtual LAN
Symptom:	Vlan name is not properly displayed .It is a cosmetic issue.		
Condition:	When VLAN with no router interface configured .		

Parent Defect ID:	SLXOS-38488	Issue ID:	SLXOS-43448
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Layer 2 Switching
Reported in Release:	SLXOS 18r.1.00aa	Technology:	MCT - Multi-Chassis Trunking
Symptom:	MCT Convergence will take more time (around 26 sec)		

Condition:	One of the MCT pair goes down
-------------------	-------------------------------

Parent Defect ID:	SLXOS-42655	Issue ID:	SLXOS-43521
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.2.00a	Technology:	CLI - Command Line Interface
Symptom:	The 'reload system' and 'firmware download' CLI's succeeds without confirming with 'Y/Yes' option.		
Condition:	When user hit ENTER without any input, the system proceeds to reboot and firmware download CLI's.		

Defects closed in 18r.1.00c

This section lists software defects with Critical, High, and Medium Technical Severity closed with and without a code change as of **6/19/2019** in 18r.1.00c.

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-22514	Issue ID:	SLXOS-30535
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Traffic Management
Reported in Release:	SLXOS 17r.1.01a	Technology:	Rate Limiting and Shaping
Symptom:	100G interfaces on SLX 9850 may not achieve line rate egress throughput.		
Condition:	On a L2VPN network 100G interfaces on SLX 9850 may not achieve line rate of egress through put.		
Workaround:	Augment performance with additional interfaces as required.		

Parent Defect ID:	SLXOS-37463	Issue ID:	SLXOS-37463
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 18r.1.00a	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	A warning is seen on console as follows. "No. of prefix received from BGP Peer 2000:31:1:8::153: exceeds warning limit 0"		
Condition:	When the maximum prefix config is at the IPv6 neighbor level and the ipv6 address-family activate cmd at the peer-group level and the device is reloaded with that saved config.		
Workaround:	Remove maximum prefix config at the neighbor and re-config.		

Parent Defect ID:	SLXOS-38394	Issue ID:	SLXOS-38394
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Security
Reported in Release:	SLXOS 18r.1.00b	Technology:	HTTP/HTTPS
Symptom:	Enabling or disabling HTTP(S) service on Virtual Routing and Forwarding(VRF) name other than management VRF("mgmt-vrf") may not succeed.		
Condition:	Enabling or disabling HTTP(S) service fails on chassis based devices		
Workaround:	None		

Parent Defect ID:	SLXOS-38406	Issue ID:	SLXOS-38406
--------------------------	-------------	------------------	-------------

Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Traffic Management
Reported in Release:	SLXOS 18r.1.00b	Technology:	Rate Limiting and Shaping
Symptom:	When egress Rate-limiter is applied on port-channel, and system is rebooted, then egress Rate-Limiter was not working.		
Condition:	When system was rebooted with Egress RL applied on port-channel		
Workaround:	After reboot, reapply egress RL.		

Parent Defect ID:	SLXOS-38447	Issue ID:	SLXOS-38447
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Layer 3 Routing/Network Layer
Reported in Release:	SLXOS 18r.1.00b	Technology:	BGP4 - IPv4 Border Gateway Protocol
Symptom:	L3VPN traffic may not be forwarded.		
Condition:	The VRFs are configured first in an order and then L3VPN config (route-target, route-distinguisher etc.) is done in a different order to those VRFs, so that the label allocation to VRFs does not happen in the order of creation of VRFs. Now if HA fail over is done, L3 VPN traffic may not be forwarded.		

Parent Defect ID:	SLXOS-27981	Issue ID:	SLXOS-38496
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 17r.1.01ah	Technology:	CLI - Command Line Interface
Symptom:	If user changes the startup config file to let management IP and default gateway in a different subnet from the management IP and default gateway that currently configured on SLX, and perform "copy tftp startup-config", then reload, SLX will keep the previously configured management IP and gateway after reload		
Condition:	User changes the startup config file to have management IP and gateway address in a different subset from the management IP and gateway that currently configured on SLX		
Workaround:	Before reload the system, remove the management IP and default gateway from system using CLI		

Parent Defect ID:	SLXOS-20017	Issue ID:	SLXOS-38877
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 17r.1.00a	Technology:	SNMP - Simple Network Management Protocol
Symptom:	Unexpected behavior with SLX		
Condition:	While trying to write port alias using SNMP application.		
Workaround:	None		

Parent Defect ID:	SLXOS-38980	Issue ID:	SLXOS-38980
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.1.00b	Technology:	SNMP - Simple Network Management Protocol
Symptom:	Snmp daemon terminates and restarts on HA failover.		
Condition:	Occurs only when there is an SNMP host configured with source-interface as management mm-ip.		
Workaround:	Keep source-interface configuration as default		

Parent Defect ID:	SLXOS-38299	Issue ID:	SLXOS-39007
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Other
Reported in Release:	SLXOS 18x.1.00a	Technology:	Other
Symptom:	Sometimes, a panic dump may be seen while rebooting the setup.		
Condition:	This is a rare condition which may be seen while device is rebooting or when sending high rate traffic to CPU.		
Workaround:	N/A		

Parent Defect ID:	SLXOS-39185	Issue ID:	SLXOS-39185
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Traffic Management
Reported in Release:	SLXOS 18r.1.00b	Technology:	Rate Limiting and Shaping
Symptom:	rate limiting clear command is not working		
Condition:	execute show command and clear command, data still shows even after clear command		

Parent Defect ID:	SLXOS-39214	Issue ID:	SLXOS-39214
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	MPLS
Reported in Release:	SLXOS 18r.1.00b	Technology:	LDP - Label Distribution Protocol
Symptom:	LDP sessions stay down despite ping functioning between the peers.		
Condition:	socket supporting LDP session is terminated by HA failover or route change. Note that the problem very rarely happens.		

Parent Defect ID:	SLXOS-39319	Issue ID:	SLXOS-39319
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Other
Reported in Release:	SLXOS 18r.1.00c	Technology:	Other
Symptom:	On the serial console, user observes output overwritten and becoming unreadable.		
Condition:	On the serial console, user changes window size and observe output overwritten and becoming unreadable.		

Parent Defect ID:	SLXOS-39220	Issue ID:	SLXOS-39349
Severity:	S1 – Critical		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18s.1.01a	Technology:	SNMP - Simple Network Management Protocol
Symptom:	LLDP-MIB::lldpLocPortId value is not correct (appears corrupted) when queried via SNMP GET operation.		
Condition:	Issue occurs only for SNMP GET operation (on LLDP-MIB::lldpLocPortId). SNMP GET-NEXT and snmpwalk returns correct values.		
Workaround:	1. Use SNMP GET-NEXT or snmpwalk instead of SNMP GET when querying LLDP-MIB::lldpLocPortId via SNMP. 2. Use CLI to query (LLDP-MIB::lldpLocPortId) instead of SNMP, if it's feasible.		

Parent Defect ID:	SLXOS-38901	Issue ID:	SLXOS-39427
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Network Automation and Orchestration
Reported in Release:	SLXOS 18r.1.00aa	Technology:	NETCONF - Network Configuration Protocol
Symptom:	Seeing error while using rpc to get port channel config.		
Condition:	If Insight enable mmld 1 command is enabled.		

Parent Defect ID:	SLXOS-39445	Issue ID:	SLXOS-39445
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Security
Reported in Release:	SLXOS 18r.1.00c	Technology:	TACACS & TACACS+
Symptom:	DCM daemon termination will be observed while executing any CLI		
Condition:	When AAA Command Authorization is enabled and the configured tacacs+ server are not reachable.		
Workaround:	Make the configured Tacacs+ server reachable.		

Parent Defect ID:	SLXOS-38336	Issue ID:	SLXOS-39626
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18x.1.00a	Technology:	CLI - Command Line Interface
Symptom:	Overlay-gateway configuration doesn't show up in running-config.		
Condition:	Overlay-gateway configuration doesn't show up in running-config after firmware upgrade with ZTP (Zero touch provisioning),		
Workaround:	None		

Parent Defect ID:	SLXOS-38493	Issue ID:	SLXOS-39702
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Other
Reported in Release:	SLXOS 18r.1.00aa	Technology:	Other
Symptom:	file transfer may be affected if destination port is udp 646 and pkt has fragment offset.		
Condition:	During file transfer if destination port is udp 646 between source and destination without “mpls ldp” being enabled on the box. UDP packet with destination port 646 is trapped to cpu even without mpls being enabled on the box.		

Parent Defect ID:	SLXOS-34817	Issue ID:	SLXOS-39748
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Layer 2 Switching
Reported in Release:	SLXOS 18r.2.00	Technology:	VRP - VLAN Registration Protocol
Symptom:	User will observe that the REST API response for mvrp interface related operational GET command fetches the value from the global bucket for non-MVRP interfaces.		
Condition:	Issue was seen only when trying to fetch MVRP information using REST API infrastructure for interfaces where MVRP was not configured.		
Workaround:	No		

Parent Defect ID:	SLXOS-39783	Issue ID:	SLXOS-39784
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Monitoring
Reported in Release:	SLXOS 18r.1.00a	Technology:	OAM - Operations, Admin & Maintenance
Symptom:	nf_contrack feature in Linux kernel track all IP packets coming to CPU. It can cause nf_contrack table full issue & fragmented packet drop issue.		
Condition:	There is no specific condition trigger this, by default the service is up and running.		

Parent Defect ID:	SLXOS-29369	Issue ID:	SLXOS-39838
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Monitoring
Reported in Release:	SLXOS 18r.2.00	Technology:	Port Mirroring
Symptom:	MTU of a destination mirror port may be a non-default MTU.		
Condition:	1. When Global MTU is configured on the device, 2. A port is configured as a destination-mirror port		

Parent Defect ID:	SLXOS-25731	Issue ID:	SLXOS-39974
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Layer 2 Switching
Reported in Release:	SLXOS 17s.1.02b	Technology:	MCT - Multi-Chassis Trunking
Symptom:	MCT daemon termination followed by switch reload		
Condition:	MCT daemon terminates when client server sends the LACP oper key as 0.		
Workaround:	Remove 'esi auto lacp' config		

Parent Defect ID:	SLXOS-39618	Issue ID:	SLXOS-40059
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	MPLS
Reported in Release:	SLXOS 18r.1.00aa	Technology:	MPLS VPLS - Virtual Private LAN Services
Symptom:	Peers MPLS interface VE MAC learned as remote VPLS mac.		
Condition:	Issue seen in egress PE node, when receiving VPLS packet has inner payload DA MAC as 0100.5e00.xxxx		

Parent Defect ID:	SLXOS-40076	Issue ID:	SLXOS-40076
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	SDN
Reported in Release:	SLXOS 18r.1.00c	Technology:	OpenFlow
Symptom:	Openflow flows are not pushed in Openflow profile 3 (Tcam profile)		
Condition:	Issue will be seen in openflow-profile-3 tcam while pushing openflow flows		

Parent Defect ID:	SLXOS-40143	Issue ID:	SLXOS-40143
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Security
Reported in Release:	SLXOS 18r.1.00c	Technology:	RADIUS
Symptom:	On console following error message will be seen - "Dcmd[3617]: pam_radius_auth: Could not open configuration file /etc/raddb/server: No such file or directory"		
Condition:	When REST/RESTCONF query is given		

Parent Defect ID:	SLXOS-40087	Issue ID:	SLXOS-40367
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.2.00	Technology:	High Availability
Symptom:	hasmd hang which was killed by SWD and switch reloaded in external login attach.		
Condition:	the issue may happen in brutal force login attack.		
Workaround:	None		

Parent Defect ID:	SLXOS-24384	Issue ID:	SLXOS-40383
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 17r.2.01	Technology:	CLI - Command Line Interface
Symptom:	ha chassisreboot command from ha inline help is not needed.		
Condition:	ha chassisreboot should have been obsoleted.		
Workaround:	Please use reload system command.		

Parent Defect ID:	SLXOS-24114	Issue ID:	SLXOS-40435
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Monitoring
Reported in Release:	SLXOS 17r.2.00	Technology:	OAM - Operations, Admin & Maintenance
Symptom:	After the devices boots up, the user will see the dcmd.sh, ccmd.sh, and netstat defunct processes.		
Condition:	The defunct processes will show up when the user runs the "ps aux" command.		
Workaround:	None. They are not harmful and so the user can just ignore them.		

Parent Defect ID:	SLXOS-39058	Issue ID:	SLXOS-40466
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Other
Reported in Release:	SLXOS 18r.1.00a	Technology:	Other
Symptom:	Switch reloaded with panic dump, impacting the data traffic forwarding.		
Condition:	High rate of software assisted layer 3 forwarding of traffic, causing connection tracking table to fill up.		
Workaround:	NA		

Parent Defect ID:	SLXOS-40476	Issue ID:	SLXOS-40477
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.2.00	Technology:	High Availability
Symptom:	During DOS attacks, flood of disable pam_unix log messages are seen on console		
Condition:	DOS attacks on system		
Workaround:	Configure syslog server to redirect these messages		

Parent Defect ID:	SLXOS-38229	Issue ID:	SLXOS-40484
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.1.00ab	Technology:	LLDP - Link Layer Discovery Protocol
Symptom:	NOS CLI "show lldp neighbors" command failed to fetch the neighbor details.		
Condition:	LLDP must be configured on the SLX device.		
Workaround:	CMSGH "show lldp neighbors" command can be used to fetch the LLDP neighbor details		

Parent Defect ID:	SLXOS-38762	Issue ID:	SLXOS-40532
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Other
Reported in Release:	SLXOS 18r.1.00aa	Technology:	Other
Symptom:	JSON output of REST bridge-domain config has duplicated URN part way through the output.		
Condition:	For vlans configured more than 100, REST bridge-domain config has duplicated URN part way through the output.		
Workaround:	No		

Parent Defect ID:	SLXOS-40884	Issue ID:	SLXOS-40884
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.1.00c	Technology:	Software Installation & Upgrade
Symptom:	Firmwaredownload may fail with dpkg confd error messages on console.		
Condition:	While upgrade/downgrade using normal firmwaredownload /fullinstall.		

Parent Defect ID:	SLXOS-39462	Issue ID:	SLXOS-40929
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Layer 2 Switching
Reported in Release:	SLXOS 18r.1.00ac	Technology:	MCT - Multi-Chassis Trunking
Symptom:	MAC is not being updated with the new ifindex on the remote LC.		
Condition:	MAC move from one client interface to another client interface when same mac changes from CCR to CCL at the same time on remote LC.		

Parent Defect ID:	SLXOS-40994	Issue ID:	SLXOS-40994
Severity:	S2 – High		

Product:	SLX-OS	Technology Group:	Other
Reported in Release:	SLXOS 18r.1.00c	Technology:	Other
Symptom:	/var/run directory not present at bootup so /var/run/racoon2 was not created.		
Condition:	/var/run and /var/run/racoon2 should be present at bootup time		
Workaround:	add mkdir /var/run and -p option for create /var/run/racoon2 in sysinit script		

Parent Defect ID:	SLXOS-39963	Issue ID:	SLXOS-41019
Severity:	S3 – Medium		
Product:	SLX-OS	Technology Group:	Monitoring
Reported in Release:	SLXOS 18r.1.00b	Technology:	sFlow
Symptom:	SFLOW controller failed to capture few flows on bi-directional traffic.		
Condition:	SFLOW configuration enabled on interface.		

Parent Defect ID:	SLXOS-39538	Issue ID:	SLXOS-41117
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Security
Reported in Release:	SLXOS 18r.1.00aa	Technology:	AAA - Authentication, Authorization, and Accounting
Symptom:	Unexpected reload		
Condition:	When TACACS authorization fails on re-try		
Workaround:	Make sure we have the proper network connectivity to avoid TACACS authorization fails at first attempt.		

Parent Defect ID:	SLXOS-41166	Issue ID:	SLXOS-41168
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Management
Reported in Release:	SLXOS 18r.1.00b	Technology:	CLI - Command Line Interface
Symptom:	Unexpected reload of the device.		
Condition:	Protocol lldp has dot1-tlv/dot3-tlv config and when "show lldp neighbors detail" command is issued.		
Workaround:	None		

Parent Defect ID:	SLXOS-40759	Issue ID:	SLXOS-41327
Severity:	S1 – Critical		
Product:	SLX-OS	Technology Group:	MPLS
Reported in Release:	SLXOS 18r.1.00aa	Technology:	MPLS VPLS - Virtual Private LAN Services
Symptom:	Not able to program MPLS tunnel		
Condition:s	Power-off/on line card on PE routers		

Parent Defect ID:	SLXOS-40826	Issue ID:	SLXOS-41816
Severity:	S2 – High		
Product:	SLX-OS	Technology Group:	Other
Reported in Release:	SLXOS 18r.1.00aa	Technology:	Other
Symptom:	SLX device experience unexpected sudden reload.		
Condition:	FWD daemon termination cause the sudden reload.		