20 June 2018

SLX-OS 17s.1.02b for SLX 9140, SLX 9240

Release Notes v1.0

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit http://www.brocade.com/support/oscd.

Contents

Document history

Version	Summary of changes	Publication date
1.0	Initial Release	20 June 2018

Preface

Contacting Extreme Technical Support

As an Extreme customer, you can contact Extreme Technical Support using one of the following methods: 24x7 online or by telephone. OEM customers should contact their OEM/solution provider.

If you require assistance, contact Extreme Networks using one of the following methods:

- GTAC (Global Technical Assistance Center) for immediate support
- Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact.
- Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge - Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub - A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal - Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Extreme resources

Visit the Extreme website to locate related documentation for your product and additional Extreme resources.

White papers, data sheets, and the most recent versions of Extreme software and hardware manuals are available at www.extremenetworks.com. Product documentation for all supported releases is available to registered users at www.extremenetworks.com/support/documentation.

Document feedback

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

You can provide feedback in two ways:

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

- Email us at internalinfodev@extremenetworks.com

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

Overview

SLX 9140 and SLX 9240 are fixed 1U switching platform based of programmable ASIC from Cavium that enables adoption of new protocols and technologies. These switches were released as a part of SLX-OS 17s.1.00.

- High density 40G/100G spine-leaf connection
- Native 1G/10G/25G server connectivity at the leaf
- High performance VXLAN routing
- Payload timestamping to enable accurate measurement of performance SLAs
- Port-to-port Latency: ~2.5us
- Architecture: Store & Forward

Software Features

The following are the three main feature categories that are supported and enhanced in SLX-OS 17s.1.02:

1. Network Packet Broker
2. EVPN VxLAN based Network Virtualization Overlay
3. Brocade SLX Visibility Services
4. Embedded Fabric Automation (EFA)

1. SLX 9140 and SLX 9240 as Network Packet Broker

The SLX 9140 and SLX 9240 switches may be used as a Network Packet Brokers.

NOTE: The Advanced Features Self Authenticated Upgrade (SAU) license enables Network Packet Broker features on the Extreme SLX 9140 and SLX 9240 switches.

Network Packet Broker (NPB) is a term first coined by Gartner to describe the part of a network visibility infrastructure responsible for aggregating network traffic and directing it to visibility applications. Visibility applications are network monitoring tools, such as nework and application performance monitoring solutions, and intrusion detection systems.

The previous SLX-OS release had support for the following packet broker features on the SLX 9240:

Feature Name	**Feature Description**
Aggregation	The ability to aggregate packets arriving from multiple TAPs or SPAN ports from upstream devices and direct the aggregated traffic to a single egress port or port group.
Replication	The ability to copy packets arriving on one or more ingress ports to multiple egress ports and port groups.
Load balancing	The ability to distribute packets from one or more ingress ports among egress ports in a port group.
L2-L4 filtering	The ability to selectively direct packets from ingress to egress ports based on fields in the L2-L4 protocol headers.

SLX-OS 17s.1.02 adds support for the same NPB features on the SLX 9140 as well. In addition, SLX-OS 17s.1.02 introduces the following NPB enhancements:

Feature Name	**Feature Description**
GTP-tunneled HTTPS filtering[1]	The ability to optionally drop all GTP-tunneled HTTPS packets.
Link Fault Signaling (LFS) management[2]	The ability to suppress link fault signaling on both the TX and RX side of a port.
Symmetric load balancing	The ability to distribute bidirectional traffic flows to the same physical egress port when load balancing packets on an egress port group. For example, packets may be kept together based on their source and destination MAC address or SIP/DIP.
VLAN stripping	The ability to optionally remove the outermost 802.1Q VLAN tag from a packet.

[1] Beta

[2] Feature supported in both NPB and NON-NPB(default) mode

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

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

The following table lists the set of new features coming in SLX-OS 17s.1.02

Feature Name	Feature Description
BGP eVPN	Standards based, Controller-less Network Virtualization Overlays with VxLAN encapsulation. Provides automatic VxLAN tunnel end point discovery, end host MAC and MAC-IP learning over the control plane.
ARP Suppression	Suppress/reduce the ARP broadcast traffic in an IP fabric.
Static Anycast Gateway	Static Anycast Gateway allows configuring Static Anycast MAC as gateway for multiple tenant systems in a virtualized data center fabric. Same Gateway address is configured across all TORs for a given Tenant/VLAN combination, thus enabling seamless VM mobility across the leaf switches in an IP Fabric deployment without any need for host gateway configuration changes.
Conversational ARP	ARP entries for active conversations only (helps optimize ARP table size)
IP Unnumbered Interfaces	Reduces consumption of IP Address space. Leaf to spine inter-switch point-to-point L3 links are configured as ip unnumbered (/31 subnets) to conserve IP addresses and optimize hardware resources.
L2 VNI capability	The L2VNI is the MAC/NVE mapping table
L3 VNI	The L3VNI is IP prefix/NVE mapping table
CML – IP Fabric	Supports conversational MAC learning (CML) for BGP-EVPN learnt MAC addresess
Improved VRF Scale	512 VRFs are supported in SLX9140 and SLX9240 platforms.
Dynamic tunnel (VxLAN) discovery	Supports Dynamic Tunnel discovery using BGP EVPN.

Cluster Management	Configuration management between MCT nodes for logical VTEP is supported.
Manageability, Monitoring, Debugging	NetConf, RESTful API provisioning, VRF support for Telnet/SNMP/SSH, VxLAN tunnel traffic statistics, Show/debug commands
OSPFv2 type3 LSA filtering	Enables OSPF ABR to filter type-3 LSA updates across areas.

3. Extreme SLX Visibility Services

Extreme SLX Visibility Services is a new feature introduced in SLX-OS 17s.1.02. There are two main elements to this service - classification and action. Similar to any ACL-based service in a switch but with additional richness, so that you can classify what is happening in overlays as well as specific workloads (vs. just port-level data).

The potential actions (such as mirror, count, etc) are dynamic and can be configured by adding a workflow that can react to specific events/criteria. That data can also be pushed to sFlow, span port, streaming APIs; to third party or Extreme tools.

SLX Visibility Services are enabled on the SLX 9240 switches so you can have visibility from the spine layer and from wire to workflow. Through additional integration with Extreme Workflow Composer, configuration can also be simplified to avoid box-by-box CLI configuration.

Feature Name	**Supported Actions**
Visibility Services* *Note: Transit rules to be applied per switch. Per interface and per logical interface is not supported in SLX-OS 17s.1.02.	**Permit** **Deny** **sFlow** **Count** **Mirror/SPAN**

Insight Interface:

The Extreme SLX 9140 includes Extreme SLX architecture delivered through this release. This new approach to network monitoring and troubleshooting provides a highly differentiated solution that makes it faster, easier, and more cost-effective to get the comprehensive, real-time visibility needed for network operations and automation. By embedding network visibility on every switch, the Extreme SLX Insight Architecture can help organizations achieve pervasive visibility throughout the network to quickly and efficiently identify problems, accelerate mean-time-to-resolution, and improve overall service levels.

SLX9140 provides a dedicated analytics path (**10G**) between the packet processor and the Guest VM running on SLX9140. This insight interface is a Port Channel with a single member port and is mapped to Eth0/73. The analytics path enables applications running in the open KVM environment (Guest VM) to extract data without disrupting the forwarding or control plane traffic of the Extreme SLX 9140.

The analytics path is not available on SLX9240. But the Guest VM is available for the user to run any applications.

Another key feature supported by SLX-OS 17s.1.02 is streaming. Instead of the traditional SNMP pull model, SLX9140/SLX9240 supports a push model to continuously stream data out of the network. JSON and GPB (Google Protocol Buffer) encoding are supported.

Consolidated Features in SLX-OS 17s.1.02

Following table lists the features present in SLX-OS 17s.1.02.

Layer 2 Switching	
• Conversational MAC Learning • Virtual Link Aggregation Group (vLAG) spanning • Layer 2 Access Control Lists (ACLs) • Address Resolution Protocol (ARP) RFC 826 • Layer 2 Loop prevention in an overlay environment • MLDv1 Snooping • IGMP v1/v2 Snooping • MAC Learning and Aging • Link Aggregation Control Protocol (LACP) IEEE 802.3ad/802.1AX • Virtual Local Area Networks (VLANs)	• VLAN Encapsulation 802.1Q • BD Support • Per-VLAN Spanning Tree (PVST+/PVRST+) • Rapid Spanning Tree Protocol (RSTP) 802.1w • Multiple Spanning Tree Protocol (MSTP) 802.1s • STP PortFast, BPDU Guard, BPDU Filter • STP Root Guard • Pause Frames 802.3x • Static MAC Configuration • Multi-Chassis Trunking (MCT) • VXLAN extenstion tunnels • Overlay services: overlay gateway instances, overlay transit instances (on spine nodes) • Link-fault signaling • IP-based management cluster
Layer 3 Routingefa	
• Border Gateway Protocol (BGP4+) • DHCP Helper • Layer 3 ACLs • OSPF v2/v3 • Static routes • IPv4/v6 ACL • Route Policies • Bidirectional Forwarding Detection (BFD) • 32-Way ECMP • VRF Lite • VRF-aware OSPF, BGP, VRRP, static routes • VRRP v2 and v3 • Anycast Gateway over VxLAN	• VRRP-E • IPv4/IPv6 dual stack • ICMPv6 Route-Advertisement Guard IPv6 ACL packet filtering • BGP-Allow AS • BGP Generalized TTL Security Mechanism (GTSM) • IPv6 routing • OSPF Type-3 LSA Filter • Wire-speed routing for IPv4 and IPv6 using any routing protocol • Multi-VRF • L3 over Bridge Domains (BD)
Automation and Programmability	
• gRPC Streaming protocol and API	• PyNOS libraries

• REST API with YANG data model • Python	• DHCP automatic provisioning • NETCONF API
Quality of Service	
• ACL-based QoS • Two Lossless priority levels for QoS • Class of Service (CoS) IEEE 802.1p • DSCP Trust • DSCP to Traffic Class Mutation • DSCP to CoS Mutation • DSCP to DSCP Mutation • CoPP (Control Plane Policing)	• Random Early Discard • Per-port QoS configuration • ACL-based Rate Limit • Dual-rate, three-color token bucket • ACL-based remarking of CoS/DSCP/Precedence • ACL-based sFlow • Overlay GW Services (ACLs, QOS, SFlow, SPAN) • Scheduling: Strict Priority (SP), Deficit Weighted Round-Robin (DWRR)
Management and Monitoring	
• 1588v2 PTP • Time Stamping • Zero-Touch Provisioning (ZTP) • IPv4/IPv6 management • Industry-standard Command Line Interface (CLI) • NETCONF API • REST API with YANG data model • SSH/SSHv2 • Link Layer Discovery Protocol (LLDP) IEEE 802.1AB • MIB II RFC 1213 MIB • Syslog (RASlog, AuditLog) • Management VRF • Switched Port Analyzer (SPAN) • Telnet	• SNMP v1, v2C, v3 • sFlow version 5 • Out-of-band management • RMON-1, RMON-2 • NTP • Management Access Control Lists (ACLs) • Role-Based Access Control (RBAC) • Range CLI support • Python • DHCP Option 82 Insertion • DHCP Option 82 (Vlan) • DHCP Relay • Guest VM support • SLX-OS and Linux Shell Interoperability
Security	
• Port-based Network Access Control 802.1X • RADIUS – Authentication and Authorization • AAA • TACACS+ • Secure Shell (SSHv2) • TLS 1.1, 1.2 • HTTP/HTTPS	• BPDU Drop • Lightweight Directory Access Protocol (LDAP) • Secure Copy Protocol • Control Plane Protection • LDAP/AD • SFTP • Port Security
IP Fabric	
• Controllerless Network Virtualization (BGP-EVPN) • ARP/ND supression • Conversational ARP • Static Anycast Gateway	• Logical VTEP (Static and EVPN) • IP Un-numbered interface • No Traffic Tromboning. • RIOT (Routing In and Out of Tunnel) (v4 and v6)
Platform	

• 25G AN/LT • Insight interface (10G analytic path in SLX9140) • 1G/10G/25G/40G/100G Auto speed detection • Multi Speed(1G/10G) Optic Support	• Digital Optical Monitoring(DOM)
NPB	
• Traffic aggregation • Traffic replication (via TVF – transparent VLAN flooding) • L2-L4 (via L2/L3 ACL matched route-map) • Load-balancing (hash-based)	• VLAN Stripping • Symmetric load balance • GTP-tunneled HTTPS filtering[3] • Link Fault Signaling (LFS)management[4]

[3] Beta

[4] Feature supported in both NPB and NON-NPB(default) mode

4. Embedded Fabric Automation

EFA is an application that can be installed on the TPVM (Third Party Virtual Machine) on the SLX-9240 (spine). The application is bundled as part of the SLX firmware and can be used to configure an IP Fabric on the SLX 9240 and SLX 9140. EFA is documented in the “Embedded Fabric Automation” chapter of the *Extreme SLX-OS IP Fabrics Configuration Guide, 17s.102b*.

There is a single SLX OS CLI command to install the application, as shown below.

```
Spine# efa deploy
```

The EFA application is installed on the TPVM and provides Linux CLIs for managing the IP Fabric. EFA provides a simplified mechanism to configure an IP Fabric one the IP addresses of the devices are provided, as in the following example.

```
TPVM$ efa fabric configure --spine 10.25.225.159,10.25.225.164 --leaf 10.25.225.191,10.25.225.221
```

EFA also provides additional CLIs as shown in the following table.

CLI command functions	Example
Deconfigure the fabric	`efa fabric deconfigure --device 10.25.225.159,10.25.225.164,10.25.225.191,10.25.225.221`
Display fabric settings	`efa fabric setting show --advanced`
Update fabric settings	`efa fabric setting update --link_ip_range 10.10.110.0/23 -- loopback_ip_range 172.32.244.0/24 -- loopback_port_number=3 --vtep_loopback_port_number=4 -- spine_asn_block=61000 --leaf_asn_block 64000-66534`
List the executions	`efa execution show`
Update device credentials	`efa device credentials update --device 10.30.20.501 --username <username> --password <pass>`

The following table lists current EFA issues and their workarounds.

EFA issues and workarounds

Reference	Summary	Conditions	Workarounds
SIPF-361	The **efa fabric configure** command with **--force** option does not clear pre-existing switchport configuration on interfaces.	EFA --**force** option will clear only configurations that were provisioned by EFA. User configurations such switchport will not be removed.	There is no workaround.
SIPF-387	The **efa deploy** command fails in the last step of verifying the deployment if user credentials of the TPVM are incorrect or TPVM is not reachable.	Verification step requires access to the TPVM with proper credentials and reachability to the TPVM.	Execute the **efa deploy** command with proper credentials and ensure IP reachability of the TPVM.
SIPF-391	The **efa deploy** command that deploys EFA on the TPVM displays "fopen: Permission denied" message even when the installation succeeds.	This message can be ignored as this does not affect the functionality of deployment of EFA on the TPVM. This is an intermittent issue.	There is no workaround.
SIPF-395	The **efa fabric deconfigure** command fails with "Management Cluster is not operational. Polling timed out" message when it is executed after an MCT pair reboots or loses configuration.	This issue is observed when one member of the MCT pair reboots or loses its configuration (config not pesisteent) and then a deconfiguration is attempted.	Use the **--persist** option in the **efa fabric configure** command, so that reboots do not erase the MCT pair configuration. If an MCT pair configuration is lost, it can be reconfigured by means of the **efa fabric configure --force** option.
SIPF-397	The **efa fabric configure** command fails to add devices with different credentials.	This issue is seen when two switches are already in the fabric and a third switch with different credentials is added.	Ensure that all switches in fabric have the same credentials.

Considerations for EFA:

- EFA supports automation for IP Fabric underlay and overlay (i.e., overlay-gateway and EVPN) configuration. EFA does not support automation for tenant configuration.

- EFA supports automation for single-homed and multi-homed (MCT) leaf configurations.

Important Notes

Advanced Features SAU License

The SAU license enables the advanced licensed features prior to purchasing a license. On the Extreme SLX 9240 and Extreme SLX 9140 platforms, the Advanced Feature license set includes OVSDB integration, BGP EVPN, Guest VM, gRPC, 1588 BC, Timestamping, TPVM and all NPB features.

NOTE:
On the Extreme SLX 9240 and Extreme SLX 9140 platforms, the available base feature set, without a license, includes the following features: L2 protocols (including L2-MCT), L3 protocols (Static + Dynamic), Standard interfaces SNMP, NetConf, REST, Python scripting, and Insight Interface.

Zero Touch Provisioning (ZTP)

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

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

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

```
ZTP, Mon Mar 27 21:00:58 2017, ========== ZTP start ==========
ZTP, Mon Mar 27 21:00:58 2017, disable raslog
ZTP, Mon Mar 27 21:00:58 2017, CLI is ready
ZTP, Mon Mar 27 21:01:35 2017, inband ports are enabled
ZTP, Mon Mar 27 21:01:36 2017, serial number = EXH3314M00A
ZTP, Mon Mar 27 21:01:36 2017, model name = SLX9140
ZTP, Mon Mar 27 21:01:36 2017, use both management interface and inband interfaces
ZTP, Mon Mar 27 21:01:36 2017, checking inband interfaces link status
ZTP, Mon Mar 27 21:02:27 2017, find link up on intefaces: eth0 Eth0.4 Eth0.43 Eth0.44
ZTP, Mon Mar 27 21:02:27 2017, start dhcp process on interfaces: eth0 Eth0.4 Eth0.43 Eth0.44
ZTP, Mon Mar 27 21:02:37 2017, retry in 10 seconds
ZTP, Mon Mar 27 21:02:47 2017, inband ports are enabled
ZTP, Mon Mar 27 21:02:47 2017, serial number = EXH3314M00A
ZTP, Mon Mar 27 21:02:47 2017, model name = SLX9140
ZTP, Mon Mar 27 21:02:47 2017, use both management interface and inband interfaces
ZTP, Mon Mar 27 21:02:47 2017, dhcp server search timeout in 3529 seconds
ZTP, Mon Mar 27 21:02:47 2017, checking inband interfaces link status
ZTP, Mon Mar 27 21:02:48 2017, find link up on intefaces: eth0 Eth0.4 Eth0.43 Eth0.44
ZTP, Mon Mar 27 21:02:48 2017, start dhcp process on interfaces: eth0 Eth0.4 Eth0.43 Eth0.44
ZTP, Mon Mar 27 21:02:58 2017, retry in 10 seconds
…
```

You may login to the switch and cancel ZTP, then reboot the switch (with “reload system”) before making any configuration change on the switch.

```
SLX# dhcp ztp cancel
Warning: This command will terminate the existing ZTP session
After ZTP has been confirmed canceled, you need to run "reload system" before configuring the
switch.
Do you want to continue? [y/n] y
SLX# ZTP, Mon Mar 27 21:08:08 2017, serial number = EXH3314M00A
ZTP, Mon Mar 27 21:08:08 2017, model name = SLX9140
ZTP, Mon Mar 27 21:08:08 2017, use both management interface and inband interfaces
ZTP, Mon Mar 27 21:08:08 2017, dhcp server search timeout in 3208 seconds
ZTP, Mon Mar 27 21:08:08 2017, checking inband interfaces link status
ZTP, Mon Mar 27 21:08:09 2017, find link up on intefaces: eth0 Eth0.4 Eth0.43 Eth0.44
ZTP, Mon Mar 27 21:08:09 2017, start dhcp process on interfaces: eth0 Eth0.4 Eth0.43 Eth0.44
```

Wait for 10 seconds. You may confirm the ZTP is canceled, re-executing the same command.

```
SLX# dhcp ztp cancel
ZTP is not enabled.

SLX# SLX# reload system

Warning: This operation will cause the chassis to reboot and
requires all existing telnet, secure telnet and SSH sessions to be
restarted.
Unsaved configuration will be lost. Please run `copy running-config startup-config` to save the current
configuration if not done already.

Are you sure you want to reboot the chassis [y/n]? y
[  940.360081] VBLADE: vblade_control: FEPORTS_DISABLE
xpDma::quiesce:307 devId=0
xpDriverWrapper::quiesce:146 devId=0
 FABOS_BLADE_MSG_BL_DISABLE received in HSLUA for chip 0
2017/03/27-21:14:13, [RAS-1007], 567,, INFO, SLX9140, System is about to reload.
…
```

Documentation supporting SLX-OS

The following lists the documentation supporting this release:

- Extreme SLX-OS Command Reference, 17s.1.02
- Extreme SLX-OS IP Fabrics Configuration Guide, 17s.1.02
- Extreme SLX-OS IP Multicast Configuration Guide, 17s.1.02
- Extreme SLX-OS Layer 2 Switching Configuration Guide, 17s.1.02
- Extreme SLX-OS Layer 3 Routing Configuration Guide, 17s.1.02
- Extreme SLX-OS Management Configuration Guide, 17s.1.02
- Extreme SLX-OS MIB Reference, 17s.1.02
- Extreme SLX-OS Monitoring Configuration Guide, 17s.1.00
- Extreme SLX-OS Network Packet Broker Configuration Guide, 17s.1.02
- Extreme SLX-OS QoS and Traffic Management Configuration Guide, 17s.1.02
- Extreme SLX-OS REST API, 17s.1.02
- Extreme SLX-OS NetCONF, 17s.1.02
- Extreme SLX-OS YANG, 17s.1.02
- Extreme SLX-OS Security Configuration Guide, 17s.1.02
- Extreme SLX-OS Software Licensing Guide, 17s.1.02
- Extreme SLX 9140 Switch Hardware Installation Guide
- Extreme SLX 9140 Switch Technical Specifications
- Extreme SLX 9240 Switch Hardware Installation Guide Example
- Extreme SLX 9240 Switch Technical Specifications

RFCs and Standards

Extreme SLX 9140, 9240 Specifications

IEEE Compliance		
Ethernet	• IEEE 802.1D Spanning Tree Protocol • IEEE 802.1s Multiple Spanning Tree • IEEE 802.1w Rapid Reconfiguration of Spanning Tree Protocol • IEEE 802.3 Ethernet • IEEE 802.3ad Link Aggregation with LACP • IEEE 802.3ae 10G Ethernet • IEEE 802.1Q VLAN Tagging • IEEE 802.1p Class of Service	• Prioritization and Tagging • IEEE 802.1v VLAN Classification by Protocol and Port • IEEE 802.1AB Link Layer Discovery Protocol (LLDP) • IEEE 802.3x Flow Control (Pause Frames) • IEEE 802.3ab 1000BASE-T • IEEE 802.3z 1000BASE-X
RFC Compliance		
General Protocols	• RFC 768 User Datagram Protocol (UDP) • RFC 783 TFTP Protocol (revision 2) • RFC 791 Internet Protocol (IP) • RFC 792 Internet Control Message Protocol (ICMP) • RFC 793 Transmission Control Protocol (TCP) • RFC 826 ARP • RFC 854 Telnet Protocol Specification • RFC 894 A Standard for the Transmission of IP Datagram over Ethernet Networks • RFC 959 FTP • RFC 1027 Using ARP to Implement Transparent Subnet Gateways (Proxy ARP) • RFC 1112 IGMP v1 • RFC 1157 Simple Network Management Protocol (SNMP) v1 and v2 • RFC 1305 Network Time Protocol (NTP) Version 3 • RFC 1492 TACACS+ • RFC 1519 Classless Inter-Domain Routing (CIDR) • RFC 1584 Multicast Extensions to OSPF • RFC 1765 OSPF Database Overflow • RFC 1812 Requirements for IP Version 4 Routers • RFC 1997 BGP Communities Attribute • RFC 2068 HTTP Server • RFC 2131 Dynamic Host Configuration Protocol (DHCP)	• RFC 2710 Multicast Listener Discovery (MLD) for IPv6 • RFC 2711 IPv6 Router Alert Option • RFC 2740 OSPFv3 for IPv6 • RFC 2865 Remote Authentication Dial-In User Service (RADIUS) • RFC 3101 The OSPF Not-So-Stubby Area (NSSA) Option • RFC 3137 OSPF Stub Router Advertisement • RFC 3176 sFlow • RFC 3392 Capabilities Advertisement with BGPv4 • RFC 3411 An Architecture for Describing SNMP Frameworks • RFC 3412 Message Processing and Dispatching for the SNMP • RFC 3587 IPv6 Global Unicast Address Format RFC 4291 IPv6 Addressing Architecture • RFC 3623 Graceful OSPF Restart—IETF Tools • RFC 3768 VRRP • RFC 4271 BGPv4 • RFC 4443 ICMPv6 (replaces 2463) • RFC 4456 BGP Route Reflection • RFC 4510 Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map • RFC 4724 Graceful Restart Mechanism for BGP • RFC4750 OSPFv2.MIB • RFC 4861 IPv6 Neighbor Discovery

	• RFC 2154 OSPF with Digital Signatures (Password, MD-5) • RFC 2236 IGMP v2 • RFC 2267 Network Ingress Filtering Option—Partial Support • RFC 2328 OSPF v2 • RFC 2370 OSPF Opaque Link-State Advertisement (LSA) • RFC 2375 IPv6 Multicast Address Assignments RFC 2385 Protection of BGP Sessions with the TCP MD5 Signature Option • RFC 2439 BGP Route Flap Damping • RFC 2460 Internet Protocol, Version 6 (v6) Specification (on management interface) • RFC 2462 IPv6 Stateless Address Auto-Configuration • RFC 2464 Transmission of IPv6 Packets over Ethernet Networks (on management interface) • RFC 2474 Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers RFC 2571 An Architecture for Describing SNMP Management Frameworks • RFC 3413 Simple Network Management Protocol (SNMP) Applications	• RFC 4893 BGP Support for Four-Octet AS Number Space • RFC 5082 Generalized TTL Security Mechanism (GTSM) • RFC 5880 Bidirectional Forwarding Detection (BFD) • RFC 5881 Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop) • RFC 5882 Generic Application of Bidirectional Forwarding Detection (BFD) • RFC 5883 Bidirectional Forwarding Detection (BFD) for Multihop Paths • RFC 5942 IPv6 Neighbor Discovery • RFC 7432 BGP-EVPN Control Plane Signaling
MIBs	• RFC 4292 IP Forwarding MIB • RFC 4293 Management Information Base for the Internet Protocol (IP) • RFC 7331 BFD MIB • RFC 7331 BFD Helper MIB • RFC 3826 SNMP-USM-AES-MIB • RFC 4273 BGP-4 MIB • RFC 2863 The Interfaces Group MIB • RFC4750 OSPFv2.MIB	• RFC 4133 Entity MIB (Version 3); rmon.mib, rmon2.mib, sflow_v5.mib, bridge.mib, pbridge.mib, qbridge.mib, rstp.mib • lag.mib, lldp.mib, lldp_ext_dot1.mib, lldp_ext_dot3.mib, • RFC 4022 TCP MIB • RFC 4113 UDP.MIB

Hardware support

SLX 9140/9240 Hardware and License SKUs

	Description
BR-SLX-9140-48V-AC-F	Extreme SLX 9140-48V Switch AC with Front to Back airflow 48x25GE/10GE/1GE + 6x100GE/40GE
BR-SLX-9140-48V-DC-F	Extreme SLX 9140-48V Switch DC with Front to Back airflow 48x25GE/10GE/1GE + 6x100GE/40GE
BR-SLX-9140-48V-AC-R	Extreme SLX 9140-48V Switch AC with Back to Front airflow 48x25GE/10GE/1GE + 6x100GE/40GE
BR-SLX-9140-48V-DC-R	Extreme SLX 9140-48V Switch DC with Back to Front airflow 48x25GE/10GE/1GE + 6x100GE/40GE
BR-SLX-9240-32C-AC-F	Extreme SLX 9240-32C Switch AC with Front to Back airflow 32x100GE/40GE
BR-SLX-9240-32C-DC-F	Extreme SLX 9240-32C Switch DC with Front to Back airflow 32x100GE/40GE
BR-SLX-9240-32C-AC-R	Extreme SLX 9240-32C Switch AC with Back to Front airflow 32x100GE/40GE
BR-SLX-9240-32C-DC-R	Extreme SLX 9240-32C Switch DC with Back to Front airflow 32x100GE/40GE
BR-SLX-9140-ADV-LIC	Advanced Software License
BR-SLX-9240-ADV-LIC	Advanced Software License

Supported Power supplies

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

	Description
BR-ACPWR-650-F	SLX FIXED AC 650W POWER SUPPLY F2B AIRFL
BR-ACPWR-650-R	SLX FIXED AC 650W POWER SUPPLY B2F AIRFL
BR-DCPWR-650-F	SLX FIXED DC 650W POWER SUPPLY F2B AIRFL
BR-DCPWR-650-R	SLX FIXED DC 650W POWER SUPPLY B2F AIRFL
BR-3250CFM-FAN-F	SLX FIXED FAN AC F2B AIRFLOW
BR-3250CFM-FAN-R	SLX FIXED FAN AC B2F AIRFLOW

Supported Optics

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

Description	Orderable PN	BRCD P/N
1000Base-SX	E1MG-SX-OM	33210-100
1000Base-LX	E1MG-LX-OM	33211-100
1GE Copper SFP (Pseudo-Branded)	E1MG-TX	33002-100
1GE Copper SFP (BR-Branded)	XBR-000190	57-1000042-02
10GE USR SFP+	10G-SFPP-USR	57-1000130-01
10GE USR SFP+	10G-SFPP-USR	57-1000130-02
10GE SR SFP+, 85C	10G-SFPP-SR	57-0000075-01
10GE SR SFP+, 70C	10G-SFPP-SR	57-1000340-01
10GE SR SFP+, 70C	10G-SFPP-SR	57-1000340-01
10GE AOC 7M	10GE-SFPP-AOC-0701	57-1000273-01
10GE AOC 10M	10GE-SFPP-AOC-1001	57-1000274-01
10GE Direct Attach 5M Active	10G-SFPP-TWX-0501	58-1000023-01
10GE Direct Attach 1M Active	10G-SFPP-TWX-0101	58-1000026-01
10GE Direct Attach 3M Passive	10G-SFPP-TWX-P-0301	58-1000025-01
10GE Direct Attach 5M Passive	10G-SFPP-TWX-P-0501	58-1000019-01
25G SR	25G-SFP28-SR	57-1000342-01
25GE Direct Attach 01M Passive	25G-SFP28-TWX-P-0101	58-0000064-01
25GE Direct Attach 03M Passive	25G-SFP28-TWX-P-0301	58-0000065-01
40GE QSFP+ SR4	40G-QSFP-SR4	57-1000128-01
40GE BiDi QSFP+	40G-QSFP-SR-BIDI	57-1000339-01
40GE QSFP+ LR4, 10KM, 70C	40G-QSFP-LR4	57-1000263-01
40GE QSFP+ SR4 to 10G-SR SFP+	40G-QSFP-SR4-INT	57-1000129-01

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

Optics supported starting SLX17s.1.01

10GE LR SFP+, 85C	10G-SFPP-LR	57-0000076-01
10GE LR SFP+ TAA	10G-SFPP-LR-SA	57-1000345-01

New Optics supported starting SLX17s.1.02

4x10GE QSFP+ LR4, 10km,	40G-QSFP-LR4-INT	57-1000477-01
10GE LR SFP+, 85C (10G, 1G mode)	10G-SFPP-LR	57-0000076-01

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

Mellanox Supports the following 10G optics:

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

DAC Cables:

- 40G-QSFP-C-0X01: passive 40G direct attached copper cables
- 40G-QSFP-QSFP-C-0X01: active 40G direct attached copper cables
- 40G-QSFP-4SFP-C-0X01: active 40G direct attached breakout copper cables

Supported Power Supplies:

BR-ACPWR-650-F SLX FIXED AC 650W POWER SUPPLY F2B AIRFL
BR-ACPWR-650-R SLX FIXED AC 650W POWER SUPPLY B2F AIRFL
BR-DCPWR-650-F SLX FIXED DC 650W POWER SUPPLY F2B AIRFL
BR-DCPWR-650-R SLX FIXED DC 650W POWER SUPPLY B2F AIRFL
BR-3250CFM-FAN-F SLX FIXED FAN AC F2B AIRFLOW
BR-3250CFM-FAN-R SLX FIXED FAN AC B2F AIRFLOW

Software upgrade and downgrade

Image file names

Download the following images from www.extremenetworks.com.

Image file name	Description
slxos17s.1.02b.tar.gz	SLX-OS 17s.1.02b software
slxos17s.1.02b_all_mibs.tar.gz	SLX-OS 17s.1.02b MIBS
slxos17s.1.02b.md5	SLX-OS md5 checksum

Migration path

Recommended upgrade/downgrade migration paths in NPB mode.

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

NOTES:

- **NPB:**
  - Starting with SLX 17s.1.01 NPB feature is supported only with “Advanced feature” licence.
  - New features will that are released in SLX 17s.1.02 should be removed before downgrading to SLX 17s.1.01 release.
  - The configuration of the newly introduced feature(s) may not be retained on downgrade and upgrade to the release where the feature is introduced.

SLX 17s.1.00a to SLX 17s.1.01/02 UPGRADE

SLX 9240 revert to DEFAULT mode prior to upgrade

1. Save running-config to either local flash or remote location
2. Restore SLX 9240 with default configuration ***(note: breakout configuration will NOT be preserved)***
3. Revert SLX 9240 to DEFAULT mode.
4. Reload system
5. FWDL upgrade to SLX 17s.1.01/02
6. Install ADVANCE FEATURE license
7. Configure SLX 9240 to NPB mode.
8. Reload system
9. If the saved configuration in *Step 2* contains breakout interfaces, manually configure breakout interfaces on the appropriate ports
   a. Copy the running config to startup config
   b. Reload system
10. Perform "*copy <file> running-config*" to load the configuration saved in *Step 2*

SLX 17s.1.01/02 to SLX 17s.1.00/00a DOWNGRADE

SLX 9240 revert to DEFAULT mode prior to downgrade

1. Save running-config to either local flash or remote location
2. Restore SLX 9240 with default configuration
3. Revert SLX 9240 to DEFAULT mode.
4. Reload system
5. FWDL downgrade to SLX 17s.1.00/00a

Recommended upgrade/downgrade migration paths in default mode (non-NPB mode)

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

NOTES:

- When 17s.1.00/00a upgraded to 17s.1.02 MCT configurations are changed.
- New features will that are released in SLX 17s.1.02 should be removed before downgrading to SLX 17s.1.01 release.
- The configuration of the newly introduced feature(s) may not be retained on downgrade and upgrade to the release where the feature is introduced.

Limitations and restrictions

Compatibility and interoperability

- IP-based management cluster

Note the following changes to behavior. We no longer support the principle priority and switch over functionality as documented in the chapter "IP-Based Management Cluster" in the *Extreme SLX-OS Layer 2 Switching Configuration Guide, 17s.1.02.*

IP-based management cluster

IP-based management cluster builds logical clusters of switches over IP, to manage cluster-wide configurations and distribution services.

This feature supports two-node clustering, to support a two-node leaf architecture for IP Fabrics. A node ID is used to identify a switch in the cluster uniquely. By default the node ID is 1. If a node is part of a cluster, an attempt to change the node ID is rejected with an error message. The node ID can be changed only after the node is removed from the cluster.

A node being added to the cluster does not need to be in the default configuration, and a node rejoining the cluster can have different global configuration settings compared to the primary node. Local configuration is preserved for a rejoining node.

A principal priority can be configured, by means of the principal-priority command, to elect the principal node during cluster formation. The lower the value, the higher the priority of the node. If all nodes have the same priority, or if no priority is configured, the node with the lower ID is considered as the principal node. At any given time, a node in the management cluster is in one of the following states:

- Standalone (from the node's perspective)
- Primary (from the node's perspective)
- Connected to the cluster (online)
- Disconnected from the cluster (offline)
- Adding in progress (coming online)
- Rejoin in progress

The selection of the principal node may not always be honored. The following are the conditions for a node to become principal.

- If a node is already the principal node, it retains this status.
- If both nodes are standalone/principal nodes, then the node with the nondefault configuration becomes the principal node. The other node in the cluster must be in the default configuration.
- If, for example, Node A is aware of its peer, Node B, and Node B is not aware of Node A, then Node A becomes the principal node. This can happen if the no peer command is executed on only a single node in the cluster.
- If none of the above conditions are met—for example, both nodes (1) are standalone nodes, (2) have a nondefault configuration, and (3) are aware of each other—, then the node with the lower node-id becomes the principal node.

The Multi-Chassis Trunk (MCT) peer command is used to configure information for both of the peer nodes. The new peer is added to the cluster automatically as long as the peer is reachable through IP connectivity. Once the cluster is formed, any subsequent configuration changes on one node is propagated to the other.

The no peer command causes a controlled failover and the target node is removed permanently from the cluster. Primary and secondary controlled failover is supported, as is primary and secondary uncontrolled failover (on loss of heartbeat).

After an entire cluster is rebooted, the copy default-config startup-config command takes the entire cluster to the default state, but the node ID is preserved. (The node ID is preserved even if the database becomes corrupted.) The copy source-file startup-config command removes the management cluster configuration.

Virtual IP and IPv6 addresses can also be configured for the cluster.

The following features are not supported for IP-based management cluster:

- Clustering of nodes that have different database schema
- Global configuration from secondary nodes
- Cluster-wide firmware upgrades

Configuring an IP-based management cluster

This task configures a Multi-Chassis Trunk (MCT) peer group and configures an IP-based management cluster.

1. Enter global configuration mode and enter the cluster command to specify the name and cluster ID of an MCT (two-node) cluster.

```
device# configure terminal device(config)# cluster MCT1 1
```

The cluster name does not appear in the prompt, but it does appear in the output of the show cluster command.

2. In MCT cluster configuration mode, enter the peer command to specify an IP address.

```
device(config-cluster-1)# peer 10.10.10.12
```

3. (Optional) In global configuration mode, enter the cluster management virtual command and specify an IP address and other options as appropriate.

```
device(config)# cluster management virtual ip address 10.10.10.13/24 inband interface ve 4
```

4. (Optional) In privileged EXEC mode, enter the cluster management node-id command to change the node ID from the default (1).

```
device# cluster management node-id 20
```

5. Enter the show cluster management command to confirm the configuration.

```
device# show cluster management CLUSTER ID : 2 Management Cluster UUID : 455451fd-205f-4482-
87d4-4ed55944132c Total Number of Nodes in Cluster : 2 Node-Id Switch MAC/WWN IP Address Status
1 10:00:c4:f5:7c:50:06:2e 10.0.0.12 Co-ordinator 48 10:00:c4:f5:7c:50:06:2d 10.0.0.13 Connected
```

- **MAC rACLs:**

  - MAC rACLs are not supported, as previously documented in the section "Guidelines for rACLs" in the *Extreme SLX-OS Security Configuration Guide, 17s.1.02.*

- **ACL:**
  - Egress ACLs, Flow-Based QOS not supported on Ports and Port-Channel/MCT interfaces on SLX 9140, SLX 9240
- **ARAS**
  - Host data Collection, Ceclone backup and restore through ipv6 address is not supported.
- **IGMPv2 snooping**
  - When upgrade from 17s.100a/17s.100 to 17s.1.02, default startup query interval of 31 seconds is changed to 100sec in the running config for IGMPv2 snooping
- **IP Fabric**
  - ACLs names are case-sensitive on Management interface.
  - In rare scenarios, Ping to BGP EVPN installed prefix route host may fail, though the route is present in control plane and in hardware.
  - With Scale, traffic convergence takes long time in IP Fabric for symmetric and asymmetric scenarios.
  - IPv6 symmetric or asymmetric routing is not supported on SLX9240 platforms when used as Leaf nodes.
  - Principal election is not pre-emptive in node join scenario.
  - nsh encapsulation not supported over IPv6 neighbor.
  - BFD session does not break if there is alternate path.
  - Host route feature is not supported for IPv6 traffic (/128).
  - MCT cluster formation takes some time in forming the cluster in scale scenarios.
  - Might notice unnecessary GARP(for host address) packets seen in the network.
  - Range command is not supported for BD
  - BFD sessions may flap when the BFD interval is configured less than 300 msec.
  - Customer tagged frames cannot be passed over VXLAN tunnel.
  - Multiple flapping of CCEP ports from each nodes one after other might result in no DF elected for some VLANs. Reboot the node to recover
  - Under certain circumstances when Layer 3 protocols like OSPF are run over MCT, the session might get stuck. Workaround is to reboot the switches or clear the arp suppression cache
  - DF may not be elected on one of the MCT peers after upgrade. Work around is to do MCT no deploy/deploy
- **Layer 2**:
  - In RSTP, when native vlan is shut, convergence is affected vlan traffic when interop with cisco devices.
- **Layer3:**
  - **VRRP:**
    - "show vrrp summary" and "show ipv6 vrrp summary" will display all sessions in default vrf.
  - **BGP:**
    - Extended community filters support is not available.
- **Muticast**

    - Frame corruption might occur while performing high rate of replication with traffic flowing at line rate

- **NetConf**
    - Netconf configuration for startup-config datastore is not supported
    - Configuring multiple commands in a single request is supported for configuration/deletion of vlan, switch port, trunk port, VE and rules under IP ACL only.
    - Range is not supported.
    - Maximum 16 sessions supported.
- **NPB**:
    - When switching from NPB to default mode, the user should un-configure the following and reload the system:
        - TVF domains, NPB policy route-map, and route-map set next-hop-tvf-domain
    - When switching from default to NPB mode, the user should revert the system to default-configuration and reload the system
    - To achieve the maximum L2/L3 ACL rules, the ACLs must be applied equally among the following four port groups
        - Port Group 0: eth0/5-12
        - Port Group 1: eth0/21-28
        - Port Group 2: eth0/1-4 and eth0/13-16
        - Port Group 3: eth0/17-20 and eth0/29-32
    - With 4k TVF/route-maps scale, system takes longer time to load on config replay.
    - IPv6 GTP packets are not supported for NPB L3 ACL filtering or GTP HTTPS filtering
    - Q-in-Q (802.1ad / 0x88A8) is not supported for the NPB VLAN stripping feature
- **Overlay Transit Service**
    - Configuration download to startup and reload with 256 overlay class map each having 1024 rules takes 1 hours 40 minutes approximately
- **Platform**:
    - **DIAG:**
        - Diag related commands work only under /offline_diag directory.
        - Diag portloopbacktest with exeternal loopback plug is not supported on SLX9240 platform.
- **Port Mirroring (SPAN)**
    - Only Flow based SPAN supported for port channel. Member ports of port channel can be enabled with port SPAN.
    - Deny rules in service ACL is pass through in Flow based QoS. Only permit rules with SPAN action will result in Flow based mirroring
    - In class map if SPAN action coexists with QOS action (e.g. DSCP marking which results in frame editing), original packet will be mirrored and not reflect the frame editing done as per the QOS action.
- **Port-Security:**
    - OUI Mac Addresses are not supported.

- **PTP**
  - Rest API operational-state GET will not correctly display the output of the following PTP "show" commands:
    - show ptp clock foreign-masters record
    - show ptp corrections
  - No REST API URL for “show ptp port-interface Ethernet|port-channel”
- **QOS:**
  - **FB QoS - Cos Marking, DSCP Marking, Sflow, SPAN**
    - SPAN with L2 ACL in egress direction (SLX 9240)
    - Flow-based QoS is not supported in egress direction
  - **QoS – WRED**
    - Byte counter is not available as part of show qos red statistics CLI for port-channel
  - **QoS – Pause/PFC/Buffer Management**
    - PFC and Flow-control statistics are not supported due to hardware limitation
    - Max allowed tx buffer in SLX9140 is 3000 and not 8000.
- **REST API**
  - REST configuration for startup-config datastore is not supported.
  - Only one command can be configured with one REST request. Configuring multiple commands in a single request is not supported.
  - Pagination and Range is not supported.
  - Maximum 30 sessions are supported.
  - in-band with user-defined vrf and default-vrf not supported
- **REST API/NetConf Operational-state calls**
  - HTTP Status throw message “501 Not Implemented” while trying to get operational state for top resource (rest/operational-state) using REST API, User can query operational-state at feature level.
  - Operational-state calls not supported for Overlay GW and Visibility Services features.
  - Yang files for Unsupported features like MPLS, ISIS are available and operational-state call returns empty value or “404 not found ”
  - Operational-state calls for supported feature mat not be accurate and may return “404 not found ” or empty value, not advisable to use it
- **Security:**
  - Login authentication service (aaa authentication login cli):
    - With “local” option specified as secondary authentication service, local authentication will be tried only when the primary authentication service -(TACACS+/RADIUS/LDAP) is either unreachable or not available.
    - When login authentication configuration is modified, the user sessions are not logged out. All connected user sessions can be explicitly logged out using “clear sessions” CLI.
  - ACLs are not supported for egress traffic flows on management interfaces.
  - Configuring TACACS+ or RADIUS without a key is not supported. If no key is configured, the switch uses a default key of “sharedsecret”. If the specific vrf is not mentioned, mgmt.-vrf will be taken as default.

    - There is a possibility that locked user accounts will get unlocked after a reboot if the running-config (before reboot) is different from startup-config of user accounts.
    - Encrypted text (taken from running-config of any user account password with encryption turned on) should not be used as input for clear-text password for the same user. This may result in login failure of the user subsequently.
- **sFlow**
    - If Port based and flow based sflow is enabled on an interface, Port based sflow takes effect
    - Flow-based Sflow is not supported on port-channel and its member ports
    - Port-based Sflow not supported on port-channel but supported on member ports
    - There will be no counter samples when only flow based sampling is enabled.
    - When multiple sampling rates are applied on an interface through multiple class-maps, the lowest sample-rate will take the effect.
- **SNMP**
    - Warning messages while loading MIBs
    - Certain MIB browsers may show warning messages while loading MIBs when dependent MIB is already not loaded. For example, in RFC 3289 MIB, DIFFSERV-MIB module has dependency on INTEGRATED-SERVICES-MIB module which is defined in the same RFC. However, DIFFSERV-MIB occurs first in the file and hence may throw a warning since INTEGRATED-SERVICES-MIB is not loaded yet. It should not be an issue as long as the MIB objects show up in the MIB browser. To avoid the warning, place the dependent MIB module file in the same folder with name as <MIB MODULE>.mib or <MIB MODULE>.my (ex: INTEGRATED-SERVICES-MIB.mib) …”
- **Telemetry Streaming**
    - Running gRPC server on non-default port not supported.
- **Traffic:**
    - On the Extreme SLX 9140 and SLX 9240 switches, traffic destined to 128.0.0.0/16 block is dropped.
    - Hash collisions may be observed with higher scale in Route, ARP/Mac and/or Tunnel tables resulting in entries not getting programmed.

Defects

TSBs—Critical issues to consider prior to installing this release

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

TSB issues resolved in SLX-OS 17s.1.02b

TSB	Summary
None	

TSB issues outstanding in SLX-OS 17s.1.02b

TSB	Summary
None	

Closed with code changes for SLX-OS v17s.1.02b

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of 06/11/2018 in SLX-OS v17s.1.02b.

Defect ID:	DEFECT000643147		
Technical Severity:	High	**Probability:**	Low
Product:	Brocade SLX-OS	**Technology Group:**	Software Installation & Upgrade
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Management
Symptom:	Observe "NOT A KNOWN ResourceId" error message		
Condition:	When user tries to make configuration updates before ZTP process is complete.		
Workaround:	Do not perform configuration changes until "ZTP Complete" message is seen.		
Recovery:	Disable ZTP with "dhcp ztp cancel" and reboot the switch.		

Defect ID:	DEFECT000645409		
Technical Severity:	High	**Probability:**	Medium
Product:	Brocade SLX-OS	**Technology Group:**	MCT - Multi-Chassis Trunking
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Layer 2 Switching
Symptom:	SLX OS commands do not respond when executed immediately after Cluster management principal switch over		
Condition:	After "cluster management principal switchover" command is issued and immediately a "show cluster management" command is issued on the non-principal peer node.		
Workaround:	Do not immediately issue any SLX OS Commands on peer node that will become the new principal co-ordinator after a "cluster management principal switchover" command has been issued.		
Recovery:	Reloading the switch.		

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

Defect ID:	DEFECT000649300		
Technical Severity:	Medium	**Probability:**	Medium
Product:	Brocade SLX-OS	**Technology Group:**	Configuration Fundamentals
Reported In Release:	SLXOS 17s.1.00	**Technology:**	Management
Symptom:	Netconf rpc call for get_config failed to complete and gets terminated unexpectedly. The netconf session is closed. Error indicates, message-id="urn:uuid:41501bb0-6397-11e7-b49f-f46d04e37122"<INFO> 7-Jul-2017::22:39:22.568 SLX9240-1 confd[2578]: netconf id=52 get-config source=running attrs: message-id="urn:uuid:41501bb0-6397-11e7-b49f-f46d04e37122"<INFO> 7-Jul-2017::22:39:22.573 SLX9240-1 confd[2578]: netconf id=52 sending rpc-reply, attrs: message-id="urn:uuid:41501bb0-6397-11e7-b49f-f46d04e37122"<INFO> 7-Jul-2017::22:39:32.534 SLX9240-1 confd[2578]: netconf id=52 couldn't retrieve all data from the data providers, closing session		
Condition:	netconf rpc call for get_config		

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

Defect ID:	DEFECT000652663		
Technical Severity:	Medium	**Probability:**	Low
Product:	Brocade SLX-OS	**Technology Group:**	MCT - Multi-Chassis Trunking
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Layer 2 Switching
Symptom:	"show mac-address-table" output incorrectly showing dynamically learnt cluster MAC as "Dynamic" MAC.		
Condition:	On the Cluster Edge ports, MACs learnt on the vlan or bridge domain that is added to an EVPN instance will be displayed as "Dynamic" MAC instead of "Dynamic-CL" MAC in the "show mac-address-table" CLI output.		

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

Defect ID:	DEFECT000653439		
Technical Severity:	High	**Probability:**	Low
Product:	Brocade SLX-OS	**Technology Group:**	MCT - Multi-Chassis Trunking
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Layer 2 Switching
Symptom:	Unexpected reload		
Condition:	When we swap the node ids and rejoin		

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

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

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

Defect ID:	DEFECT000655155		
Technical Severity:	High	**Probability:**	High
Product:	Brocade SLX-OS	**Technology Group:**	VXLAN - Virtual Extensible LAN
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Layer 2 Switching
Symptom:	Invalid dynamic MAC count value displayed in REST API call to show bridge-domain brief command.		
Condition:	If dynamically learnt MAC count exceeds 4096, the REST API always returns 4096 as the count.		

Defect ID:	DEFECT000655470		
Technical Severity:	High	**Probability:**	High
Product:	Brocade SLX-OS	**Technology Group:**	MCT - Multi-Chassis Trunking
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Layer 2 Switching
Symptom:	MCT cluster formation may fail		
Condition:	Changing cluster management node-id may cause cluster formation to fail.		

Defect ID:	DEFECT000655496		
Technical Severity:	High	**Probability:**	Low
Product:	Brocade SLX-OS	**Technology Group:**	VXLAN - Virtual Extensible LAN
Reported In Release:	SLXOS 18s.1.00	**Technology:**	Layer 2 Switching
Symptom:	Switch may reload unexpectedly during boot-up process.		
Condition:	hardware profile overlay-visibility tunnel-vni configuration may result in unexpected reload during boot up process		

Defect ID:	DEFECT000656564		
Technical Severity:	High	**Probability:**	High
Product:	Brocade SLX-OS	**Technology Group:**	MCT - Multi-Chassis Trunking
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Layer 2 Switching
Symptom:	MAC addresses may not get learnt on the switch		
Condition:	When STP is enabled on the interfaces MAC learning may be impacted.		

Defect ID:	DEFECT000657391		
Technical Severity:	High	**Probability:**	High
Product:	Brocade SLX-OS	**Technology Group:**	VXLAN - Virtual Extensible LAN
Reported In Release:	SLXOS 17r.2.00	**Technology:**	Layer 2 Switching
Symptom:	If (a) the nodes of management cluster are segmented and (b) the existing overlay-gateway is deleted on one of the nodes, then the subsequent node rejoins will fail.		
Condition:	If (a) the nodes of management cluster are segmented and (b) the existing overlay-gateway is deleted on one of the nodes		

Defect ID:	DEFECT000658019		
Technical Severity:	Medium	**Probability:**	High
Product:	Brocade SLX-OS	**Technology Group:**	CLI - Command Line Interface
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Management
Symptom:	Privilege level CLI commands are being displayed to all unprivileged users.		
Condition:	Unprivileged users may be able to access privileged CLI commands.		

Defect ID:	DEFECT000658190		
Technical Severity:	High	**Probability:**	High
Product:	Brocade SLX-OS	**Technology Group:**	VXLAN - Virtual Extensible LAN
Reported In Release:	SLXOS 17r.2.00	**Technology:**	Layer 2 Switching
Symptom:	If (a) the nodes of management cluster are segmented, (b) BGP-EVPN created vxlan tunnel exists with a destination ip IP1, on one of the nodes (c) static vxlan tunnel is created with a destination ip IP1, on the same node, then the subsequent node rejoins will fail.		
Condition:	If (a) the nodes of management cluster are segmented, (b) BGP-EVPN created vxlan tunnel exists with a destination ip IP1, on one of the nodes (c) static vxlan tunnel is created with a destination ip IP1, on the same node,		

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

Defect ID:	DEFECT000659616		
Technical Severity:	Medium	**Probability:**	Low
Product:	Brocade SLX-OS	**Technology Group:**	ARP - Address Resolution Protocol
Reported In Release:	SLXOS 18s.1.00	**Technology:**	Layer 3 Routing/Network Layer
Symptom:	ARP does not get learnt on the switch.		
Condition:	Reloading the switch may result in ARP learn failure on DAI enabled VLANs.		

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

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

Defect ID:	DEFECT000660883		
Technical Severity:	Medium	**Probability:**	High
Product:	Brocade SLX-OS	**Technology Group:**	VXLAN - Virtual Extensible LAN
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Layer 2 Switching
Symptom:	Conversational MAC ageing time will show an ageing value of "1800" after un-configuring the configured conversational MAC ageing time.		
Condition:	After removing the configured conversational MAC ageing time using the CLI command "no mac-address-table aging-time conversational", the ageing timer will show a value of "1800" when observed through the "show running-config [mac-address-table]" CLI command.		

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

Defect ID:	DEFECT000661115		
Technical Severity:	High	**Probability:**	High
Product:	Brocade SLX-OS	**Technology Group:**	MCT - Multi-Chassis Trunking
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Layer 2 Switching
Symptom:	Multi Chassis Trunking management cluster may not be up on an Multi Chassis Trunking network involving SLX 9140 or SLX 9240.		
Condition:	Multi Chassis Trunking management cluster may fail to come up when the Multi Chassis Trunking source IP (used as the peer IP on the remote node) is changed from IP_address1 to IP_address2 and back to IP_address1.		
Workaround:	Avoid changing Multi Chassis Trunking source IP address during the life of the Multi Chassis Trunking cluster.		
Recovery:	SLX switch may have to be reloaded if the same source IP which was configured earlier has to be used again.		

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

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

Known Issues for SLX-OS v17s.1.02b

This section lists open software defects with Critical, High, and Medium Technical Severity as of 06/19/18 in SLX-OS 17s.1.02b.

Defect ID:	DEFECT000662742		
Technical Severity:	High	**Probability:**	High
Product:	Brocade SLX-OS	**Technology Group:**	Layer 3 Routing/Network Layer
Reported In Release:	SLXOS 17s.1.02	**Technology:**	Static Routing (IPv4)
Symptom:	Unexpected termination of Dcmd software daemon may occur along with the message “"Error: failed to create path - application communication failure" when applying the VRF configuration "route-target import <value> evpn" or "route-target export <value> evpn".		
Condition:	Unexpected termination of Dcmd software daemon may happen when the VRF configuration "route-target import <value> evpn" or "route-target export <value> evpn" is done incorrectly without the "evpn" keyword via any non-CLI based management interface such as Netconf and if the exact same configuration is applied via the CLI.		
Workaround:	Ensure to include the "evpn" keyword when performing VRF configuration "route-target import <value> evpn" or "route-target export <value> evpn" through any of the available management interfaces.		