

28 September 2017



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

Release Notes v1.0

© 2017 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, and MyBrocade are registered trademarks of Brocade Communications Systems, Inc., in the United States and in other countries. Other brands, product names, or service names mentioned of Brocade Communications Systems, Inc. are listed at www.brocade.com/en/legal/brocade-Legal-intellectual-property/brocade-legal-trademarks.html. Other marks may belong to third parties.

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	4
Preface	5
Contacting Brocade Technical Support.....	5
Related documentation	5
Document feedback.....	6
Overview	7
Software Features.....	7
Important Notes.....	13
Documentation supporting SLX-OS.....	15
RFCs and Standards.....	17
Hardware support.....	19
Software upgrade and downgrade	22
Limitations and restrictions	25
Defects	29

Document history

Version	Summary of changes	Publication date
1.0	Initial Release	September 28, 2017

Preface

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online or by telephone. Brocade OEM Customers should contact their OEM/solution provider.

Brocade Customers

For product support information and the latest information on contacting the Technical Assistance Center, go to www.brocade.com and select Support.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone
Preferred method of contact for non-urgent issues: <ul style="list-style-type: none">• My Cases through MyBrocade• Software downloads and licensing tools• Knowledge Base	Required for Sev 1-Critical and Sev 2-High issues: <ul style="list-style-type: none">• Continental US: 1-800-752-8061• Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33)• For areas unable to access toll free number: +1-408-333-6061• Toll-free numbers are available in many countries.

Brocade OEM Customers

If you have purchased Brocade product support from a Brocade OEM/solution provider, contact your OEM/solution provider for all of your product support needs.

- OEM/solution providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/solution provider.

Related documentation

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

White papers, data sheets, and the most recent versions of Brocade software and hardware manuals are available at www.brocade.com.

Product documentation for all supported releases is available to registered users at MyBrocade. Click the Support tab and select Document Library to access documentation on MyBrocade or www.brocade.com. You can locate documentation by product or by operating system.

Release notes are bundled with software downloads on MyBrocade. Links to software downloads are available on the MyBrocade landing page and in the Document Library.

Document feedback

Quality is our first concern at Brocade, 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:

- Through the online feedback form in the HTML documents posted on www.brocade.com
- By sending your feedback to documentation@brocade.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

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 Brocade 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 network 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. When LFS is ignored on the RX side of a port, an egress port will remain UP, even if there is no fiber connected to the RX side.
Symmetric load balancing	The ability to specify which packets are distributed to the same egress port when load balancing packets among ports in 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 8021Q 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

Brocade® 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 Brocade open data center design stack elements, Brocade 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 addresses
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. Brocade SLX Visibility Services

Brocade 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 Brocade 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 Brocade 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 Brocade SLX 9140 includes Brocade 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 Brocade 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 Brocade 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 Packet 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	
<ul style="list-style-type: none"> • 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) 	<ul style="list-style-type: none"> • 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 extension tunnels • Overlay services: overlay gateway instances, overlay transit instances (on spine nodes) • Link-fault signaling • IP-based management cluster
Layer 3 Routing	
<ul style="list-style-type: none"> • Border Gateway Protocol (BGP4+) • DHCP Helper • Layer 3 ACLs • OSPF v2/v3 • Static routes • IPv4/v6 ACL • Route Policies • Bidirectional Forwarding Detection (BFD) 	<ul style="list-style-type: none"> • 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

<ul style="list-style-type: none"> • 32-Way ECMP • VRF Lite • VRF-aware OSPF, BGP, VRRP, static routes • VRRP v2 and v3 • Anycast Gateway over VxLAN 	<ul style="list-style-type: none"> • 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	
<ul style="list-style-type: none"> • gRPC Streaming protocol and API • REST API with YANG data model • Python 	<ul style="list-style-type: none"> • PyNOS libraries • DHCP automatic provisioning • NETCONF API
Quality of Service	
<ul style="list-style-type: none"> • 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) 	<ul style="list-style-type: none"> • 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	
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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	
<ul style="list-style-type: none"> • Port-based Network Access Control 802.1X • RADIUS – Authentication and Authorization • AAA • TACACS+ • Secure Shell (SSHv2) • TLS 1.1, 1.2 • HTTP/HTTPS 	<ul style="list-style-type: none"> • BPDU Drop • Lightweight Directory Access Protocol (LDAP) • Secure Copy Protocol • Control Plane Protection • LDAP/AD • SFTP • Port Security

IP Fabric	
<ul style="list-style-type: none"> • Controllerless Network Virtualization (BGP-EVPN) • ARP suppression • Conversational ARP • Static Anycast Gateway 	<ul style="list-style-type: none"> • Logical VTEP (Static and EVPN) • IP Un-numbered interface • No Traffic Tromboning. • RIOT (Routing In and Out of Tunnel) (v4 and v6)
Platform	
<ul style="list-style-type: none"> • 25G AN/LT • Insight interface (10G analytic path in SLX9140) • 1G/10G/25G/40G/100G Auto speed detection • Multi Speed(1G/10G) Optic Support 	<ul style="list-style-type: none"> • Digital Optical Monitoring(DOM)
NPB	
<ul style="list-style-type: none"> • Traffic aggregation • Traffic replication (via TVF – transparent VLAN flooding) • L2-L4 (via L2/L3 ACL matched route-map) • Load-balancing (hash-based) 	<ul style="list-style-type: none"> • VLAN Stripping • Symmetric load balance • GTP-tunneled HTTPS filtering³ • Link Fault Signaling (LFS)management⁴

Important Notes

Advanced Features SAU License

The SAU license enables the advanced licensed features prior to purchasing a license. On the Brocade SLX 9240 and Brocade 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 Brocade SLX 9240 and Brocade 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.

³ Beta

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

- 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 interfaces: 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 interfaces: 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 interfaces: 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 most recent versions of Brocade software manuals and hardware manuals are available on the mybrocade.com website.

DOCUMENTATION ON MYBROCADE.COM

1. Log into mybrocade.com
2. Go to the documentation tab.
3. Under Product Manuals, from the “downloaded by” drop down box, select SLX Operating System (SLX OS).
4. Select your publication.

The following lists the documentation supporting this release:

- Brocade SLX-OS Command Reference, 17s.1.02
- Brocade SLX-OS IP Fabrics Configuration Guide, 17s.1.02
- Brocade SLX-OS IP Multicast Configuration Guide, 17s.1.02
- Brocade SLX-OS Layer 2 Switching Configuration Guide, 17s.1.02
- Brocade SLX-OS Layer 3 Routing Configuration Guide, 17s.1.02
- Brocade SLX-OS Management Configuration Guide, 17s.1.02
- Brocade SLX-OS MIB Reference, 17s.1.02
- Brocade SLX-OS Monitoring Configuration Guide, 17s.1.00
- Brocade SLX-OS Network Packet Broker Configuration Guide, 17s.1.02
- Brocade SLX-OS QoS and Traffic Management Configuration Guide, 17s.1.02
- Brocade SLX-OS REST API, 17s.1.02
- Brocade SLX-OS NetCONF, 17s.1.02
- Brocade SLX-OS YANG, 17s.1.02
- Brocade SLX-OS Security Configuration Guide, 17s.1.02
- Brocade SLX-OS Software Licensing Guide, 17s.1.02

- Brocade SLX 9140 Switch Hardware Installation Guide
- Brocade SLX 9140 Switch Technical Specifications
- Brocade SLX 9240 Switch Hardware Installation Guide
- Brocade SLX 9240 Switch Technical Specifications

RFCs and Standards

Brocade SLX 9140, 9240 Specifications

IEEE Compliance		
Ethernet	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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) 	<ul style="list-style-type: none"> • 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

	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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	Brocade SLX 9140-48V Switch AC with Front to Back airflow 48x25GE/10GE/1GE + 6x100GE/40GE
BR-SLX-9140-48V-DC-F	Brocade SLX 9140-48V Switch DC with Front to Back airflow 48x25GE/10GE/1GE + 6x100GE/40GE
BR-SLX-9140-48V-AC-R	Brocade SLX 9140-48V Switch AC with Back to Front airflow 48x25GE/10GE/1GE + 6x100GE/40GE
BR-SLX-9140-48V-DC-R	Brocade SLX 9140-48V Switch DC with Back to Front airflow 48x25GE/10GE/1GE + 6x100GE/40GE
BR-SLX-9240-32C-AC-F	Brocade SLX 9240-32C Switch AC with Front to Back airflow 32x100GE/40GE
BR-SLX-9240-32C-DC-F	Brocade SLX 9240-32C Switch DC with Front to Back airflow 32x100GE/40GE
BR-SLX-9240-32C-AC-R	Brocade SLX 9240-32C Switch AC with Back to Front airflow 32x100GE/40GE
BR-SLX-9240-32C-DC-R	Brocade 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 Brocade, refer to the latest version of the Brocade Optics Family Data Sheet available online at www.brocade.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)	40G-QSFP-C-0101	58-0000033-01
40GE QSFP to QSFP 3M Cable(Passive)	40G-QSFP-C-0301	58-0000034-01

40GE QSFP to QSFP 5M Cable(Passive)	40G-QSFP-C-0501	58-0000035-01
4x10GE QSFP+ to 4 SFP+ Active copper cable - 1m	40G-QSFP-4SFP-C-0101	58-0000051-01
4x10GE QSFP+ to 4 SFP+ Active copper cable - 3m	40G-QSFP-4SFP-C-0301	58-0000052-01
4x10GE QSFP+ to 4 SFP+ Active copper cable - 5m	40G-QSFP-4SFP-C-0501	58-0000053-01
40GE QSFP to QSFP cable - 10m AOC	40G-QSFP-QSFP-AOC-1001	57-1000306-01
100GE QSFP28 SR4	100G-QSFP28-SR4	57-1000326-01
100GE QSFP28 LR4 (3.5W)	100G-QSFP28-LR4-LP-10KM	57-1000338-01
100GE QSFP28 CWDM	100G-QSFP28-CWDM4-2KM	57-1000336-01
100G QSFP-28 Active Optical (10m)	100G-QSFP-QSFP-AOC-1001	57-1000347-01

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.

Software upgrade and downgrade

Image file names

Download the following images from www.brocade.com.

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

Migration path

Recommended upgrade/downgrade migration paths in NPB mode.

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

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

- **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**
 - Route leak prefixes show as Best Routes (BE) in BGP VRF even after the L3 VNI VLAN and VEs are deleted.
 - 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.
 - "LeakArp" ARP entries are not cleared after removing leaked static route and doing "clear arp no-refresh"
 - With Scale, traffic convergence takes long time in IP Fabric for symmetric and asymmetric scenarios.
 - After delete and add the vlan to vni mapping for L3 VNI, Tunnel membership is not established for these L3VNI.
 - In IP Fabric, L3 ECMP is not supported over IP-Unnumbered uplink.
 - IP MTU is not honored on the VE interfaces.
 - In some occurrences, Inclusive Multicast Routes (IMR) getting filtered after remove/add evpn config on one of the MCT node causing traffic loss.
 - In some scenarios, BFD process restarted on MCT node while flapping loopback interface
 - 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).
 - When IPv6 address and static anycast address configured on the interface, some IPv6 ND entries are not advertised to evpn peer.
 - 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

- If a MAC is learnt on a CEP port on a local VLAN and latter if the VLAN is extended across the tunnel, the MAC will continue show Dynamic. Clear the MAC address to update with the new flag – Dynamic CL
- 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.
- **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 external 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 may 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 Brocade SLX 9140 and SLX 9240, 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. On <http://my.brocade.com> (sign-in required) this product documentation can be found by selecting **Support > Document Library** then under **Explore by Content Type** select **View All > Technical Service Bulletin** (note that TSBs are generated for all Brocade platforms and products, so not all TSBs apply to this release).

TSB issues resolved in SLX-OS 17s.1.02

TSB	Summary
None	

TSB issues outstanding in SLX-OS 17s.1.02

TSB	Summary
None	

Closed with code changes for SLX-OS v17s.1.02

This section lists software defects with Critical, High, and Medium Technical Severity closed with a code change as of September 28, 2017 in SLX-OS v17s.1.02.

Defect ID: DEFECT000610503	
Technical Severity: High	Probability: High
Product: Brocade SLX-OS	Technology Group: Monitoring
Reported In Release: SLXOS 17s.1.02	Technology: Hardware Monitoring
Symptom: Transceiver field under 'show media' command sometime shows invalid data.	
Condition: The issue is seen only when running 'show media' command on an interface with 100Gbps speed supported optics inserted.	

Defect ID: DEFECT000625516	
Technical Severity: Medium	Probability: Medium
Product: Brocade SLX-OS	Technology Group: Layer 3 Routing/Network Layer
Reported In Release: SLXOS 17s.1.02	Technology: IPv6 Addressing
Symptom: SNMP Trap is not generated for a VE interface 'no shut' operation.	
Condition: "no shut" command is issued on a VE interface.	
Recovery: Issue a "shut", "no shut" command for the VE interface.	

Defect ID: DEFECT000630360	
Technical Severity: High	Probability: Medium
Product: Brocade SLX-OS	Technology Group: Security
Reported In Release: SLXOS 17s.1.02	Technology: ACLs - Access Control Lists
Symptom: Applying "permit ipv6 any any" ipv6 access-list on management interface blocks all incoming management traffic (telnet,ssh, ntp etc.)	
Condition: When IPv6 ACL with "permit ipv6 any any" rule applied on management interface.	
Workaround: Work around is to have permit rule for each of the application ports SLX(conf-ip6acl-ext)# do show running-config ipv6 access-list ipv6 access-list extended 456 seq 30 permit udp any eq ntp any seq 40 permit tcp any eq telnet any seq 50 permit tcp any eq 22 any seq 60 permit ipv6 any any	

Defect ID: DEFECT000634550	
Technical Severity: High	Probability: High
Product: Brocade SLX-OS	Technology Group: Layer 2 Switching
Reported In Release: SLXOS 17s.1.02	Technology: VLAN - Virtual LAN
Symptom: Traffic on VLAN 1 on a logical interface with BD enabled MAC's will not be learnt or flooded.	
Condition: When user tries to change the switchport mode from "switchport mode trunk-no-default-native" to "switchport mode trunk mode".	
Recovery: Do "no switchport", "switchport" on that interface.	

Closed without code changes for SLX-OS v17s.1.02

This section lists software defects with Critical, High, and Medium Technical Severity closed without a code change as of September 28, 2017 in SLX-OS v17s.1.02.

Defect ID: DEFECT000629903	Technical Severity: Medium
Reason Code: Will Not Fix	Probability: Low
Product: Brocade SLX-OS	Technology Group: Layer 3 Routing/Network Layer
Reported In Release: SLXOS 17s.1.02	Technology: VRRPv3 - Virtual Router Redundancy Protocol Version 3
Symptom: Port-channel could not be added as the track interface to an IPv6 VRRPE session	
Condition: Through a NETCONF session adding a track interface to an IPv6 VRRPE session would not be possible.	
Workaround: Use CLI to do this configuration.	

Defect ID: DEFECT000631502	Technical Severity: Medium
Reason Code: Will Not Fix	Probability: Medium
Product: Brocade SLX-OS	Technology Group: Management
Reported In Release: SLXOS 17s.1.02	Technology: SNMP - Simple Network Management Protocol
Symptom: The objects tcpConnectionLocalAddress and tcpConnectionRemAddress which are INDICES to the table tcpConnectionTable show up in reverse order when queried as part of the objects in this table.	
Condition: This is limited to objects tcpConnectionLocalAddress and tcpConnectionRemAddress in the tcpConnectionTable	

Defect ID: DEFECT000634943	Technical Severity: High
Reason Code: Will Not Fix	Probability: Medium
Product: Brocade SLX-OS	Technology Group: Layer 2 Switching
Reported In Release: SLXOS 17s.1.02	Technology: VLAN - Virtual LAN
Symptom: Response to 'show -config' command will be slow	
Condition: Response to 'show running-config' command will be slow when (a) snmpwalk, (b) telemetry streaming and (c) REST API running in parallel	
Workaround: Stop REST API temporarily while running 'show running-config' through CLI	

Defect ID: DEFECT000634975	Technical Severity: High
Reason Code: Not Reproducible	Probability: Medium
Product: Brocade SLX-OS	Technology Group: Layer 3 Routing/Network Layer
Reported In Release: SLXOS 17s.1.02	Technology: IP Addressing
Symptom: Under conditions of multi dimensional scale and deleting interfaces, routing component (ribmgr) may run out of memory with error messages (5066 failed to refresh). System may become non responsive.	
Condition: Deleting interface under conditions of multi dimensional scale	

Known issues for SLX-OS v17s.1.02

This section lists open software defects with Critical, High, and Medium Technical Severity closed with a code change as of September 28, 2017 in SLX-OS v17s.1.02.

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

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

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

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

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

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

Defect ID: DEFECT000643147	
Technical Severity: High	Probability: Low
Product: Brocade SLX-OS	Technology Group: Management
Reported In Release: SLXOS 17s.1.02	Technology: Software Installation & Upgrade
Symptom: Observe "N O T A K N O W N R e s o u r c e I d" error message	
Condition: 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: DEFECT000643184	
Technical Severity: High	Probability: High
Product: Brocade SLX-OS	Technology Group: Security
Reported In Release: SLXOS 17s.1.02	Technology: RADIUS
Symptom: After reload, the user role mapped with RADIUS of the existing users can't be modified.	
Condition: Modifying user role is not allowed after switch reload.	
Workaround: Remove user and reconfigure.	

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

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

Defect ID: DEFECT000645409	
Technical Severity: High	Probability: Medium
Product: Brocade SLX-OS	Technology Group: Layer 2 Switching
Reported In Release: SLXOS 17s.1.02	Technology: MCT - Multi-Chassis Trunking
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: DEFECT000645964	
Technical Severity: Medium	Probability: Medium
Product: Brocade SLX-OS	Technology Group: Management
Reported In Release: SLXOS 17s.1.02	Technology: Configuration Fundamentals
Symptom: When configuring timestamp on a range of interfaces, only the first interface in the range is being configured.	
Condition: Configure timestamp configuration on a range of interfaces	
Workaround: Configure timestamp on an individual port basis.	
Recovery: Configure timestamp on an individual port basis.	

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

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

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

Defect ID: DEFECT000646799	
Technical Severity: High	Probability: Medium
Product: Brocade SLX-OS	Technology Group: Layer 3 Routing/Network Layer
Reported In Release: SLXOS 17s.1.02	Technology: DHCP - Dynamic Host Configuration Protocol
Symptom: DHCP client relay frames are dropped in the switch.	
Condition: When both DHCP L2 relay and L3 relay is configured on the switch.	

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

Defect ID: DEFECT000647507	
Technical Severity: High	Probability: Medium
Product: Brocade SLX-OS	Technology Group: Monitoring
Reported In Release: SLXOS 17s.1.02	Technology: Hardware Monitoring
Symptom: "show optical monitoring" command displays TX Power as 0 instead of N/A.	
Condition: "show optical monitoring" command displays TX Power as 0 instead of N/A.	
Workaround: "show media interface" displays correctly as N/A	

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

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

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

Defect ID: DEFECT000649255	
Technical Severity: High	Probability: Low
Product: Brocade SLX-OS	Technology Group: Layer 2 Switching
Reported In Release: SLXOS 17s.1.02	Technology: MCT - Multi-Chassis Trunking
Symptom: "show mac-address-table conversational linecard 0" displays MAC addresses on internal VlanId 8184.	
Condition: With "Conversational Learning Mode" enabled and unconfiguring a range of VLANs.	
Workaround: Macs learnt will automatically age-out or run the command "clear mac-address-table conversational linecard 0"	

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

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

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

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

Defect ID: DEFECT000651174	
Technical Severity: High	Probability: High
Product: Brocade SLX-OS	Technology Group: Layer 3 Routing/Network Layer
Reported In Release: SLXOS 17s.1.02	Technology: BGP4 - IPv4 Border Gateway Protocol
Symptom: Few entries (ARP, MAC, Tunnel and IP/IPv6) may not be added to HW table due to hash collisions.This may result in traffic drop/flood and/or high CPU usage.	
Condition: When Scale (ARP, MAC, Tunnel and IP/IPv6) reaches above 80%, depending on the input data set we may see hash collisions.	

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

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

Defect ID: DEFECT000652763	
Technical Severity: High	Probability: Medium
Product: Brocade SLX-OS	Technology Group: Layer 2 Switching
Reported In Release: SLXOS 17s.1.02	Technology: VLAN - Virtual LAN
Symptom: REST operational-state query on tvf-domain-list-state does not return all instances of interfaces added for a tvf_domain.	
Condition: REST operational-state query on tvf-domain-list-state	
Workaround: Use CLI command "show tvf-domain brief"	

Defect ID: DEFECT000652870	
Technical Severity: Medium	Probability: High
Product: Brocade SLX-OS	Technology Group: Monitoring
Reported In Release: SLXOS 17s.1.02	Technology: OAM - Operations, Admin & Maintenance
Symptom: "link-fault-signaling counter" statistics are not cleared with "clear counter all".	
Condition: "clear counter all" does not clear "link-fault-signaling counter" statistics.	

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

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

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

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

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

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