Extreme™
Customer-Driven Networking

Data Sheet

Highlights

Stats

- Transform complex network data into clinical-centric, actionable information
- Centralize and simplify the definition, management, and enforcement of policies such as medical devices and guest access
- Easily integrate with clinical apps with Software Defined Networking

Operational Efficiency

- Reduce IT administrative effort with the automation of routine tasks and web-based dashboard
- Streamline management with the integration of wired and wireless networks
- Easily enforce policies network-wide for QoS, bandwidth, etc.
- Troubleshoot with the convenience of a smart phone or tablet
- Integrate with enterprise management platforms

Security

- Protect patient data with centralized monitoring, control, and real-time response
- Enhance existing investments in network security
- Preserve LAN/WLAN network integrity with unified policies

Service and Support

- Industry-leading first call resolution rates and customer satisfaction rates
- Personalized services, including site surveys, network design, installation, and training

BUILT ON BROADCOM

ExtremeRouting™ SLX® 9640

Next Generation Fixed Router to Simplify the Core and Scale the Internet Border and Interconnect

With cloud services, 4K HD video streaming, Internet of Things (IoT), and mobile connectivity for billions of devices becoming standard, organizations must modernize the way they communicate and conduct business. Increasingly organizations are expanding from on premise, private and hybrid cloud to full multi-cloud architectures to address agility, scale, security, reliability and cost requirements as digital transformation reshapes their business environment.

To succeed in the digital era, organizations need network platforms with the adaptability to address these rapidly evolving demands and enable them to simplify and scale operations while driving out cost. Such platforms deliver innovative software optimized with programmable hardware to analyze and automate network operations, thereby reducing OpEx, and provide flexible deployment options with forwarding performance and scale to dramatically reduce CapEx.

An Adaptable Internet-scale Routing Platform

The ExtremeRouting SLX 9640 is designed to cost-effectively deliver the scale and performance needed to address the explosive growth in network bandwidth, devices, and services—today and well into the future. This flexible platform, powered by Extreme SLX-OS, provides carrier-class advanced features that leverage proven Extreme routing, MPLS, Carrier Ethernet, and VXLAN overlay technology currently deployed in the most demanding service provider, data center, and enterprise networks. And it is all delivered through space- and power-efficient forwarding hardware.

The flexible architecture is designed for optimal operations, supporting diverse deployment options—such as Internet border, collapsed border routing and data center interconnect, and network packet broker aggregation deployments—that require deep buffering for lossless forwarding, advanced MPLS, Carrier Ethernet features or VXLAN network virtualization overlays, and greater bandwidth. In addition, the SLX 9540 helps address the increasing agility and analytics needs of digital organizations with innovative network automation and visibility, capabilities enabled through Extreme Workflow Composer™ with turnkey automation suites and the Extreme SLX Insight Architecture.

Flexible Border Routing with Internet Route Scale, Ultra-Deep Buffers, MPLS and EVPN

The SLX 9640 is the industry's most powerful compact deep buffer Internet border router, providing a cost-efficient solution that is purpose-built for the most demanding service provider and enterprise data centers and MAN/WAN applications. The robust system architecture — supported by SLX-OS and a versatile feature set including IPv4, IPv6, MPLS/VPLS, and OpenFlow forwarding — combines with Carrier Ethernet 2.0 and OAM capabilities to provide deployment flexibility. This enables the SLX 9640 to scale from the data center border to data center interconnect and MAN/WAN environments while supporting the route and policy scale of demanding peering and network packet broker aggregation needs.

Designed with state-of-the-art network processor technology, the SLX 9640 has a switch fabric capacity of up to 900 Gbps in a 1U form factor. Advanced hardware with fine-grained QoS support enables full-duplex, high-speed performance for any mix of IPv4, IPv6, and MPLS/VPLS services.

SLX 9640 hardware supports flexible port configurations with 24 ports of dual mode 10 GbE / 1 GbE and 12 ports of dual mode 100 GbE / 40 GbE. In addition, each 100 GbE port can support 4 ports of 25 GbE via breakout, while each 40 GbE port can support 4 ports of 10 GbE via breakout.

This approach provides financial and operational flexibility for diverse business and service deployment needs.

Modular, Virtualized Operating System

The SLX 9640 runs SLX-OS, a fully virtualized Linux-based operating system that delivers process-level resiliency and fault isolation. SLX-OS supports advanced routing, MPLS, and Carrier Ethernet 2.0 features. It is highly programmable with support for REST and NETCONF, enabling full network lifecycle automation with Extreme Workflow Composer and turnkey automation suites. In addition, SLX-OS is based on Ubuntu Linux, which offers all the advantages of open source and access to commonly used Linux tools.

SLX-OS runs in a virtualized environment over a KVM hypervisor, with the operating system compartmentalized and abstracted from the underlying hardware. The core operating system functions for the SLX 9640 are hosted in the system VM.

This approach provides clean failure domain isolation for the switch operating system while leveraging the x86 ecosystem — thereby removing single vendor lock-in for system tools development and delivery. In addition, it supports a guest VM, which is an open KVM environment for running third-party and customized monitoring, troubleshooting, and analytics applications.

SLX 9640 Architecture

The SLX 9640 architecture is designed to support connectivity needs today and well into the future as bandwidth and application workload requirements change. Extreme Networks offers multiple SLX 9640 configurations with software licenses to help organizations optimize port density and capabilities. These switches leverage the latest Intel x86 CPU and merchant silicon packet processor technology for optimal space, power, and cooling in a highly reliable, carrier-class compact fixed switching platform.

The SLX 9640 delivers:

- Multiple 1/10/25/40/100 GbE configurations for deployment flexibility
- Ultra-deep buffers for lossless forwarding in demanding data center and WAN applications
- Advanced forwarding—including IPv4, IPv6, MPLS/VPLS, BGP-EVPN, and OpenFlow — to support diverse use cases
- Support for up to 4M IPv4 and 1M IPv6 routes in the Forwarding Information Base (FIB), high policy scale with required statistics and Internet peering
- Extreme OptiScale™ optimizes the programmable hardware and software capabilities of the adaptive SLX 9640 to accelerate innovation and deliver investment protection

Embedded Network Visibility

The SLX 9640 includes the Extreme SLX Insight Architecture delivered through SLX-OS and SLX 9640 hardware innovation. 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 or router, 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.

The highly flexible Extreme SLX Insight Architecture enables required data to be extracted from the network and optimized locally on-device for cost-effective delivery off-device to cloud-scale management, operational intelligence, and automation systems for additional analysis, action, or archiving.

As seen in Figure 1, the key components of the Extreme SLX Insight Architecture include:

- **Flexible Packet Filtering** – The Extreme SLX Insight Architecture begins with flexible packet filtering in the packet processors for each interface. Organizations have access to a rich set of filters for capturing the desired traffic type for visibility processing.
- **Guest VM** – The Extreme SLX Insight Architecture provides an open KVM environment that runs third-party applications and customized monitoring, troubleshooting, and analytics tools. Enabled by SLX-OS, this preconfigured guest VM is on each SLX 9640 Switch. It hosts third-party network operations and analytics applications on every device, extending visibility to the entire network.

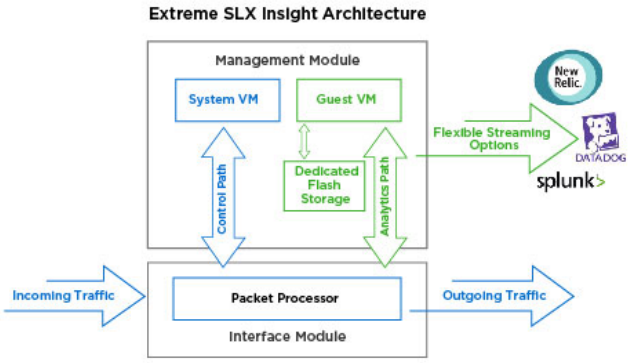

Figure 1: The SLX Insight Architecture, inherent in SLX switches and routers, delivers pervasive visibility for greater insight into network traffic.

- **Dedicated Analytics Path** – The Extreme SLX Insight Architecture provides an innovative 10 Gbps internal analytics path between the packet processor for the SLX 9640 interfaces and the architecture's open KVM environment running on the dedicated cores of the Intel CPU. This enables applications running in the open KVM environment to extract forwarding data without disrupting the normal operation of the SLX 9640.
- **Flexible Streaming** – The Extreme SLX Insight Architecture provides flexible streaming options, enabling captured data to be delivered to analytics applications off the platform.[1]
- **Dedicated Analytics Storage** – The SLX 9640 provides 128 GB of on-device storage dedicated to the Extreme SLX Insight Architecture for applications running in the open KVM environment. This enables real-time data capture for fast and easy access.

Extreme SLX Insight Architecture

The Extreme SLX Insight Architecture delivers dynamic flow identification, intelligent pre-processing, and flexible data streaming capabilities on each router to support key network operations use cases without disrupting network traffic. Use cases include:

- Real-time monitoring
- Overlay and underlay visibility
- Intelligent automation

Improved Business Agility with Workflow Automation

With DevOps-style automation, the SLX 9640 and Extreme Workflow Composer help organizations improve business agility and accelerate innovation by automating the entire network lifecycle—from provisioning, validation, and troubleshooting to the remediation of network services. At the same time, these solutions align workflow automation to IT operations and modern DevOps tool chains.

By automating and orchestrating across domains within the services delivery chain, Extreme Workflow Composer connects functional domains—such as the network, compute, storage, and applications—to minimize the number of transitions between functions. This streamlines the delivery of services and infrastructure changes so that they are fast, reliable, and repeatable (see Figure 2). In addition, turnkey automation suites enable organizations to easily deploy Extreme Workflow Composer with Extreme SLX switches and routers using a modular, customizable approach, helping to jumpstart the automation journey.

ExtremeRouting SLX 9640 and Extreme Workflow Composer

The SLX 9640 with Extreme Workflow Composer enables automation of the entire network lifecycle with event-driven automation, including:

- Automation of the full network lifecylce – provisioning, validation, troubleshooting, and remediation of network services
- End-to-end IT workflow automation through cross-domain integration
- Customizable and do-it-yourself workflow automation options in multivendor network environments
- DevOps methodologies, open source technologies, and a thriving technical community
- Industry-standard REST/NETCONF-based APIs with Yang models, OpenFlow, scripting languages, and streaming APIs
- Turnkey automation with Extreme Workflow Composer Automation Suites, and Extreme SLX switches and routers

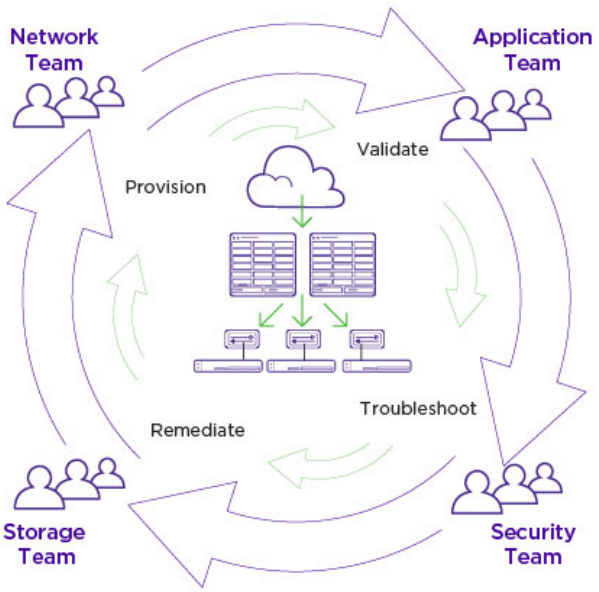

Figure 2

SLX 9640 and Ansible

Ansible Network modules deliver the benefits of simple, powerful, agentless automation to network administrators. Ansible SLX network modules can be used to configure, test and validate existing network state on SLX family of devices.

Extreme Management Center for Insights, Visibility and Control

The SLX family of switches and routers, including SLX 9640 can be managed by Extreme Management Center (XMC). XMC includes a suite of applications, empowering administrators to deliver a superior quality experience to end users through a single pane of glass and a common set of tools to provision, manage and troubleshoot the network. It works across wired and wireless networks, from the edge to the data center and private cloud.

XMC provides a consolidated view of users, devices and applications for wired and wireless networks – from data center to edge. Zero touch provisioning lets one quickly bring new infrastructure online. A granular view of users, devices and applications with an easy to understand dashboard enables efficient inventory and network topology management.

XMC also provides ecosystem integration, includes off the box integrations with major enterprise data center virtual environments such as VMWare, OpenStack and Nutanix to provide VM visibility and enforce security settings.

Get more information on Extreme Management Center.

SLX 9640 Front View

SLX 9640 Rear View with Fan Modules

Specifications

Item	Extreme SLX 9640
Maximum 100 GbE/40 GbE ports	12[2]
Maximum 10/1 GbE, 100 Meg	24
Switch fabric capacity (data rate, full duplex)	900 Gbps
Forwarding capacity (data rate, full duplex)	810 Mpps
Airflow	Front to back or back to front (orderable option)
Fan module slots	6 (5+1 redundancy)
Maximum AC power supply rating	650 W
Power Supplies Modular	650W AC power supply (up to two PSUs)
Power Supplies Modular	650W DC power supply (up to two PSUs)
Height	1.69 in./4.30 cm
Width	17.26 in./43.85 cm
Depth chassis only without cable management or fan handles	18.11 in./46.00 cm
Weight Chassis	2 PS, 6 fans: 20.05 lb, 9.09 kg
Weight Chassis	2 PS, 6 fans, rack mount kit: 21.65 lb 9.82 kg
Weight Empty chassis (no PS, no fans)	14.50 lb, 6.58 kg, Fan: 0.35 lb, 0.59 kg., PS: 1.70 lb, 0.77 kg
Port type	100 GbE QSFP-28, 40 GbE QSFP+, 10 GbE SFP+, 1 GbE SFP+
Packet buffers per switch	6 GB
MAC address scale	640,000
VLAN scale	4,096
Route scale	4,000,000 (IPv4), 1,000,000 (IPv6)
OptiScale™ Internet Routing	Yes, 5,700,000 (IPv4), 1,400,000 (IPv6)
Jumbo frame (maximum size)	9,216 bytes
QoS priority queues (per port)	8
MPLS	With Extreme SLX-OS advanced feature license
NSX	With Extreme SLX-OS advanced feature license
OptiScale(TM) Internet Routing	With Extreme SLX-OS advanced feature license

[2] Software upgrade licenses are available for the Extreme SLX 9640-24S for Ports on Demand (PoD) to enable 100 GbE/40 GbE ports.

Power and Heat Dissipation

	650W AC PSU 23-1000076-02/23-1000075-02	650W DC PSU 23-1000078-02/23-1000077-02
Dimensions	2.15” x 9.0” x 1.57” 54.5mm x 228.6mm x 40mm	2.15” x 9.0” x 1.57” 54.5mm x 228.6mm x 40mm
Weight	1.63 lb (0.741 kg)	1.74 lb (0.789 kg)
Voltage Input Range	90 to 264 Vac	-44 to -72 Vdc
Line Frequency Range	47 to 63 Hz	N/A
PSU Input Socket	IEC 320, C14	IEC 320, C14

Maximum Heat Dissipation (BTU/hr) (Fans high, all ports 100% traffic, 2 PSU)	Maximum Power Dissipation (BTU/hr) (Fans high, all ports 100% traffic, 2 PSU)
1,481 BTU/hr	434 W

Acoustics

Location	Bystander Sound Pressure
Front	51.9 dBA, re: 20 µPa
Rear	55.7 dBA, re: 20 µPa
Right Side	53.4 dBA, re: 20 µPa
Left Side	53.4 dBA, re: 20 µPa
Average	53.8 dBA, re: 20 µPa

Note: Bystander A-weighted Sound Pressure Level, LpAm-By, measured at 27°C ambient.

Specifications

IEEE Compliance

- Ethernet
  - 802.3-2005 CSMA/CD Access Method and Physical Layer Specifications
  - 802.3ab 1000BASE-T
  - 802.3ae 10 Gigabit Ethernet
  - 802.3u 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbps with Auto-Negotiation
  - 802.3x Flow Control
  - 802.3z 1000BASE-X Gigabit Ethernet over fiber optic at 1 Gbps
  - 802.3ad Link Aggregation
  - 802.1Q Virtual Bridged LANs
  - 802.1D MAC Bridges
  - 802.1w Rapid STP
  - 802.1s Multiple Spanning Trees
  - 802.1ag Connectivity Fault Management (CFM)
  - 8023.ba 100 Gigabit Ethernet
  - 802.1ab Link Layer Discovery Protocol
  - 802.1x Port-Based Network Access Control
  - 802.3ah Ethernet in the First Mile Link OAM3 ITU-T G.8013/Y.1731 OAM mechanisms for Ethernet[4]

RFC Compliance

- General Protocols
  - RFC 768 UDP
  - RFC 791 IP
  - RFC 792 ICMP
  - RFC 793 TCP
  - RFC 826 ARP
  - RFC 854 TELNET
  - RFC 894 IP over Ethernet
  - RFC 903 RARP
  - RFC 906 TFTP Bootstrap
  - RFC 950 Subnet
  - RFC 951 BootP
  - RFC 1027 Proxy ARP
  - RFC 1042 Standard for The Transmission of IP
  - RFC 1166 Internet Numbers
  - RFC 1122 Host Extensions for IP Multicasting
  - RFC 1191 Path MTU Discovery
  - RFC 1340 Assigned Numbers
  - RFC 1542 BootP Extensions
  - RFC 1591 DNS (client)
  - RFC 1812 Requirements for IPv4 Routers
  - RFC 1858 Security Considerations for IP Fragment Filtering
  - RFC 2131 BootP/DHCP Helper
  - RFC 2578 Structure of Management Information Version 2
  - RFC 2784 Generic Routing Encapsulation
  - RFC 3021 Using 31-Bit Prefixes on IPv4 Point-to-Point Links
  - RFC 3768 VRRP
  - RFC 4001 Textual Conventions for Internet Network Addresses
  - RFC 4632 Classless Interdomain Routing (CIDR)
  - RFC 4950 ICMP Extensions for MPLS
  - RFC 5880 Bidirectional Forwarding Detection3
  - RFC 5881 Bidirectional Forwarding Detection for IPv4 and IPv6 (Single Hop)3
  - RFC 5882 Generic Application of Bidirectional ForwardingDetection[3]
  - RFC 5884 Bidirectional Forwarding Detection for Multihop Paths3 Egress ACL Rate Limiting
- BGP4
  - RFC 1745 OSPF Interactions
  - RFC 1772 Application of BGP in the Internet
  - RFC 1997 Communities and Attributes
  - RFC 2385 BGP Session Protection via TCP MD5
  - RFC 2439 Route Flap Dampening
  - RFC 2918 Route Refresh Capability
  - RFC 3392 Capability Advertisement
  - RFC 3682 Generalized TT L Security Mechanism for eBGP Session Protection
  - RFC 4271 BGPv4
  - RFC 4364 BGP/MPLS IP Virtual Private Networks
  - RFC 4456 Route Reflection
  - RFC 4486 Sub Codes for BGP Cease Notification Message
  - RFC 4724 Graceful Restart Mechanism for BGP
  - RFC 4893 BGP Support for Four-octet AS Number Space
  - RFC 6793 BGP Support for Four-octet AS Number Space
  - RFC 5065 BGP4 Confederations
  - RFC 5291 Outbound Route Filtering Capability for BGP-4
  - RFC 5396 Textual Representation of Autonomous System (AS) Numbers
  - RFC 5668 4-Octect AS specific BGP Extended Community
  - draft-ietf-rtgwg-bgp-pic-07.txt - BGP Prefix Independent Convergence
  - RFC 5575 - Dissemination of Flow Specification Rules (BGP Flow Spec)
  - RFC 8092 BGP Large Community Attribute sFlow BGP AS path
- OSPF
  - RFC 1745 OSPF Interactions
  - RFC 1765 OSPF Database Overflow
  - RFC 2154 OSPF with Digital Signature (Password, MD-5)
  - RFC 2328 OSPF v2
  - RFC 3101 OSPF NSSA
  - RFC 3137 OSPF Stub Router Advertisement
  - RFC 3630 TE Extensions to OSPF v2
  - RFC 3623 Graceful OSPF Restart
  - RFC 4222 Prioritized Treatment of Specific OSPF Version 2
  - RFC 5250 OSPF Opaque LSA Option

- IS-IS
  - RFC 1195 Routing in TCP/IP and Dual Environments
  - RFC 1142 OSI IS-IS Intra-domain Routing Protocol
  - RFC 3277 IS-IS Blackhole Avoidance
  - RFC 5120 IS-IS Multi-Topology Support
  - RFC 5301 Dynamic Host Name Exchange
  - RFC 5302 Domain-wide Prefix Distribution
  - RFC 5303 Three-Way Handshake for IS-IS Point-to-Point
  - RFC 5304 IS-IS Cryptographic Authentication (MD-5)
  - RFC 5306 Restart Signaling for ISIS (helper mode)
  - RFC 5309 Point-to-point operation over LAN in link state routing protocols
- IPv4 Multicast
  - RFC 1112 IGMP v1
  - RFC 2236 IGMP v2
  - RFC 4601 PIM-SM
  - RFC 4607 PIM-SSM
  - RFC 4610 Anycast RP using PIM
  - RFC 5059 BSR for PIM
  - PIM IPv4 MCT
- QOS
  - RFC 2474 DiffServ Definition
  - RFC 2475 An Architecture for Differentiated Services
  - RFC 2597 Assured Forwarding PHB Group
  - RFC 2697 Single Rate Three-Color Marker
  - RFC 2698 A Two-Rate Three-Color Marker
  - RFC 3246 An Expedited Forwarding PHB
- IPv6 Core
  - RFC 1887 IPv6 unicast address allocation architecture
  - RFC 1981 IPv6 Path MTU Discovery
  - RFC 2375 IPv6 Multicast Address Assignments
  - RFC 2450 Proposed TLA and NLA Assignment Rules
  - RFC 2460 IPv6 Specification
  - RFC 4862 IPv6 Stateless Address - Auto Configuration
  - RFC 2464 Transmission of IPv6 over Ethernet Networks
  - RFC 2471 IPv6 Testing Address allocation
  - RFC 2711 IPv6 Router Alert Option
  - RFC 3587 IPv6 Global Unicast—Address Format
  - RFC 4193 Unique Local IPv6 Unicast Addresses
  - RFC 4291 IPv6 Addressing Architecture
  - RFC 4301 IP Security Architecture
  - RFC 4303 Encapsulation Security Payload
  - RFC 4305 ESP and AH cryptography
  - RFC 4443 ICMPv6
  - RFC 4552 Auth for OSPFv3 using AH /ESP
  - RFC 4835 Cryptographic Alg. Req. for ESP
  - RFC 4861 Neighbor Discovery for IP version 6 (IPv6)
  - RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- IPv6 Routing
  - RFC 5340 OSPF for IPv6
  - RFC 2545 Use of BGP-MP for IPv6
  - RFC 5308 Routing IPv6 with IS-IS
  - Support for IPv6 Router Advertisements with DNS Attributes
  - RFC 8106 Support for IPv6 Router Advertisements with DNS Attributes
  - RFC 6164 Using 127-Bit IPv6 Prefixes on Inter-Router Links
- MPLS
  - RFC 2205 RSVP v1 Functional Specification
  - RFC 2209 RSVP v1 Message Processing Rules
  - RFC 2702 TE over MPLS
  - RFC 2961 RSVP Refresh Overhead Reduction Extensions
  - RFC 3031 MPLS Architecture
  - RFC 3032 MPLS Label Stack Encoding
  - RFC 3037 LDP Applicability
  - RFC 3097 RSVP Cryptographic Authentication
  - RFC 3209 RSVP-TE
  - RFC 3270 MPLS Support of Differentiated Services
  - RFC 3478 LDP Graceful Restart
  - RFC 3815 Definition of Managed Objects for the MPLS, LDP
  - RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels
  - RFC 4364 BGP/MPLS IP Virtual Private Networks
  - RFC 4379 OAM
  - RFC 4448 Encapsulation methods for transport of Ethernet over MPLS networks
  - RFC 5036 LDP Specification
  - RFC 5305 ISIS-TE
  - RFC 5443 LDP IG P Synchronization
  - RFC 5561 LDP Capabilities
  - RFC 5712 MPLS Traffic Engineering Soft Preemption
  - RFC 5918 LDP “Typed Wildcard” FEC
  - RFC 5919 Signaling LDP Label Advertisement Completion
- Layer 2 VPN and PWE3
  - RFC 3343 TT L Processing in MPLS networks
  - RFC 3985 Pseudowire Emulation Edge to Edge (PWE3) Architecture
  - RFC 4364 BGP/MPLS IP Virtual Private Networks4
  - RFC 4447 Pseudowire Setup and Maintenance using LDP4
  - RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks
  - RFC 4664 Framework for Layer 2 Virtual Private Networks
  - RFC 4665 Service Requirements for Layer 2 Provider-Provisioned Virtual Private Networks
  - RFC 4762 VPLS using LDP Signaling
  - RFC 5542 Definitions of Textual Conventions for Pseudowire (PW) Management
  - RFC 6391 Flow-Aware Transport of Pseudowires
  - RFC 6870 PW Preferential Forwarding Status Bit3
  - RFC 7432 BGP MPLS-Based Ethernet VPN - Partial4
  - RFC 7348 Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks (Partial)
  - draft-sd-l2vpn-evpn-overlay-03 (A Network Virtualization Overlay Solution using EVPN) Partial4
  - draft-ietf-bess-evpn-overlay-04 (A Network Virtualization Overlay Solution using EVPN with VXLAN encapsulation) Partial4
  - draft-ietf-bess-evpn-overlay-12 A Network Virtualization Overlay Solution using EVPN
  - draft-ietf-bess-evpn-igmp-mld-proxy-00 (IGMP and MLD Proxy for EVPN)

[3] Supported with Extreme SLX-OS 17r.1.00 and later software.
[4] Supported with Extreme SLX-OS 17r.1.01 and later software.

Management and Visibility

- Integrated industry-standard Command Line Interface (CLI)
- RFC 854 Telnet
- RFC 2068 HTTP
- RFC 2818 HTTPS
- RFC 3176 sFlow v5
- sFlow extension to VXLAN
- RFC 4253 Secure Shell (SSH)
- Secure Copy (SCP v2)
- SFTP
- RFC 8040 RESTCONF Protocol - PATCH, PUT, POST, DELETE support.
- RFC 5905 Network Time Protocol Version 4
- RFC 3986 Uniform Resource Identifier (URI): Generic Syntax
- RFC 6241 NETCONF Configuration Protocol (Partial)
- RFC 4742 “Using the NETCONF Configuration Protocol over Secure Shell (SSH)”
- RFC 6020, “YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)”
- RFC 6021, “Common YANG Data Types”
- RFC 4741 NETCONF (Partial)
- OpenFlow 1.3
- Chrome
- Curl
- Tcpdump
- Wireshark
- SNMP Infrastructure (v1, v2c, v3)
- RFC 1157 Simple Network Management Protocol
- RFC 1908 Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
- RFC 2578 Structure of Management Information Version 2
- RFC 2579 Textual Conventions for SMIv2
- RFC 2580 Conformance Statements for SMIv2
- RFC 3410 Introduction and Applicability Statements for Internet Standard Management Framework
- RFC 3411 An Architecture for Describing SNMP Management Frameworks
- RFC 3412 Message Processing and Dispatching
- RFC 3413 SNMP Applications
- RFC 3414 User-based Security Model
- RFC 3415 View-based Access Control Model
- RFC 3416 Version 2 of SNMP Protocol Operations
- RFC 3417 Transport Mappings
- RFC 3418 Management Information Base (MIB) for the SNMP
- RFC 3584 Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
- RFC 3826 The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
- SNMP MIBs
- IANA-ADDRESS-FAMILY-NUMBERS-MIB
- IANA ifType-MIB
- sFlow v5 MIB
- RFC 1213 Management Information Base for Network Management of TCP/IP-based internets: MIB-II
- RFC 2790 Host Resource MIB
- RFC 2819 RMON Groups 1, 2, 3, 9
- RFC 2863 The Interfaces Group MIB (IF)
- RFC 3289 Diffserv MIB
- RFC 3635 Etherlike Interface Type MIB
- RFC 3811 MPLS TC STD MIB
- RFC 3812 MPLS TE STD MIB
- RFC 3813 MPLS LSR MIB
- RFC 4001 Textual Conventions for Internet Network Addresses
- RFC 4022 Textual Conventions for Internet Network Addresses (TCP)
- RFC 4113 Management Information Base for the User Datagram Protocol (UDP)
- RFC 4133 Entity MIB
- RFC 4273 BGP-4 MIB
- RFC 4188 Bridge MIB
- RFC 4292 IP Forwarding Table MIB (IP-FORWARD)
- RFC 4293 Management Information Base for the Internet Protocol (IP)
- RFC 4363 Dot1q MIB
- RFC 4444 IS-IS MIB
- RFC 4750 OSPF v2 MIB
- RFC 4878 DOT3-OAM-MIB
- RFC 7257 VPLS MIB (Partial)
- RFC 7331 BFD MIB
- IEEE/MEF MIBs
- IEEE-802 LLDP MIB
- MEF-SOAM-PM-MIB
- IEEE-8021-CFM-MIB
- IEEE-8021-CFM-V2-MIB

Element Security

- AAA
- Username/Password (Challenge and Response)
- Bi-level Access Mode (Standard and EXEC Level)
- Role-Based Access Control (RBAC)
- RFC 2865 RADIUS
- RFC 2866 RADIUS Accounting
- TACACS/TACACS+ draft-grant-tacacs-02 TACACS+ - Command Authorization, Authentication, AccountingRFC 5905 NTP Version 4
- NTP 4.2.8p 10
- RFC 5961 TCP Security
- RFC 4250 Secure Shell (SSH) Protocol Assigned Numbers
- RFC 4251 Secure Shell (SSH) Protocol Architecture
- RFC 4252 Secure Shell (SSH) Authentication Protocol
- RFC 4253 Secure Shell (SSH) Transport Layer Protocol
- RFC 4254 Secure Shell (SSH) Connection Protocol
- RFC 4344 SSH Transport Layer Encryption Modes
- RFC 4419 Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
- draft-ietf-secsh-filexfer-13.txt SSH File Transfer Protocol (SFTP)
- Secure Copy (SCP v2) (see RFC 4251)
- RFC 2068 HTTPRFC 4346 TLS 1.1
- RFC 5246 TLS 1.2
- Protection against Denial of Service (DoS) attacks such as TCP SYN or Smurf Attacks

Environment

- Operating temperature: 0°C to 40°C (32°F to 104°F)
- Storage temperature: –25°C to 55°C (–13°F to 131°F)
- Relative humidity: 5% to 90%, at 40°C (104°F), non-condensing
- Storage humidity: 95% maximum relative humidity, non-condensing
- Operating altitude: 6,600 ft (2,012 m)
- Storage altitude: 15,000 ft (4,500 m) maximum

Safety Agency Approvals

- CAN/CSA-C22.2 No. 60950-1-07
- ANSI/UL 60950-1
- IEC 60950-1
- EN 60950-1 Safety of Information Technology Equipment
- EN 60825-1
- EN 60825-2

Power and Grounding

- ETS 300 132-1 Equipment Requirements for AC Power Equipment Derived from DC Sources
- ETS 300 132-2 Equipment Requirements for DC Powered Equipment
- ETS 300 253 Facility Requirements

Physical Design and Mounting

- 19-inch rack mount supporting racks compliant with:
  - ANSI/EIA -310-D
  - GR-63-CORE Seismic Zone 4

Environmental Regulatory Compliance

- EU 2011/65/EU RoHS
- EU 2012/19/EU WEEE
- EC/1907/2006 REACH

Ordering Information

Part Number	Description
Extreme SLX 9640 Switch Hardware	
EN-SLX-9640-24S	Base unit with 24 1G/10G SFP+ ports, 4 10Gb/25Gb/40Gb/50Gb/100Gb capable QSFP28 ports, 2 unpopulated power supply slots, 6 unpopulated fan slots.
EN-SLX-9640-24S-AC-F	Base unit with 24 1G/10G SFP+ ports, 4 10Gb/25Gb/40Gb/50Gb/100Gb capable QSFP28 ports, 1 AC power supply, 6 fan modules, front-to-back airflow
EN-SLX-9640-24S-12C	Base unit with 24 1G/10G SFP+ ports, 12 10Gb/25Gb/40Gb/50Gb/100Gb capable QSFP28 ports, 2 unpopulated power supply slots, 6 unpopulated fan slots.
EN-SLX-9640-24S-12C-AC-F	Base unit with 24 1G/10G SFP+ ports, 12 10Gb/25Gb/40Gb/.50Gb/100Gb capable QSFP28 ports, 1 AC power supply, 6 fan modules, front-to-back airflow
XBR-R000297	SLX Fixed Rackmount kit. 2-post/4-post, mid/flush mount compatible
XBR-ACPWR-650-F	SLX Fixed AC 650W Power Supply Front to Back airflow. Power cords not included.
XBR-ACPWR-650-R	SLX Fixed AC 650W Power Supply Back to Front. Power cords not included.
XBR-DCPWR-650-F	SLX Fixed DC 650W Power Supply Front to Back airflow. Power cords not included.
XBR-DCPWR-650-R	SLX Fixed DC 650W Power Supply Back to Front. Power cords not included.
XEN-SLX9640-FAN-F	SLX 9640 FAN Front to Back airflow
XEN-SLX9640-FAN-R	SLX 9640 FAN Back to Front airflow
Extreme SLX 9640 Upgrade Software Licenses	
EN-SLX-9640-4C-POD-P	Ports on Demand to enable 4×100 GbE/40 GbE ports (for Extreme SLX 9640-24S)
EN-SLX-9640-ADV-LIC-P	Advanced Feature License for MPLS, BGP-EVPN, CE2.0, NSX, OptiScale™ Internet Routing (for Extreme SLX 9640-24S and SLX 9640 24S-12C)

Extreme™
Customer-Driven Networking

http://www.extremenetworks.com/contact