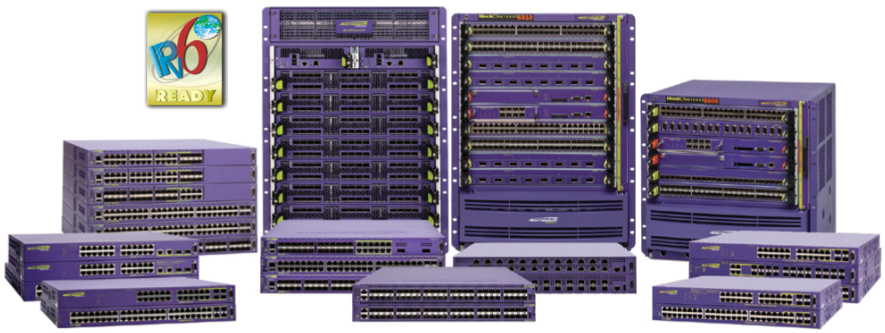
Highlights

ExtremeXOS has a robust set of Layer 2 and Layer 3 control protocols, provides a flexible architecture for highly resilient networks and has been designed to support the nextgeneration Internet Protocol, IPv6. ExtremeXOS is a highly available and extensible software foundation for converged networks. ExtremeXOS offers high availability for carriergrade voice and video services over IP and for supporting mission-critical business applications such as CRM.

- Modular Operating System
- High Availability Architecture
- Rich set of Layer-2 and Layer-3 protocols and features
- Secure Network Access through role based policy or Identity Management
- Extensibility
- Integrated Security with NetLogin, MAC Security, IP Security
- User, location, and time-based dynamic security policies with Identity Management
- Insight, control and automation for virtualized data centers with XNV (ExtremeXOS Network Virtualization)
- Enhanced resiliency, synchronization, performance for 2G/3G/4G mobile backhaul
- ExtremeXOS InSite SDK Software Defined Networking Ready with OpenFlow and OpenStack support
- Ethernet Audio Video Bridging (AVB) enabled



ExtremeXOS® Operating System

Version 16.2, 21.1, 22.7, and 30.4

Overview

Extreme Networks has created the ExtremeXOS modular Operating System (OS) – for highly available, extensible, high-performance networks. ExtremeXOS high availability architecture with EAPS protocol helps reduce network downtime for business continuity and access to mission-critical applications such as CRM, data warehouses and VoIP for carrier and voice grade networks.

Built-in security capabilities provide network access control integrated with endpoint integrity checking, identity management, and protection for the network control and management planes.

With ExtremeXOS you can extend the capabilities of your network by integrating specialized application appliances such as security devices into the network, providing insight and control at the network, application and user level.

Architectural Highlights

- Memory protection for processes
- Self-healing process recovery via process restart or hitless failover
- Dynamic loading of new functionality
- Scriptable CLI for automation and event-triggered actions
- XML open APIs for integrating third-party applications
- Dual-stack IPv4 and IPv6 support

High Availability Architecture

- Reduce network downtime using hitless failover and module-level software upgrade
- Prevent system corruption using memory protection for processes
- Avoid system reboots using self-healing process recovery
- Extend high availability across switches with Multi-Switch Link Aggregation Groups
- Network topology based software upgrade without impacting end users

Extensibility

- Integrate best-of-breed applications with an open, yet secure XML-based Application Programming Interface (API)
- Integrate Extreme and third-party developed software applications using open standards-based POSIX interfaces
- Scripting-based device management for incremental configuration deployment and ease of management

Integrated Security

- Guard network access through authentication, Network Login/802.1x, host integrity checking, and Identity Management
- Role-Based Policy enables support for policy profiles to secure and provision network resources based upon the role the user or device plays within the network.
- Harden the network infrastructure with Denial of Service (DoS) protection and IP Security against man-in-the-middle and DoS attacks
- Secure management using authentication and encryption

High Availability

Modular Operating System

The modular design of ExtremeXOS allows the adding or upgrading of individual software modules, dynamically without requiring a system reboot, leading to higher availability in the network (see Figure 1).

Preemptive multitasking and memory protection allow each of many applications – such as Open Shortest Path First (OSPF) and Spanning Tree Protocol (STP) – to run as separate OS processes that are protected from each other. This drives increased system integrity and inherently helps protect against cross-platform DoS attacks. ExtremeXOS increases network availability using process monitoring and restart. Each independent OS process is monitored in real time. If process becomes unresponsive or stops running, it can be automatically restarted.

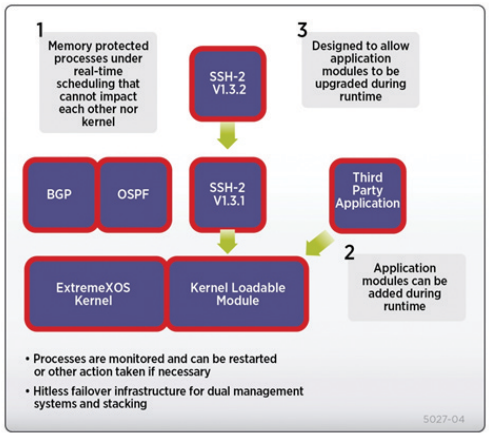


Figure 1: ExtremeXOS Modular Design

Hitless Failover and Graceful Restart

With dual management modules on chassis systems and advanced stacking support with fixed-configuration switches, ExtremeXOS is capable of preserving the state of resiliency and security protocols such as STP, EAPS and Network Login, thus allowing hitless failover between management modules/redundant masters in case a module or master fails.

Graceful restart is a way for OSPFv2, BGP4 and IS-IS protocols to restart without disrupting traffic forwarding. Without graceful restart, adjacent routers will assume that information previously received from the restarting router is stale and it won't be used to forward traffic to that router. If the peer routers support the graceful restart extensions, then the router can restart the routing protocol and continue to forward traffic correctly.

If the network topology is not changing, the static routing table remains correct. In most cases, networks can remain stable (i.e. would not re-converge) during the time for restarting OSPF, BGP or IS-IS. Should route updates still exist, graceful restart incrementally performs these updates after the restart.

Denial of Service Protection

ExtremeXOS switches provides effective Denial of Service (DOS) attack protection. If the switch detects an unusually large number of packets in the CPU input queue, it assembles ACLs that automatically stop these packets reaching CPU. After a period of time these ACLs are removed, and reinstalled if the attach continues. ASIC-based LPM routing eliminates the need for control plane software to learn new flows, allowing more network resiliency against DOS attacks.

Extensibility

Dynamic Module Loading

ExtremeXOS provides an infrastructure to dynamically load, start and gracefully stop new applications. ExtremeXOS embraces POSIX-compliant interfaces that ease the integration of new applications. ExtremeXOS uses this infrastructure to dynamically load Extreme Networks developed functionality such as SSH/SCP/SSL that is export-controlled, avoiding the requirement for new operating system image installs to gain this functionality. The same infrastructure is also used to integrate third-party developed applications. An example is a VoIP application layer monitoring agent developed to simulate and closely monitor VoIP connection behavior in a network.

Scripting

ExtremeXOS provides a CLI scripting infrastructure through Python or Tcl languages. Scripting can be used to add incremental configuration to the network infrastructure, such as a list of VLANs to be configured. This capability eases the roll-out of networks, reduces repetitive tasks and configuration errors. Scripting capabilities, such as system- and user-defined environment variables, such as if/then and loops, allow automating regular management tasks in scripts and deploying configurations such as QoS, rate limiting and ACLs, for example, to multiple ports. Scripts can access CLI output, and a rich set of Python or Tcl functions that provide a utility library of string manipulation, search or mathematical functions. By leveraging scripting for switch configuration, rolling out a new switch can be reduced to minutes and just a few commands for switch-specific settings. Scripting is also used in the ExtremeXOS Universal Port framework to define trigger event actions.

XML Application Programming Interfaces

Extreme Networks uses XML APIs – concepts originally developed in the emerging field of Web services. ExtremeXOS can provide a secure, simple mechanism to access processes and information within the switch. For example, a security appliance can utilize ExtremeXOS to limit access, control bandwidth or redirect traffic from a client that is attempting to connect to the network. XML also provides a scalable and reliable transport for device configuration and statistics, for example OSS and service provisioning systems in Carrier Ethernet deployments. This XML infrastructure embraces the concept of open yet secure communications to allow business applications to easily interact with the network for security policy enforcement, regulatory compliance and performance management, and higher security. The XML infrastructure is also used by ExtremeXOS ScreenPlay™ Web-based management interface.

Ease of Management

Link Layer Discovery Protocol (LLDP, IEEE 802.1AB)

ExtremeXOS support of IEEE 802.1ab standards-based discovery protocol provides vendor-independent device discovery as well as integration with VoIP infrastructure and phones, including E911 ECS location, inventory information, PoE budgeting and configuration of information such as VLANs and QoS tagging.

LLDP not only simplifies deployment and locating of access devices, but it can also be used as a troubleshooting and firmware management tool. LLDP is tightly integrated with the IEEE 802.1x authentication at edge ports. As endpoint devices are first authenticated, the LLDP-provided information is trustable and can be used for automated configuration, helping protect the network from attacks against automated configuration mechanisms.

Network Traffic Monitoring

sFLOW and IPFIX

ExtremeXOS sFlow and IPFIX standards-based data monitoring support provides Layer 2-7 visibility into the network, including statistics on which applications are running over your network, biggest talkers, etc.

sFlow is a sampling technology that meets the key requirements for a network traffic monitoring solution: sFlow provides a network-wide view of usage and active

routes. It is a scalable technique for measuring network traffic, and collecting, storing, and analyzing traffic data. This enables thousands of interfaces to be monitored from a single location.

sFlow is scalable, thereby enabling it to monitor links of speeds up to 10 Gigabits per Second (Gbps) and beyond without impacting the performance even of core Internet routers and switches, and without adding significant network load. IPFIX (Internet Protocol Flow Information eXport), or RFC 3917, can be used as an alternative to sFlow. IPFIX offers templates for the data to be transferred, or network managers can define data types to adapt to their specific needs.

Application Telemetry

Application Telemetry is a unique feature ofv ExtremeAnalytics that enables ExtremeSwitching systems to provide granular visibility into application performance, users, locations and devices. This all without the need for expensive dedicated sensors or collectors. Application Telemetry combines packet flow (e.g., sFlow) information from the ExtremeSwitching system, along with deep packet inspection abilities of ExtremeAnalytics, to deliver actionable insights into network and application performance.

Universal Port

ExtremeXOS Universal Port infrastructure is a powerful framework of event-driven activation of CLI scripts. While Universal Port can leverage any system event log message as an event trigger, the most popular use cases are time/user/location-based dynamic security policies as well as VoIP auto-configuration. For these applications, Universal Port uses standards authentication (Network Login/802.1x) and discovery protocols (LLDP + LLDPMED) as trigger events. Configurable CLI scripts can be tied to events

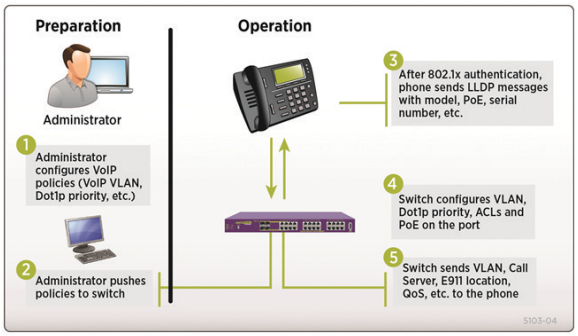


Figure 2: VoIP Auto Configuration with ExtremeXOS Universal Port

on a per-port basis. As such, dynamic security policies, including fine-grained access control via ACLs, can follow a user independently of where he logs into the network. VoIP phones and the connecting switch edge port can be auto-configured for the voice VLAN and QoS. The switch can receive the exact power budget requirements from the

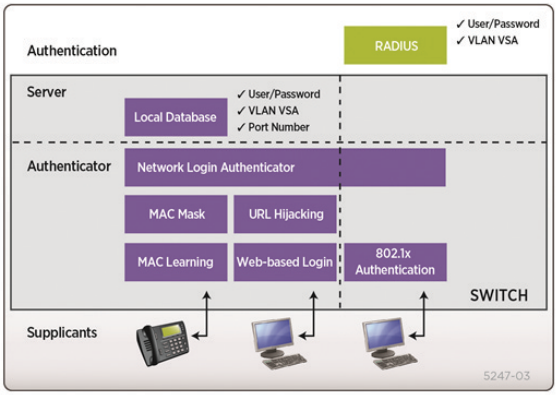


Figure 3: Network Login

phone and provision it accordingly. The phone can receive the E911 ECS location from the switch as well as the call server address in order to receive additional configuration.

Deploying VoIP endpoints is as easy as opening the package, programming the extension, and plugging into the network. The following diagram explains the mechanism. Note that steps 1 and 2 are only done once using scripting, and then rolled out to all voice-capable ports. Steps 3 to 5 are the resulting automatic runtime events.

Integrated Security

Network Login

Extreme Networks open, standards-based approach allows network access control on all edge ports of a network through the use of authentication. Authentication allows organizations to provide secure network access and provide mobility to users and devices. ExtremeXOS Network Login provides support for simultaneous authentication methods and can support multiple concurrent authentication techniques, including: IEEE 802.1X, MAC-based and Web-based methods.

Additionally Network Login provides support for multi-user authentication. This allows multiple users and devices to be connected to the same physical port and each user or device to be authenticated individually using one of the authentication technique (802.1X, MAC, Web). The major

benefit of multiuser authentication is to authorize multiple users, either using dynamic policy or VLAN assignment for each authenticated user.

Multi-user authentication and role-based policy can provide significant benefits to customers by extending security services to users connected through unmanaged devices, third party switches/routers, VPN concentrators, or wireless LAN access points at the edge of their network. Authentication provides security, priority, and bandwidth control while protecting existing network investments.

Integrated Security

Role-Based Policy

Utilizing ExtremeControl Policy Management, the role-based policy framework empowers a network administrator to define distinct roles or profiles that represent industry specific operational groups that may exist in an education or a business environment (e.g., administrator, teacher, student, guest). Each defined role is granted individualized access to specific network services and applications and these access privileges remain associated with users as they move across both wired and wireless network access points.

Users can be authenticated via IEEE 802.1X, MAC address, or web authentication, and then assigned a pre-defined operational role. Network operations can be seamlessly tailored to meet business-oriented requirements by providing each role with individualized access to network services and applications, thus aligning network resource utilization with business goals and priorities.

In addition, administrators can easily transition from basic VLAN and complex ACL deployments to the Extreme Networks rolebased policy framework in a seamless fashion, without the need to make changes to their RADIUS infrastructure.

MAC Security

MAC Security allows the lockdown of a port to a given MAC address and limiting the number of MAC addresses on a port. This capability can be used to dedicate ports to specific hosts or devices such as VoIP phones or printers and avoid abuse of the port – a capability that can be especially useful in hospitality markets. In addition, an aging timer can be configured for the MAC lockdown, protecting the network from the effects of attacks using (often rapidly) changing MAC addresses.

IP Security

ExtremeXOS IP security framework protects the network infrastructure, network services such as DHCP and DNS and host computers from spoofing and man-in-the-middle attacks. It also protects the network from statically configured and/or spoofed IP addresses and building an external trusted database of MAC/IP/port bindings providing the traffic source from a specific address for immediate defense.

Identity Manager

Identity Manager allows network managers to track users who access their network. User identity is captured based on NetLogin authentication, LLDP discovery, and Kerberos snooping. ExtremeXOS then reports on the MAC, VLAN, computer hostname, and port location of the user. Further, Identity Manager can create both roles and policies, and then bind them together to create role-based profiles based on organizational structure or other logical groupings, and apply them across multiple users to allow appropriate access to network resources.

In addition, support for Wide Key ACLs improves security by going beyond source/destination and MAC address as identification criteria access mechanism to provide filtering capabilities.

Secure Management

ExtremeXOS provides secure management via SSH2/SCP2/SSL and SNMPv3, providing authentication and protection against replay attacks, as well as data privacy via encryption.

Access profiles for device management allow filters to be set on device management to connections only from specified sources.

CPU DoS Protect throttles traffic directed to the switch and can automatically set an ACL for defense, thus protecting the switch from the effects of DoS attacks such as “Ping of Death” and others. This defense mechanism works for all CPU bound traffic – Layer 2, IPv4 and IPv6.

Switching: Network Resiliency and Forwarding Control

Layer 2+

For network resiliency, ExtremeXOS offers a choice between standard protocols and more advanced Layer 2+ protocols, optimized for faster resiliency, larger scaling and simpler operation.

Spanning Tree Protocol: ExtremeXOS supports IEEE 802.1D STP, 802.1w RSTP and 802.1s MSTP. In Extreme Multiple Instance STP mode, ExtremeXOS allows a port or VLAN to belong to multiple STP domains and therefore adds flexibility to STP network design, further increasing resiliency. The implementation is also compatible with PVST+ and IEEE 802.1Q.

Ethernet Automatic Protection Switching (EAPS, RFC 3619) allows the IP network to provide the level of resiliency and uptime that users expect from their traditional voice network. EAPS is more adaptable than Spanning Tree or Rapid Spanning Tree protocols and can achieve sub-second recovery that delivers consistent failover regardless of the number of VLANs, network nodes or network topology in Extreme Networks-recommended configurations. EAPS functionality increases network recovery time, which results in significant reduction in Voice-over IP call drop rates and improvement in digital video performance in supported solution configuration.

Resiliency Features: the Virtual Router Redundancy Protocol (VRRP) enables a group of routers to function as a single virtual default gateway. Extreme Standby Router Protocol™ (ESRP) can be implemented at both Layers 2 and 3. ESRP tracks link connectivity, VLANs, learned routes and ping responses. ESRP can be used as an STP and VRRP substitute, providing simplicity via a single protocol for Layer 2 and Layer 3 redundancy. Multiple instances of ESRP in the same VLAN allow direct host attachment to standby switches.

Virtual Private LAN Services (VPLS, RFC 4762) are used for signaling and provisioning subscriber VLANs and vMANs over the IP network core. Extreme's VPLS implementation interoperates with EAPS, ESRP, and STP to provide a connectivity option for delivering fault-tolerant Layer 2 services over a Layer 3 network core.

To further harden the network resiliency protocols of ExtremeXOS, Extreme Link Status Monitoring (ELSM) protects the network and resiliency protocols from the effects of unidirectional links to protocols. For bandwidth scaling, link aggregation (static and dynamic via LACP) utilizes the bandwidth of multiple links. IGMP Snooping and Multicast VLAN Registration preserve network bandwidth by forwarding only to ports and to VLANs with subscribers from a single multicast VLAN. If desired, static IGMP membership allows the force-forwarding of traffic through the network for high subscription response, and filters provide control over transmitted content.

IPv4

ExtremeXOS also offers a set of Layer 3 switching features to increase control and management on very large networks. The switching software implements static routes, RIP, OSPFv2, IS-IS and BGP4 for External BGP (EBGP) and Internal BGP (IBGP).

ExtremeXOS fields a rich set of IP multicast routing protocols, including PIM Dense Mode (PIM-DM), PIM Sparse Mode (PIM-SM) and PIM Source Specific Multicast (PIM-SSM), which work hand in hand with the built-in IGMPv1/v2/v3 support. Multicast source routes can be shared between sites using MSDP and MBGP, for example, to share sources of distance learning multicast streams in a university backbone network. IGMP v2/v3 SSM mapping allows both IGMPv2 and IGMPv3 in the network, upgrading to the more powerful and secure IGMPv3 where needed.

Designed for IPv6

IPv6 offers improved network intelligence and a considerable number of new capabilities over IPv4. However, there are specific challenges regarding whether to choose to actively participate in the transition to IPv6 or hold off to further evaluate. Extreme has taken a ground-up approach to addressing these challenges by designing IPv6 intelligence into ExtremeXOS from the beginning.

Extreme Networks has designed an architecture for the performance, flexibility and security requirements of IPv6 without compromising operational simplicity.

Features include Layer 2 and Layer 3 IPv6 forwarding, Quality of Service (QoS) to provide different level of service to different groups of IPv6 traffic, routing protocols and tunnels. ExtremeXOS provides investment protection and allows a safe and smooth transition by tunneling IPv6 traffic across non-IPv6- aware parts of the network.

ExtremeXOS platforms offer wire-speed ACLs – providing defense and control over the next generation of IP. Even when operating with IPv4, ExtremeXOS can harden the network to attacks using IPv6 transport.

Designed For Cloud Data Centers and Central Office

Direct Attach (VEPA)

With optional feature pack, EXOS can support Direct Attach (VEPA), which eliminates the virtual switch layer, simplifying the network and improving performance. Direct Attach enables data center simplification by reducing network tiers from 4 or 5 tiers to just 3 or 2 tiers, depending on the size of the data center.

ExtremeXOS Network Virtualization (XNV)

To further enhance data center operations, EXOS supports XNV (ExtremeXOS Network Virtualization), which is natively supported in the ExtremeXOS operating system. XNV provides insight, control and automation for highly virtualized data centers.

OpenFlow

ExtremeXOS implementation of OpenFlow APIs allow an external OpenFlow-based SDN controller to access and control the forwarding plane of ExtremeXOS network devices. ExtremeXOSbased switches offer a programming interface through OpenFlow to enable a high degree of automation in provisioning network services for many upper layer business critical applications running the OpenFlow-based SDN controller.

OpenStack

ExtremeXOS based switches also allow for integration with the OpenStack open source cloud computing platforms for public and private clouds through the Extreme Networks Quantum plugin. The plugin provides a scalable, automated, rich API driven system that enables networking-as-a-service model managing data center interconnect solutions and large multitenant networks.

PFC

ExtremeXOS supports Priority-based Flow Control (PFC or IEEE 802.1Qbb), which allows network traffic to be controlled independently based on Class of Service. PFC allows network traffic that requires lossless throughput to be prioritized, while other traffic types that do not require or perform better without PFC can continue as normal.

Data Center Bridging (DCB)

DCB features such as PFC, Enhanced Transmission Selection (ETS), and Data Center Bridging eXchange (DCBX) are supported in ExtremeXOS for data center convergence. Multi-Switch Link Aggregation Groups (M-LAG) can address bandwidth limitations and improve network resiliency, in part by routing network traffic around bottlenecks, reducing the risks of a single point of failure, and allowing load balancing across multiple switches.

Service-Provider Central Offices

Service providers and their central office facilities face unique challenges in serving thousands to hundreds of thousands of subscribers, often with multiple services, as well as residential, business Ethernet, and/or Ethernet mobile backhaul. ExtremeXOS includes multiple features and capabilities to support the rigorous demands of the carrier environment.

Virtual eXtensible Local Area Network (VXLAN)

VXLAN provides a means to create a logical layer 2 network spanning layer 3 boundaries via the use of encapsulation. VXLAN provides the same Ethernet layer 2 network services as VLAN environments do today, but with greater extensibility and flexibility. VXLAN segments are independent of the underlying network topology and as a fabric overlay or data center interconnect solution VXLAN can efficiently utilize available network paths. VXLAN packets are transported through the underlying network based on layer 3 header information and can take full advantage of L3 equal-cost multipath (ECMP) to use all available paths. As virtualization becomes more common with vendors increasingly adopting VXLAN, it is still rare to have a completely virtualized environment in a data center. A data center that has native VXLAN virtual machines as well as bare-metal non-VXLAN-capable devices can take advantage of the high-performance hardwarebased VXLAN gateway capability on EXOS supported platforms.

MPLS

On ExtremeXOS-based switches MultiProtocol Label Switching (MPLS) can be enabled, by way of an optional feature pack. MPLS provides the ability to implement traffic engineering and multi-service networks, and improve network resiliency. The MPLS protocol suite provides the ability to deploy services based on L2VPNS (VPLS/VPWS), BGP-based L3VPNS; LSP Establishment based on LDP, RSVP-TE, static provisioning; integrated OAM tools like VCCV, BFD and CFM; and MPLS fast reroute to support local convergence around network failure.

Mobile Backhaul

ExtremeXOS is capable of providing carrier grade resiliency, synchronization and high performance Gigabit Ethernet switching for deploying true 4G mobile backhaul solutions.

ExtremeXOS-based switches supports two packet ring resiliency protocols, Ethernet Automatic Protection Switching (EAPS) RFC 3619, and ITU G.8032 standard for Ethernet Ring Protection Switching, to enable carrier grade resiliency for a superior subscriber experience and ensuring service level agreements.

ExtremeXOS is capable of providing Synchronous Ethernet through dedicated hardware support for ITU-T G.8262 Synchronous Ethernet (SyncE) and IEEE 1588v2 Precision Time Protocol. SyncE distributes the clock between nodes and provides the benefit of deterministic frequency distribution. IEEE 1588v2 uses timestamps to distribute both time and frequency between nodes. Synchronous Ethernet ensures that 2G/3G TDM traffic encapsulated in TDM pseudowires and other Ethernet traffic are synchronized over fiber or microwave connections to provide exceptional subscriber quality experience when hand-off occurs between cell towers as subscriber roams with their mobile devices.

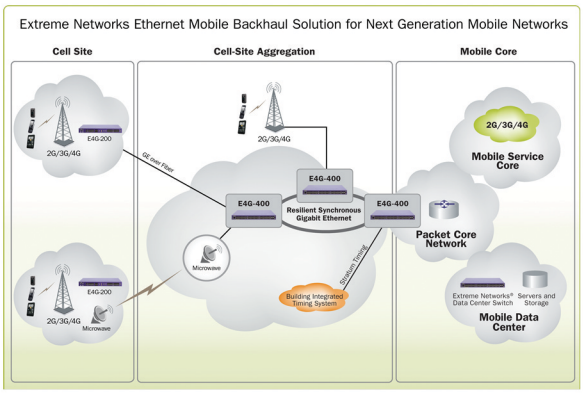


Figure 4: Extreme Networks Ethernet Mobile Backhaul Solution for Next Generation Mobile Networks

ExtremeXOS and Ansible

Ansible network modules deliver the benefit of simple, powerful, agentless automation to network administrators. Ansible modules for ExtremeXOS can be used to configure, test and validate existing network state on ExtremeXOS devices.

Extended Edge Switching

ExtremeXOS supports Extreme's Extended Edge Switching solution which simplifies the deployment and operation of edge switches. Based on the 802.1BR specification, Extended Edge Switching collapses multiple network layers into a single-tier design that reduces the complexity of traditional two and three-tier switch architectures. A central ExtremeXOS aggregation switch can act as a single point of control for multiple V300 and V400 edge switches and seamlessly deliver ExtremeXOS services to these edge switches. The solution, in effect, allows users to create a "virtual" ExtremeXOS switching system, independent of location, for simplified operations and reduced costs

Software Defined Networking Ready

ExtremeXOS-based switches are SDN-ready, supporting industry standard OpenFlow and OpenStack. ExtremeXOS implementation of OpenFlow is based on OpenFlow 1.0 APIs allowing an external OpenFlow based SDN controller to access and control the forwarding plane of the ExtremeXOS-based network device.

Thus ExtremeXOS-based switches offer a programming interface through OpenFlow to enable a high degree of automation in provisioning network services for many upper layer business critical applications that run on the OpenFlow-based SDN controller.

ExtremeXOS based switches also allow for integration with the OpenStack open source cloud computing platform for public and private clouds through its Extreme Quantum plugin. The plugin provides a scalable, automated, rich API-driven system that enables networking-as-a-service model managing data center interconnect solutions and large multi-tenant networks.

Ethernet Audio Video Bridging

ExtremeXOS supports the latest IEEE 802.1 Audio Video Bridging (AVB) standards to enable reliable, real-time audio/video transmission over Ethernet for today's high-definition and time-sensitive multimedia streams with perfect Quality of Service (QoS).

IEEE 802.1BA Audio Video Bridging Systems

ExtremeXOS uses these AVB technologies to identify and reserve the network resources for AVB traffic streams and supports precise synchronous streaming capability for reliable and high quality audio/video transmission over Ethernet. The AVB protocols enables time sensitive multimedia streams to be sent over the Ethernet network with low latency and guarantees service quality for today's real-time, high definition information and entertainment options.

ExtremeXOS Supported Protocols and Standards – Legend			
•	Yes	NT	Requires Network Timing Feature Pack
-	No	DA	Requires Direct Attach Feature Pack
AE	Requires Advanced Edge License Upgrade	AV	Requires AVB Multi-media Feature Pack
C	Requires Core License Upgrade	OF	Requires SDN-OpenFlow Feature Pack
MP	Requires MPLS Feature Pack		

ExtremeXOS Supported Protocols and Standards

	X440-G2	X450-G2	X460-G2	X465	X480	X590	X620	X670	X670-G2	X690	X770	X870
Switching												
IEEE 802.1D – 1998 Spanning Tree Protocol	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1D – 2004 Spanning Tree Protocol (STP and RSTP)	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1w – 2001 Rapid Reconfiguration for STP, RSTP	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1Q – 2003 (formerly IEEE 802.1s) Multiple Instances of STP, MSTP	•	•	•	•	•	•	•	•	•	•	•	•
EMISTP, Extreme Multiple Instances of Spanning Tree Protocol	•	•	•	•	•	•	•	•	•	•	•	•
PVST+, Per VLAN STP (802.1Q interoperable)	•	•	•	•	•	•	•	•	•	•	•	•
Draft-ietf-bridge-rstpmib-03.txt – Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol	•	•	•	•	•	•	•	•	•	•	•	•
Extreme Standby Router Protocol (ESRP)	AE	AE	AE	AE	AE	AE	AE	AE	AE	AE	AE	AE
IEEE 802.1Q – 1998 Virtual Bridged Local Area Networks	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.3ad Static load sharing configuration and LACP based dynamic configuration	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1AX-2008 Link Aggregation	•	•	•	•	•	•	•	•	•	•	•	•
Software Redundant Ports	•	•	•	•	•	•	•	•	•	•	•	•
Multi-Switch Link Aggregation Groups (M-LAG)	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1AB – LLDP Link Layer Discovery Protocol	•	•	•	•	•	•	•	•	•	•	•	•
LLDP Media Endpoint Discovery (LLDP-MED), ANSI/TIA-1057, draft 08	•	•	•	•	•	•	•	•	•	•	•	•
Extreme Discovery Protocol (EDP)	•	•	•	•	•	•	•	•	•	•	•	•
Cisco Discovery Protocol (CDP) v1	•	•	•	•	•	•	•	•	•	•	•	•
Cisco Discovery Protocol (CDP) v2[17]	•	•	•	-	-	-	•	-	•	-	•	-
Extreme Loop Recovery Protocol (ELRP)	•	•	•	•	•	•	•	•	•	•	•	•
Extreme Link State Monitoring (ELSM)	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1ag L2 Ping and traceroute, Connectivity Fault Management	•	•	•	•	•	•	•	•	•	•	•	•
ITU-T Y.1731 Frame Delay	•	•	•	•	•	•	•	•	•	•	•	•
ITU-T Y.1731 Frame Loss	-	-	•	•	•	•	-	•	•	•	•	•
IEEE 802.3ah Ethernet OAM – Unidirectional Link Fault Management	•	•	•	•	-	•	•	•	•	•	•	•

[17] CDPv2 is supported on X440-G2, X450-G2, X460-G2, X620, X670-G2, and X770 series switches running EXOS 21.1 or beyond code

ExtremeXOS Supported Protocols and Standards (cont.)

	X440-G2	X450-G2	X460-G2	X465	X480	X590	X620	X670	X670-G2	X690	X770	X870
Switching (cont.)												
RFC 3619 Ethernet Automatic Protection Switching (EAPS) Version 1	•	•	•	•	•	•	•	•	•	•	•	•
ITU G.8032 Ethernet Ring Protection Switching	•	•	•	•	•	•	•	•	•	•	•	•
Extended Edge Switching Control Bridge	-	-	-	•	-	•	-	-	•	•	-	-
IEEE 802.1 Audio Video Bridging (AVB) standards	AV	AV	AV	-	-	-	AV	-	AV	-	AV	-
IEEE 802.1Qjc Fabric Attach	•	•	•	•	-	•	•	-	•	•	•	•
LRM/MACsec Adapter[18]	•	•	•	-	-	•	•	-	•	•	-	-
OpenFlow Protocol 1.0	OF	OF	OF	-	OF	-	OF	OF	OF	OF	OF	OF
- Management and Traffic Analysis												
RFC 2030 SNTP, Simple Network Time Protocol v4	•	•	•	•	•	•	•	•	•	•	•	•
RFC 5905 1 – Network Time Protocol Version 4: Protocol and Algorithms Specification	•	•	•	•	•	•	•	•	•	•	•	•
RFC 854 Telnet client and server	•	•	•	•	•	•	•	•	•	•	•	•
RFC 783 TFTP Protocol (revision 2)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 951, 1542 BootP	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2131 BOOTP/DHCP relay agent and DHCP server	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3315, Dynamic Host Configuration Protocol for IPV6 (DHCPv6), Client and Relay Function(Secondary IP address only) support.	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1591 DNS (client operation)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 6106, IPv6 Router Advertisement Options for DNS Configuration	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1155 Structure of Management Information (SMIv1)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1157 SNMPv1	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1212, RFC 1213, RFC 1215 MIB-II, Ethernet-Like MIB and TRAPs	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1573 Evolution of Interface	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1650 Ethernet-Like MIB (update of RFC 1213 for SNMPv2)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1901 to – 1908 SNMPv2c, SMIv2 and Revised MIB-II	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3 of the Internet standard Network Management Framework	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2578 – 2580 SMIv2 (update to RFC 1902 – 1903)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3410 – 3415 SNMPv3, user based security, encryption and authentication	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3416 – Protocol Operations for Version 2 of SNMP	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2418 – Management Information Base for SNMP	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3826 – The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1AB LLDP Basic MIB, LLDP-EXT-DOT1-MIB, LLDP-EXT-DOT3-MIB	•	•	•	•	•	•	•	•	•	•	•	•

[18] Requires a MACsec Feature Pack license for MACsec encryption

ExtremeXOS Supported Protocols and Standards (cont.)

	X440-G2	X450-G2	X460-G2	X465	X480	X590	X620	X670	X670-G2	X690	X770	X870
Management and Traffic Analysis (cont.)												
RFC 1757 RMON 4 groups: Stats, History, Alarms and Events	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2021 RMON2 (probe configuration)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2613 SMON MIB	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2925 Ping/Traceroute MIB	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2665 – Definitions of Managed Objects for the Ethernet-like Interface types	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2668 802.3 Medium Attachment Units (MAU) MIB	•	•	•	•	•	•	•	•	•	•	•	•
draft-ietf-hubmib-mau- mib-v3-02.txt	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1643 Ethernet MIB	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1493 Bridge MIB	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2096 IPv4 Forwarding Table MIB	•	•	•	•	•	•	•	•	•	•	•	•
RFC 6933 Entity MIB v4	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2233 Interface MIB	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3621 PoE-MIB (PoE switches only)	•	•	•	-	•	-	-	-	-	-	-	-
PIM MIB draft-ieft-pim-mib-v2-01.txt	•	•	•	•	•	•	•	•	•	•	•	•
IEEE-8021-PAE-MIB	•	•	•	•	•	•	•	•	•	•	•	•
IEEE-8021x-EXTENSIONS- MIB	•	•	•	•	•	•	•	•	•	•	•	•
EAPS MIB supports get functions	•	•	•	•	•	•	•	•	•	•	•	•
Secure Shell (SSH-2) client and server	•	•	•	•	•	•	•	•	•	•	•	•
Secure Copy (SCP-2) client and server	•	•	•	•	•	•	•	•	•	•	•	•
Secure FTP (SFTP) server	•	•	•	•	•	•	•	•	•	•	•	•
sFlow version 5	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3917 IPFIX	-	-	•	-	•	-	-	-	-	-	-	-
Application Telemetry	•	•	•	•	-	•	•	-	•	•	•	•
Extreme Insight Architecture	-	-	-	•	-	-	-	-	-	-	-	-
Configuration logging	•	•	•	•	•	•	•	•	•	•	•	•
Multiple Images, Multiple Configs	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3164 BSD Syslog Protocol with Multiple Syslog Servers – 999 Local Messages (criticals stored across reboots)	•	•	•	•	•	•	•	•	•	•	•	•
Extreme Networks vendor MIBs (includes statistics, FDB, PoE, CPU, Memory, ACL, CLEAR-Flow etc MIBs)	•	•	•	•	•	•	•	•	•	•	•	•
XML APIs over Telnet/SSH and HTTP/HTTPS	•	•	•	•	•	•	•	•	•	•	•	•
Multiple Images, Multiple Configs	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3164 BSD Syslog Protocol with Multiple Syslog Servers – 999 Local Messages (criticals stored across reboots)	•	•	•	•	•	•	•	•	•	•	•	•
Extreme Networks vendor MIBs (includes statistics, FDB, PoE, CPU, Memory, ACL, CLEAR-Flow etc MIBs)	•	•	•	•	•	•	•	•	•	•	•	•
XML APIs over Telnet/SSH and HTTP/HTTPS	•	•	•	•	•	•	•	•	•	•	•	•

ExtremeXOS Supported Protocols and Standards (cont.)

	X440-G2	X450-G2	X460-G2	X465	X480	X590	X620	X670	X670-G2	X690	X770	X870
Management and Traffic Analysis (cont.)												
Web-based device management interface – ExtremeXOS Chalet	•	•	•	•	•	•	•	•	•	•	•	•
IP Route Compression	•	•	•	•	•	•	•	•	•	•	•	•
RFC4805 - Managed Objects for DS1, J1, E1, DS2 and E2 interfaces	-	-	•	-	-	-	-	-	-	-	-	-
IEEE802.1 Q BRIDGE MIB	•	•	•	•	•	•	•	•	•	•	•	•
ENTERASYS-MAC-LOCKING	•	•	•	•	•	•	•	•	•	•	•	•
ENTERASYS-POLICY-PROFILE-MIB	•	•	•	•	-	•	•	-	•	•	•	•
ENTERASYS-UPN-TC-MIB	•	•	•	•	-	•	•	-	•	•	•	•
ENTERASYS-CLASS-OF-SERVICE-MIB	•	•	•	•	•	•	•	•	•	•	•	•
ENTERASYS-RADIUS-ACCT-CLIENT-EXT-MIB	•	•	•	•	•	•	•	•	•	•	•	•
ENTERASYS-RADIUS-AUTH-CLIENT-MIB	•	•	•	•	•	•	•	•	•	•	•	•
ENTERASYS-MULTI-AUTH-MIB	•	•	•	•	-	•	•	-	•	•	•	•
ENTERASYS-MAC-AUTHENTICATION-MIB	•	•	•	•	•	•	•	•	•	•	•	•
ENTERASYS-MULTI-USER-8021X-MIB	•	•	•	•	-	•	•	-	•	•	•	•
ENTERASYS-VLAN-AUTHORIZATION-MIB	•	•	•	•	-	•	•	-	•	•	•	•
RFC5604 - Managed Objects for Time Division Multiplexing (TDM)	-	-	-	-	-	-	-	-	-	-	-	-
IPv6 Router Advertisement Filtering	•	•	•	•	•	•	•	•	•	•	•	•
SFF-8472 DDMI (Digital Diagnostics Monitoring Interface)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3014 Notification Log MIB	•	•	•	•	•	•	•	•	•	•	•	•
draft-ietf-bfd-mib-14 BFD MIB	•	•	•	-	•	-	•	•	•	-	•	•
draft-ietf-bfd-tc-mib-02 Definitions of Textual Conventions (TCs) for BFD Management	•	•	•	•	•	•	•	•	•	•	•	•
MEF-36 Y.1731 Compliant Performance Monitoring SNMP MIB	•	•	•	•	•	•	•	•	•	•	•	•
Stacking SummitStack	-	•	•	-	-	-	-	-	-	-	-	-
Stacking SummitStackV	•	•	•[14]	-	•	-	•	•	•	-	•	-
Stacking SummitStackV80	-	-	-	-	•	-	-	•[16]	•[16]	-	•	-
Stacking SummitStackV84	-	•	-	-	-	-	-	-	-	-	-	-
Stacking SummitStackV160	-	-	•	•	•	•	-	•[16]	•[16]	•	•	-
Stacking SummitStackV320	-	-	-	-	•	•	-	•[16]	•[16]	•	•	•
Stacking SummitStackV400	-	-	-	-	-	•	-	-	-	•	-	•
Stacking SummitStack128	-	-	-	-	•[3]	-	-	-	-	-	-	-
Power Over Ethernet (PoE)												
RFC 3621 Power over Ethernet MIB	•	•	•	•	•	-	-	-	-	-	-	-
IEEE 802.3af Standard	•	•	•	•	•	-	-	-	-	-	-	-
IEEE 802.3bt Standard	-	-	-	•	-	-	•	-	-	-	-	-

[14] SummitStackV is not support on 1G variants of X460-G2

[16] Supported on QSFP+ ports only—X670V with VIMG4X and X670-G2-48x-4q

ExtremeXOS Supported Protocols and Standards (cont.)

	X440-G2	X450-G2	X460-G2	X465	X480	X590	X620	X670	X670-G2	X690	X770	X870
Power Over Ethernet (PoE) (cont.)												
IEEE 802.az Energy Efficient Ethernet (EEE)	•	•	•	•	-	-	-	•	-	-	-	-
Fast PoE	-	-	-	•	-	-	-	-	-	-	-	-
Perpetual PoE	-	-	-	•	-	-	-	-	-	-	-	-
Security, Switch, and Network Protection												
Role Based Policy	•	•	•	•	-	•	•	-	•	•	•	•
Multi-User, Multi-method authentication and policy	•	•	•	•	•	•	•	•	•	•	•	•
Secure Shell (SSH-2), Secure Copy (SCP-2), and SFTP client/server with encryption/authentication	•	•	•	•	•	•	•	•	•	•	•	•
SNMPv3 user based security, with encryption/ authentication	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1492 TACACS+	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2865 RADIUS Authentication	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2866 RADIUS Accounting	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3579 RADIUS EAP support for 802.1x	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3580 IEEE 802.1x RADIUS Guidelines, Dynamic VLAN assignment via RADIUS tunnel attributes	•	•	•	•	•	•	•	•	•	•	•	•
RADIUS Per-command Authentication	•	•	•	•	•	•	•	•	•	•	•	•
RADIUS Server Load Balancing	•	•	•	•	•	•	•	•	•	•	•	•
Access Profiles on All Routing Protocols	•	•	•	•	•	•	•	•	•	•	•	•
Access Policies for Telnet/ SSH-2/SCP-2	•	•	•	•	•	•	•	•	•	•	•	•
Network Login – 802.1x, Web and MAC-based mechanisms	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1x – 2004 Port-Based Network Access Control for Network Login	•	•	•	•	•	•	•	•	•	•	•	•
RFC 4668 RADIUS Authentication Client MIB for IPv6	•	•	•	•	•	•	•	•	•	•	•	•
RFC 4670 RADIUS Accounting Client MIB for IPv6	•	•	•	•	•	•	•	•	•	•	•	•
Multiple supplicants with multiple VLANs for Network Login (all modes)	•	•	•	•	•	•	•	•	•	•	•	•
Fallback to local authentication database (MAC and Web-based methods)	•	•	•	•	•	•	•	•	•	•	•	•
Guest VLAN for 802.1x	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1866 HTML – used for Web-based Network Login and ExtremeXOS Chalet	•	•	•	•	•	•	•	•	•	•	•	•
SSL/TLS transport – used for Web-based Network Login and ExtremeXOS Chalet	•	•	•	•	•	•	•	•	•	•	•	•
MAC Security – Lockdown and Limit	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1AE MACsec Link Encryption	•[19]	•[19]	•[19, 20]	•	-	•[19]	•[19]	-	•[19]	•[19]	-	-
IP Security – RFC 3046 DHCP Option 82 with port and VLAN ID	•	•	•	•	•	•	•	•	•	•	•	•
IP Security – Trusted DHCP Server	•	•	•	•	•	•	•	•	•	•	•	•
Layer 2/3/4 Access Control Lists (ACLs)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2267 Network Ingress Filtering	•	•	•	•	•	•	•	•	•	•	•	•
RPF (Unicast Reverse Path Forwarding) Control via ACLs	•	•	•	•	•	•	•	•	•	•	•	•

[3] X480 with conversion cable to SummitStack256

[16] Supported on QSFP+ ports only—X670V with VIMG4X and X670-G2-48x-4q

ExtremeXOS Supported Protocols and Standards (cont.)

	X440-G2	X450-G2	X460-G2	X465	X480	X590	X620	X670	X670-G2	X690	X770	X870
Security, Switch, and Network Protection (cont.)												
Wire-speed ACLs	•	•	•	•	•	•	•	•	•	•	•	•
Rate Limiting/Shaping by ACLs	•	•	•	•	•	•	•	•	•	•	•	•
IP Broadcast Forwarding Control	•	•	•	•	•	•	•	•	•	•	•	•
ICMP and IP-Option Response Control	•	•	•	•	•	•	•	•	•	•	•	•
SYN attack protection	•	•	•	•	•	•	•	•	•	•	•	•
CPU DoS Protection with traffi rate-limiting to management CPU	•	•	•	•	•	•	•	•	•	•	•	•
Security, Router Protection												
IP Security – DHCP enforcement via Disable ARP Learning	•	•	•	•	•	•	•	•	•	•	•	•
IP Security – Gratuitous ARP Protection	•	•	•	•	•	•	•	•	•	•	•	•
IP Security – DHCP Secured ARP/ARP Validation	•	•	•	•	•	•	•	•	•	•	•	•
Routing protocol MD5 authentication	•	•	•	•	•	•	•	•	•	•	•	•
CLEAR-Flow, threshold- based alerts and actions	•	•	•	•	•	•	•	•	•	•	•	•
Identity Manager	•	•	•	•	•	•	•	•	•	•	•	•
IPv4 Host Services												
RFC 1122 Requirements for internal hosts – Communication Layers	•	•	•	•	•	•	•	•	•	•	•	•
RFC 768 User Datagram Protocol (UDP)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 791 Internet Protocol (IP)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 792 Internet Control Message Protocol (ICMP)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 793 Transmission Control Protocol (TCP)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 826 Address Resolution Protocol (ARP)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 894 IP over Ethernet	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3021 Using 31-Bit Prefixes on IPv4 Point-to-Point Links	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1027 Proxy ARP	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2068 HTTP server	•	•	•	•	•	•	•	•	•	•	•	•
IGMP v1/v2 Snooping with Configurable Router Registration Forwarding	•	•	•	•	•	•	•	•	•	•	•	•
IGMP v3 Snooping with Configurable Router Registration Forwarding	•	•	•	•	•	•	•	•	•	•	•	•
IGMP Filters	•	•	•	•	•	•	•	•	•	•	•	•
PIM Snooping	•	•	•	•	•	•	•	•	•	•	•	•
Static IGMP Membership	•	•	•	•	•	•	•	•	•	•	•	•
Multicast VLAN Registration (MVR)	•	•	•	•	•	•	•	•	•	•	•	•
Static Unicast Routes	•	•	•	•	•	•	•	•	•	•	•	•
Static Multicast Routes	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1112 IGMP v1	•	•	•	•	•	•	•	•	•	•	•	•

[19] MACsec encryption supported using the external LRM/MACsec Adapter; also requires a MACsec Feature Pack license.

[20] MACsec encryption supported natively on X460-G2-24t-24ht-10GE4 and X460-G2-24p-24hp-10GE4 models; requires a MACsec Feature Pack License.

ExtremeXOS Supported Protocols and Standards (cont.)

	X440-G2	X450-G2	X460-G2	X465	X480	X590	X620	X670	X670-G2	X690	X770	X870
IPv4 Host Services (cont.)												
RFC 2236 IGMP v2	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3376 IGMP v3	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2933 IGMP MIB	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1812 Requirements for IP Version 4 Routers	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1519 An architecture for IP Address allocation with CIDR	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1256 IPv4 ICMP Router Discovery (IRDP)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1058 RIP v1	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2453 RIP v2	•	•	•	•	•	•	•	•	•	•	•	•
Static ECMP	-	•	•	•	•	•	•	•	•	•	•	•
RFC 2096 IPv4 Forwarding Table MIB	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1724 RIPv2 MIB	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2338 Virtual Router Redundancy Protocol	AE	AE	AE	•	•	•	AE	•	•	•	•	•
RFC 3768 VRRPv2	AE	AE	AE	•	•	•	AE	•	•	•	•	•
RFC 2787 VRRP MIB	AE	AE	AE	•	•	•	AE	•	•	•	•	•
RFC 2328 OSPF v2 (Edge-mode)	AE	AE	AE	•	•	•	AE	•	•	•	•	•
OSPF ECMP	-	AE	AE	•	•	•	AE	•	•	•	•	•
OSPF MD5 Authentication	AE	AE	AE	•	•	•	AE	•	•	•	•	•
RFC 1587 OSPF NSSA Option	AE	AE	AE	•	•	•	AE	•	•	•	•	•
RFC 1765 OSPF Database Overflow	AE	AE	AE	•	•	•	AE	•	•	•	•	•
RFC 2370 OSPF Opaque LSA Option	AE	AE	AE	•	•	•	AE	•	•	•	•	•
RFC 3623 OSPF Graceful Restart	AE	AE	AE	•	•	•	AE	•	•	•	•	•
RFC 1850 OSPFv2 MIB	AE	AE	AE	•	•	•	AE	•	•	•	•	•
RFC 2362 Protocol Independent Multicast – Sparse Mode PIM-SM (Edge- mode)	AE	AE	AE	•	•	•	AE	•	•	•	•	•
RFC 2934 Protocol Independent Multicast MIB	AE	AE	AE	•	•	•	AE	•	•	•	•	•
RFC 3569, draft-ietf-ssm- arch-06.txt PIM-SSM PIM Source Specific Multicast	AE	AE	AE	•	•	•	AE	•	•	•	•	•
draft-ietf-pim-mib-v2-o1.txt	AE	AE	AE	•	•	•	AE	•	•	•	•	•
Mtrace, a “traceroute” facility for IP Multicast: draft-ietf- idmr-traceroute-ipm-07	AE	AE	AE	•	•	•	AE	•	•	•	•	•
Mrinfo, the multicast router information tool based on Appendix-B of draft-ietf- idmr-dvmrp-v3-11	AE	AE	AE	•	•	•	AE	•	•	•	•	•
PIM ECMP Load Splitting	AE	AE	•	•	•	•	AE	•	•	•	•	•
PIM-SM	AE	AE	•	•	•	•	AE	•	•	•	•	•
RFC 3587, Global Unicast Address Format	•	•	•	•	•	•	•	•	•	•	•	•
Ping over IPv6 transport	•	•	•	•	•	•	•	•	•	•	•	•
Traceroute over IPv6 transport	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2460, Internet Protocol, Version 6 (IPv6) Specification	•	•	•	•	•	•	•	•	•	•	•	•

ExtremeXOS Supported Protocols and Standards (cont.)

	X440-G2	X450-G2	X460-G2	X465	X480	X590	X620	X670	X670-G2	X690	X770	X870
IPv4 Host Services (cont.)												
RFC 5095, Internet Protocol, Version 6 (IPv6) Specification	•	•	•	•	•	•	•	•	•	•	•	•
RFC 4861, Neighbor Discovery for IP Version 6, (IPv6)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2464, Transmission of IPv6 Packets over Ethernet Networks	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2465, IPv6 MIB, General Group and Textual Conventions	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2466, MIB for ICMPv6	•	•	•	•	•	•	•	•	•	•	•	•
RFC 4293, Management Information Base for the Internet Protocol (partial)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2462, IPv6 Stateless Address Auto configuration – Host Requirements	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1981, Path MTU Discovery for IPv6, August 1996 – Host Requirements	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3484, Default Address Selection for IPv6	•	•	•	•	•	•	•	•	•	•	•	•
Telnet server over IPv6 transport	•	•	•	•	•	•	•	•	•	•	•	•
SSH-2 server over IPv6 transport	•	•	•	•	•	•	•	•	•	•	•	•
RFC 4193, Unique Local IPv6 Unicast Addresses	•	•	•	•	•	•	•	•	•	•	•	•
RFC 5722, Handling of Overlapping IPv6	•	•	•	•	•	•	•	•	•	•	•	•
IPv6 Interworking and Migration												
RFC 2893, Configured Tunnels	-	AE	AE	•	•	•	-	•	•	•	•	•
RFC 3056, 6to4	-	AE	AE	•	•	•	-	•	•	•	•	•
IPv6 Router Services												
RFC 2462, IPv6 Stateless Address Auto Configuration – Router Requirements	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1981, Path MTU Discovery for IPv6, August 1996 – Router Requirements	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol	•	•	•	•	•	•	•	•	•	•	•	•
RFC 4291, IP Version 6 Addressing Architecture	•	•	•	•	•	•	•	•	•	•	•	•
RFC 4862, IPv6 Stateless Address Autoconfiguration	•	•	•	•	•	•	•	•	•	•	•	•
RFC 4443,Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	•	•	•	•	•	•	•	•	•	•	•	•
RFC 4541, Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches	•	•	•	•	•	•	•	•	•	•	•	•
Static Unicast routes for IPv6	•	•	•	•	•	•	•	•	•	•	•	•
RFC 6164, Using 127-Bit IPv6 Prefixes on Inter-Router Links	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2080, RIPng	•	•	•	•	•	•	•	•	•	•	•	•

ExtremeXOS Supported Protocols and Standards (cont.)

	X440-G2	X450-G2	X460-G2	X465	X480	X590	X620	X670	X670-G2	X690	X770	X870
IPv6 Router Services (cont.)												
RFC 2740 OSPF v3 for IPv6 (Edge-mode)	AE	AE	AE	•	•	•	AE	•	•	•	•	•
RFC 5187,OSPFv3 Graceful Restart	AE	AE	AE	•	-	•	AE	-	AE	•	AE	•
RFC 5340, OSPFv3, OSPF for IPv6	AE	AE	AE	•	-	•	AE	-	AE	•	AE	•
Static ECMP	-	•	•	•	•	•	•	•	•	•	•	•
RFC 5798 Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6	AE	AE	AE	•	•	•	AE	•	•	•	•	•
draft-ietf-vrrp-unified- mib-08.txt - Definitions of Managed Objects for VRRPv3	AE	AE	AE	•	•	•	AE	•	•	•	•	•
Core Protocols For Layer 2, IPv4 and IPv6												
EAPS multiple rings	-	AE	AE	•	•	•	AE	•	•	•	•	•
EAPSv2 Shared ports	-	AE	AE	•	C	AE	AE	C	•	•	•	•
PIM-DM Draft IETF PIM Dense Mode draft-ietf-idmr-pim-dm-05.txt, draft-ietf- pim-dm-new-v2-04.txt	-	C	C	C	C	C	-	C	C	C	C	C
Draft-ietf-idr-bgp4- mibv2-02.txt – Enhanced BGP-4 MIB	-	C	C	C	C	C	-	C	C	C	C	C
RFC 4724 Graceful Restart Mechanism for BGP	-	C	C	C	C	C	-	C	C	C	C	C
IOS 10589 OSI IS-IS Intra- Domain Routing Protocol (RFC 1142)	-	C	C	C	C	C	-	C	C	C	C	C
Draft-ietf-isis-ipv6-06 Routing IPv6 with IS-IS	-	C	C	C	C	C	-	C	C	C	C	C
Draft-ietf-isis-restart-02 Restart Signaling for IS-IS	-	C	C	C	C	C	-	C	C	C	C	C
Draft-ietf-isis-wg-multi- topology-11 Multi Topology (MT) Routing in IS-IS	-	C	C	C	C	C	-	C	C	C	C	C
RFC 1195 Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (TCP/IP transport only)	-	C	C	C	C	C	-	C	C	C	C	C
Draft-ietf-isis-ipv6-06 Routing IPv6 with IS-IS	-	C	C	C	C	C	-	C	C	C	C	C
Draft-ietf-isis-restart-02 Restart Signaling for IS-IS	-	C	C	C	C	C	-	C	C	C	C	C
Draft-ietf-isis-wg-multi- topology-11 Multi Topology (MT) Routing in IS-IS	-	C	C	C	C	C	-	C	C	C	C	C
RFC 1195 Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (TCP/IP transport only)	-	C	C	C	C	C	-	C	C	C	C	C
RFC 1745 BGP4/IDRP for IP-OSPF Interaction	-	C	C	C	C	C	-	C	C	C	C	C
RFC 1997 BGP Communities Attribute	-	C	C	C	C	C	-	C	C	C	C	C
RFC 2439 BGP Route Flap Damping	-	C	C	C	C	C	-	C	C	C	C	C
RFC 2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	-	C	C	C	C	C	-	C	C	C	C	C
RFC 2740 OSPFv3, OSPF for IPv6	-	C	C	C	C	C	-	C	C	C	C	C
RFC 2763 Dynamic Hostname Exchange Mechanism for IS-IS	-	C	C	C	C	C	-	C	C	C	C	C
RFC 2858 Multiprotocol Extensions for BGP-4 (Obsoletes RFC 2283)	-	C	C	C	C	C	-	C	C	C	C	C
RFC 2918 Route Refresh Capability for BGP-4	-	C	C	C	C	C	-	C	C	C	C	C
RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS	-	C	C	C	C	C	-	C	C	C	C	C
RFC 2973 IS-IS Mesh Groups	-	C	C	C	C	C	-	C	C	C	C	C

ExtremeXOS Supported Protocols and Standards (cont.)

	X440-G2	X450-G2	X460-G2	X465	X480	X590	X620	X670	X670-G2	X690	X770	X870
Core Protocols For Layer 2, IPv4 and IPv6 (cont.)												
RFC 3107 Carrying Label Information in BGP-4	-	C	C	C	C	C	-	C	C	C	C	C
RFC 3373 Three-way Handshake for IS-IS Point-to-Point Adjacencies	-	C	C	C	C	C	-	C	C	C	C	C
RFC 5492 Capabilities Advertisement with BGP-4	-	C	C	C	C	C	-	C	C	C	C	C
RFC 3446 Anycast RP using PIM and MSDP	-	C	C	C	C	C	-	C	C	C	C	C
RFC 3618 Multicast Source Discovery Protocol (MSDP)	-	C	C	C	C	C	-	C	C	C	C	C
RFC 3784 IS-IS Extensions for Traffic Engineering (wide metrics only)	-	C	C	C	C	C	-	C	C	C	C	C
RFC 4271 A Border Gateway Protocol 4 (BGP-4) (Obsoletes RFC 1771)	-	C	C	C	C	C	-	C	C	C	C	C
RFC 4273 Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2	-	C	C	C	C	C	-	C	C	C	C	C
RFC 4360 BGP Extended Communities Attribute	-	C	C	C	C	C	-	C	C	C	C	C
RFC 4456 BGP Route Reflection: An alternative to full mesh internal BGP (Obsoletes RFC 1966)	-	C	C	C	C	C	-	C	C	C	C	C
RFC 4486 Subcodes for BGP Cease Notification message	-	C	C	C	C	C	-	C	C	C	C	C
RFC 4760 Multiprotocol extensions for BGP-4	-	C	C	C	C	C	-	C	C	C	C	C
RFC 6793 BGP Support for Four-octet AS Number Space	-	C	C	C	C	C	-	C	C	C	C	C
RFC 5065 Autonomous System Confederations for BGP	-	C	C	C	C	C	-	C	C	C	C	C
RFC 5396 Textual Representation of Autonomous System (AS) Attributes	-	C	C	C	C	C	-	C	C	C	C	C
QoS and VLAN Services												
Quality of Service and Policies												
IEEE 802.1D – 1998 (802.1p) Packet Priority	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2474 DiffServ Precedence, including 8 queues/port	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2598 DiffServ Expedited Forwarding (EF)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2597 DiffServ Assured Forwarding (AF)	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2475 DiffServ Core and Edge Router Functions	•	•	•	•	•	•	•	•	•	•	•	•
Weighted Random Early Detection (WRED)	-	-	•	•	•	•	•	•	•	•	•	•
VLAN Services: VLANS, VMANS												
IEEE 802.1Q VLAN Tagging	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1v: VLAN classification by Protocol and Port	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.3ad Static Load sharing configuration and LACP based dynamic configuration	•	•	•	•	•	•	•	•	•	•	•	•
Port-based VLANs	•	•	•	•	•	•	•	•	•	•	•	•
Protocol-based VLANs	•	•	•	•	•	•	•	•	•	•	•	•
MAC-based VLANs	•	•	•	•	•	•	•	•	•	•	•	•
Multiple STP domains per VLAN	•	•	•	•	•	•	•	•	•	•	•	•

ExtremeXOS Supported Protocols and Standards (cont.)

	X440-G2	X450-G2	X460-G2	X465	X480	X590	X620	X670	X670-G2	X690	X770	X870
VLAN Services: VLANS, VMANS (cont.)												
Upstream Forwarding Only/Disable Flooding	•	•	•	•	•	•	•	•	•	•	•	•
VLAN Translation	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1ad Provider Bridge Network, virtual MANs (vMANs)	•	•	•	•	•	•	•	•	•	•	•	•
vMAN Ethertype Translation/Secondary vMAN Ethertype	•	•	•	•	•	•	•	•	•	•	•	•
Multicast Support for PVLAN	•	•	•	•	•	•	•	•	•	•	•	•
Multicast Support for VLAN Aggregation	•	•	•	•	•	•	•	•	•	•	•	•
VLAN Aggregation	•	AE	•	•	•	•	•	•	•	•	•	•
VLAN Bridging	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1AK MVRP and MRP	•	•	•	•	•	•	•	•	•	•	•	•
MPLS and VPN Services												
Multi-Protocol Label Switching (MPLS)												
RFC 2961 RSVP Refresh Overhead Reduction Extensions	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 3031 Multiprotocol Label Switching Architecture	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 3032 MPLS Label Stack Encoding	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 5036 Label Distribution Protocol (LDP)	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 3630 Traffic Engineering Extensions to OSPFv2	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 3811 Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 3812 Multiprotocol Label Switching (MPLS) Traffi Engineering (TE) Management Information Base (MIB)	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 3813 Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) MIB	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP[4]	MP
RFC 3815 Definition of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP[4]	MP
RFC 4090 Fast Re-route Extensions to RSVP-TE for LSP (Detour Paths)	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP[4]	MP
RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures (LSP Ping)	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP[4]	MP
draft-ietf-bfd-base-09.txt Bidirectional Forwarding Detection	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP[4]	MP
Layer 2 VPNs												
RFC 4447 Pseudowire Setup and Maintenance using the Label Distribution Protocol (LDP)	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 4762 Virtual Private LAN Services (VPLS) using Label Distribution Protocol (LDP) Signaling	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV)	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP

ExtremeXOS Supported Protocols and Standards (cont.)

	X440-G2	X450-G2	X460-G2	X465	X480	X590	X620	X670	X670-G2	X690	X770	X870
Layer 2 VPNs (cont.)												
RFC 5542 Definitions of Textual Conventions for Pseudowire (PW) Management	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 5601 Pseudowire Management Information Base (MIB)	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 5602 Pseudowire over MPLS PSN MIB	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 5603 Ethernet Pseudowire MIB	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
draft-ietf-l2vpn-vpls- mib-02.txt Virtual Private LAN Services (VPLS) MIB	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
Pseudowire LSP Loadsharing	-	-	MP	MP	-	MP	-	MP	MP	MP	MP	MP
RFC 5602 Pseudowire over MPLS PSN MIB	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
RFC 5603 Ethernet Pseudowire MIB	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
draft-ietf-l2vpn-vpls- mib-02.txt Virtual Private LAN Services (VPLS) MIB	-	-	MP	MP	MP	MP	-	MP	MP	MP	MP	MP
Pseudowire LSP Loadsharing	-	-	MP	MP	-	MP	-	MP	MP	MP	MP	MP
Layer 3 VPNs												
RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)	-	-	MP[8]	MP[8]	MP[8]	MP[8]	-	MP[8]	MP[8]	MP[8]	MP[8]	MP[8]
RFC 4382 MPLS/BGP Layer 3 Virtual Private Network (VPN) MIB	-	-	MP[9]	MP[9]	MP[9]	MP[9]	-	MP[9]	MP[9]	MP[9]	MP[9]	MP[9]
Timing Protocol												
Network Time Protocol	•	•	•	•	•	•	•	•	•	•	•	•
ITU-T G.8262 / G.8264 Synchronous Ethernet	-	-	•[15]	-	-	-	-	-	-	-	-	-
IEEE 1588v2 Precision Time Protocol (Slave/Ordinary clock)	-	-	NT[13]	-	-	-	-	-	NT	-	NT	-
IEEE 1588v2 Precision Time Protocol (Boundary and Transparent clock)	-	-	NT	-	-	-	-	-	NT	-	NT	-
Data Center												
RFC 7348 - Virtual eXtensible Local Area Network (VXLAN)	-	-	-	•	-	•	-	-	•	•	•	•
Direct Attach (IEEE 802 VEPA)	DA	DA	DA	•	DA	•	DA	DA	DA	•	DA	•
Priority Flow Control (IEEE 802.1Qbb)	-	-	•	•	-	•	•	•[11]	•	•	•	•
Data Center Bridging eXchange (DCBX) (IEEE P802.1Qaz/D2.3)	•	•	•	•	•	•	•	•	•	•	•	•
XNV (ExtremeXOS Network Virtualization)	•	-	•	•	•	•	•	•	•	•	•	•
SDN OpenStack	•	•	•	•	•	•	•	•	•	•	•	•
RestConf API	•	•	•	•	-	•	•	•	-	•	•	•

[8] Full except for section 9 and 10

[9] Full except for 1 table: mplsL3VpnVrfSecTable

[13] Requires X460-G2-TM-CLK module

[15] Supported on the first 8 copper ports of the t and p switch models. Supported on all x switch models and VIM-2t and VIM-2x

[4] In non-SummitStack configuration only

EXOS Release	Supported Platforms
16.X Release	• ExtremeSwitching X450-G2, X460-G2, X480, X670, X670-G2, X770 fixed series switches • ExtremeSwtiching X8 and 8800 modular series switching
21.X Release	• ExtremeSwitching X440-G2, X450-G2, X460-G2, X620, X670-G2, and X770 fixed series switches
22.X Release	• ExtremeSwitching X440-G2, X450-G2, X460-G2, X590, X620, X670-G2, X690, X770, and X870 fixed series switches • Extended Edge Switching V400 Port Extender switches
30.X Release	• ExtremeSwitching X440-G2, X450-G2, X465, X590 X460-G2, X620, X670-G2, X690, and X870 fixed series switches. • Extended Edge Switching V300-8P-2T-W and V400 Port Extender switches

**Except for the section titled "Technical Specification" Extreme Networks makes no warranty whatsoever with respect to any other data contained in this data sheet including any (A) Warranty of mechantability; or (B) Warranty of fitbess for a particular purpose; whether express or implied by law, course of dealing, course of performance, usage of trade or otherwise.

Extreme™
Customer-Driven Networking

http://www.extremenetworks.com/contact