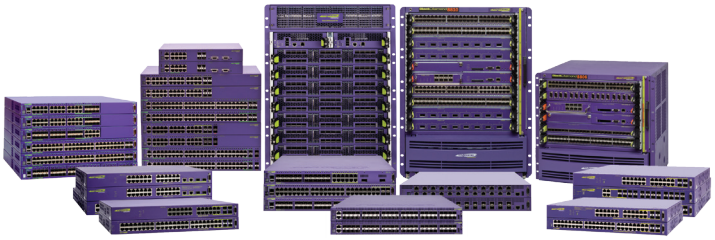
ExtremeXOS Operating System, Version 15.1



New in 15.1

ExtremeXOS® 15.1 provides enhanced identity-based policy management, availability, security and efficiency features and capabilities, including:

- BGP IPv6
- IPv6 Policy Based Routing
- Identity Manager enhancements including blacklists, whitelists, manual role assignment and LLDP-based roles
- ITU-T G.8032 Ethernet Ring Protection
- XNV™ (ExtremeXOS Network Virtualization) enhancements including VPP refresh and multiple ACLs
- ITU G.8262 SyncE and IEEE 1588v2PTP
- TDM Pseudowire
- Y.1731
- BOOTP Relay per VLAN
- WRED (Select Models)

Overview

ExtremeXOS is a modular, time hardened, extensible network operating system for robust, high performance networks. ExtremeXOS is built on a high availability architecture with rapid failover features such as Ethernet Automatic Protection Switching (EAPS), which helps reduce network downtime and ensure 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 end-point integrity checking, identity management, and protection for the network control and management planes.

Scripting capabilities allow automation of complex tasks, reducing the chance for human error and downtime.

Powerful APIs allow integration of specialized network 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

Extensibility

- Integrate best-of-breed applications to your network with an open, yet secure XML-based Application Programming Interface (API)
- Integrate Extreme Networks 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 access to the network through authentication, Network Login/802.1x, host integrity checking, and Identity Management
- Harden 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

Preemptive scheduling and memory protection allow applications or protocols, such as Open Shortest Path First (OSPF) and Spanning Tree Protocol (STP) – to run as separate processes that are protected from each other. This provides increased system integrity and inherent protection against DoS attacks.

ExtremeXOS offers high network availability using process monitoring and restart, where processes that have become unresponsive can be automatically restarted.

The modular design of ExtremeXOS allows applications, including security stacks such as SSH and SSL, to be upgraded while the switch is running, which reduces downtime due to updates which leads to higher availability (see Figure 1).

Hitless Failover and Graceful Restart

With dual management modules on BlackDiamond® chassis systems and advanced stacking support with Summit® 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 OSPF-2, BGP-4 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.

CPU Denial of Service Protection

A DoS attack is an attempt to degrade or disable a switch by using exploits that consume system resources, overwhelming the switch. ExtremeXOS CPU DoS protection helps prevent these attacks by detecting, analyzing and responding to these threats.

Extensibility

Dynamic Module Loading

ExtremeXOS provides a platform that can 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 export controlled functionality such

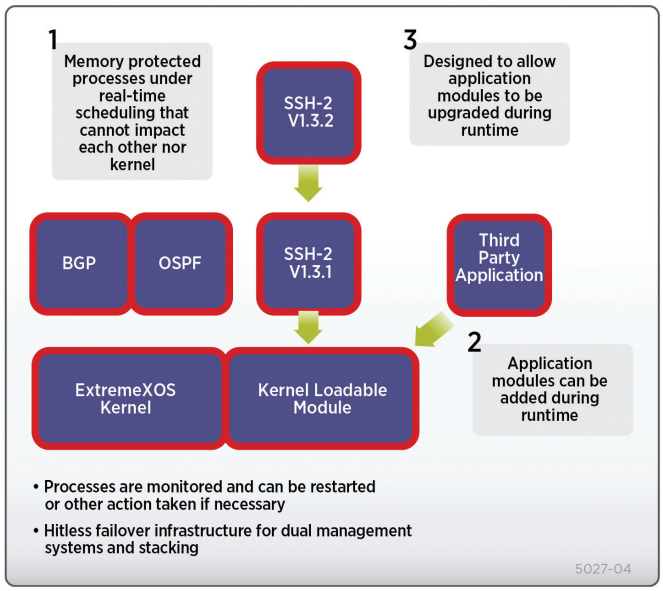


Figure 1: ExtremeXOS Modular Design

as SSH/SCP/SSL, avoiding the requirement for new operating system image installs to add these capabilities. 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 includes CLI-based scripting capabilities. Scripts can be used for a variety of tasks, automating network administration, which helps reduce errors stemming from manual configuration. Scripting capabilities, such as system- and user-defined environment variables, and constructs, such as if/then and loops, allow automating regular management tasks in scripts. This can help aid the deployment of configurations such as QoS, rate limiting and ACLs. Scripts can access CLI output, and a rich set of TCL functions provides 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 to provide a simple, secure mechanism to read information from the switch and push configuration, if desired. For example, a security appliance can use API hooks to limit access, control bandwidth or redirect traffic when integrated with Extreme Networks systems. 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

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.

Universal Port

ExtremeXOS Universal Port infrastructure is a powerful framework enabling event-driven activation of CLI scripts. Universal Port can leverage system event log messages as event triggers. 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-based authentication (Network Login/802.1x) and discovery protocols (LLDP + LLDP-MED) as trigger events. Actions in the form of fully configurable CLI scripts can be tied to events 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, fine-grained power budget requirements from the 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. Figure 2, below, explains the process. Please 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.

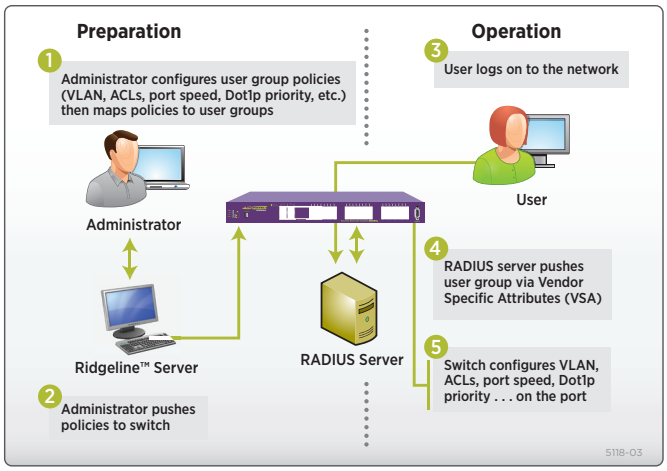


Figure 2: VoIP Auto Configuration with ExtremeXOS Universal Port

Integrated Security

Network Login

Extreme Networks open, standards-based approach allows network access control on all edge ports of a network. Access control works with or without dedicated authentication support on client devices, such as VoIP phones and printers.

Network Login enforces authentication before granting access to the network.

ExtremeXOS Network Login supports multiple supplicants on the same switch edge port, even in separate VLANs. For example, a VoIP phone can be authenticated into the voice VLAN, and a PC connected to the data port of the phone can be authenticated into a user-specific VLAN.

Network Login supports three methods: 802.1x, Web-based and MAC-based. All methods can be enabled individually or together to provide smooth implementation of a secured network.

Integrated Security

Dynamic security policies can be deployed via RADIUS Vendor Specific Attributes (VSAs). As an example, the VLAN for a given user or device can be dynamically assigned. Network Login can also create the VLAN if it does not exist on the edge switch, dramatically reducing the burden of managing VLANs. (see Figure 4).

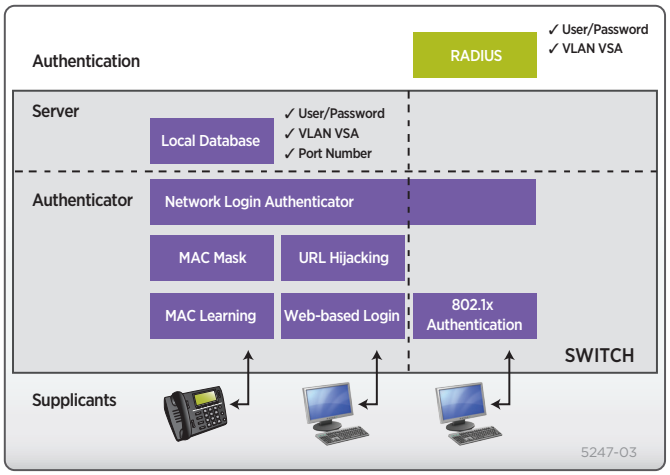


Figure 3: Network Login

Dynamic policies may also include rate limiting, QoS and dynamic ACLs. Dynamic security policies are activated and deactivated based on authentication and hosts connecting or disconnecting from the network. As the actual implementation of the policy can be changed from port to port, the framework allows for location-based policies. Integration with a timer event provides time-based policies, such as disabling wireless access after business hours.

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 can be used to dedicate ports to specific hosts or devices such as VoIP phones, cameras or printers and to avoid abuse of the port. 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

The ExtremeXOS IP security framework protects the network infrastructure, network services such as DHCP and DNS and even host computers from spoofing and man-in-the-middle attacks. It also provides network protection from statically configured and/or spoofed IP addresses as well as building an external trusted database of MAC/IP/port bindings providing insight into network traffic, allowing for immediate defense.

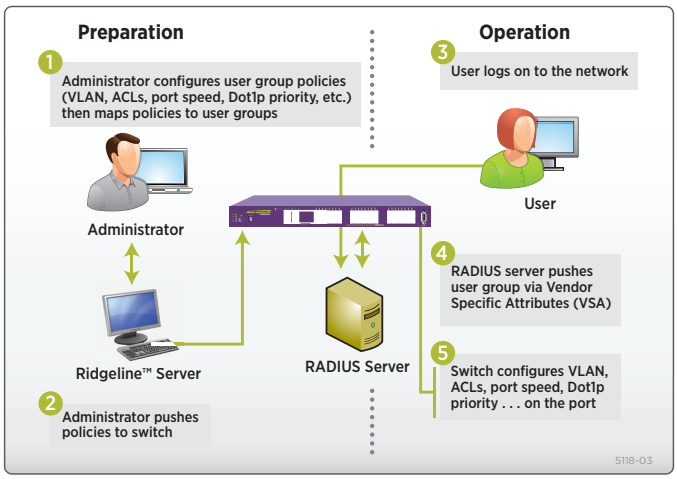


Figure 4: Universal Port Dynamic Policies

Identity Manager

Identity Manager allows network managers to track users who access their network. User identity is captured based on Network Login authentication, LLDP discovery and Kerberos snooping. ExtremeXOS uses the information to then report 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 further improves security by going beyond source/destination and MAC address as identification criteria to examine the IP address and VLAN of the user as well.

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, accepting 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.

Routing protocols such as OSPF-2 and BGP4 authenticate via MD5.

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 Networks 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), invented by Extreme Networks, is designed to prevent loops in a ring topology running Layer 2 traffic. Its role is similar to STP but it is able to rapidly converge when a link breaks in a manner transparent to VoIP and independent of the number of switches in a ring. Timing will be sub 50 ms in most deployments.

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 Networks 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 all geared to increasing 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, including a virtually unlimited address space. However, there are specific challenges regarding whether or not to transition to IPv6 now or hold off to further evaluate. Extreme Networks 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, 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 against attacks using IPv6 transport.

In the Data Center and in the Central Office

Data Centers

Data center managers face unique challenges, such as virtual machine mobility and security. ExtremeXOS supports multiple capabilities and features to support this ever-evolving environment.

XNV (ExtremeXOS Network Virtualization), available in the Data Center Feature Pack for Ridgeline™, a network and service management package, brings insight, control and automation for highly virtualized data centers to the network.

ExtremeXOS Direct Attach™, eliminates switching at 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. Direct Attach is available through the Direct Attach Feature Pack for select Extreme Networks switches.

Priority-based Flow Control (PFC), or IEEE 802.1Qbb, 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 eXchange (DCBX) or IEEE 802.1Qaz is used by Data Center Bridging (DCB) devices to exchange configuration information with directly connected peers. The protocol can be used for configuring PFC, ETS, and application parameters on peers. The protocol can also be used to detect misconfiguration in peers.

Multi-Switch Link Aggregation Groups (MLAG) can help 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.

MPLS

MPLS and H-VPLS are supported on multiple ExtremeXOS-based switches through licensable software modules. MPLS (Multi Protocol Label Switching) can support multiple service offerings and models, and offers traffic engineering, traffic management and out-of-band control. H-VPLS (Hierarchical Virtual Private LAN Service) allows business Ethernet service offerings to be deployed across geographically dispersed locations using Multi-Tenant Unit (MTU) switches.

Mobile Backhaul

With E4G cell site and cell site aggregation routers, ExtremeXOS is capable of providing carrier grade resiliency, synchronization and high performance Gigabit Ethernet switching for deploying true 4G mobile backhaul solutions.

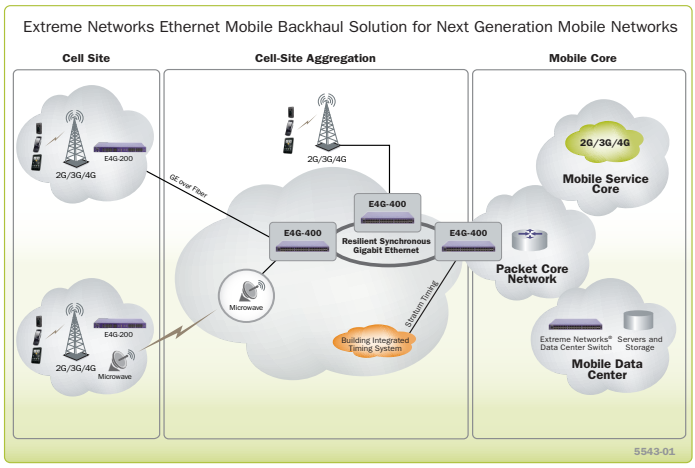


Figure 5: Mobile Backhaul

ExtremeXOS-based switches support two packet ring resiliency protocols, Ethernet Automatic Protection Switching (EAPS) – RFC 3619 and ITU-T 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

Technical Specifications

	Product Series													
ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
Switching														
IEEE 802.1D – 1998 Spanning Tree Protocol (STP)	•	•	•	•	•	•	•	•	•	•	•	•	•	•
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)	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1Q – 1998 Virtual Bridged Local Area Networks	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.3ad Static load sharing configuration and LACP based dynamic configuration	•	•	•	•	•	•	•	•	•	•	•	•	•	•

• Yes

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
Software Redundant Ports	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Multi-Switch Link Aggregation Groups (MLAG)	–	•	–	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1AB – LLDP Link Layer Discovery Protocol	•	•	•	•	•	•	•	•	•	•	•	•	•	•
LLDP Media Endpoint Discovery (LLDP-MED), ANSI/TIA-1057, draft 08	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Extreme Discovery Protocol (EDP)	•	•	•	•	•	•	•	•	•	•	•	•	•	•
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 measurements	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.3ah Ethernet OAM – Unidirectional Link Fault Management	–	–	–	–	–	• [1]	–	–	–	–	–	–	•	•
RFC 3619 Ethernet Automatic Protection Switching (EAPS) Version 1 and Version 2	•	•	•	•	•	•	•	•	•	•	•	•	•	•
ITU-T G.8032 Ethernet Ring Protection Switching	•	•	•	•	•	•	•	•	•	•	•	•	•	•
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 1591 DNS (client operation)	•	•	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1155 Structure of Management Information (SMIv1)	•	•	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1157 SNMPv1	•	•	•	•	•	•	•	•	•	•	•	•	•	•

[1] Only IPv4 server and peer address configuration is supported

• Yes | – No

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
RFC 1212, RFC 1213, RFC 1215 MIB-II, Ethernet-Like MIB & 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	•	•	•	•	•	•	•	•	•	•	•	•	•	•
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	•	•	•	•	•	•	•	•	•	•	•	•	•	•

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
RFC 2096 IPv4 Forwarding Table MIB	•	•	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2737 Entity MIB v2	•	•	•	•	•	•	•	•	•	•	•	•	•	•
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	•	•	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1657 Definitions of Managed Objects for BGPv4 using SNMPv2	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IEEE 802.1ag MIB	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Secure Shell (SSH-2) client and server	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Secure Copy (SCP-2) client and server	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Secure FTP (SFTP) server	•	•	•	•	•	•	•	•	•	•	•	•	•	•
sFlow version 5	•	•	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3917 IPFIX	–	–	–	–	–	–	•	•	–	–	• [2]	–	–	–
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	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Web-based device management interface – ExtremeXOS ScreenPlay™	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IP Route Compression	•	•	•	•	•	•	•	•	•	•	•	•	•	•
RFC4805 - Managed Objects for DS1, J1, E1, DS2 & E2 interfaces	–	–	–	–	–	–	–	–	–	–	–	–	•	•
RFC5604 - Managed Objects for Time Division Multiplexing (TDM)	–	–	–	–	–	–	–	–	–	–	–	–	•	•

[2] Support for Read-Only objects only

• Yes | – No

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
SFF-8472 DDMI (Digital Diagnostics Monitoring Interface)	–	–	–	–	–	–	–	•	–	–	•	–	–	–
Stacking – SummitStack™	–	•	–	•	•	•	•	•	•	–	–	–	–	•
Stacking – SummitStack-V	–	–	–	–	•	•	•	•	•	•	–	–	–	–
Stacking – SummitStack-V80	–	–	–	–	–	–	•	•	–	•	–	–	–	•
Stacking – SummitStack-V160	–	–	–	–	–	–	–	•	•	•	–	–	–	–
Stacking – SummitStack128	–	–	–	–	–	–	–	• [3]	–	–	–	–	–	–
Stacking – SummitStack256	–	–	–	–	–	–	–	–	•	–	–	–	–	–
Stacking – SummitStack512	–	–	–	–	–	–	–	–	•	–	–	–	–	–
Power over Ethernet (PoE)														
RFC 3621 Power over Ethernet MIB	•	•	–	•	•	•	•	•	–	–	•	–	•	•
IEEE 802.3af standard	•	•	–	•	•	•	•	•	–	–	•	–	•	•
Security, Switch and Network Protection														
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 2138 RADIUS Authentication	•	•	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2139 RADIUS Accounting	•	•	•	•	•	•	•	•	•	•	•	•	•	•
RFC 3579 RADIUS EAP support for 802.1x	•	•	•	•	•	•	•	•	•	•	•	•	•	•
RADIUS Per-command Authentication	•	•	•	•	•	•	•	•	•	•	•	•	•	•
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 – 2001 Port-Based Network Access Control for Network Login	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Multiple supplicants with multiple VLANs for Network Login (all modes)	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Fallback to local authentication database (MAC and Web-based methods)	•	•	•	•	•	•	•	•	•	•	•	•	•	•

[3] Supported on the following BlackDiamond 8800 modules - MSM48, MSM-48c, MSM-128, 8900-G48T-xl, 8900-10G24X-c, 8900-G48X-xl, 8900-10G8X-xl, 8900-G96T-c and 8900-40G

• Yes | – No

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
Guest VLAN for 802.1x	•	•	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1866 HTML – used for Web-based Network Login and ExtremeXOS ScreenPlay	•	•	•	•	•	•	•	•	•	•	•	•	•	•
SSL/TLS transport – used for Web-based Network Login and ExtremeXOS ScreenPlay	•	•	•	•	•	•	•	•	•	•	•	•	•	•
MAC Security – Lockdown and Limit	•	•	•	•	•	•	•	•	•	•	•	•	•	•
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	•	•	•	•	•	•	•	•	•	•	•	•	•	•
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 traffic rate-limiting to management CPU	•	•	•	•	•	•	•	•	•	•	•	•	•	•

• Yes

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
Robust against common network attacks: CERT (http://www.cert.org); CA-2003-04: "SQL Slammer;" CA-2002-36: "SSHredder;" CA-2002-03: SNMP vulnerabilities; CA-98-13: tcp-denial-of-service; CA-98.01: smurf; CA-97.28:Teardrop_Land -Teardrop and "LAND" attack; CA-96.26: ping; CA-96.21: tcp_syn_flooding; CA-96.01: UDP_service_ denial; CA-95.01: IP_Spoofing_Attacks_ and_Hijacked_ Terminal_ Connections; IP Options Attack	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Host Attack Protection: Teardrop, boink, opentear, jolt2, newtear, nestea, syndrop, smurf, fraggle, papasmurf, synk4, raped, winfreeze, ping –f, ping of death, pepsi5, Latierra, Winnuke, Simping, Sping, Ascend, Stream, Land, Octopus	•	•	•	•	•	•	•	•	•	•	•	•	•	•
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	–	•	–	•	•	•	•	•	•	•	•	•	•	•
Security Detection and Protection														
CLEAR-Flow, threshold-based alerts and actions	–	•	–	•	•	• [4]	•	• [4]	• [4]	•	•	•	•	•
Identity Manager	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IPv4 Host Services														
RFC 1122 Requirements for internal hosts – Communication Layers	•	•	•	•	•	•	•	•	•	•	•	•	•	•
RFC 768 User Datagram Protocol (UDP)	•	•	•	•	•	•	•	•	•	•	•	•	•	•

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
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 1027 Proxy ARP	•	•	•	•	•	•	•	•	•	•	•	•	•	•
RFC 2068 HTTP server	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IGMP v1/v2/v3 Snooping with Configurable Router Registration Forwarding	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IGMP Filters	•	•	•	•	•	•	•	•	•	•	•	•	•	•
PIM Snooping	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Static IGMP Membership	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Multicast VLAN Registration (MVR)	•	•	•	•	•	•	•	•	•	•	•	•	•	•
IPv4 Router Services														
Static Unicast Routes	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Static Multicast Routes	•	•	•	•	•	•	•	•	•	•	•	•	•	•
RFC 1112 IGMP v1	•	•	•	•	•	•	•	•	•	•	•	•	•	•
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	•	AE	•	•	•	•	•	•	•
OSPF MD5 Authentication	–	AE	–	AE	AE	•	AE	•	•	•	•	•	•	•

• Yes | – No | AE Requires Advanced Edge License Upgrade

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
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	•	•	•	•	•	•	•
IPv6 Host Services														
RFC 3587, Global Unicast Address Format	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Ping over IPv6 transport	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Traceroute over IPv6 transport	•	•	•	•	•	•	•	•	•	•	•	•	•	•
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 2462, IPv6 Stateless Address Auto configuration Host Requirements	–	•	–	•	•	•	•	•	•	•	•	•	•	•

• Yes | – No | AE Requires Advanced Edge License Upgrade

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
RFC 1981, Path MTU Discovery for IPv6, August 1996 – Host Requirements	–	•	–	•	•	•	•	•	•	•	•	•	•	•
RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture	–	•	–	•	•	•	•	•	•	•	•	•	•	•
Telnet server over IPv6 transport	–	•	–	•	•	•	•	•	•	•	•	•	•	•
SSH-2 server over IPv6 transport	–	•	–	•	•	•	•	•	•	•	•	•	•	•
IPv6 Interworking and Migration														
RFC 2893, Configured Tunnels	–	AE	–	AE	AE	•	AE	•	•	•	•	•	•	•
RFC 3056, 6to4	–	AE	–	AE	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	–	•	–	•	•	•	•	•	•	•	•	•	•	•
Static Unicast routes for IPv6	–	•	–	•	•	•	•	•	•	•	•	•	•	•
RFC 2080, RIPng	–	•	–	•	•	•	•	•	•	•	•	•	•	•
RFC 2740 OSPF v3 for IPv6 (Edge-mode)	–	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[2] - Definitions of Managed Objects for VRRPv3	–	AE	–	AE	AE	•	AE	•	•	•	•	•	•	•
Core Protocols for Layer 2, IPv4 and IPv6														
EAPSv2 Shared Ports – multiple interconnections between rings	–	–	–	–	–	C	C	C	C	C	C	C	C	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

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
Draft-ietf-idr-bgp4-mibv2-02.txt – Enhanced BGP-4 MIB	–	–	–	–	–	C	C	C	C	C	C	C	C	C
draft-ietf-idr-restart-10.txt Graceful Restart Mechanism for BGP	–	–	–	–	–	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
Draft-ietf-isis-ipv6-06 Routing IPv6 with IS-IS	–	–	–	–	–	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
Draft-ietf-isis-wg-multi-topology-11 Multi Topology (MT) Routing in IS-IS	–	–	–	–	–	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
RFC 1657 BGP-4 MIB	–	–	–	–	–	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
RFC 1771 Border Gateway Protocol 4	–	–	–	–	–	C	C	C	C	C	C	C	C	C
RFC 1965 Autonomous System Confederations for BGP	–	–	–	–	–	C	C	C	C	C	C	C	C	C
RFC 1997 BGP Communities Attribute	–	–	–	–	–	C	C	C	C	C	C	C	C	C
RFC 2283 Multiprotocol Extensions for BGP-4	–	–	–	–	–	C	C	C	C	C	C	C	C	C
RFC 2385 TCP MD5 Authentication for BGPv4	–	–	–	–	–	C	C	C	C	C	C	C	C	C
RFC 2439 BGP Route Flap Damping	–	–	–	–	–	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
RFC 2740 OSPFv3, OSPF for IPv6	–	–	–	–	–	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
RFC 2858 Multiprotocol Extensions for BGP-4 (Obsoletes RFC 2283)	–	–	–	–	–	C	C	C	C	C	C	C	C	C
RFC 2796 BGP Route Reflection (supersedes RFC 1966)	–	–	–	–	–	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

– No | C Requires Core License Upgrade

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS	–	–	–	–	–	C	C	C	C	C	C	C	C	C
RFC 2973 IS-IS Mesh Groups	–	–	–	–	–	C	C	C	C	C	C	C	C	C
RFC 3107 Carrying Label Information in BGP-4	–	–	–	–	–	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
RFC 3392 Capabilities Advertisement with BGP-4	–	–	–	–	–	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
RFC 3618 Multicast Source Discovery Protocol (MSDP)	–	–	–	–	–	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
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
RFC 4360 BGP Extended Communities Attribute	–	–	–	–	–	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
RFC 4486 Subcodes for BGP Cease Notification message	–	–	–	–	–	C	C	C	C	C	C	C	C	C
RFC 4274 Graceful Restart Mechanism for BGP (Obsoletes draft-ietf-idr-restart-10.txt)	–	–	–	–	–	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
RFC 4893 BGP Support for Four-octet AS Number Space	–	–	–	–	–	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
RFC 5396 Textual Representation of Autonomous System (AS) Attributes	–	–	–	–	–	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	•	•	•	•	•	•	•	•	•	•	•	•	•	•

• Yes | – No | C Requires Core License Upgrade

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
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)	–	–	–	–	–	–	•	•	•	•	•[3]	•	•	•
Traffic Engineering														
RFC 3784 IS-IS Externs for Traffic Engineering (wide metrics only)	•	•	•	•	•	•	•	•	•	•	•	•	•	•
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 & LACP based dynamic configuration	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Port-based VLANs	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Protocol-based VLANs	•	•	•	•	•	•	•	•	•	•	•	•	•	•
MAC-based VLANs	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Multiple STP domains per VLAN	•	•	•	•	•	•	•	•	•	•	•	•	•	•
Upstream Forwarding Only/ Disable Flooding	•	•	•	•	•	•	•	•	•	•	•	•	•	•
RFC 5517 Private VLANs	•	•	•	•	•	•	•	•	•	•	•	•	•	•
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	–	AE	AE	•	AE	•	•	•	•	•	•	•

[3] Supported on the following BlackDiamond 8800 modules - MSM48, MSM-48c, MSM-128, 8900-G48T-xl, 8900-10G24X-c, 8900-G48X-xl, 8900-10G8X-xl, 8900-G96T-c and 8900-40G

• Yes | – No | AE Requires Advanced Edge License Upgrade

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
MPLS and VPN Services														
Multi-Protocol Label Switching (MPLS)														
RFC 2961 RSVP Refresh Overhead Reduction Extensions	–	–	–	–	–	–	MP	MP	–	MP	MP[5]	MP	AE	•
RFC 3031 Multiprotocol Label Switching Architecture	–	–	–	–	–	–	MP	MP	–	MP	MP[5]	MP	AE	•
RFC 3032 MPLS Label Stack Encoding	–	–	–	–	–	–	MP	MP	–	MP	MP[5]	MP	AE	•
RFC 3036 Label Distribution Protocol (LDP)	–	–	–	–	–	–	MP	MP	–	MP	MP[5]	MP	AE	•
RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels	–	–	–	–	–	–	MP	MP	–	MP	MP[5]	MP	AE	•
RFC 3630 Traffic Engineering Extensions to OSPFv2	–	–	–	–	–	–	MP	MP	–	MP	MP[5]	MP	AE	•
RFC 3784 IS-IS extensions for traffic engineering only (wide metrics only)	–	–	–	–	–	–	MP	MP	–	MP	MP[5]	MP	AE	•
RFC 3811 Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management	–	–	–	–	–	–	MP	MP	–	MP	MP[5]	MP	AE	•
RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)	–	–	–	–	–	–	MP	MP	–	MP	MP[5]	MP	AE	•
RFC 3813 Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) MIB	–	–	–	–	–	–	MP	MP	–	MP	MP[5]	MP	AE	•
RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)	–	–	–	–	–	–	MP	MP	–	MP	MP[5]	MP	AE	•
RFC 4090 Fast Re-route Extensions to RSVP-TE for LSP (Detour Paths)	–	–	–	–	–	–	MP	MP	–	MP	MP[5]	MP	AE	•
RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures (LSP Ping)	–	–	–	–	–	–	MP	MP	–	MP	MP[5]	MP	AE	•
draft-ietf-bfd-base-09.txt Bidirectional Forwarding Detection	–	–	–	–	–	–	MP	MP	–	MP	MP[5]	MP	AE	•

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
Layer 2 VPNs														
RFC 4447 Pseudowire Setup and Maintenance using the Label Distribution Protocol (LDP)	–	–	–	–	–	–	MP	MP	–	MP	MP	MP	AE	•
RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks	–	–	–	–	–	–	MP	MP	–	MP	MP	MP	AE	•
RFC 4762 Virtual Private LAN Services (VPLS) using Label Distribution Protocol (LDP) Signaling	–	–	–	–	–	–	MP	MP	–	MP	MP	MP	AE	•
RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV)	–	–	–	–	–	–	MP	MP	–	MP	MP	MP	AE	•
RFC 5542 Definitions of Textual Conventions for Pseudowire (PW) Management	–	–	–	–	–	–	MP	MP	–	MP	MP	MP	AE	•
RFC 5601 Pseudowire Management Information Base (MIB)	–	–	–	–	–	–	MP	MP	–	MP	MP	MP	AE	•
RFC 5602 Pseudowire over MPLS PSN MIB	–	–	–	–	–	–	MP	MP	–	MP	MP	MP	AE	•
RFC 5603 Ethernet Pseudowire MIB	–	–	–	–	–	–	MP	MP	–	MP	MP	MP	AE	•
draft-ietf-l2vpn-vpls-mib-02.txt Virtual Private LAN Services (VPLS) MIB	–	–	–	–	–	–	MP	MP	–	MP	MP	MP	AE	•
Timing Protocol														
Network Time Protocol	•	•	•	•	•	•	•	•	•	•	•	•	•	•
ITU-T G.8262 Synchronous Ethernet	–	–	–	–	–	–	Y	–	-	–	–	–	•	•
IEEE 1588v2 Precision Time Protocol (Slave/Ordinary clock)	–	–	–	–	–	–	–	–	–	–	–	–	•	•
IEEE 1588v2 Precision Time Protocol (Boundary & Transparent clock)													NT[6]	NT[6]

ExtremeXOS 15.1 Supported Protocols and Standards	Summit X150	Summit X250e	Summit X350	Summit X440	Summit X450e	Summit X450a	Summit X460	Summit X480	Summit X650	Summit X670	BlackDiamond 8800	BlackDiamond X8	E4G-200	E4G-400
Data Center														
Direct Attach (IEEE 802 VEPA)	–	–	–	–	–	DA	DA	DA	DA	DA	DA	DA	–	–
Priority Flow Control (IEEE 802.1Qbb)	–	–	–	–	–	–	–	–	• [7]	–	• [8]	•	–	–
Data Center Bridging eXchange (DCBX) (IEEE P802.1Qaz/D2.3)	•	•	•	•	•	•	•	•	•	•	•	•	–	–
XNV (ExtremeXOS Network Virtualization)	–	–	–	–	–	•	•	•	•	•	•	•	–	–

Legend	
•	Yes
–	No
AE	Requires Advanced Edge License Upgrade
C	Requires Core License Upgrade
MP	Requires MPLS Feature Pack
NT	Requires Network Timing Feature Pack
DA	Requires Direct Attach Feature Pack

[1] Supported only in Summit X450a-24x
[2] Supported with BlackDiamond 8900-10G8X-xl, 8900-G48T-xl, 8900-G48X-xl or 8900-G96T-c modules only
[3] Summit X480 with conversion cable to SummitStack 256
[4] In non-SummitStack configuration only.
[5] Requires MPLS Feature Pack license, MSM128 and BlackDiamond 8900-10G8X-xl, 8900-G48X-xl or 8900-G48T-xl interface modules.
[6] Current support on Summit X460-24x and -48x with Network Timing Feature Pack only
[7] Summit X650 part numbers 17001B, 17002b and 17012B only
[8] BlackDiamond 8800 series with 10G24X module only (part number 41632B)

Make Your Network Mobile

Corporate and North America
Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, CA 95051 USA
Phone +1 408 579 2800

Europe, Middle East, Africa and South America
Phone +31 30 800 5100

Asia Pacific
Phone +65 6836 5437

Japan
Phone +81 3 5842 4011

extremenetworks.com