Summit® X450 Series

Summit X450 series switches—based on the revolutionary ExtremeXOS™ core-class operating system from Extreme Networks®.

Voice-Class Availability

- Modular ExtremeXOS operating system
- Ethernet Automatic Protection Switching (EAPS) resiliency protocol
- Resilient system design

Advanced Features Enable Versatile Deployment

- High bandwidth, non-blocking architecture for demanding edge applications
- High density gigabit ports with optional 10 gigabit uplinks that enable a high-performance aggregation layer
- Advanced routing protocols such OSPF, BGP and multicast for an efficient and productive small network core
- Exceptional Quality of Service (QoS) and traffic management features for triple play services in metro Ethernet networks

Comprehensive Security to Ward Off Attacks

- User policy and host integrity enforcement
- Detection and response to network intrusion
- Network infrastructure hardened against attacks

Summit X450 series switches extend the benefits of the modular ExtremeXOS operating system beyond the network core in a compact and versatile stackable switch.

The powerful and compact Summit X450 series switches are based on the revolutionary ExtremeXOS core-class operating system (OS) from Extreme Networks. ExtremeXOS is a highly resilient, modular OS that offers high availability and greatly enhances manageability. Summit X450 series switches have the same high-performance, non-blocking hardware technology used on Extreme Networks BlackDiamond® 8800 series switches, continuing in the Extreme Networks' tradition of simplifying network deployments through the use of common hardware and software throughout the network.

The extremely versatile Summit X450 series switches, with high-density gigabit plus optional 10 Gigabit Ethernet in a compact 1RU format, support a full range of Layer 2 to Layer 4 features on every port to help ensure highest productivity. Summit X450 series switches are available in two versions: fiber to support flexible and convenient modular optics, and copper suitable for local data distribution. Both versions have optional redundant power supplies to help ensure against power anomalies.

Target Applications

- Edge switch providing gigabit to the desk top in a simple two-tier network running ExtremeXOS from core to edge
- Single or redundant core of a small network
- Aggregation switch in a traditional three-tiered network extending the benefits of ExtremeXOS to the aggregation layer
- Highly available fixed switch providing server connectivity
- Aggregation switch in a metro Ethernet network

Voice-Class Availability

ExtremeXOS on Summit X450 switches supports process recovery and application upgrades without the need for a system reboot. The versatile Summit X450 switches, with the high network availability required for converged applications, can be used to connect switches at the aggregation layer or at the core of a small network.

Modular Operating System for Non-Stop Operation

True Preemptive Multitasking and Protected Memory

Summit X450 series switches allow each of the many tasks such as Ethernet Automatic Protection Switching (EAPS) and Virtual Router Redundancy Protocol (VRRP) to run as separate OS tasks that are protected from each other as shown in Figure 1.

Process Monitoring and Restart

ExtremeXOS dramatically increases network availability by monitoring in real time the independent OS processes. If any of them become unresponsive, or stop running, they are automatically restarted.

Loadable Software Modules

The modular design of ExtremeXOS allows the extension of switch functionality without loading a new OS image and restarting the switch. New functionality can be added to the switch on the fly.

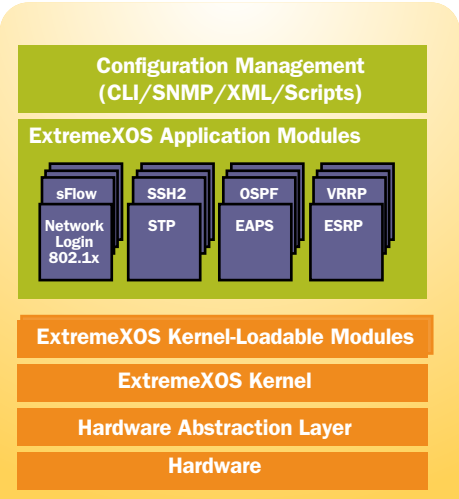


Figure 1: ExtremeXOS Modular Operating System

High Availability Network Protocols

Ethernet Automatic Protection Switching

EAPS allows the IP network to provide the level of resiliency and uptime that users expect from their traditional voice networks. EAPS is superior to Spanning Tree or Rapid Spanning Tree protocols and offers sub-second (less than 50 milliseconds) recovery that delivers consistent failover regardless of the number of VLANs, number of the network nodes or network topology. In most situations, Voice-over-IP calls don't drop and digital video feeds don't freeze or pixelize because EAPS enables the network to recover almost transparently from link failure.

Spanning Tree/Rapid Spanning Tree Protocols

Summit X450 series switches support Spanning Tree (802.1D), Per VLAN Spanning Tree (PVST+), Rapid Spanning Tree (802.1w) and Multiple Instances of Spanning Tree (802.1s) protocols for Layer 2 resiliency.

Software-Enhanced Availability

Software-enhanced availability allows users to remain connected to the network even if part of the network infrastructure is down. Summit X450 series switches constantly check for problems in the uplink connections using advanced Layer 3 protocols like OSPF, VRRP and ESRP (ESRP supported in Layer 2 or Layer 3), and dynamically routes around the problem.

Equal Cost Multipath

Equal Cost Multipath (ECMP) enables uplinks to be load balanced for performance and cost savings while also supporting redundant failover. If an uplink fails, traffic is automatically routed to the remaining uplinks and connectivity is maintained.

Link Aggregation (802.3ad)

Cross module link aggregation allows trunking of up to eight links on a single logical connection, for up to 80 gigabits per second (Gbps) of redundant bandwidth per logical connection.

Resilient System Design

Protected Data and OS for Availability

Summit X450 series switches are built with Error Checking and Correcting (ECC) RAM to protect routing tables and continue operation in spite of potentially disruptive memory events. Furthermore, the systems are designed with enough durable flash memory to contain dual OS images as well as two copies of configuration files as an added layer of precaution against potential crippling disruption.

Resilient Uplink Bandwidth

Summit X450 series switches offers optional dual 10 gigabit uplinks to provide near line-rate 24-to-20 user to uplink bandwidth ratio. Depending on requirements, full failover resilient links can be supported at Layer 2 with 802.3ad link aggregation, or Layer 3 with OSPF ECMP. Common deployments may call for 2.4:1 oversubscription, for which Summit X450 series switches deliver superior resiliency with the EAPS protocol.

Redundant Power Supplies

Summit X450 series switches support redundant power through their External Power Systems that provides a convenient, easy field upgradeable option for protection against power anomalies.

Advanced Features Enable Versatile Deployment

Summit X450 series switches provide a high bandwidth, non-blocking architecture with fiber or tri-speed copper gigabit ports for demanding edge applications. With optional 10 gigabit trunks, a Summit X450 connecting to gigabit edge devices can enable a high-performance aggregation layer in a traditional three-tier LAN. Summit X450 supports advanced protocols in the ExtremeXOS core license for an efficient small network core. For metro Ethernet networks, Summit X450 delivers exceptional QoS and traffic management capabilities. With superior resiliency, comprehensive security features and non-blocking performance, Summit X450 series switches are the cornerstone of a high-performance network.

High Bandwidth, Non-Blocking Architecture for Demanding Edge Applications

When deployed as an access switch, a Summit X450 series switch provides the bandwidth required by the most demanding application, thanks to its modular 10 gigabit ports and integrated fiber gigabit ports. With more than 20 gigabits of uplink capacity, bottlenecks don't exist, and with line-rate throughput and support for jumbo frames up to 9,216 bytes, transfers complete in minimal time.

High Density Gigabit Ports with Optional 10 Gigabit Uplinks That Enable a High-Performance Aggregation Layer

Gigabit to 10 Gigabit Aggregation

Summit X450 series switches provide a significant performance and feature upgrade for the aggregation layer. They eliminate the need to funnel traffic through a low bandwidth gigabit trunk by providing non-blocking 10 gigabit links to the core. Summit X450 series switches also provide superior network management with sFlow statistical sampling that samples traffic passing through the switch to facilitate detecting, diagnosing, and fixing network problems, congestion management, trending, and capacity planning. Summit X450 switches offer comprehensive traffic classification and security with their powerful Layers 2 – 4 Access Control Lists (ACLs) for greatest deployment flexibility.

Link Redundancy Protocols

Because of its location in the network at the crossroads of high-density traffic from many users, every connection to and from an aggregation switch must be redundant to allow a safe failover of traffic to a secondary path in case of link or device failure. Summit X450 series switches support superior link redundancy to provide a highly available aggregation layer.

For example, where voice-grade resiliency is required, only EAPS allows links to failover rapidly enough that voice call sessions are not dropped. Other link resiliency services in Summit X450 series switches include OSPF ECMP and VRRP, providing standards-based Layer 3 dual homing; ESRP that offers dual homing at both Layer 2 and Layer 3; and unique Software Redundant Port that allows easy-to-configure port redundancy without requiring any loop detection protocol.

Advanced Routing Protocols for Small Network Core

Supporting core deployments requires full protocol support. The Summit X450 series switches provide the advanced protocol environment for an efficient and productive small network core. Summit X450 series switches provide static and RIP routing for simple Layer 3 deployment. An optional ExtremeXOS core license extends the feature set to include important core features such as:

- Full OSPF for much greater extensibility than RIP can provide
- BGP for support of inter-autonomous system forwarding
- PIM, sparse and dense modes for routing of multicast streams
- OSPFv3 for IPv6 slow path support
- IPv6 tunnels, IPv6-to-IPv4 translation, IPv6 multicast discovery for extensive IPv6 support

Exceptional Quality of Service and Traffic Management for Triple Play Services

Metro deployments require exceptional QoS, an area where Summit X450 series switches excel, with eight hardware queues per port to support granular traffic classification, and 128 classifiers per ingress port that can use information from Layers 1 through 4 to prioritize and meter incoming packets at line-rate. When metering traffic, Summit X450 series switches can drop out of spec traffic or flag it for later action. To expedite upstream traffic handling, a packet's classification can be carried forward with Layer 2 (802.1p) and Layer 3 (DiffServ) markings. Summit X450 series switches' advanced traffic management features enable support for delivering the triple play of voice, video and data services.

Summit X450 series switches support Extreme Networks VMAN tag stacking mechanism which is compliant with the soon to be completed IEEE 802.1ad Provider Bridging standard. VMAN lets service providers aggregate over 16 million subscribers by using stacked Q-tags.

Summit X450 series switches are compliant with the UNI 1.0 Metro Ethernet Forum specification and support all the service parameters of MEF 6, the traffic management specification. Summit X450 series switches provide low latency and hardware-based support for multicast traffic, making them an excellent solution for deploying IPTV over a metro Ethernet infrastructure.

Enhanced Manageability with an ExtremeXOS Network

Within the Summit X450 series switches, Extreme Networks' innovative ExtremeXOS OS is the first modular OS to be universally deployed from the core to the edge of the network, significantly enhancing network manageability. Common ExtremeXOS from core to edge brings the immediate benefit of greatly reduced setup, configuration, and maintenance time, thanks to a common CLI and feature set. Deploying ExtremeXOS from edge to core extends the power of sFlow statistical reporting to assist in end-to-end congestion management and troubleshooting. ExtremeXOS is one of the first OSs to support Link Layer Discovery Protocol (LLDP), which allows discovery and configuration of LLDP-compliant objects on the network to speed installation, management and troubleshooting. At a global level, an ExtremeXOS-based network can be managed by EPICenter® to simplify global status monitoring, deployment of policies and network troubleshooting.

The ExtremeXOS-based network delivers consistent security, resiliency, QoS, and generally simplifies management to reduce the Total Cost of Ownership.

Comprehensive Security To Ward Off Attacks

Implementing a secure network requires the switches in the infrastructure to support a comprehensive set of security features. Security on Summit X450 series switches encompass three main areas: user and host integrity, threat detection and response, and hardened network infrastructure.

User and Host Integrity

Intelligent Network Access

Intelligent network access enforces user admission and usage policies. Summit X450 series switches support a comprehensive range of Network Login options by providing an 802.1x agent-based approach, a web-based (agentless) login capability for guests, and a MAC-based authentication model for devices. With these modes of Network Login, only authorized users and devices can connect to the network and assigned to the appropriate VLAN.

Multiple Supplicant Support

Multiple supplicant support secures IP Telephony and wireless access. Converged network designs often involve the use of shared ports. Examples include:

- PC plugging into an IP telephone
- Multiple users connecting to a wireless Access Point (AP) over the air and thereby sharing the same physical port

Shared ports represent a potential vulnerability in a network. Multiple supplicant capability on a switch allows it to uniquely recognize and apply the appropriate policies for each user or device on a shared port.

Media Access Control (MAC)

MAC lockdown secures printers, wireless APs and servers. The MAC address security/lockdown feature enables Summit X450 series switches to block access to any Ethernet port when the MAC address of a station attempting to access the port is different from the configured MAC address. This feature is used to "lock down" any device to a specific port.

Host Integrity Checking

Host integrity checking helps keep infected or non-compliant machines off the network. Summit X450 series switches support a host integrity or end point integrity solution that is based on the model from the Trusted Computing Group.

Detection and Response to Network Intrusion

sFlow

Providing powerful network visibility, sFlow is a sampling technology that provides the ability to continuously monitor application level traffic flows on all interfaces simultaneously. The sFlow agent is a software process that runs on Summit X450 series switches, and packages data into sFlow datagrams that are sent over the network to an sFlow Collector. The Collector has an up-to-the-minute view of traffic across the network, which can be used to troubleshoot network problems, control congestion and to detect network security threats.

Port Mirroring

In order to provide intrusion detection and prevention, Summit X450 series switches support many-to-one port mirroring. This can be used to mirror traffic to an external network appliance such as an intrusion detection device for trend analysis or be utilized by a network administrator as a diagnostic tool when fending off a network attack.

Line-Rate ACLs

ACLs are one of the most powerful tools to control network resource utilization and to secure and protect the network. Summit X450 series switches support ACLs based on Layer 2, 3 or 4-header information such as the MAC address or IP source/destination address.

Network Infrastructure Hardened Against Attacks

Denial of Service Protection

Summit X450 switches handle Denial of Service (DoS) attacks gracefully. If the switch detects an unusually large number of packets in the CPU input queue, it will assemble ACLs that automatically stop these packets from reaching the CPU. After a period of time, the ACLs are removed. If the attack continues, they are reinstalled. ASIC-based LPM routing eliminates the need for control plane software to learn new flows and allows the network to be resilient under a DoS attack.

Secure Management

The use of protocols like SSH2, SCP and SNMPv3 supported by Summit X450 series switches prevents the interception of management communications and man-in-the middle attacks. MD5 authentication of routing protocols prevents attackers from tampering valid messages and attacking routing sessions.

IPv6 Forwarding

For more than a decade, a new version of the ubiquitous Internet Protocol (IP) that powers global network interconnectivity has been under development, with the primary goal of expanding IP's address range to allow a unique IP address for any device in the world that might some day need to be addressable. Summit X450 series switches offer this next generation IP, forwarding both IPv4 and IPv6 traffic, with IPv6 being forwarded in software. The following is just a sample of IPv6 features that are supported with the optional core license:

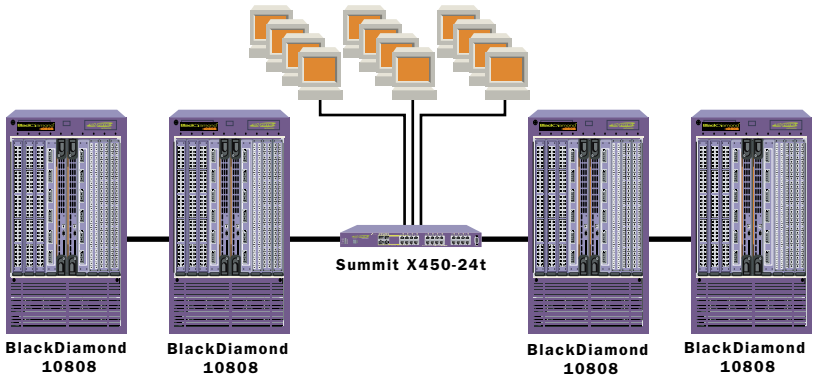
- IPv6 ACLs
- IPv4/IPv6 dual mode IP stack
- RIPng—RIP Next Generation, IPv6 enabled
- OSPFv3—OSPF for IPv6
- Multicast Listener Discovery (MLD) for IPv6
- Path MTU Discovery for IPv6
- IPv6 to IPv4 translation
- IPv6 Tunnels
- ICMPv6 messaging, traceroute, ping, SSH2

ExtremeXOS on Summit X450 series switches deliver more than just IPv6 forwarding; it provides the power to control undesired IPv6 traffic to assure network uptime in the presence of IPv6. Summit X450 series switches help provide investment protection by enabling the rollout of IPv6 in your network now or in the future, when needed.

Target Applications

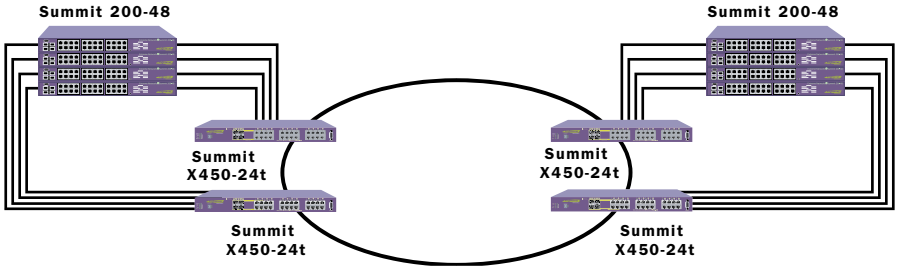
High-Performance Gigabit Edge

Summit X450 series switches provide high bandwidth access for demanding edge applications with their non-blocking architecture and optional dual 10 gigabit uplinks. They provide complete user authentication to protect the network from unauthorized access, and offer high availability features including resilient operating system, memory protection, and redundant power supplies to preserve user productivity.



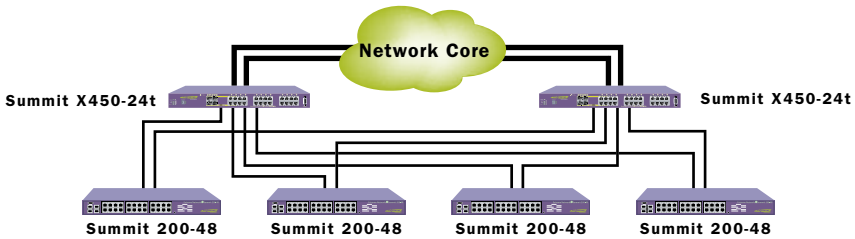
Small Network Core Switch

Summit X450 series switches are ideal small network core switches. Their optional 10 gigabit ports are perfect to set up a high bandwidth 10 gigabit backbone, or multiples of gigabit ports can be aggregated for inter-switch connectivity. All necessary core protocols are available, even BGPv4 and IPv6. With non-blocking performance, extensive DoS protection, Longest Prefix Match routing, and superior management including sFlow, a Summit X450 series switch is designed from the ground up to be a small core switch.



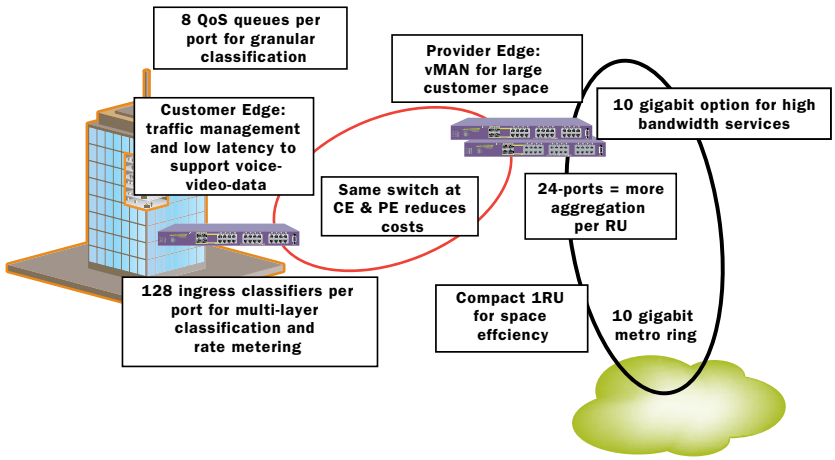
Traditional Aggregation Layer

Summit X450 series switches are easily deployed as a technology upgrade to a traditional aggregation layer, bringing 10 gigabit uplinks and high availability. For common fiber deployments, a pair of Summit X450-24xs provide multiple aggregation capacity of most switches in their class that have only twelve fiber ports, and no 10 gigabit ports.



Metro Ethernet Services

Summit X450 series switches are ideal service delivery platforms for metro Ethernet networks. Their advanced traffic management, resiliency and scalability features give them the flexibility to be deployed at the CE or as an aggregation switch at the PE. By supporting both CE and PE service delivery requirements, Summit X450 series switches greatly reduce a service provider's operational expense.



Technical Specifications

ExtremeXOS 11.6 Supported Protocols

Switching
- RFC 3619 Ethernet Automatic Protection Switching (EAPS) and EAPSv2
- 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)
- 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
- 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)
- Software Redundant Ports

VLANs, vMANs + MAC-in-MAC
- IEEE 802.1Q VLAN Tagging
- IEEE 802.1v: VLAN classification by Protocol and Port
- Port-based VLANs
- Protocol-based VLANs
- Multiple STP domains per VLAN
- IEEE 802.1ad Virtual MANs (vMANs)

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

IPv4
- RFC 1812 Requirements for IP Version 4 Routers
- RFC 1519 CIDR
- RFC 1256 IPv4 ICMP Router Discovery (IRDP)
- RFC 1122 Host Requirements
- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 894 IP over Ethernet
- RFC 1027 Proxy ARP
- RFC 2068 HTTP server – Used for web-based Network Login
- RFC 2338 VRRP
- Static Unicast Routes
- Static Multicast Routes
- RFC 1058 RIP v1
- RFC 2453 RIP v2
- RFC 2328 OSPF v2 (including MD5 authentication)
- RFC 1587 OSPF NSSA Option
- RFC 1765 OSPF Database Overflow
- RFC 2370 OSPF Opaque LSA Option
- RFC 3623 OSPF Graceful Restart
- RFC 1112 IGMP v1
- RFC 2236 IGMP v2
- RFC 3376 IGMP v3
- IGMP v1/v2/v3 Snooping with Configurable Router Registration Forwarding
- IGMP Filters
- Static IGMP Membership
- Multicast VLAN Registration
- RFC 2362 PIM-SM
- RFC 3569, draft-ietf-ssm-arch-06.txt PIM-SSM PIM Source Specific Multicast

IPv6
- RFC 2460, Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461, Neighbor Discovery for IP Version 6, (IPv6)
- RFC 2462, IPv6 Stateless Address Auto configuration – Router Requirements
- 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 1981, Path MTU Discovery for IPv6, August 1996 – Router requirements
- RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3587, Global Unicast Address Format
- RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol
- RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol
- RFC 2080, RIPng
- RFC 2893, Configured Tunnels
- RFC 3056, 6to4
- Static Unicast routes for IPv6
- Telnet server over IPv6 transport
- SSH-2 server over IPv6 transport
- Ping over IPv6 transport
- Traceroute over IPv6 transport

Management and Traffic Analysis
- RFC 2030 SNTP, Simple Network Time Protocol v4
- 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 Mgmt Information (SMIv1)
- RFC 1157 SNMPv1
- 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 – 1908 SNMP v2c, SMIv2 and Revised MIB-II
- RFC 2570 – 2575 SNMPv3, user based security, encryption and authentication
- RFC 2576 Coexistence between SNMP Version 1, Version 2 and Version 3
- RFC 1757 RMON 4 groups: Stats, History, Alarms and Events
- RFC 2021 RMON2 (probe configuration)
- RFC 2668 802.3 MAU MIB
- RFC 1643 Ethernet MIB
- RFC 1493 Bridge MIB
- RFC 1354 IPv4 Forwarding Table MIB
- RFC 2737 Entity MIB v2
- RFC 2233 Interface MIB
- RFC 3621 PoE-MIB (BlackDiamond 8800 only)
- RFC 1354 IP Forwarding Table MIB
- RFC 1724 RIPv2 MIB
- RFC 1850 OSPFv2 MIB
- RFC 1657 BGP-4 MIB
- Draft-ietf-idr-bgp4-mibv2-02.txt – Enhanced BGP-4 MIB
- draft-ietf-pim-mib-v2-o1.txt
- RFC 2787 VRRP MIB
- Draft-ietf-bridge-rstpmib-03.txt – Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
- Secure Shell (SSH-2) client and server
- Secure Copy (SCP-2) client and server
- Secure FTP (SFTP) server
- sFlow version 5
- Configuration logging
- Multiple Images, Multiple Configs
- BSD System Logging Protocol (SYSLOG), with Multiple Syslog Servers
- 999 Local Messages (criticals stored across reboots)
- ExtremeWare vendor MIBs (includes FDB, PoE, CPU, Memory MIBs) http://www.extremenetworks.com/services/documentation

Security
- Routing protocol MD5 authentication (see above)
- Secure Shell (SSH-2), Secure Copy (SCP-2) and SFTP client/server with encryption/authentication (requires export controlled encryption module)
- SNMPv3 user based security, with encryption/authentication (see above)
- 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)
- Guest VLAN for 802.1x
- RFC 1866 HTML – Used for web-based Network Login
- SSL/TLS transport – used for for web-based Network Login, (requires export controlled encryption module)
- MAC Security – Lockdown and Limit
- IP Security – RFC 3046 DHCP Option 82 with port and VLAN ID
- IP Security – DHCP enforcement via Disable ARP Learning
- IP Security – Gratuitous ARP Protection
- IP Security – Trusted DHCP Server
- IP Security – DHCP Secured ARP / ARP Validation
- Layer 2/3/4 Access Control Lists (ACLs)

Denial of Service Protection:
- RFC 2267 Network Ingress Filtering
- RPF (Unicast Reverse Path Forwarding) Control via ACLs
- Wire-speed ACLs

Technical Specifications

- 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
- 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 Attacks
  - 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

Core Protocols: only available on switches with Core-License capability:

- PIM-DM Draft IETF PIM Dense Mode draft-ietf-idmr-pim-dm-05.txt, draft-ietf-pim-dm-new-v2-04.txt
- RFC 2740, OSPF for IPv6
- RFC 1771 Border Gateway Protocol 4
- RFC 1965 Autonomous System Confederations for BGP
- RFC 2796 BGP Route Reflection (supersedes RFC 1966)
- RFC 1997 BGP Communities Attribute
- RFC 1745 BGP4/IDRP for IP – OSPF Interaction
- RFC 2385 TCP MD5 Authentication for BGPv4
- RFC 2439 BGP Route Flap Damping
- RFC 2842 Capabilities Advertisement with BGP-4
- RFC 2918 Route Refresh Capability for BGP-4
- draft-ietf-idr-restart-10.txt Graceful Restart Mechanism for BGP
- EAPSv2 Shared Ports – multiple interconnections between rings

General Specifications

Performance

- 160 Gbps switch fabric bandwidth
- 65 Mpps frame forwarding rate
- 9216 Byte maximum packet size (Jumbo Frame)
- 32 load sharing trunks, up to 8 members per trunk
- 8 QoS queues/port
- 4096 VLANs (Port, Protocol, IEEE 802.1Q)
- 3072 total number of ACL Rules/lines
- 128 rules per port
- ACL rules can be applied to ingress

Forwarding Tables

- Layer 2/MAC Addresses: 16K
- Layer 3 Host Addresses: 8K
- Layer 3 LPM Entries: 64K
- Layer 3 Static Routes: 1K
- Layer 3 Interfaces: 512
- OSPF External Routes: >100K

Rate Limiting

- Ingress bandwidth policing/rate limiting: packets are classified after Ingress into flows using ACLs and a rate limiter is assigned to a given flow
- Rate Limiting Granularity: 64Kbps (1Mbps on 10 gigabit port)
- Available Rate Limiters: 128 per port

Indicators

- Per port status LED including power status
- System Status LEDs: management, fan and power

Summit X450-24t

Ports

- 24 ports 10/100/1000BASE-T with auto-speed and auto-polarity
- 4 ports SFP (mini-GBIC, shared PHY with 4 10/100/1000BASE-T ports)
- 1 port Serial (control port)
- 1 10/100BASE-T out-of-band management Port

Option Slot

- Slot for XGM dual 10 gigabit option module

Summit X450-24x

Ports

- 24 mini-GBIC (SFP) ports
- 4 ports 10/100/1000BASE-T with auto-speed and auto-polarity, shared PHY with 4 mini-GBIC ports
- 1 port Serial (control port)
- 1 10/100BASE-T out-of-band management Port

Option Slot

- Slot for XGM dual 10 gigabit option module

Physical Specifications

Summit X450-24t

Dimensions

Height Inches/Cm: 1.73 Inches/4.4 Cm
Width Inches/Cm: 17.4 Inches/44.1 Cm
Depth Inches/Cm: 16.4 Inches/41.6 Cm
Weight Lbs/Kg: 14 lbs/6.35 Kg

Summit X450-24x

Dimensions

Height: 1.73 Inches/4.4 Cm
Width: 17.4 Inches/44.1 Cm
Depth: 16.4 Inches/41.6 Cm
Weight: 13.8 lbs/6.3 Kg

EPS Dimensions

EPS-T

Height: 1.75 Inches/4.4 Cm
Width: 17.4 Inches/44 Cm
Depth: 7.6 Inches/19.3 Cm

EPS-160

Height : 1.7 Inches/4.3 Cm
Width: 7.4 Inches/18.8 Cm
Depth: 7.9 Inches/20 Cm
Power Cable Length 1 Meter

Operating Specifications

Temperature

- Operating Temperature Range, Degrees Celsius/Fahrenheit: 0 to 40 °C (32 to 104 °F)
- Operating Humidity Range (worst case, not for extended duration): 10-95% (RH) non-condensing
- Storage and Transportation Temperature Range (worst case), Celsius/Fahrenheit: -40 to +70 °C (-40 to 158 °F)

Shock

- Operating (half sine): 30 m/s2 (3g)
- Non-operating (Flat PSD): 300m/s2 (30g)

Vibration

- Operating: 5-20Hz @ 1.0 ASD m2/s3
- 20-200Hz @ -3 dB/oct
- Non-operating: 3-500MHz @ 1.5g rms Power
- Auto-ranging 90-240VAC, 50-60 Hz
- Line Frequency: 50-60 Hz
- Min Voltage/Associated Current: 4A @100VAC
- Max Voltage/Associated Current: 2A @ 240VAC
- Heat Dissipation, Watts/BTU: 160W/546BTU/hr
- External Power System connector
- External Power System EPS-160 module:
  - Heat Dissipation, Watts/BTU:
  - 160W/546BTU/hr
  - Current 100-240VAC: 4A-2A

Acoustic

- Bystander sound pressure Per NEBS GR-63
  Summit X450-24x: 49dBA
  Summit X450-24t: 51dBA

Regulatory/Safety

North America

- cULus Listed device
  - UL 60950 3rd Edition (U.S. Safety)
  - CAN/CSA-C22.2 No. 60950-00
  - (Canadian Safety)

Europe

- Low Voltage Directive (LVD)
  - TUV-R GS Mark by German Notified Body
  - EN60950:2000 (European Safety)

International

- CB Scheme
  - IEC60950: 2000 with all country deviations
  - (International Safety)

Country Specific

- Mexico NOM/NYCE (Product Safety & EMC Approval)
- Australia/New Zealand AS/NZS 3260 (ACA DoC, Safety of ITE)
- Argentina S-Mark
- GOST (Russia)

Laser Safety

- North America
  - FCC 21 CFR subpart (J) (Safety of Laser Products)
  - CDRH Letter of Approval (U.S. FDA Approval)
- Europe
  - EN60825-2 (European Safety of Lasers)

EMI/EMC

- North America EMC for ITE
  - FCC 47 CFR Part 15 Class A (U.S. Emissions)
  - ICES-003 Class A (Canada Emissions)

Europe

- 89/336/EEC EMC Directive
- ETSI/EN 300 386:2001 (EU Telecommunication Emissions & Immunity)
- EN55022:1998 Class A (Europe Emissions)
- EN55024:1998 includes IEC/EN 61000-2,3,4,5,6,11 (Europe Immunity)
- EN 61000-3-2, -3 (Europe Harmonics and Flicker)

Technical Specifications

International
- IEC/CISPR 22:1997 Class A (International Emissions)
- IEC/CISPR 24:1998 (International Immunity)
- IEC/EN 61000-4-2 Electrostatic Discharge
- IEC/EN 61000-4-3 Radiated Immunity
- IEC/EN 61000-4-4 Transient Bursts
- IEC/EN 61000-4-5 Surge
- IEC/EN 61000-4-6 Conducted Immunity
- IEC/EN 61000-4-11 Power Dips & Interruptions

- Country Specific
  - Japan Class A (VCCI Registration, Emissions)
  - Australia/New Zealand AS/NZS 3548 (ACA DoC, Emissions)
  - Korean MIC Mark (MIC Approval, Emissions & Immunity)
  - Mexico NOM/NYCE (Product Safety & EMC Approval)
  - GOST (Russia)
  - Taiwan CNS 13438:1997 Class A (BSMI Approval, Emissions)

Environmental
- EN 300 019-2-1 (2000-09) – Storage Class 1.2 – Packaged
- EN 300 019-2-2 (1999-09) – Transportation Class 2.3 - Packaged
- EN 300 019-2-2 (1999-09) – Stationary Use at Weather Protected locations, Class 3.1e – Operational
- EN 300 753 (1997-10) – Acoustic Noise – Operational
- ASTM D5276 * – Drop – Packaged
- ASTM D3332 * – Shock - Unpackaged
- ASTM D3580 * – Random Vibration Unpackaged
- ASTM D6179 * – Tilt – Packaged

*Additional testing requested by Extreme Networks

Warranty

- 1-year on Hardware
- 90-days on Software

Ordering Information

Part Number	Name	Description
16121	Summit X450-24x	24 mini-GBIC, 4 10/100/1000BASE-T ports, option slot for XGM-2xn 10 gigabit module, ExtremeXOS Adv Edge License, 1 AC PSU, connector for EPS-160
16122	ExtremeXOS Core license, Summit X450-24x	ExtremeXOS Core license feature upgrade for Summit X450-24x
16123	Summit X450-24t	24 10/100/1000BASE-T, 4 mini-GBIC ports, option slot for XGM-2xn 10 gigabit module, ExtremeXOS Adv Edge License, 1 AC PSU, connector for EPS-160
16124	ExtremeXOS Core license, Summit X450-24t	ExtremeXOS Core license feature upgrade for Summit X450-24t
16111	XGM-2xn	Option module with two unpopulated XENPAK ports for Summit X450 series and Summit 400-48t
10906	EPS-T	External Power System power tray. Accepts up to two EPS-T power modules
10907	EPS-160	External Power System power module for EPS-T, 160 Watts, with cable
10110	SR XENPAK	10 Gigabit Ethernet XENPAK Transceiver, 850nm, up to 300m on multimode fiber, SC connector
10111	LR XENPAK	10 Gigabit Ethernet XENPAK Transceiver, 1310nm, up to 10km on single-mode fiber, SC connector
10112	ER XENPAK	10 Gigabit Ethernet XENPAK Transceiver, 1550nm, up to 40km on single-mode fiber, SC connector
10113	ZR XENPAK	10 Gigabit Ethernet XENPAK Transceiver, 1550nm, up to 80km on single-mode fiber, SC connector
10114	LX4 XENPAK	10 Gigabit Ethernet WWDM XENPAK Transceiver, 1310 nm, up to 300 m on multi-mode fiber and up to 10 km on a single-mode fiber, SC connector
10051	SX mini-GBIC	Mini-GBIC, SFP, 1000BASE-SX, LC Connector
10052	LX mini-GBIC	Mini-GBIC, SFP, 1000BASE-LX, LC connector
10053	ZX mini-GBIC	Mini-GBIC, SFP, Extra long distance SMF 70 Km/21 dB budget, LC connector
10060	100 FX/1000LX mini-GBIC	Mini-GBIC, SFP, dual-speed 100 FX/1000LX, LC Connector

www.extremenetworks.com email: info@extremenetworks.com

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 +852 2517 1123

Japan
Phone +81 3 5842 4011