SUMMIT X450 SERIES

The powerful and compact Summit® X450 series is the first fixed-format switch based on the revolutionary ExtremeWare® XOS™ core-class operating system. ExtremeWare XOS introduced by Extreme Networks in 2003, is a highly resilient, modular operating system that takes availability to the highest levels and greatly enhances manageability. The Summit X450 series also uses the same high-performance, non-blocking hardware technology used on Extreme Networks BlackDiamond® 8800 Series, continuing an Extreme Networks' tradition of simplifying network deployments through the use of common hardware and software throughout the network.

The extremely versatile Summit X450 series, with high-density gigabit plus optional 10 Gigabit Ethernet in a compact one rack-unit format, supports a full range of Layer 2 to Layer 4 features on every port to ensure highest productivity. It is available in two versions, a fiber version supporting flexible and convenient modular optics, and a copper version suitable for local data distribution, both versions having optional redundant power supplies to provide insurance against power anomalies.

TARGET APPLICATIONS

- **As an edge switch providing gigabit to the desktop in a simple two-tier network running ExtremeWare XOS from core to edge**
- **As the single or redundant core of a small network with its resiliency and ExtremeWare XOS core features**
- **As an aggregation switch in a traditional three-tiered network extending the benefits of ExtremeWare XOS to the aggregation layer**
- **As a highly available fixed switch providing server connectivity**
- **Or as an aggregation switch in a Metro Ethernet network.**

VOICE-CLASS AVAILABILITY

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

ADVANCED FEATURES ENABLE VERSITILE DEPLOYMENT

- Non-blocking high-performance edge
- Multi-gigabit distribution layer
- Small network core
- Metro Ethernet services aggregation

COMPREHENSIVE SECURITY TO WARD OFF ATTACKS

- User policy and host integrity enforcement
- Instrumentation to react to network intrusion
- Hardened against attacks

A high-performance network connection, whether used to connect PCs and IP telephones at the access layer, to interconnect switches at the aggregation layer or to serve as the core of a small network, is only useful if it is also highly available. The Summit X450 modular switching family incorporates hardware redundancy and a modular operating system–ExtremeWare XOS. ExtremeWare XOS supports system recovery and application upgrades without the need for a system reboot, as well as networking protocols that provide the network recovery required by converged applications.

Modular Operating System for Non-stop Operations

True Preemptive Multitasking and Protected Memory

Summit X450 series allows each of the many tasks–such as Open Shortest Path First (OSPF) and Spanning Tree–to run as separate operating system (OS) tasks that are protected from each other as shown in Figure 1.

Process Monitoring and Restart

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

Loadable Software Modules

The modular design of ExtremeWare XOS 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.

High Availability Network Protocols

Ethernet Automatic Protection Switching

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 the Spanning Tree or Rapid Spanning Tree Protocols and offers sub-second (less than 50 milliseconds) recovery that delivers consistent failover regardless of number of VLANs, number of network nodes or network topology. In most situations, Voice-over-IP (VoIP) 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 supports Spanning Tree, VLAN Spanning Tree (802.1D), and Rapid Spanning Tree (802.1w) 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. The Summit X450 series constantly checks 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 enables 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

The Summit X450 series is built with Error Checking and Correcting (ECC) RAM to protect routing tables and continue operation in spite of potentially disruptive memory events. Furthermore, the system is 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

The Summit X450 series provides 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 Equal Cost Multi-Path (ECMP). Common deployments may call for 2.4:1 oversubscription, for which the Summit X450 series delivers superior resiliency with the EAPS protocol.

Redundant Power Supplies

The Summit X450 series supports redundant power through its External Power System that provides a convenient, easily field upgradeable option for protection against power delivery anomalies.

MODULAR OPERATING SYSTEM FOR NON-STOP OPERATIONS

- True preemptive multitasking and protected memory
- Process monitoring and restart
- Loadable software

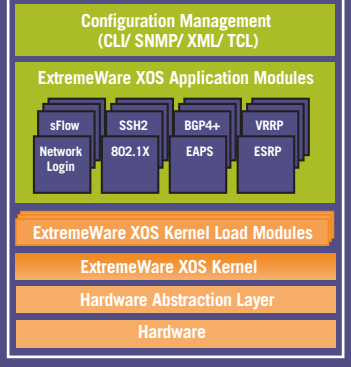


Figure 1: ExtremeWare XOS Modular Operating System

The Summit X450 series, available in fiber or tri-speed copper gigabit formats, serves equally well as edge switch for high-performance LAN access deployment, Metropolitan Area Network (MAN) customer edge or provider edge switch, small network core switch, or as the distribution switch from 10 gigabit trunks to gigabit-attached devices. The Summit X450 series delivers voice-class availability, deftly switching voice, video and data traffic. Summit X450 series' non-blocking ports can interconnect a rack of servers for high performance cluster computing (HPCC). With its superior resiliency, comprehensive security features, and non-blocking performance, the Summit X450 series is a cornerstone of a highly productive network.

Non-Blocking High-Performance Edge

High Bandwidth Access

When deployed as an access switch the Summit X450 series provides all 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.

Asset Protection

Seats on the network where high-performance is required are often locations with access to sensitive enterprise data. Guarding access to this intellectual property is of highest priority, and the Summit X450 series easily fulfills this requirement, delivering superior access authentication with its unique multiple supplicant network login, available in convenient web format or 802.1x. Superior network access protection, always at line rate, is just one more of the many benefits delivered by the Summit X450 series.

Enhanced Productivity

Availability to sustain productivity is another hallmark of the Summit X450 series. Starting with its highly resilient ExtremeWare XOS operating system and carried through its reliable hardware design that incorporates error checking and correcting (ECC) memory and dual software and configuration images and redundant power supplies, the Summit X450 series is designed from the ground up for resiliency. Furthermore, the ExtremeWare XOS operating system offers a diverse variety of redundant link protocols from unique Software Redundant Ports to extremely fast EAPS and full OSPF ECMP. Delivering constantly available high throughput access, the Summit X450 series boosts productivity and provides a rapid return on investment.

Multi-Gigabit Distribution Layer

Gigabit to 10 Gigabit Aggregation

In a traditional three-layer LAN, an aggregation layer combines traffic from multiple edge switches into a Gigabit Ethernet trunk running to the network core. The Summit X450 series provides a significant performance and feature upgrade for the aggregation layer. It eliminates the need to funnel traffic through a low bandwidth gigabit trunk by providing non-blocking 10 gigabit links to the core. But the Summit X450 series does much more than boost bandwidth - it also enables superior network management with sFlow statistical sampling. sFlow samples 100% of traffic passing through the switch to facilitate detecting, diagnosing, and fixing network problems, congestion management, trending, and capacity planning. It also provides comprehensive traffic classification and security with its powerful Layer 2-4 access control lists (ACLs) with an incredible 3,072 rules per switch 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 fail-over of traffic to a secondary path in case of link or device failure. That safe failover is managed by a link redundancy protocol, and depending on the applications flowing over the network, the redundancy protocol can make a great difference in how a network performs. For example, where voice-grade resiliency is required, only EAPS allows links to fail over rapidly enough that voice call sessions are not dropped. Other Summit X450 series link resiliency services include OSPF ECMP, which provides a standards-based option that doubles available redundant link bandwidth; VRRP, which provides standards-based Layer 3 dual homing; ESRP that provides 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. With the fastest failover protocol (EAPS), simplest protocol (Software Redundant Port) and the large number of resiliency protocol options, the Summit X450 series supports superior link redundancy to best enable a highly available aggregation layer.

Non-Blocking Architecture

An essential feature at the aggregation layer is non-blocking forwarding. The Summit X450 series, with a full 160 gigabit per second fabric, delivers non-blocking forwarding. Its optional pair of 10 Gigabit Ethernet fiber ports provides a new level of uplink bandwidth for a fixed format switch, removing the bandwidth bottleneck present in legacy aggregation switch deployments. Not only does the Summit X450 series provide a significant boost in bandwidth, but also it does so with low latency typically less than 10 milliseconds, adding very little to end-to-end latency for optimal support of voice and video applications. With microscopic jitter, line rate forwarding, and both traffic classification and security delivered at line rate, the Summit X450 series aggregation layer is uniquely transparent.

Small Network Core

The Summit X450 series is designed with all the necessary features – residency, security, availability and necessary protocols – to perform all the functions of a small network core switch. With its core operating system, it is truly a core switch in a compact 1RU package.

Advanced Protocols

Supporting core deployments requires full protocol support. The Summit X450 series provides static and RIP routing for simple Layer 3 deployment. An optional ExtremeWare XOS 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
- RIPng for IPv6 slow-path support
- OSPFv3 for IPv6 slow path support
- IPv6 tunnels, IPv6-to-IPv4 translation, IPv6 multicast Discovery for extensive IPv6 support

Of course all of this is in addition to the extensive Layer 2 forwarding and resiliency such as EAPS and 802.1w the Summit X450 series provides, in total providing the advanced protocol environment for an efficient and productive small network core.

DOS Protection
As the focus of most network activity, the network core must be protected from Denial of Service (DoS) attacks, whose resulting network down time are so costly in terms of lost productivity. The ExtremeWare XOS that runs on the Summit X450 series has been designed to fend against an extensive suite of known DoS attacks, and in addition has the ability to detect a new Day Zero attack and create and launch an appropriate defense against it. The Summit X450 series is architected with Longest Prefix Match (LPM) Layer 3 forwarding, a feature normally found only in some core switches, that boosts routing efficiency by significantly extending the number of hardware-resident forwarding entries. This allows the switch to continue to operate even while a DoS or scanning attack is in progress. With its extensive DoS protection, the Summit X450 series delivers unique availability protection to make it a top choice for small network core deployment.

High Availability
The Summit X450 series achieves voice-class availability by combining a modular operating system, unique software resiliency features and hardware redundancy.

ExtremeWare XOS is a fully modular operating system, delivering the highest levels of software availability. Unlike monolithic operating systems, ExtremeWare XOS keeps running even if individual processes fail. The modular OS further increases uptime by monitoring all processes in real time, automatically restarting any that are unresponsive or stalled. ExtremeWare XOS also allows the addition of software features to the switch without taking the unit out of service, eliminating "scheduled outages."

The Summit X450 series runs a contingent of high-availability protocols, including EAPS. In most situations, since EAPS fails over in less than 50 milliseconds, the Summit X450 series recovers from link faults without impacting service. This ensures toll-quality voice and picture-perfect video.

Other Layer 2 and Layer 3 resiliency protocols as well as hardware redundancies further extend the availability of the Summit X450 series. OSPF ECMP not only provides redundant network paths, but also increases productive bandwidth. ESRP operates at both Layer 2 and Layer 3 to support dual homed devices. The Summit X450 series also supports VRRP for standards-based dual homing of devices or hosts. Providing assurances of continuously productive LAN service are redundant power supplies that deliver transparent backup failover in the event of power glitches, redundant uplink ports at both gigabit and 10 gigabit levels, and redundant OS and configuration images.

Metro Ethernet Services Platform
The Summit X450 series is an ideal service delivery platform for Metro Ethernet networks. Its advanced traffic management, resiliency and scalability features give it the flexibility to be deployed at the Customer Edge (CE) or as an aggregation switch at the Provider Edge (PE). By supporting both CE and PE service delivery requirements, the Summit X450 series greatly reduces a Service Provider's operational expense (OPEX).

Exceptional QoS
Metro deployments require exceptional Quality of Service (QoS), an area where the Summit X450 series excels with eight hardware queues per port to support granular traffic classification, and 128 classifiers per ingress port that can use information from Layer 1 through 4 to prioritize and meter incoming packets at line rate. When metering traffic, the Summit X450 series 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.

Triple Play
Deployed as Customer Edge equipment, the Summit X450 series' advanced traffic management features enable support for delivering the triple play of voice, video and data services. The Summit X450 series is compliant with the UNI 1.0 Metro Ethernet Forum specification and supports all the service parameters of MEF 6, the Traffic Management specification. The Summit X450 series' low latency and hardware support for multi-cast traffic make it an excellent solution for deploying IP TV over a Metro Ethernet infrastructure.

Service Aggregator
Used to deliver network-based services at the Provider Edge of the Metro Ethernet network, the Summit X450 series scalability enables it to support successful deployments as an effective aggregator for many thousands of subscriber services. The Summit X450 series supports 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.

ENHANCED MANAGEABILITY WITH AN XOS NETWORK
The introduction of the Summit X450 series makes Extreme Networks' innovative ExtremeWare XOS the first modular operating system to be universally deployed from the core to the edge of the network, significantly enhancing network manageability. Common XOS 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 XOS from edge to core extends the power of sFlow statistical reporting to assist in end-to-end congestion management and troubleshooting. ExtremeWare XOS is one of the first operating systems 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 ExtremeWare XOS based network can be managed by EPICenter to simplify global status monitoring, deployment of policies and network troubleshooting.

The ExtremeWare XOS based network delivers consistent security, resiliency, quality of service, and generally simplifies management to reduce total cost of ownership.

Implementing a secure network requires the switches in the infrastructure to support a comprehensive set of security features. Security on the Summit X450 series encompasses 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. The Summit X450 series supports a comprehensive range of Network Login options by providing an 802.1x agent-based approach, a web-based (agent-less) 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 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 access points (APs) and servers. The MAC address security/lockdown feature enables the Summit X450 series 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. The Summit X450 series supports a host integrity or end point integrity solution that is based on the model from the Trusted Computing Group.

Threat Detection and Response

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 the Summit X450 series, and packages data into sFlow datagrams that are sent over the network to an sFlow Collector. The Collector has 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, the Summit X450 series supports 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 Access Control Lists (ACLs)

ACLs are one of the most powerful tools to control network resource utilization and to secure and protect the network. The Summit X450 series supports up to 48,000 ACLs based on Layer 2, 3 or 4-header information such as the MAC address or IP source/destination address.

Hardened Network Infrastructure

Denial of Service (DoS) Protection

Summit X450 switches handle 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 Longest Prefix Match (LPM)

LPM routing eliminates the need for control plane software to learn new flows and allows the network to be resilient under a denial of service attack.

Secure Management

The use of protocols like SSH2, SCP and SNMPv3 supported by the Summit X450 series prevents the interception of management communications and man-in-the middle attacks.

MD5 Authentication of Routing Protocols

MD5 authentication of routing protocols prevents attackers from tampering valid messages and attacking routing sessions.

IPv6 FORWARDING

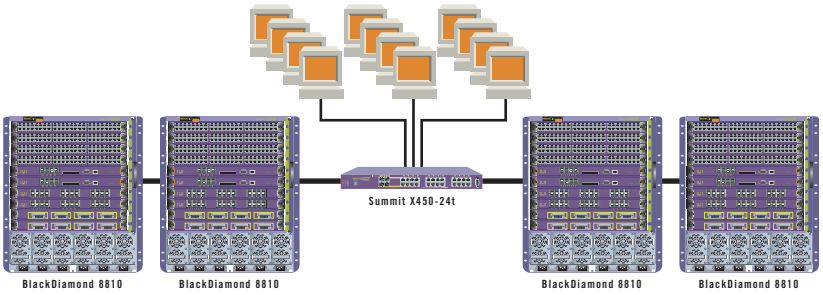
For more than a decade, a new version of the ubiquitous Internet Protocol (IP) that powers global network interconnectivity has been under development, with the primary goal of expanding IP's address range to allow a unique IP address for any device in the world that might some day need to be addressable. The Summit X450 series offers this next generation Internet Protocol, 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 Access Control Lists
- 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

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

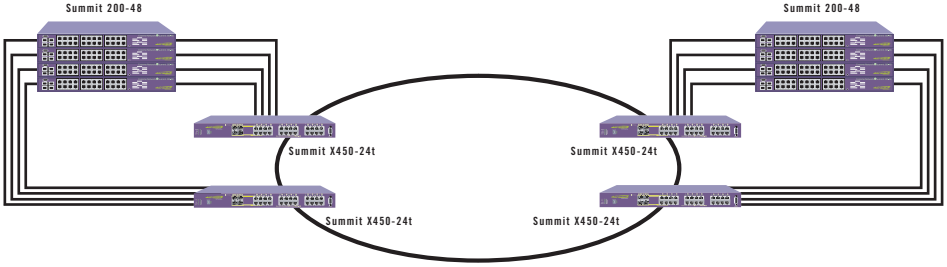
High-Performance Gigabit Edge

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



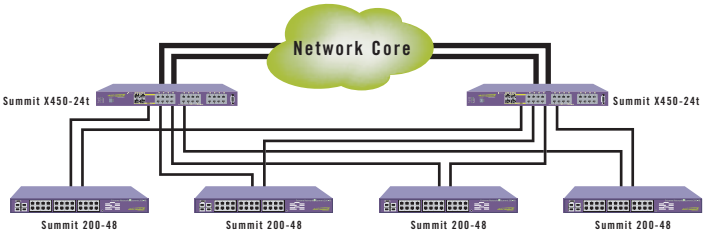
Small Network Core Switch

The Summit X450 series is the ideal small network core switch. Its 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, the Summit X450 series is designed from the ground up to be a small core switch.



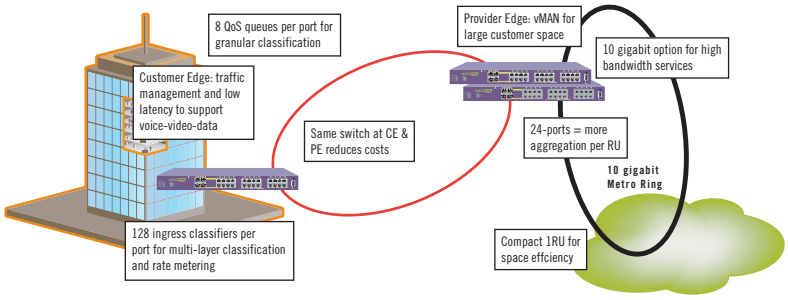
Traditional Aggregation Layer

The Summit X450 series is 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 multiples aggregation capacity of most switches in their class that have only twelve fiber ports, and no 10 gigabit ports.



Metro Ethernet Services

The Summit X450 series is an ideal service delivery platform for Metro Ethernet networks. Its advanced traffic management, resiliency and scalability features give it the flexibility to be deployed at the Customer Edge (CE) or as an aggregation switch at the Provider Edge (PE). By supporting both CE and PE service delivery requirements, the Summit X450 series greatly reduces a Service Provider's operational expense.



PHYSICAL

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

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

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

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: 13.8 lbs / 6.3 Kg

EPS Dimensions
EPS-T
Height Inches/Cm: 1.75 Inches / 4.4 Cm
Width Inches/Cm: 17.4 Inches / 44 Cm
Depth Inches/Cm: 7.6 Inches / 19.3 Cm
EPS-160
Height Inches/Cm: 1.7 Inches / 4.3 Cm
Width Inches/Cm: 7.4 Inches / 18.8 Cm
Depth Inches/Cm: 7.9 Inches / 20 Cm
Power Cable Length 1 Meter

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

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/s^2 (3g)
- Non-operating (Flat PSD): 300m/s^2 (30g)

Vibration
- Operating: 5-20Hz @ 1.0 ASD m^2/s^3 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

Forwarding Tables
- Layer 2/MAC Addresses: 16K
- Layer 3 Host Addresses: 8K
- Layer 3 LPM Entries: 64K
- L3 Static Routes: 1K
- Layer 3 Interfaces: 512
- OSPF External Routes: >100K

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, MAC-based, IEEE 802.1Q)
- 3072 total number of ACL Rules/lines
- 128 rules per port
- ACL rules can be applied to ingress

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

Warranty
- Hardware: 1 Year
- Software: 90 Days

Acoustic
- 44dBA Sound Pressure

REGULATORY COMPLIANCE

North America
- cULus Listed device
  - UL 60950 3rd Edition (US 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 (US FDA Approval)
- Europe
  - EN60825-2 (European Safety of Lasers)

EMI/EMC
- North America EMC for ITE
  - FCC 47 CFR Part 15 Class A (US 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)
- 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*

SOFTWARE

- ExtremeWare XOS 11.2 Supported Protocols

General Routing and Switching

- 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 1866 HTML – Used for webbased Network Login
- RFC 2068 HTTP server – Used for webbased Network Login
- RFC 2338 VRRP
- RFC 3619 Ethernet Automatic Protection Switching (EAPS) and EAPSv2
- IEEE 802.1D - 1998 Spanning Tree Protocol (STP)
- IEEE 802.1w – 2001 Rapid Reconfiguration for STP, RSTP
- IEEE 802.1Q - 1998 Virtual Bridged Local Area Networks
- IEEE 802.1AB – LLDP Link Layer Discovery Protocol
- EMISTP, Extreme Multiple Instances of Spanning Tree Protocol
- PVST+, Per VLAN STP (802.1Q interoperable)
- Extreme Standby Router Protocol (ESRP)
- Extreme Discovery Protocol (EDP)
- Static Unicast Routes
- Loop detection via Layer 2 ELRP
- Software Redundant Ports

VLANs

- IEEE 802.1Q VLAN Tagging
- IEEE 802.3ad Static configuration
- IEEE 802.1v: VLAN classification by Protocol and Port
- Port-based VLANs
- Protocol-based VLANs
- Multiple STP domains per VLAN
- 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

RIP

- RFC 1058 RIP v1
- RFC 2453 RIP v2

OSPF

- RFC 2328 OSPF v2 (including MD5 authentication)
- RFC 1587 OSPF NSSA Option
- RFC 1765 OSPF Database Overflow
- RFC 2370 OSPF Opaque LSA Option

BGP4 (Advanced Core license on MSM-1XL)

- 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

IP Multicast

- RFC 2362 PIM-SM
- PIM-DM Draft IETF PIM Dense Mode v2-dm-03
- 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

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 2665 Ethernet-Like-MIB
- 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 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
- RFC 2787 VRRP MIB
- RFC 2925 Ping / Traceroute / NSLOOKUP MIB
- Draft-ietf-bridge-rstpmib-03.txt – Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
- Secure Shell (SSHv2) client and server
- Secure Copy (SCPv2) 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, 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
- 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 for Network Login (all modes)
- Guest VLAN for 802.1x
- SSL/TLS transport – used for web-based Network Login, (requires export controlled encryption module)
- MAC Address Security - Lockdown and Limit
- IP Address Security - DHCP Option 82 and Gratuitous ARP Protection
- Layer 2/3/4/7 Access Control Lists (ACLs)

Denial of Service Protection

- RFC 2267 Network Ingress Filtering
- RPF (Unicast Reverse Path Forwarding) Control via ACLs
- Wire-speed ACLs
- Rate Limiting 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

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 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 2464, Transmission of IPv6 Packets over Ethernet Networks
- RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol
- RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol
- RFC 2740, OSPF for IPv6
- RFC 2080, RIPng
- RFC 2893, Configured Tunnels
- RFC 3056, 6to4
- Static Unicast routes for IPv6
- Telnet over IPv6 transport
- SSH-2 over IPv6 transport
- Ping over IPv6 transport
- Traceroute over IPv6 transport

ORDERING INFORMATION

Part Number	Part Name	Description
16121	Summit X450-24x	24 mini-GBIC, 4 10/100/1000BASE-T ports, option slot for XGM-2xn 10 gigabit module, ExtremeWare XOS Adv Edge License, 1 AC PSU, connector for EPS-160
16122	XOS Core license, Summit X450-24x	ExtremeWare XOS 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, ExtremeWare XOS Adv Edge License, 1 AC PSU, connector for EPS-160
16124	XOS Core license, Summit X450-24t	ExtremeWare XOS 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
10051	SX mini-GBIC	Mini-GBIC, SFP, 1000BASESX, LC Connector
10052	LX mini-GBIC	Mini-GBIC, SFP, 1000BASELX, LC connector
10053	ZX mini-GBIC	Mini-GBIC, SFP, Extra long distance SMF 70 Km/21 dB budget, LC connector

3585 Monroe Street Santa Clara, CA 95051-1450 Phone 408.579.2800 Fax 408.579.3000
Email info@extremenetworks.com Web www.extremenetworks.com