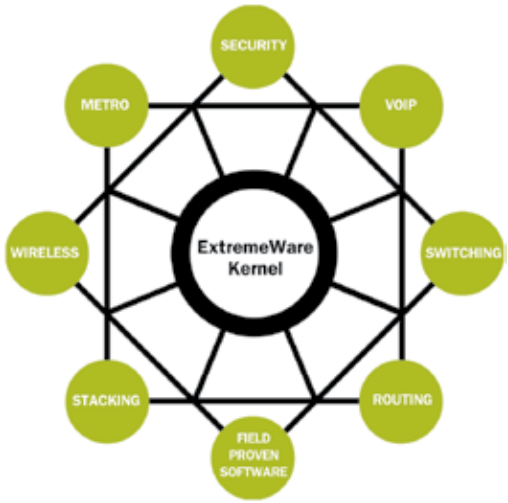
ExtremeWare® Operating System, Version 7.7



ExtremeWare is a secure operating system capable of simplifying the convergence of applications on today's networks.

Comprehensive Security

- Create a hardened network infrastructure against exploits and misuse
- Enforce dynamic policy-based network privileges using 802.1x, web-based or MAC-based authentication
- Mitigate security violations with threat detection and response

Easily Managed Growth

- Aggregate large quantities of desktops, servers, clusters, wireless laptops, PDAs and VoIP phones
- Scale networks simply and transparently using UniStack™—Layer 2 and Layer 3 switch stacking
- Seamlessly integrate networks mixed with ExtremeWare and ExtremeXOS™ based platforms

Field-Proven Operating System

- Establish network reliability with a proven architecture, running on over 10 million ports worldwide
- Increase the integrity of emerging real-time convergence applications such as: IP Telephony, streaming media and wireless
- Increase network availability with EAPS sub 50ms failover

ExtremeWare Operating System (OS) delivers the comprehensive security, intuitive management and robust network service required in today's demanding service provider and enterprise networks.

ExtremeWare starts by establishing a secure network environment. Advanced features such as policy-based network access and Denial of Service (DoS) protection help to meet the high expectations of network security. This foundation of a well-guarded and highly available network infrastructure is essential in today's business environment, especially as the stakes rise due to compliance requirements and new security legislation.

Management complexity can be a common hindrance associated with the growth and repurposing taking place as service providers roll out new services and enterprises centralize networks and continue to build out applications such as storage and data warehousing. This is complicated by the integration of new applications such as wireless and VoIP. ExtremeWare simplifies this next wave of network growth with powerful features such as Link Layer Discovery Protocol (LLDP) device discovery, UniStack stacking technology and sFlow flow-based monitoring that simplify the setup and maintenance of large convergence networks.

A field-proven OS, ExtremeWare has benefited from extensive deployment in a wide range of network topologies and service applications. This has enabled continuous refinement of ExtremeWare, establishing a basis for resilient networks, capable of voice-quality connections.

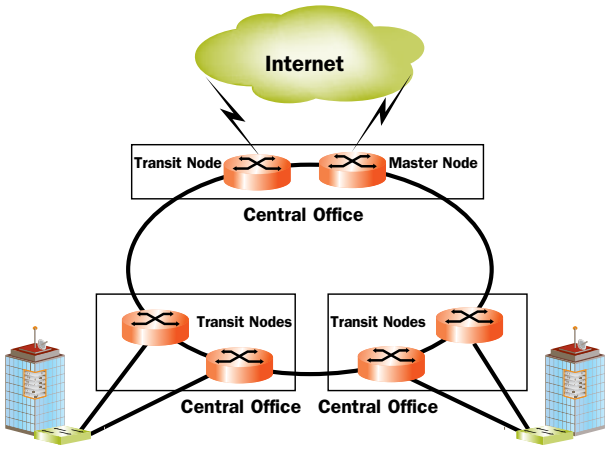
ExtremeWare Innovation

EAPS V2—Carrier-Class Ethernet Resiliency

To support the triple play of voice, video and data, networks must deliver highly-reliable transport for the three different application types. Network failure events should be completely transparent to the end users, making interruptions in voice, video or data applications imperceptible.

The answer to the challenge of service resiliency over Ethernet networks is Ethernet Automatic Protection Switching (EAPS) from Extreme Networks®. A service-aware ring-based protection scheme, EAPS uses a standard Ethernet MAC and is capable of meeting the carrier-class benchmark of 50ms.

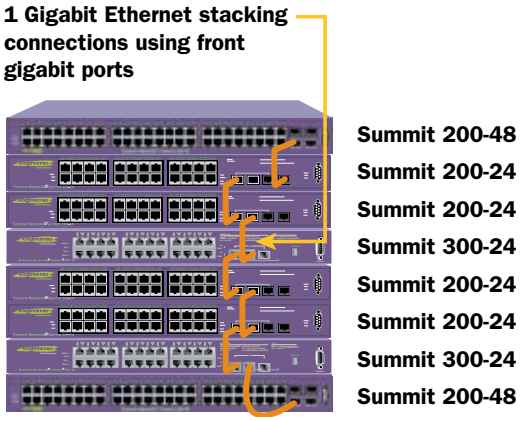
EAPS v2 supports a variety of complex network topologies, including dual-attached rings and subtended rings giving metro Ethernet service providers and enterprise networks greater flexibility for protecting a broad variety of network architectures and topologies.



UniStack Stacking Technology

UniStack stacking delivers the benefits of a chassis at the cost of a stackable, in an architecture designed to support today's evolving network applications. This network simplification can result in lower management and maintenance costs while enhancing overall availability.

Stacking allows for a network configuration where multiple chassis are physically linked together and logically act as a single manageable switch. As a result, network complexity is greatly reduced, leading the way to a simple, inexpensive and resilient architecture. Stacking may be used with the Summit® 400-24 and Summit 400-48 or with the Summit 200-24, Summit 200-48 and Summit 300-24. Stacking allows for redundant uplinks on two different switches, which is considerably more resilient than having both redundant ports on a single non-stacked switch. Even in the very unlikely event of multiple failures, stacking will continue to operate.

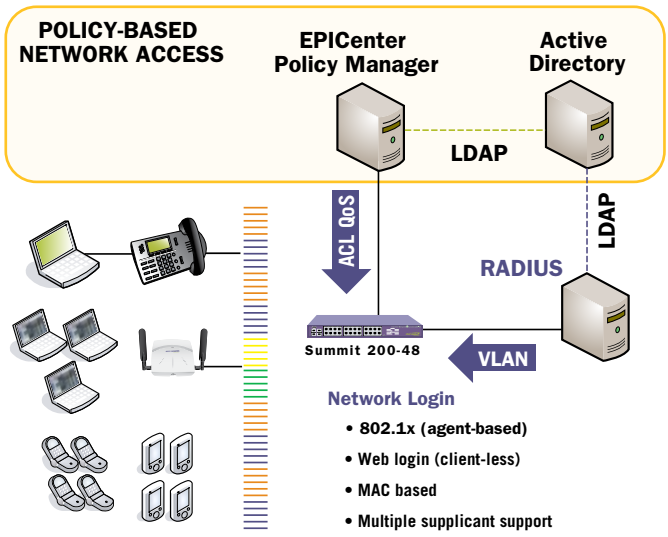


Intelligent Network Access

ExtremeWare provides advanced Layer 3 features that can be used to increase the security of a network, reducing the susceptibility to virus and worm outbreaks, and establishing consistent application performance.

By leveraging VLANs, ACLs and QoS, each network user is given a different level of access to the network. In order to deliver these dynamic policies, Network Login is used, providing standards based 802.1x, web-based and MAC-based authentication. This means that either an 802.1x client or some form of basic web browser is used to take advantage of dynamic policy assignment. To authenticate devices such as VoIP phones, MAC address-based techniques such as MAC-based VLANs or MAC-based RADIUS authentication can be used as an alternative.

Working with EPICenter® Policy Manager, ExtremeWare effectively creates a linkage between networks resources and users, automating network security configuration and performance parameters and reducing the complexity of configuration of these policies.



ExtremeWare 7.7 Feature Highlights

ExtremeWare Operating System 7.7 runs on all Extreme Networks "i" series switches, and on Summit 200, Summit 300 and Summit 400 series edge switches. Common code with Extreme Networks' switches means Plug-and-Play compatibility on Extreme Networks Summit, Alpine® and BlackDiamond® 6800 family of switches, as well as consistent behavior and stable performance right out of the box.

Security

- Network Login with MAC-based, web-based and 802.1x access methods
- Guest VLANs for 802.1x
- Integrated with Sygate host integrity checking
- Denial of Service (DoS) Protection
- MAC Address Security with lockdown, limiting and aging
- IP Address Security with DHCP Option 82 and DHCP Enforcement, Source IP Lockdown
- IP Destination Address (IPDA) Subnet Lookup
- NAT
- Layers 2 – 4 Access Control Lists (ACLs)
- RADIUS/TACACS+ authentication
- SSH2/SCP2/SFTP secure shell and copy
- SNMPv3 authentication and encryption
- Access profile for SNMP/Vista/CLI
- Routing Access Policies and Authentication
- Port Mirroring—tagged and untagged

Scalability

- IP Multinetting
- VLAN support
- UniStack—Switch stacking for up to eight chassis per stack. Ring or Daisy chain (Available on select Summit platforms)
- VLAN translation, remapping of VLAN IDs (*i*)
- VMAN, VLAN tunnels of 802.1 Q or Cisco ISL VLANs (*i*)
- Static multicast routes
- PIM/SM sparse mode
- IGMP snooping, static membership and filters
- PIM Snooping (*i*)
- PIM/DM dense mode (*i*)
- DVMRP (*i*)

Ease of Management

- RMON, rich set of MIBs
- SMON, sFlow, NetFlow (*i*)
- Tightly integrated with EPICenter network management system
- IEEE 802.1ab LLDP

High Availability

- Hitless failover and hitless upgrade support on BlackDiamond 6800 MSM-3
- LACP IEEE 802.3ad
- Layer 2 loop detection
- Spanning Tree IEEE 802.1D, IEEE 802.1Q and IEEE 802.1w, IEEE 802.1s and PVST+, per VLAN Spanning Tree
- Extreme Multiple Instances of Spanning Tree Protocol (EMISTP)
- Ethernet Automatic Protection Switching (EAPS) v2
- RIPv1/v2
- Open Shortest Path First (OSPF)v2, NSSA Option, Opaque LSAs
- Equal Cost Multi Path (ECMP)
- VRRP and Extreme Standby Router Protocol (ESRP)
- BGP4, E-BGP, I-BGP, Route Reflection, Community Attributes and Route Flap Damping (*i*)
- IS-IS (*i*)
- Policy-based routing (*i*)
- Server load balancing (*i*)
- Web cache redirection (*i*)

(i) An item appended by this symbol is only supported with the "i" series of Extreme Network products. Please see the individual switch data sheets for a list of supported standards and features on each platform.

ExtremeWare 7.7 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 2338 VRRP
- Static Unicast Routes
- Software Redundant Ports
- 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 802.1s – 2004 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 - 2003 Virtual Bridged Local Area Networks
- IEEE 802.1AB – LLDP Link Layer Discovery Protocol
- Extreme Discovery Protocol (EDP)
- Extreme Loop Recovery Protocol (ELRP)
- Extreme Link State Monitoring (ELSM)
- IPX RIP/SAP Router specification (*i*)

VLANs
- IEEE 802.1Q VLAN Tagging
- IEEE 802.3ad Static configuration and dynamic (LACP) for server attached
- IEEE 802.1v: VLAN classification by Protocol and Port
- Port-based VLANs
- MAC-based VLANs
- Protocol-based VLANs (not available on Summit 200/Summit 300)
- Multiple STP domains per VLAN
- RFC-3069 VLAN Aggregation for Efficient IP Address Allocation (*i*)
- Virtual MANs (vMANs) (*i*)
- VLAN Translation (*i*)

Quality of Service and Policies
- IEEE 802.1D – 1998 (802.1p) Packet Priority
- RFC 2474 DiffServ Precedence, including 8 queues/port (4 on Summit 200/300)
- RFC 2598 DiffServ Expedited Forwarding (EF)
- RFC 2597 DiffServ Assured Forwarding (AF)
- RFC 2475 DiffServ Core and Edge Router Functions
- RED as described in "Random Early Detection Gateways for Congestion Avoidance, Sally Floyd and Van Jacobson" (*i*)
- RED as recommended in RFC 2309 (*i*)
- Bi-directional Rate Shaping (*i*)
- Ingress Rate Limiting
- Layer 1-4, Layer 7 (user name) Policy-Based Mapping
- Policy-Based Mapping/Overwriting of DiffServ code points, .1p priority
- Network Login/802.1x and DLCS (Dynamic Link Context System, WINS snooping) based integration with EPICenter Policy Manager for dynamic user/device based policies
- Layer 1-4, Layer 7 (user name) Policy-Based Mapping
- Policy-Based Mapping/Overwriting of DiffServ code points, .1p priority
- Network Login/802.1x and DLCS (Dynamic Link Context System, WINS snooping) based integration with EPICenter Policy Manager for dynamic user/device based policies

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

Note: OSPF Edge License includes 2 active interfaces, router priority 0)

IS-IS (*i*)
- RFC 1142 (ISO 10589), IS-IS protocol
- RFC 1195, Use of OSI IS-IS for routing in TCP/IP and dual environments
- RFC 2104, HMAC: Keyed-Hashing for Message Authentication, IS-IS HMAC-MD5 Authentication
- RFC 2763 (Dynamic Host Name Exchange for IS-IS)

BGP4 (*i*)
- 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

IP Multicast
- RFC 2362 PIM-SM
- PIM-DM Draft IETF PIM Dense Mode v2-dm-03 (*i*)
- PIM Snooping (*i*)
- DVMRP v3 draft IETF DVMRP v3-07 (*i*)
- RFC 1112 IGMP v1
- RFC 2236 IGMP v2
- IGMP Snooping with Configurable Router Registration Forwarding
- IGMP Filters
- Static IGMP Membership
- Static Multicast Routes
- Mtrace, draft-ietf-idmr-traceroute-ipm-07
- Mrinfo

Management and Traffic Analysis
- RFC 2030 SNTP, Simple Network Time Protocol v4
- RFC 1866 HTML – web-based device management and Network Login
- RFC 2068 HTTP server
- 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 1901 – 1908 SNMP Version 2c, 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 2613 SMON MIB (*i*)
- RFC 2668 802.3 MAU MIB
- RFC 1643 Ethernet MIB
- RFC 1493 Bridge MIB
- RFC 2737 Entity MIB, Version 2
- RFC 2674 802.1p / 802.1Q MIBs
- RFC 1354 IPv4 Forwarding Table MIB
- RFC 2233 Interface MIB
- RFC 2096 IP Forwarding Table MIB
- RFC 1724 RIPv2 MIB
- RFC 1850 OSPFv2 MIB
- RFC 1657 BGPv4 MIB (*i*)
- RFC 2787 VRRP MIB
- RFC 2925 Ping / Traceroute / NSLOOKUP MIB
- RFC 2932 – IPv4 Multicast Routing MIB
- RFC 2933 – Internet Group Management Protocol MIB
- RFC 2934 – Protocol Independent Multicast MIB for IPv4
- Draft-ietf-bridge-rstpmib-03.txt – Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
- draft-ietf-bridge-8021x-01.txt (IEEE8021-PAE-MIB)
- IEEE 802.1x – 2001 MIB
- Extreme extensions to 802.1x-MIB
- Secure Shell (SSHv2) clients and servers
- Secure Copy (SCPv2) client and server
- Secure FTP (SFTP) server
- SFlow version 5 (*i*)
- NetFlow version 1 export (*i*)
- Configuration logging
- Multiple Images, Multiple Configs
- BSD System Logging Protocol (SYSLOG), with Multiple Syslog Servers
- Local Messages (criticals stored across reboots)
- IEEE 802.1ab Link Layer Discovery Protocol (LLDP)

ExtremeWare vendor MIBs:includes ACL, MAC FDB, IP FDB, MAC Address Security, Software Redundant Port, NetFlow, DoS-Protect MIB, QoS policy, Cable Diagnostics, VLAN config, vMAN, VLAN Translation and VLAN Aggregation MIBs

Security
- Routing protocol MD5 authentication (see above)
- Secure Shell (SSHv2),Secure Copy (SCPv2) and SFTP with encryption/authentication
- SNMPv3 user based security, with encryption/authentication (see above)
- RFC 1492 TACACS+
- RFC 2865 RADIUS Authentication
- RFC 2866 RADIUS Accounting
- RFC 3579 RADIUS Support for Extensible Authentication Protocol (EAP)
- RFC 3580 802.1X RADIUS
- RADIUS Per-command Authentication
- MAC based Network Login using Radius
- Access Profiles on All Routing Protocols
- Access Profiles on All Management Methods
- Network Login (web-based DHCP / HTTP/ RADIUS mechanism)
- RFC 2246 TLS 1.0 + SSL v2/v3 encryption for web-based Network Login

ExtremeWare 7.7 Supported Protocols

- IEEE 802.1x – 2001 Port-Based Network Access Control for Network Login
- Multiple supplicants for Network Login (web-based and 802.1x modes)
- Guest VLAN for 802.1x
- MAC Address Security – Lockdown, limit and aging
- IP Address Security with DHCP Option 82, DHCP Enforce / Duplicate IP Protection via ARP Learning Disable
- Network Address Translation (NAT)
- Layer 2/3/4/7 Access Control Lists (ACLs)
- Source IP Lockdown – Dynamic filtering against invalidly sourced traffic

Denial of Service Protection:

- RFC 2267 Network Ingress Filtering
- RPF (Unicast Reverse Path Forwarding) Control via ACLs
- Wire-speed ACLs
- Rate Limiting ACLs
- Rate Shaping by ACLs (*i*)
- IP Broadcast Forwarding Control
- ICMP and IP-Option Response Control
- Server Load Balancing with Layer 3,4 Protection of Servers (*i*)
- SYN attack protection
- FDB table resource protection via IPDA Subnet Lookup
- CPU DOS protection with ACL integration: Identifies packet floods to CPU and sets an ACL automatically, configurable
- Traffic rate limiting to management CPU / Enhanced DoS Protect (*i*)
- Uni-directional Session Control

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

(*i*) *An item appended by this symbol is only supported on the “i” series of Extreme Networks products. Please review product datasheets for details regarding support for individual features.*

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