

Alpine® 3800 Series Switches



The Alpine 3800 series switches enable new converged technologies, such as wireless and Voice-over-IP (VoIP).

Availability

- Hot-swappable I/O modules and fan trays
- Fully redundant, load-sharing, hot-swappable power supplies
- Ethernet Automatic Protection Switching (EAPS) for SONET-like resiliency

Security

- Protection against Denial of Service (DoS) attacks
- Network Login and 802.1x to authenticate and protect networks at the point of entry
- Hardware based Layers 2 – 4 Access Control Lists (ACLs) at wire-speed

Scalability

- 802.3af Power-over-Ethernet (PoE) to support converged network applications
- Policy-Based Quality of Service (QoS) at wire-speed to allocate bandwidth and prioritize traffic
- Bidirectional rate shaping to provision and manage bandwidth by the slice from 1Kbps to 1Gbps
- Jumbo frames to efficiently utilize high-performance connections

Management

- Secure Shell (SSH2) encrypts remote telnet management connections across the network
- End-to-end ExtremeWare® and EPICenter® software

Extreme Networks® award-winning Alpine 3800 chassis switches support the scalability, flexibility, security and management features required to build complete enterprise networks, including large campuses, branch offices, data centers and wiring closets. Alpine 3800 series switches enable enterprise networks to adopt new technologies, such as wireless and VoIP, by offering intelligent security and availability features to keep network convergence simple and manageable.

Providing advanced availability, scalability and management features, Alpine 3800 series switches are ideally suited for service providers and metropolitan area networks.

Alpine 3800 series switches support a wide offering of high-performance Ethernet connections including standard Category 5, fiber optic media, legacy WAN, and PoE. With the flexibility and scalability of a modular chassis, Alpine switches provide a complete solution for Ethernet network connectivity.

Target Applications

- Highly available, simple converged networks supporting VoIP and wireless applications.
- Server farms with high density 10/100 and gigabit traffic control requirements.
- Gigabit metro Ethernet networks with requirements for VPN and Telco WAN links to interconnect enterprise sites.

Technology that Preserves Your Investment

Alpine 3800 Chassis Switch Features

High Availability

The Alpine 3800 series chassis support hot swappable I/O modules and fan trays along with fully redundant, hot swappable power supplies that ensure high availability. The Alpine 3800 switches are NEBS Level 3 compliant and meets the highest level of quality demanded by network service providers around the world.

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, offering sub-second (less than 50 milliseconds) recovery and delivers consistent failover regardless of number of VLANs, number of network nodes or network topology. In most situations, digital video feeds don't freeze or pixelize because EAPS enables the network to recover almost transparently from link failure. The Alpine 3800 series supports Spanning Tree, VLAN Spanning Tree (802.1D), and Rapid Spanning Tree (802.1w) protocols for Layer 2 resiliency. Software enhanced availability allows users to remain connected to the network even if part of the network infrastructure is down.

Alpine 3800 series switches constantly check for problems in the uplink connections using advanced Layer 3 protocols such as OSPF, VRRP and ESRP (ESRP supported in Layer 2 or Layer 3), and dynamically routes around the problem. 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 enables trunking of up to eight links on a single logical connection, to provide a single trunk of redundant bandwidth per logical connection.

Extensive Traffic Management Capabilities

Extreme Networks revolutionary rate shaping capabilities provide Layer 3 IP/Ethernet networks that deliver a fixed latency, guaranteed transit path for voice or video traffic equal to that achievable with ATM but at a fraction of the cost and complexity. This makes the implementation of VoIP or VOD or other delay sensitive traffic feasible, without requiring bandwidth over-provisioning.

IETF DiffServ combined with Policy-Based QoS enables classes of services to be defined and enforced end-to-end across the network. Extreme Networks capability to classify packets using Layer 1 through Layer 4 attributes regardless of whether traffic is being switched or routed, combined with the ability to also honor priorities assigned before the traffic entered their network as well as re-write the signaling attributes (i.e. DiffServ), gives service providers unique control of application and service quality. These advanced capabilities ensure high bandwidth management and congestion control.

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 Alpine 3800 series switches, and packages data into sFlow datagrams that are sent over the network to an sFlow Collector that has an up-to-the-minute view of traffic across the network. sFlow can be used to troubleshoot network problems, control congestion and to detect network security threats.

Comprehensive Security Features

VMANs allow service providers to securely preserve the integrity of their customers' data while mixing and matching traffic from multiple sources over the same shared backbone. Providing intrusion detection and prevention, Alpine 3800 series switches support line-rate 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.

ACLs are one of the most powerful tools to control network resource utilization and to secure and protect the network. The Alpine 3800 series supports ACLs based on Layer 2, 3 or 4-header information such as the MAC address or IP source/destination address.

The use of protocols like SSH2, SCP and SNMPv3 supported by an Alpine 3800 series switch prevents the interception of management communications and man-in-the-middle attacks. When a hub or Wireless Access Point (WAP) is attached to a switch running 802.1x, only the first user on the hub or WAP is authenticated; any subsequent users connected to the hub or WAP are allowed to pass unchallenged. Multiple supplicant (client) support on the Alpine 3800 enables multiple clients to be individually authenticated on the same port.

The IPDA SUBNET lookup feature reduces exposure to malicious users or virus infected end clients and accelerates packet forwarding.

Alpine 3800 series 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.

Ease of Management

Extreme Networks has developed tools that save you time and resources in managing your network. EPICenter® provides all fault configuration, accounting, performance, and security functions to manage Extreme Networks' multilayer switching equipment in a converged network. EPICenter Policy Manager provides layer independent policy enforcement for Layers 1 – 4. Extreme Networks' software application, ServiceWatch®, delivers powerful, Layers 4 – 7 monitoring and management for mission-critical network services.

Technical Specifications

ExtremeWare v7.6 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
- 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
- Extreme Multiple Instances of Spanning Tree Protocol (EMISTP)
- PVST+, Per VLAN STP (802.1Q interoperable)
- Extreme Standby Router Protocol (ESRP)
- IEEE 802.1Q – 2003 Virtual Bridged Local Area Networks
- Extreme Discovery Protocol (EDP)
- Static Unicast Routes
- Extreme Loop Recovery Protocol (ELRP)
- Software Redundant Ports
- IPX RIP/SAP Router specification

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
- Multiple STP domains per VLAN
- RFC-3069 VLAN Aggregation for Efficient IP Address Allocation
- Virtual MANs (vMANs)
- VLAN Translation

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
- RED as described in “Random Early Detection Gateways for Congestion Avoidance, Sally Floyd and Van Jacobson”
- RED as recommended in RFC 2309
- Bidirectional Rate Shaping
- 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

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

- 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

- 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
- PIM Snooping
- DVMRP v3 draft IETF DVMRP v3-07
- 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
- 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
- RFC 2787 VRRP MIB
- RFC 2925 Ping/Traceroute/NSLOOKUP MIB
- Draft-ietf-bridge-rstpmb-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
- NetFlow version 1 export
- 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
- 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 ACLs
- Source IP Lockdown – Dynamic filtering against invalidly sourced traffic

Technical Specifications

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
- IP Broadcast Forwarding Control
- ICMP and IP-Option Response Control
- Server Load Balancing with Layer 3, 4 Protection of Servers
- 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
- Unidirectional 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

Ordering Information

Part Number	Description
Chassis	
45061	Alpine 3802 3-slot Chassis (includes SMMi, single AC PSU, fan tray)
45062	Alpine 3802 3-slot Chassis (includes SMMi, dual AC PSU, fan tray)
45064	Alpine 3802 3-slot Chassis (includes SMMi, dual DC PSU, fan tray)
45040	Alpine 3804 5-slot Chassis (includes fan tray)
45080	Alpine 3808 9-slot Chassis (includes fan tray)
45014	Alpine 3800 Switch Management Module
I/O Modules	
45122	Alpine 3800 16-port auto-negotiating 10/100/1000BASE-TX (RJ-45) Module
45121	Alpine 3800 16-port 1000BASE-X module with 16 unpopulated mini-GBIC 1000BASE-X ports (SFP)
45113	Alpine 3800 4-port auto-negotiating 100/1000BASE-T (RJ-45) Module
45112	Alpine 3800 4-port 1000BASE-X GBIC-based (unpopulated) Module
45110	Alpine 3800 4-port 1000BASE-SX (MT-RJ-based) Module
45210	Alpine 3800 32-port 10/100BASE-TX (RJ-45) Module
45220	Alpine 3800 32-port Power over Ethernet 10/100BASE-TX (RJ-45) Modules
45213	Alpine 3800 24-port 10/100BASE-TX (RJ-21) Module
45211	Alpine 3800 24-port 100BASE-FX (MT-RJ) Multimode Module
45302	Alpine 3800 4-port T1 (RJ-48) WAN Module
45305	Alpine 3800 1-port T3 (BNC) WAN Module
45306	Alpine 3800 4-port E1(RJ-48) WAN Module
45310	Alpine 3800 Eight-port VDSL (RJ-21) Module
45380	Alpine 3800 VDSL CPE with 10BASE-T Interface
Software	
45033	ExtremeWare full Layer 3 voucher for the Alpine 3804 and 3808
45034	ExtremeWare full Layer 3 voucher for the Alpine 3802
Power Supplies and Accessories	
45012	Alpine 3800 AC Power Supply; Includes power cord for US & Japan
45022	Alpine 3800 DC Power Supply
45005	Alpine 3800 Blank Faceplate (spare)
45013	Alpine 3808 Spare Fan Tray
45015	Alpine 3804 Spare Fan Tray
45019	External PoE Power System (Summit® 300-24 cable included; Alpine FM-32Pi cable not included)
46101	Cable to connect Alpine FM-32Pi to single EPS-LD PSU
46102	Cable to connect Alpine FM-32Pi to redundant EPS-LD PSUs
10011	Extreme 1000BASE-SX GBIC-based transceiver, SC connector, for use with multi-mode fiber with distances up to 550 meters
10013	Extreme 1000BASE-LX GBIC-based transceiver for distances up to 10km; SC connector, for use with single mode fiber
10017	Extreme 1000BASE-ZX GBIC based transceiver, extra long distance single mode fiber: 70Km/21dB Budget. SC connector
10051	Mini-GBIC, SFP, 1000BASE-SX, LC Connector (multimode fiber)
10052	Mini-GBIC, SFP, 1000BASE-LX, LC Connector (single/multimode fiber)
10053	Mini-GBIC, SFP, 1000BASE-ZX, LC Connector (single mode fiber)



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

© 2006 Extreme Networks, Inc. All rights reserved.
 Extreme Networks, the Extreme Networks Logo, Alpine, EPICenter, ExtremeWare, ServiceWatch and Summit are either registered trademarks or trademarks of Extreme Networks, Inc. in the United States and/or other countries.
 Specifications are subject to change without notice.