Data Sheet

SUMMIT 300-24
UNIFIED ACCESS SWITCH

Industry leading versatility for converged networks: Power over Ethernet and wireless LAN capabilities integrated with advanced Layer 3 features.

The Summit® 300-24 sets a new standard for edge connectivity in today's most demanding converged networks. Building on a solid foundation of performance, security, availability, and management capabilities, it additionally offers Power over Ethernet (PoE) on every one of its 24 ports. With its integrated PoE, the Summit 300-24 can power up to 24 Class 3 (15.4 watt) devices such as Voice over IP (VoIP) phones, surveillance cameras, and badge readers. Finally, by utilizing Extreme's unique Unified Access architecture, wireless access points can be seamlessly and securely deployed and managed throughout a facility for any number of wireless data or voice applications.

Based on the award-winning ExtremeWare® Layer 3 software, the Summit 300-24 provides 24 ports of 10/100 Ethernet with four physical Gigabit Ethernet uplinks (two active and two redundant). Every port delivers a vast array of ExtremeWare Layer 3 and Layer 2 features; ranging from OSPF routing and advanced Quality of Service (QoS) classification to the latest advancements in security. Years of development based on the requirements of thousands of customers enables ExtremeWare to deliver the most comprehensive Layer 3 advanced software solution set at the edge while allowing easy expansion and addition of services without major upgrades.

Once again, Extreme Networks® demonstrates why it is the leader in Layer 3 switching for today's most demanding converged networks.

Summit 300-24 Benefits

High Performance

- Non-blocking wire-speed architecture ensures performance for the most demanding wired and wireless applications. Extreme's Altitude access points support 802.11 a, b, and g, today's fastest wireless LAN standards.

Extraordinary Availability

- Redundant copper and fiber Gigabit uplinks, dual-homed configurations, and sub-second EAPS failover provide mission-critical resiliency. The switch continuously monitors "heartbeats" generated by the Altitude access points, ensuring continuous wireless user operation.

Industry-Leading Security

- Extreme's Unified Access architecture provides a single wired/wireless authentication infrastructure for consistent, policy-based security from the edge to the core. Wireless security includes hardware-accelerated AES and RC4 encryption. Extreme also offers rogue access point detection for defending the wireless perimeter of a network.

Scalability

- The Summit 300-24 powers every port to the full Class 3 specification of 15.4 watts per voice, video, wireless, or data device.

End-to-End Manageability

- As a member of Extreme's comprehensive family of switches, the Summit 300-24 can be centrally deployed, managed, and monitored using Extreme's EPICenter management platform or any SNMP-based product. In addition, Extreme offers RF Manager for simplified wireless design and its AccessAdapt utility for no-config installation of the Altitude access points.

Extraordinary 10/100 Performance, PoE, and Wireless

With its non-blocking architecture the Summit 300-24 has an 8.8 Gbps switch fabric that enables all RJ-45 copper 10/100 ports to operate at line rate. Four hardware queues per port provide granularity and guarantee low latency and low jitter for time-sensitive voice and multi-media applications. These applications also benefit from features such as DiffServ and 802.1p which deliver varied levels of service and ensure efficient bandwidth usage. The 4 Gigabit Ethernet uplink ports (two 1000BASE-T RJ-45 copper and two fiber gigabit) can be configured with 2 active and 2 redundant for fast Layer 1 failover. These uplink ports provide the added flexibility of port redundancy between copper and fiber ports, enabling backup links to the active uplinks with sub-second (50 msec) failover capability through EAPS.

The Summit 300-24 offers a number of features that improve the performance of the network, such as RIP, OSPF, Network Address Translation, QoS classification, dynamic VLANs, and Access Control Lists. For converged applications involving voice or rich media, the switch provides multicast, re-writing 802.1p tag prioritization, or prioritization using Layer 2/3/4.

The Summit 300-24 delivers advanced high availability features traditionally reserved for carrier networks. Ethernet Automatic Protection Switching (EAPS, RFC 3619) delivers sub-second (less than 50 msec recovery) protection switching to interconnected switches in an Ethernet ring topology. Similar to the Spanning Tree Protocol (STP), EAPS offers the advantage of converging in significantly less time than STP or even Rapid Spanning Tree (802.1W) when a link breaks in the ring. Extreme Standby Routing Protocol™ (ESRP) can be implemented at both Layers 2 and 3 and extends the Virtual Redundant Redundancy Protocol's (VRRP) capabilities, adding Layer 2 resiliency and loop prevention and Layer 3 default router redundancy. It can be used as a STP substitute and can be scaled to protect thousands of VLANs. Multiple instances of ESRP in the same VLAN allow direct host attachment to standby switches.

Equal Cost Multipath (ECMP) adds network resiliency as multiple equal-cost routes can be used concurrently to an end destination. With Software redundant port feature, a specified primary port can be backed up by another port. Should the link go down on the primary port, the redundant port will establish link and become active. Thus multi-homed redundancy can be easily designed without the implementing complexity of a protocol.

For Power over Ethernet, a 370 Watt power supply generates 15.4 watts of PoE to all 24 ports for devices such as VoIP phones, surveillance cameras, badge readers, Extreme's Altitude access points, and "fat" access points sold by other vendors. Redundant power is available via an optional external power supply. Altitude access points simultaneously broadcast both 802.11a and 802.11b/g ensuring wireless performance. Extreme has also implemented the SpectraLink Voice Protocol (SVP), a QoS standard used by the leading wireless LAN handsets today for recognizing and prioritizing voice packets. When enabled in tandem with the Inter-Access Point Protocol (IAPP) which allows Layer 2 roaming between AP's, Voice over Wireless LAN (VoWLAN) users can productively communicate with customers, patients, emergency personnel and employees anytime within a facility.

The Summit 300-24 enables high quality Voice-over-Wireless LAN (VoWLAN) with leading handsets such as SpectraLink.

Compared to other vendors' point solutions, the Summit 300-24 offers a low total cost of ownership because it is fully integrated into Extreme's family of edge and core end-to-end solutions. ExtremeWare Layer 2 and Layer 3 features implemented in the Summit 300-24 are shared with all other Extreme platforms in the Summit product line as well as with Alpine™ and BlackDiamond® switches.

From a PoE/wireless perspective, the 300-24 is complementary to the 48 port Summit 300-48 and the chassis-based Alpine 3800 PoE blade. Each of these switches contribute to Extreme's Unified Access initiative, providing a seamless infrastructure for voice and data support on both wired and wireless networks. The common ExtremeWare software used by these products makes it easy to develop centralized configuration and management policies throughout the network. The Summit 300-24 also uses the same command line interface (CLI), the EPICenter™ graphical management interface and the same management commands as other Extreme switches so training time and expense are reduced as operational expertise can be shared over an entire network solution.

Intelligence at the Edge – Where You Need It

Enterprise networks need both Layer 2 and Layer 3 intelligent services at the edge to ensure maximum network efficiency. Intelligence supports critical functionality such as security to prevent unauthorized access, high availability to ensure network uptime, and common management to reduce expenses.

Security is a paramount concern in today's converged networks. Extreme's Unified Access architecture provides consistent wired and wireless security from the edge to the core. ExtremeWare supports multiple authentication options including 802.1x, web-based login with SSL, and MAC address. With IEEE 802.1x login, Network Managers can always control who is accessing and connected to the network. Web-based network login offers the freedom of authenticating through any HTTP-compliant web browser. During the authentication process, SSL (Secure Sockets Layer) encrypts logon information.

MAC Address Security prevents unauthorized port abuse from rogue wireless access points or hubs/switches on edge ports. Port abuse can be prevented using lockdown on a per port basis and/or limiting of the number of MAC addresses learned by a port. The lockdown feature and saving learned MAC addresses between reboot can be used, for example, to protect dedicated ports for VoIP phones or printers from abuse. Limiting the number of MAC addresses learned on a port also allows enforcement of service level agreements in tenant or service provider environments. MAC Address Security can also be used in conjunction with a RADIUS server to allow devices such as bar code readers that do not support 802.1x to enter the network based on their MAC address.

Multiple Supplicant (client) enables clients to be individually authenticated on the same port. Thus it is possible for two client stations to be connected to the same port, with one being authenticated and the other not. Wire speed Layer 2-4 Access Control Lists enable port security without worrying about the degrading performance and disrupting business applications or reducing productivity. SSHv2 allows Network Managers to securely and remotely configure the switch without any risk of packet snooping or man-in-the-middle attacks. SSHv2, denial of service protection, TACACS+ and RADIUS provide reliable and secure configuration traffic (encryption) and authentication.

As part of its Unified Access architecture, Extreme has comprehensively designed for wireless security. The Altitude access point offers scalable, hardware-accelerated AES and RC4 encryption. Perimeter defense is ensured through rogue access point and client detection, which is monitored and reported by EPICenter, which also offers a "one-click" command to disable the rogues. Optional directional antennas

Extreme Networks' Altitude access point provides secure wireless connectivity with the Summit 300-24.

can be used to focus the wireless beam into the enterprise's facility. And finally, the Altitude is a "thin" access point, preventing the physical theft of critical security parameters because it loses its configuration as soon as it is unplugged.

SUMMIT 300-24 FEATURE SET SUMMARY

Hardware Features

- 24 10/100 auto-negotiating Ethernet ports in a 1 RU footprint allow more network connections per inch of rack space
- 2 10/100/1000BASE-T copper ports and 2 mini-GBIC ports deliver two active gigabit uplinks for greater throughput and two redundant uplinks for high availability
- Single AC power supply. Provides 370W of available power for PoE devices, supporting up to 24 IEEE 802.3af Class 3 (15.4W) devices. External redundant power supply available optionally.

Performance Features

- Non-blocking wire speed architecture
- 8.8 Gbps switch fabric, enabling all 10/100 ports to operate at line rate
- Flow-based central rate limiting that can be applied to any classified packet flow
- 255 port based and MAC based VLANs
- 8,191 MAC addresses
- 4 hardware queues per port
- 4 Gigabit Ethernet uplink ports, 2 active and 2 redundant with Layer 1 failover
- ACLs for optimal security and diverse traffic classification

ExtremeWare Intelligent Services

- Security
  - Denial of Service (DoS) protection
  - Intelligent Network Access with EPICenter Policy Manager, including compatibility with Sygate host integrity checking
  - IP Address Security: DHCP Option 82
  - IP Address Security: Disable ARP learning
  - Layer 2/3/4 Access Control points
  - MAC Address Security (lockdown + limit)
  - Management Security: SNMPv3, SSH2-client, SCP/SFTP
  - Multiple supplicants
  - Network Login
    - 802.1x
    - Web-based Network Login
  - RADIUS authentication separated between Network Access and Device Management Security
  - SSH2 server
  - TACACS+ support
- Availability
  - ESRP (in Advanced Edge license)
  - Ethernet Automatic Protection Switching-edge (EAPS-edge)
  - Loop detection via Lbdetect and ELRP CLI
  - Network Address Translation
  - RSTP: 802.1w Rapid Spanning Tree
  - Software Redundant Port
  - STP: Compatibility mode for PVST+, EMISTP (1 domain per port)
  - VRRP (in Advanced Edge license)
- QoS
  - 4 priority queues
  - 802.1p priority marking
  - Layer 2 classification
  - Layer 3 DiffServ
  - Layer 2/3/4 Access Control Lists (ACLs)
- Extensibility
  - Multicast: static IGMP membership
  - Static Multicast Routes
- Scalability
  - LACP for edge deployment (server connectivity)
- Routing
  - Extreme Standby Router Protocol (ESRP)
  - OSPF Edge
  - RIP v1/v2
- Multicast - edge
  - IGMP v1/v2
  - IGMP snooping
  - PIM/SM edge
- Simplicity
  - Entity MIB for inventory
  - mtrace/mrinfo

Management Features

- Serial management port on the front panel for ease of installation
- Extensive management through SNMP, RMON and command line interface
- Secure remote management with strong encryption using SSH2
- Port mirroring

PRODUCT SPECIFICATIONS

Switch Fabric

- Bandwidth: nonblocking, 8.8 Gbps

Forwarding Rate

- 6.55 million packets/second
- Max Packet Size: 1522

Ports

- 24 RJ-45 10/100 ports (IEEE 802.3 Type 10BASE-T; 802.3u Type 100BASE-TX)
- 2 dual personality ports: Either RJ-45 10/100/1000 ports (IEEE 802.3 Type 10BASE-T; 802.3u Type 100BASE-TX; 802.3ab 1000BASE-T Gigabit Ethernet) or open mini-GBIC slot

General

- Number of QoS queues/port: 4
- Number of VLANs: 255
- VLAN Types: Port, IEEE 802.1Q, and MAC-based
- Number of ACL Rules/lines: 1014 (can be applied to either ingress or egress)

Forwarding Tables

- Layer 2/MAC Addresses: 8K
- Layer 3 forwarding database in hardware: 2K
- Layer 3 Routing table size: 8K

Rate Limiting

- Flow-based Bandwidth policing/rate limiting: pool of 315 rate limiters that can be applied to any classified ACL flow (ingress flows)
- Rate Limiting Granularity: 1Mb/s on 10/100BASE-T ports. 8Mb/s on 1000BASE-T ports

Physical And Environmental

Dimensions

- Height: 1.75 Inches/4.4 Cm
- Width: 17.35 Inches/44.1 Cm
- Depth: 15.3 Inches/37.5 Cm
- Weight: 14 lbs/6.4Kg
- Operating Temperature Range: 0° to 40° C (32° to 104° F)
- Storage Temperature Range: -40° to +70° C (-40° to 158° F)
- Humidity Range: 10-95% (RH) non-condensing
- Acoustic:
  - 43.6 dBA Sound Pressure per ISO 7779 clause 8
  - 5.2 belsA Sound Power per ISO 7779 clause 7 in accordance with EN 300 753 as specified in EN/ETSI 300 019

Power

The Summit 300-24 supports 802.3af PoE power management

- Power requirements with no PoE devices connected to the ports:
  - Min Voltage/Associated Current: 100VAC/0.60A
  - Max Voltage/Associated Current: 240VAC/0.25A
  - Heat Dissipation, Watts: 60 W/198 BTU/hr
  - Total AC power consumption: 60 W
- Power requirements with a total of 370 watts of PoE delivered to the ports:
  - Min Voltage/Associated Current: 100VAC/5.5A
  - Max Voltage/Associated Current: 240VAC/2.3A
  - Heat Dissipation, Watts: 144 W/490 BTU/hr
  - Total AC power consumption: 510 W

Regulatory

Safety

North America

- cULus Listed device – UL 60950:2000 (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 CFR1040.10 & 1040.11 (Safety of Laser Products)
- CDRH Letter of Approval (US FDA Approval)

Europe

- EN60825-2 (European Safety of Lasers)

EMI/EMC

North America

- 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)

Environmmental

Standard

- 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 D3332 * - Shock - Unpackaged
- ASTM D3580 * - Random Vibration – Unpackaged

Reliability

- Calculated MTBF: 142,333 hours

Warranty

- Limited Lifetime Warranty

ExtremeWare Protocols Enabled by the Summit 300-24 Edge and Advanced Edge Licenses

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)
- 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
- EMISTP, Extreme Multiple Instances of Spanning Tree Protocol compatibility mode (one domain per port)

- PVST+, Per VLAN STP (802.1Q interoperable) compatibility mode (one domain / VLAN per port)
- Extreme Standby Router Protocol (ESRP)
- Static Unicast Routes
- Loop detection / protection via Layer 2 LBdetect and ELRP
- Software Redundant Ports

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

Quality of Service and Policies

- IEEE 802.1D -1998 (802.1p) Packet Priority
- RFC 2474 DiffServ Precedence, including 4 (8 on S400) queues/port
- RFC 2598 DiffServ Expedited Forwarding (EF)
- RFC 2597 DiffServ Assured Forwarding (AF)
- RFC 2475 DiffServ Core and Edge Router Functions
- Ingress Rate Limiting
- Layer 1-Layer 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 Edge (2 Active Interfaces, router priority 0)

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

IP Multicast

- RFC 2362 PIM-SM Edge (2 active interfaces as first-hop router, no RP/BSR role)
- 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 and TRAPs
- RFC 1573 Evolution of Interface
- RFC 1650 Ethernet-Like MIB (update of RFC 1213 for SNMPv2)
- 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 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 1724 RIPv2 MIB
- RFC 1850 OSPFv2 MIB
- RFC 2787 VRRP MIB
- RFC 2925 Ping/Traceroute /NSLOOKUP MIB
- Draft-ietf-bridge-rstpmib-03.txt (Definitions of Managed Objects for Bridges with RSTP)
- 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
- Configuration logging
- Multiple Images, Multiple Configs
- BSD System Logging Protocol (SYSLOG), with Multiple Syslog Servers
- Local Messages (critical messages stored across reboots)

ExtremeWare vendor MIBs (includes ACL, MAC FDB, IP FDB, MAC Address Security, Software Redundant Port, DoS-Protect MIB, QoS policy, Cable Diagnostics, VLAN config.
http://www.extremenetworks.com/services/documentation

Security

- Routing protocol MD5 authentication
- Secure Shell (SSHv2),Secure Copy (SCPv2) and SFTP with encryption/authentication
- 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 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)
- MAC Address Security - Lockdown, Limit and Trusted OID
- 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)

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
- Unidirectional Session Control
- CPU DoS protection with ACL integration: Identifies packet floods to CPU and sets an ACL automatically, configurable
- CPU DoS Protection with traffic ratelimiting 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	fraggle	Latierra
boink	papasmurf	Winnuke
opentear	synk4	Simping
jolt2	raped	Sping
newtear	winfreeze	Ascend
nestea	ping –f	Stream
syndrop	ping of death	Land
smurf	pepsi5	Octopus

Ordering Information

Part Number	Name	Description
13245	Summit 300-24	Summit 300-24, 24 10/100 ports w/Power over Ethernet, 2 1000BT, 2 mini-GBIC, Edge EW
13246	Voucher, Summit 300-24 Advanced Edge	Voucher, Summit 300-24 Advanced Edge ExtremeWare Upgrade License. Includes wireless

Accessories

Part Number	Name	Description
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
45019	EPS-LD External AC PSU	External PoE Power System (S300-24 cable included; Alpine FM-32Pi cable not included)

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