Summit® WM Series WLAN Switches

The Summit WM series switches—a fresh approach to managing the complexity of configuring and operating wireless networks.

Ease of Installation and Operation

- Wireless mobility access domains for multiple access types
- AutoCell® dynamic Radio Frequency (RF) management
- Plug and Play AP installation

Voice-Grade Performance

- High-speed, cross-subnet roaming
- End-to-end Quality of Service (QoS)
- High availability to meet voice service expectation

Comprehensive Security

- Directory-integrated link security simplifies user access management
- Rich set of authentication options and access control options for every application and device
- Wireless intrusion detection

The Summit WM series switch is ready to support the most advanced wireless applications.

Summit WM series switches deliver a high-performance wireless LAN solution that is easy to use and is secure. In today's Enterprise environments, dedicated resources are rarely available to build and operate the wireless network. By focusing on ease of installation and management, the Summit wireless mobility solution from Extreme Networks® helps IT organizations simplify the task of mobilizing their users without sacrificing security or performance.

Summit WM series switches are ready to support the most advanced wireless applications. With the capability to support high-speed, cross-subnet roaming and sophisticated multicast support, Summit WM series switches can meet nearly any mobile voice or multimedia networking challenge. With capacities of up to 200 access points (APs) per switch, Summit WM series switches can scale to support the largest WLAN installations while providing centralized management for remote branch office installations. Available in a 4X Fast Ethernet or 2X Gigabit Ethernet version, both with redundant power supplies, Summit WM series switches are an ideal solution for your mobile data and voice challenges.

Target Applications

- Wireless connectivity for multiple user types and devices.
- WLAN to support high-performance applications such as voice over Wi-Fi.
- Distributed wireless connectivity with plug and play installation and centralized support.
- Applications requiring high availability and RF management.
- Sites requiring both connectivity and wireless intrusion detection.

Ease of Installation and Operation

Wireless LAN systems have been difficult to install, configure and operate. The Summit WM series provides a fresh approach to managing the complexity of configuring and operating wireless networks through a number of unique capabilities.

Summit Wireless Mobility Access Domains

Summit Wireless Mobility Access Domains (WM-AD) help administrators easily define profiles for different categories of users, groups, devices or applications. Compared to the other approaches that require the configuration of a multitude of security and performance parameters, WM-ADs are a simple and powerful approach to the changing access challenges of the dynamic Enterprise. For example, one Access Domain may be developed for guest access, another for Voice over Wireless LAN (VoWLAN) handsets, and a third for secure employee access.

After the administrator has defined Access Domains for the different types of users, each Access Domain is assigned to one or more Altitude 350-2 APs. The appropriate APs begin broadcasting service availability. For example, an Access Domain for guest access might be advertised by the APs in the lobby only, while a second Access Domain for VoWLAN phones could be supported by APs covering the factory floor.

From the user's perspective, each Access Domain will appear to be a standalone virtual AP, available only at the locations selected by the administrator. When a user or device associates with one of these virtual APs, the connection will be governed by the associated Access Domain parameters for authentication, privacy, QoS, and access to network resources.

AutoCell® Dynamic RF Management

Summit WM series switches simplify setup and operation through their extensive dynamic RF management capabilities. Dynamic RF management is enabled via AutoCell technology (optional on the Summit WM100). AutoCell automatically optimizes RF coverage in an area, selecting channels and adjusting power levels to provide trouble-free client connectivity while maximizing coverage.

Keeping up with changes that affect coverage can be a challenge. With AutoCell, calibration and adjustment automatically occur 24 hours a day, eliminating the need to manually set or tune power levels as conditions change. Should an AP fail, AutoCell provides fault tolerance by detecting the failure and compensating by increasing output power of the neighboring APs.

AutoCell uses a distributed algorithm that does not require a connection to a centralized resource. As a result, branch office support is simplified and the solution is highly scalable. AutoCell is very stable and does not "flap" during operation—meaning the WLAN remains available and reliable even when RF conditions are changing.

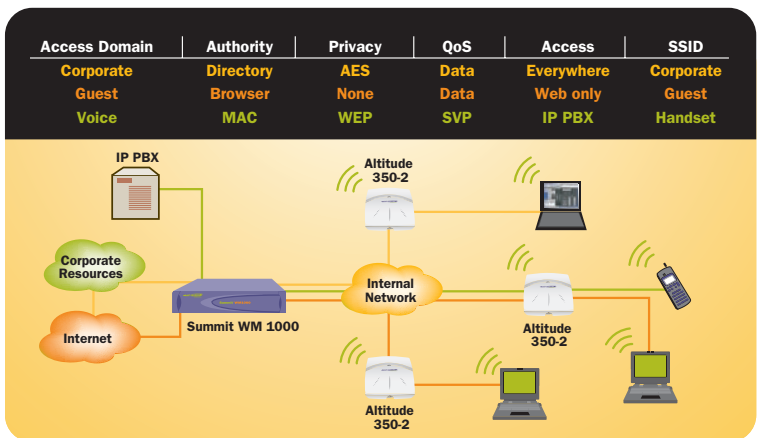
Plug and Play AP Installation and Intuitive Management

Out-of-the-box AP installation is a breeze. Using AccessAdapt™ technology, the Altitude 350-2 APs automatically discover the Summit WM switch and download configuration and operating parameters—without any pre-configuration of the AP. After receiving configuration information and being provisioned with the appropriate WM-ADs, APs begin broadcasting multiple Service Set Identifiers (SSIDs) to clients in the area. Technicians can quickly add new APs to an existing system without specialized WLAN knowledge.

The Summit wireless mobility solution is very easy to add to existing IP networks and wireless clients. Enterprises can enjoy outstanding performance, high security, and seamless roaming without needing to install and manage client drivers. Since APs and switches communicate using IP, designers do not need to configure network-wide VLANs when installing the wireless network.

The theme of simplicity continues with the intuitive Summit wireless mobility graphical management interface. It offers centralized configuration and management of users, devices, and applications and can be accessed via a web browser over the network or directly through a management port on the system. The interface provides remote performance and session monitoring, statistics, status monitoring, and reporting. The system supports SSL, SNMP v2, FTP, RADIUS accounting, statistics, syslog, and Secure Shell (SSH) interface.

Example: Profiles using wireless mobility access domains.



Voice-Grade Performance

Today's enterprise wireless LANs must perform the same tasks with the same expectations for performance and quality, as their wired counterparts. Summit WM series switches deliver outstanding performance for advanced, latency-sensitive applications such as voice over WLAN.

High-Speed Cross Subnet Roaming

Summit WM series switches offer scalable, voice-grade performance, meaning that VoWLAN users can roam from AP to AP—even across subnets—without experiencing annoying echoes or dropped connections. When roaming, client IP addresses do not change as users move and applications are not affected. These capabilities are easy to add to existing networks without configuration changes, topology modifications, or client software.

Summit WM series switches are capable of taking advantage of new roaming enhancements based on the 802.11i standard. With pre-authentication and key caching, users can quickly move between APs even when authenticating to centralized network RADIUS resources. Security is not compromised with the high-speed roaming—the Summit WM series switches generate a unique key only for the APs to which the client is likely to roam.

End-to-end Mobile Quality of Service

QoS is critical, especially for VoWLAN or high-priority users. The Summit WM switches' architecture offers end-to-end QoS from the wireless client to the packet destination. In addition, QoS is easy to configure for different classes of users through the WM-ADs.

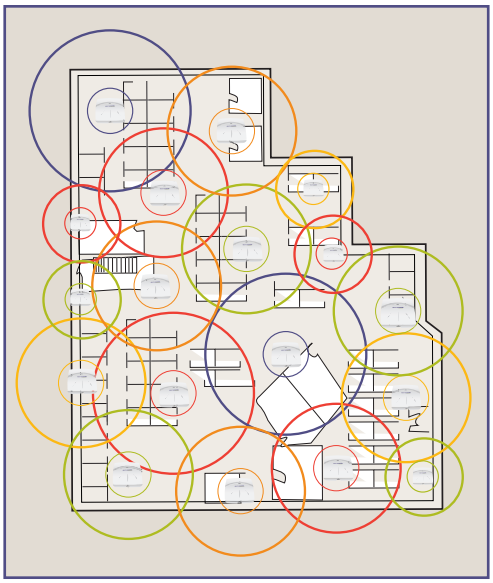
Extreme Networks' wireless QoS solution maintains the correct traffic priority from client to destination. Over the air, latency-sensitive traffic is given priority transmit access using either the SpectraLink Voice Protocol (SVP) or 802.11e Wireless Multimedia Extension (WME) priority management. Then before the APs tunnels latency-sensitive traffic to the switch, it adds a high-priority Type of Service (ToS) field to the tunneled packet. Finally, the Summit WM switch maintains the ToS field setting when the traffic is delivered to the enterprise LAN so that the traffic priority is maintained at every step of the way.

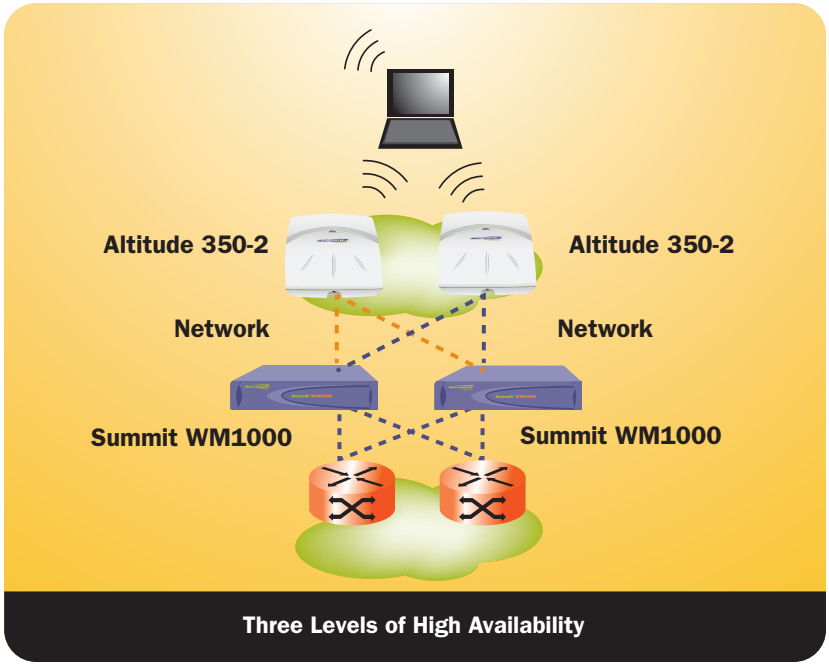
Mission-Critical High Availability

All aspects of the Summit wireless mobility solution provide enterprise-grade high availability. At the radio level, AutoCell will detect AP failures and boost the power output of the neighboring APs to compensate for the gap in coverage. This eliminates middle of the night support calls when an AP fails.

To enhance switch availability, the Summit WM switch ships with redundant power supplies, eliminating concerns about power supply failure. In addition, the switch can be configured in redundant mode with a second Summit WM switch. Should either switch fail, APs on that switch would detect the failure network link fail, the Summit WM switch can select a new network route, often over a different physical interface, using Open Shortest Path First (OSPF).

Dynamic RF Management Using AutoCell





Comprehensive Security

Security is justifiably a key concern for WLAN systems. Summit WM series switches offer state of the art security for link access and intrusion detection, all delivered using a single AP infrastructure.

Directory-integrated Link Security

The Summit wireless mobility solution delivers comprehensive link security capabilities that leverage existing directory resources to streamline management of user access. Link security characteristics are defined within the context of each WM-AD. To ensure high availability, multiple Authentication, Authorization, and Accounting (AAA) resources can be defined for specific WM-ADs.

Summit WM series switches offer a complete range of privacy options ranging from unencrypted communication for guests, shared key for phones and PDAs, to WPA-v1, and WPA–v2. For high-performance and scalability, all over-the-air encryption connections are terminated at the AP with hardware acceleration.

Multiple Authentication and Access Control Options

Each WM-AD specifies how the wireless user or device should authenticate, with options for browser-based login, MAC address verification, or 802.1x Enterprise AAA identity management. MAC address authentication can be combined with other link security types for additional protection.

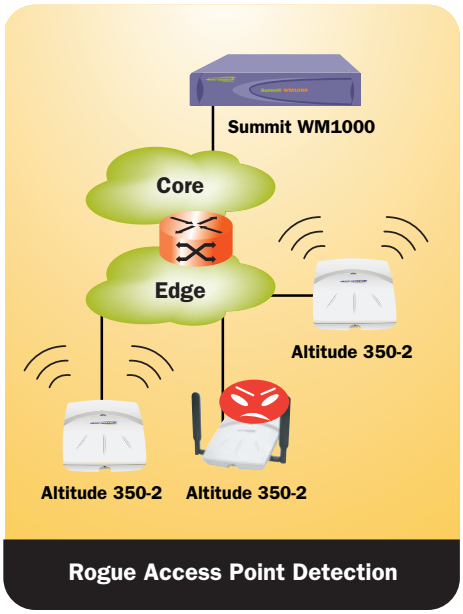
After users are placed on the network it is important to limit their access to the resources they need. WM-ADs offer comprehensive filtering options for each connection based on WM-AD membership, authentication status, and specific filtering instructions provided as a part of the RADIUS authentication message. Guests can be restricted to a "walled garden" or routed directly to the Internet. Traffic from specific WM-ADs can be restricted to selected ports and/or network locations using next-hop routing.

The Summit WM switch offers unique and powerful enhancements to basic network access control. Using information exchanged between the Summit WM switch and the RADIUS server, administrators can design sophisticated access control solutions that tailor access rights to specific locations, users, or roles. WM-ADs also simplify integration with VPN and firewall solutions by aggregating traffic through a specific physical port to the VPN or firewall resource, eliminating the need for standalone or redundant VPN systems for wired and wireless users.

Wireless Intrusion Detection

Rogue APs or unauthorized networks represent a significant threat to the integrity of Enterprise networks—even when wireless networks are not officially supported. Today's users have easy and inexpensive access to WLAN gear and may not understand the security risks associated with the installation of an unmanaged AP.

The Summit WM Spy capability provides intrusion detection by scanning multiple bands and channels to locate unauthorized rogue APs and Peer-to-Peer wireless networks. It does this by using the same Altitude 350-2 APs that are used for wireless connectivity support. If a rogue device/network is found, it is reported on the management console.



Rogue Access Point Detection

ACCESS TYPE	AUTHENTICATION	PRIVACY	ACCESS POLICY			
			SSID	Timeout	Location	Network
Casual Access Guests, Contractors	Browser-Based with Guest Password	None, Traffic is in the Clear	Guest	1 Hour	Lobbies and Conference Rooms	Internet Only
Devices Handsets, Bar code Readers	Shared Key or MAC Address	None, WEP, or WPA-PSK	Handset	None	Factory Floor	Application Network
Corporate Access Sensitive Users and Applications	EAP-TTLS, EAP-TLS, PEAP, EAP-MD5	Up to WPAv2 with AES	Corp	None	Anywhere	By User

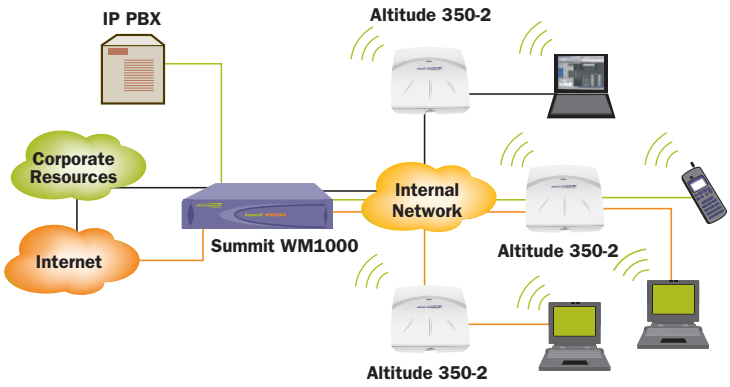
Three Examples of Link Security

Technical Applications

Enterprises Needing Wireless Connectivity for Multiple User Types and Devices

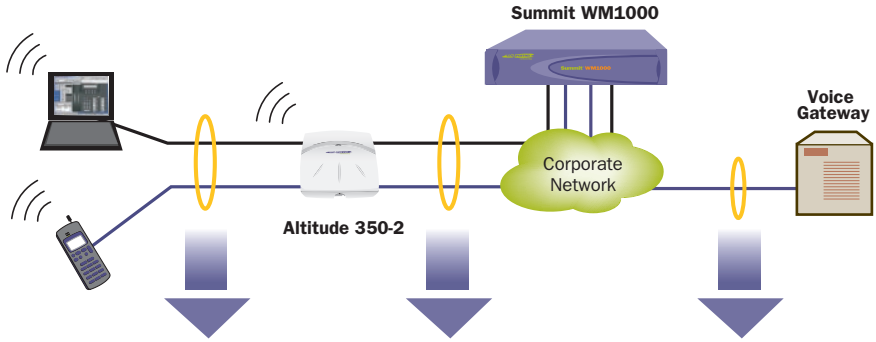
With Summit WM series switches, administrators can quickly and easily configure the system to support different categories of wireless users, such as guests, high-performance voice users, and employees with secure access to corporate resources. Each category has a number of easy-to-set customized parameters such as security, QoS, radio resources, and network access.

Access Domain	Authority	Privacy	QoS	Access	SSID
Corporate	Directory	AES	Data	Everywhere	Corporate (not broadcasted)
Guest	Browser	None	Data	Web only	Guest
Voice	Device address	Shared key	Priority	IP PBX	Handset



WLAN Solutions Supporting High-Performance Applications Such as Voice over WLAN

Summit WM series switches support voice-grade Layer 3 roaming across APs, with pre-authentication to preserve security and IP persistence to minimize dropped connections. Not only is this roaming available across subnets, but also across APs that are operating off of different Summit WM switches. This is ideal for voice handsets or roaming applications such as a wireless device mounted on a warehouse forklift.



Over The Air

- AP and clients transmit priority traffic first
- How: SVP or WME

To The Switch

- AP expedites high priority traffic to switch
- How: Map wired TOS field to priority WLAN traffic

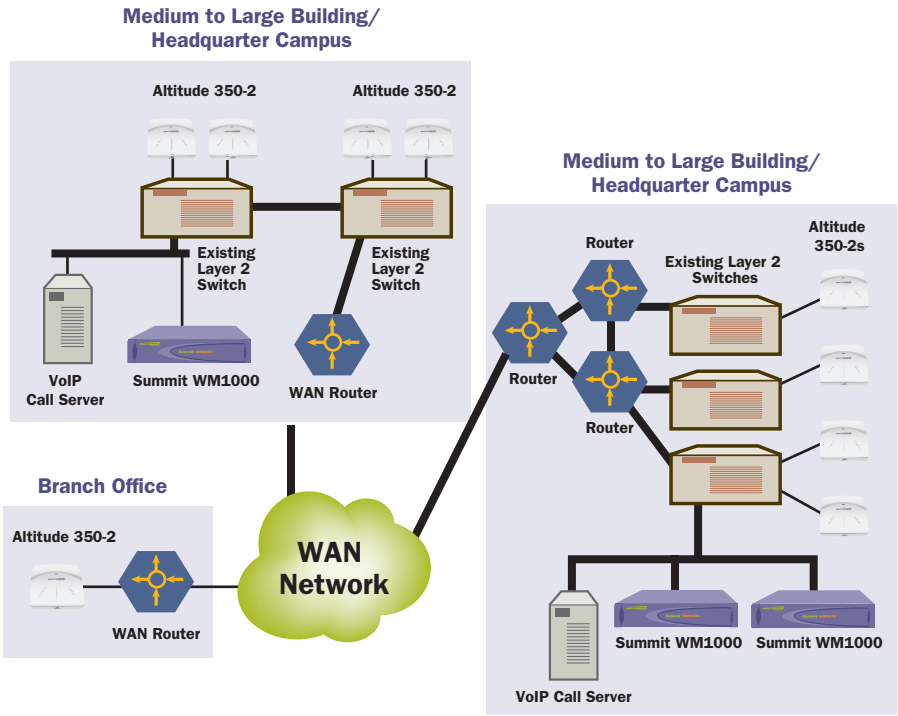
To The Destination

- Switch routes traffic to final destination
- How: Switch maintains ToS marking on high priority traffic

Technical Applications

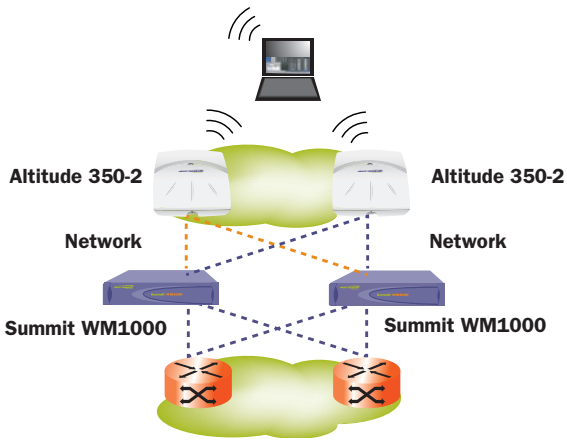
Deployments Requiring Distributed Wireless Connectivity with Plug and Play Installation and Centralized Support

Summit wireless mobility is ideal for multi-site enterprise deployments with a centralized Summit WM switch installed in the headquarters facility. APs can be shipped to remote sites and installed by non-skilled labor. When connected to the network, the APs will automatically find and connect to the Summit WM switch. With branch office mode, remote APs bridge to the local switching infrastructure, offering high-performance for local wireless users while still being centrally managed from the Summit WM switch.



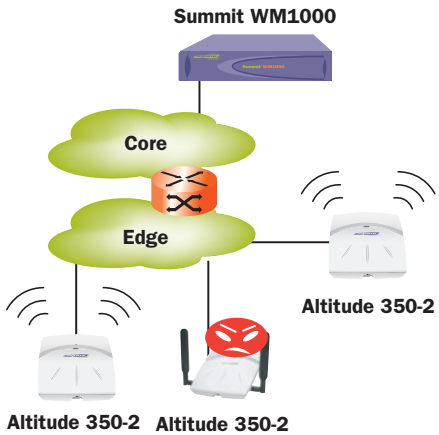
Applications Requiring High Availability and RF Management

Summit WM switches offer availability features such as redundant power supplies, with failover coverage, and the use of OSPF for protection against network outages. In addition, with AutoCell, RF coverage is monitored and should any changes in the environment occur (such as pallets of RF-blocking materials moved into a warehouse) or an AP fail, AutoCell will boost the power of neighboring APs to compensate for the coverage gap.



Sites Requiring Both Connectivity and Wireless Intrusion Detection

Summit wireless mobility allows installation of Altitude 350-2 APs for both wireless connectivity and for wireless intrusion detection. The APs can scan multiple channels in order to detect rogue APs and Peer-to-Peer networks. The results from the scanning can be collected, analyzed, and reported a central Summit WM system, allowing the administrator to identify the unauthorized devices.



Technical Specifications

Supported Protocols

Security

Authentication
- Captive Portal—URL Redirect to a Web Page
- Walled Garden—unauthenticated access to restricted sites
- 802.1x—WPA, EAP-TLS, EAP-TTLS, PEAP, EAP-MD5
- RADIUS, Rogue AP Detection

Encryption
- WEP (40 & 128 bit), TKIP, AES

IETF RFCs

- RFC 79 – IPv4
- RFC 1812 – Minimum Router Requirements
- RFC 793 – Transport Control Protocol (TCP)
- RFC 768 – User Datagram Protocol (UDP)
- RFC 792 – nternet Control Message Protocol (ICMP)
- RFC 826 – Address Resolution Protocol (ARP)
- RFC 2865 – Remote Access Dial In User Service (RADIUS)
- RFC 2866 RADIUS Accounting
- RFC 2165, 2608 - Service Location Protocol (SLP)
- RFC 2131 – Dynamic Host Configuration Protocol (DHCP)
- RFC 2328 – Open Shortest Path First (OSPF v2)
- RFC 1587 - OSPF Not So Stubby Area (NSSA) Option
- RFC1350: The TFTP Protocol (Revision 2)
- RFC 2716 – EAP-TLS
- RFC 1155 – Structure and identification of management information for TCP/IP-based internets
- RFC 1157 – Simple Network Management Protocol (SNMP)
- RFC 1212 – Concise MIB definitions.
- RFC 1213 – Management Information Base for Network Management of TCP/IP-based internets - MIB-II
- RFC 1215 – Convention for defining traps for use with the SNMP
- RFC 1901 – Introduction to Community-based
- SNMPv2 (SNMPv2c).
- RFC 2011 – SNMPv2 Management Information Base for the Internet Protocol using SMIv2.
- RFC 2012 – SNMPv2 Management Information
- Base for the Transmission Control Protocol using SMIv2
- RFC 2013 – SNMPv2 Management Information
- Base for the User Datagram Protocol using SMIv2
- RFC 2578 – Structure of Management Information Version 2 (SMIv2)
- RFC 2579 – Textual Conventions for SMIv2
- 2580 Conformance Statements for SMIv2
- RFC 2863 – The Interfaces Group MIB
- RFC 3416 – Version 2 of the Protocol
- Operations for the Simple Network Management Protocol (SNMP)
- RFC 3417 – Transport Mappings for the Simple Network Management Protocol (SNMP)
- RFC 3418 – Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC 959 – File Transfer Protocol (FTP)
- RFC 2660 – The Secure HyperText Transfer Protocol (HTTPS)
- RFC 2030 Simple Network Time Protocol v4
- RFC 1191 – Path MTU Discovery
- Internet Draft - Secure Shell v2 (SSHv2)
- Internet Draft - EAP-TTLS
- Internet Draft - EAP-PEAP
- Internet Draft - CAPWAP Tunneling Protocol (CTP)

IEEE Standards

- 802.11d - 802.11 Extensions to Operate in Additional Regulatory Domains
- 802.11h - Spectrum managed 802.11a (in 5 GHz band in Europe)
- 802.11i - WLAN security and provide better network access control
- 802.1x - Port based network access control
- 802.11e - MAC Enhancements for Quality of Service (future)
- 802.1aa - 802.1x maintenance
- 802.3af - DTE Power via MDI (Power over Ethernet)
- 802.3 - CSMA/CD (Ethernet)
- 802.3i - 10BASE-T
- 802.3u - 100BASE-T
- 802.3x - Full Duplex
- 802.3z - 1000BASE-X (Gigabit Ethernet)
- 802.1d - MAC bridges
- 802.11 MIB - Management information base for 802.11

Physical

Unit Dimensions (with secured plastic cover)
Length 54.4 cm (21.4 in)
Width 42.2 cm (17.0 in)
Height 8.9 cm (3.5 in) – 2U
Weight unpackaged 13.6 kg (30 lbs)

Packaging Specifications
Length 67.3 cm (26.5 in)
Width 58.7 cm (23.1 in)
Height 24.1 cm (9.5 in)
Weight 17.2 kg (38 lbs)
LEDs
- Status—3 colors (R,O,G)
- Activity—3 colors (R,O,G)

Storage & Transportation
- Temperature -40ºC to 70ºC (-40ºF to 158ºF)
- Relative Humidity 10 - 95% (Non-Condensing)
- Shock 10G, 6ms, 600 Shocks
- Random Vibration 5-20Hz @ 1.0 ASD W/-3dB/oct from 20-200Hz
- Drop at 39.4”, 14 drops, packaged

Mounting Requirements
- 2U Rack Mount Configuration fitting standard 19” rack
- Adjustable mounting ears (included) allow cabling at front, middle or rear of unit

General Specifications

Ports
- 2 1000BASE-SX ports (MTRJ connector) - Summit WM1000
- 4 10/100BASE-T ports – Summit WM100
- 1 10/100BASE-T management port
- 1 DB9 Serial console port

Primary Power Supply
- Voltage Range—90-264 VAC
- Frequency Range—43-63 Hz
- Max Input Current—6.0A @ 100 VAC
  —3.0A @ 240VAC
- In-rush Current—60/80A @ 115/240 VAC

Redundant Power Supply (Included)
- Hot-Swappable module
- Voltage Range—90-264 VAC
- Frequency Range —43-63 Hz
- Max Input Current—6.0A @ 100 VAC
  —3.0A @ 240VAC
- In-rush Current—60/80A @ 115/240 VAC

Input Power Cord
- 2 North American PS cords provided Input Power Cord outside of U.S.
- Country specific certifications required
- Input Socket - IEC 60320 C13
- Minimum Wire Size: 0.75mm^2 (18/3AWG) copper stranded minimum
- 10 ft max length

Operating Specifications

- Temperature 0ºC to 40ºC (32ºF to 104ºF)
- Relative Humidity 10 - 95% (Non-Condensing)
- Altitude 0 - 3000 meters (9,850 ft)
- Shock 3G, 11ms, 60 Shocks
- Sine Vibration 5-100-5 Hz @.2G, 0-peak, 1/10 Oct/min
- Random Vibration 3-500Hz 1.5Grms

Regulatory/Safety

Safety
- cULus per 60950-1:2003
- CB per IEC 60950-1:2001 with all available country deviations
- GS Mark per EN60950-1:2001
- 73/23/EEC Low Voltage Directive
- Laser Safety per EN60825-1:A2:2001
- FCC 21 CFR 1040.10 LN#50 7-01
- CDRH Letter of Approval

Emissions
North America EMC for ITE
- FCC CFR 47 part 15 Class A (USA)
- ICES-003 Class A (Canada)

European EMC standards
- EN 55022:2003 Class A
- EN 55024:1998 Class A includes IEC/EN 61000-4-2, 3, 4, 5, 6, 8, 11
- EN 61000-3-2,3 (Harmonics & Flicker)
- ETSI EN 300 386:2001 (EMC Telecommunications)
- EN60601-1-2 (Medical)
- 89/336/EEC EMC Directive

International EMC Certifications
- CISPR22:2003:A1:2004 Class A (International Emissions)
- CISPR 24:1997 Class A (International Immunity)
- IEC/EN 61000-4-2 Electrostatic Discharge
- IEC/EN 61000-4-3 Radiated Immunity
- IEC/EN 61000-4-4 Transient Burst
- IEC/EN 61000-4-5 Surge
- IEC/EN 61000-4-6 Conducted Immunity
- IEC/EN 61000-4-11 Power Dips & Interruptions

Technical Specifications

Country Specific
- VCCI Class A (Japan Emissions)
- AS/NZS 3548 ACA (Australia Emissions)
- CNS 13438:1997 Class A (BSMI-Taiwan)

Environmental
- EN/ETSI 300 019-2-1 v2.1.2 – Class 1.2 Storage
- EN/ETSI 300 019-2-2 v2.1.2 – Class 2.3 Transportation
- EN/ETSI 300 019-2-3 v2.1.2 – Class 3.1e Operational
- EN/ETSI 300 753 (1997-10) – Acoustic Noise
- ASTM D3580 Random Vibration Unpackaged 1.5G

Ordering Information

Part Number	Name	Description
15937	Summit WM1000 switch	Summit WM1000 Switch with 2X gigabit interfaces; supports 100 Altitude 350-2 APs. Includes AutoCell dynamic RF management, two 15942 PSUs, rack mount brackets, two U.S. power cords. Upgradeable to support 200 APs with 15941 upgrade.
15945	Summit WM100 switch	Summit WM100 Switch with 4X Fast Ethernet interfaces; supports 50 Altitude 350-2 APs. Includes two 15942 PSUs, rack mount brackets, two U.S. power cords. Upgradeable to AutoCell dynamic RF management with 15940 upgrade.
15938	Altitude 350-2 Integ. Ant. AP	Dual-radio Access Point capable of supporting 802.11a/b/g standards; requires Summit WM series switch for operation. Includes internal antennas and standard mounting bracket. Use 802.3af PoE or optional ext. Altitude 350-2 AC to DC 6V adapter.
15939	Altitude 350-2 Detach. Ant. AP	Dual-radio Access Point capable of supporting 802.11a/b/g standards; requires Summit WM series switch. Includes bracket and two 15931 “paddle” external antennas. Use 802.3af PoE or optional ext. Altitude 350-2 AC to DC 6V adapter. Two RP-SMA connectors.
15940	Summit WM100 AutoCell Software Upgrade	Enables AutoCell dynamic RF management capabilities for up to 50 Access Points on the Summit WM100 switch; requires Summit WM100 switch.
15941	Summit WM1000 Capacity Upgrade	Summit WM1000 capacity upgrade; supports 100 additional Altitude 350-2 APs (for a total of 200 APs); AutoCell dynamic RF management capabilities is included; requires Summit WM1000 switch

Accessories

15925	Altitude 350 AC PSU, NA	External Power Adapter for the Altitude 350, AC to 6 Volt DC, U.S./Canada only
15926	Altitude 350 AC PSU, EMEA	External Power Adapter for the Altitude 350, AC to 6 Volt DC, European Union
15928	Altitude 350 AC PSU, GBR	External Power Adapter for the Altitude 350, AC to 6 Volt DC, United Kingdom

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

Corporate Headquarters 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