

Summit® WM20 WLAN Controller



Summit WM20—The next generation wireless LAN controller platform for advanced wireless services.

Fast and Easy Deployment

- Plug-and-Play Access Points (APs)
- Dynamic Radio Management (DRM)
- Summit Wireless Mobility Access Domains (WM-AD)

Scalability for Future Proofing

- Investment protection for emerging technologies
- Extended Mobility Domain to support tens of thousands of users
- Cost effective distributed enterprise support

Enterprise-Grade Voice Solution

- High-speed, cross-subnet roaming
- End-to-end Quality of Service (QoS)
- Automatic power save mode to extend the battery life of handsets

Comprehensive Security Network-Wide

- Directory-integrated link security
- Multiple authentication and access control options
- Wireless intrusion detection
- Integration with security solutions from Extreme Networks®

High Availability

- Cost-effective controller redundancy
- Self-healing radio network

The Summit WM20 controller is ready to support advanced wireless applications.

Summit WM20 WLAN controller is ideal for branch and regional offices of large Enterprises as well as Small to Medium Enterprises (SME). Supporting up to 32 Access Points (APs), it complements the existing line of Summit WM200/2000 controllers. In today's enterprise environments, dedicated resources are rarely available to build and operate the wireless network. By focusing on the ease of installation and management, the Summit wireless mobility solution from Extreme Networks helps enable IT organizations to simplify the task of mobilizing their users without compromising security or performance.

Summit WM series controllers 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 controllers can meet nearly any mobile voice or multimedia networking challenge. The Summit WM series product line can scale to support the largest WLAN installations while providing centralized management for remote branch office installations.

Target Applications

- Support for high-performance application such as Voice over WLAN (VoWLAN)
- SME and branch/regional office locations with centralized support
- Guest access applications



Fast and Easy Deployment

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

Plug-and-Play

Out-of-the-box AP installation is a breeze. Using AccessAdapt™ technology, Altitude™ APs automatically discover the Summit WM controller 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 incorporates easily with 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 controllers communicate using IP, designers have the option of not needing to configure network-wide VLANs when installing the wireless network. If desired, however, VLANs can be used for traffic between the APs and the controller as well as from the controller into the switching network.

Dynamic Radio Management (DRM)

Summit WM series controllers simplify setup and operation through their extensive DRM capabilities. DRM

automatically optimizes radio frequency 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 DRM, calibration and adjustment automatically occur 24 hours a day, eliminating the need to manually set or tune power levels as conditions change. In addition, should an AP fail, DRM provides fault tolerance by detecting the failure and compensating by increasing output power of the neighboring APs.

DRM 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. DRM is stable and does not “flap” during operation—meaning the WLAN remains available and reliable even when radio frequency conditions are changing.

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 VoWLAN handsets, and a third for secure employee access (see Figure 1).

After the administrator has defined Access Domains for the different types of users, each Access Domain is assigned to one or more Altitude 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.

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.

For customers looking for increased operational efficiencies, Extreme Networks offers its EPICenter® network management platform for managing Summit WM systems as well as Extreme Networks stackable and modular switching products. With EPICenter, administrators can discover and view Extreme’s network products, receive traps and alarms, view topology and inventory, and generate comprehensive reports.

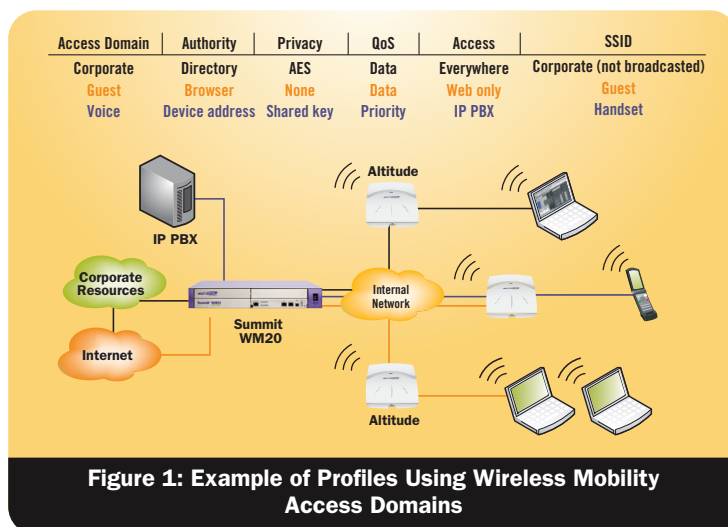


Figure 1: Example of Profiles Using Wireless Mobility Access Domains

Scalability for Future Proofing

Summit WM20 offers scalability in capacity and performance and helps protect user investment against early obsolescence.

Cost-Effective Distributed Enterprise Support

Branch Office Mode capability enables one or more standard Altitude APs to be installed in remote sites and across the WAN without a local controller. These APs download their configuration from the central Summit WM controller and then operate independently at the local site. This provides a number of advantages, the first being capital cost savings. There is no need for a controller at every remote site. There are also operational savings since an administrator can manage all the Branch Office APs from a central controller. Thirdly, the Branch Office Mode used at remote and branch office locations enables the remote AP to bridge traffic to a local VLAN at the remote site, rather than tunneling it all back across a slow WAN link. This provides better performance to the branch office user, offloading the central controller and also reducing bandwidth demands on the WAN link. Finally, Branch Office Mode provides survivability—users at the branch can continue to operate, even if the WAN is intermittent or fails. With such scalable architecture, enterprises can deploy wireless in hundreds and even thousands of branch offices. Figure 2 shows Branch Office Mode deployment.

Summit WM system supports Wireless Distribution System (WDS) that enables wireless bridging and backhaul for deployment of untethered outdoor APs.

Investment Protection for Emerging Technologies

Summit WM20 offers the broadest range of AP support in its class. It can be economically deployed at a branch office of a large enterprise or at an SME with scalability to support up to 32 APs without having to fork lift upgrade the controller. Summit WM20 is “802.11n Ready” which is the emerging high speed WLAN radio technology.

Extended Mobility Domain

The Mobility Domain, which is a powerful Summit WM architectural capability, defines a domain within which users can roam and enable seamless session mobility. Mobility Domain is a cluster of Summit WM controllers and attached APs that share a distributed database for client, RF and security key management. This enables session mobility with fast handoffs for wireless users and devices across Layer 2 and Layer 3 networks. Up to 12 controllers can be configured into a single roaming domain, enabling up to tens of thousands of users to transparently roam across up to

2,400 APs. This allows an enterprise customer to confidently deploy a secure and robust wireless network across a large multi-building and multi-site campus.

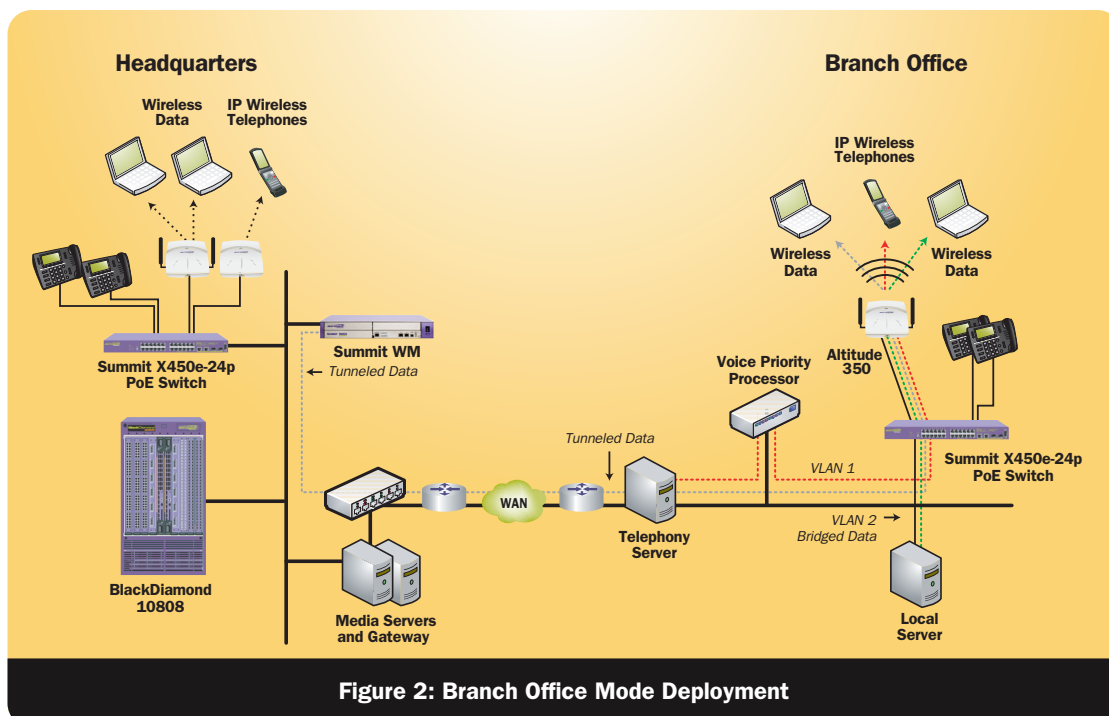


Figure 2: Branch Office Mode Deployment

Enterprise-Grade Voice Solution

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 controllers deliver outstanding performance for advanced, latency-sensitive applications such as VoWLAN.

High-Speed Cross Subnet Roaming

Summit WM series controllers 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 easily added to existing networks without configuration changes, topology modifications or client software.

Summit WM series controllers are capable of taking advantage of 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—Summit WM series controllers generate a unique key only for the APs to which the client is likely to roam. The Summit WM system supports PMK caching and Opportunistic Key caching schemes to enable faster roaming.

End-to-end Mobile QoS

QoS is critical, especially for VoWLAN or high-priority users. Summit WM controllers' 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.

The wireless QoS solution from Extreme Networks 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 (WMM) priority management. Summit WM controllers map the wireless QoS to wired Layer 2 (802.1p) and Layer 3 (DSCP) QoS markings for upstream and downstream traffic. In addition, Summit WM20 supports priority queuing on the egress ports, based on the traffic stream priority. This way WM-ADs with mixed traffic (such as voice and data) can prioritize voice over the other traffic. It also provides enforcement of traffic priority across the wired and wireless networks. Figure 3 shows end-to-end QoS priority.

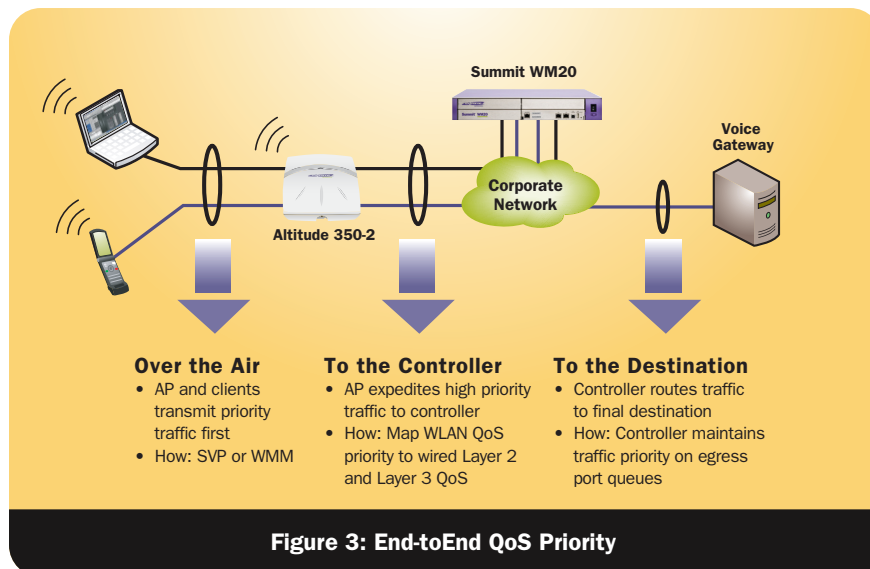
Summit WM WLAN solution supports Call Admission Control (CAC) as per IEEE 802.11e based Traffic Specifications (TSPEC). CAC is a traffic management technique that regulates the number of calls for better roaming. A client can request a new voice session with specific traffic stream parameters including QoS. These parameters are part of the TSPEC associated with a session request. Summit WM can accept or reject the session request based on the availability of

network resources to deliver the requested level of service. It also prevents oversubscription of network resources that can result in service degradation and poor voice quality. It prevents resources from being oversubscribed in a way that impairs QoS.

In addition to CAC, Summit WM offers QoS Basis Service Set (QBSS)-based intelligent roaming to enable clients to make informed decisions during roaming, based on the loading factor of an AP. The QBSS load is an indicator in the Information Element that represents the percentage of time that the channel is in use by the AP. A low QBSS means that an AP is not heavily utilized. A QoS enabled client will select an appropriate lightly loaded AP before beginning the TSPEC negotiation.

Automatic Power Save Mode to Extend Handset Battery Life

To maximize battery life on handheld devices like a VoWLAN or dual-mode handsets, Summit WM has implemented a standards-based (802.11e) Unscheduled Automatic Power Save Delivery (U-APSD) mechanism. During a session, a U-APSD enabled client can go into periodic sleep mode to save battery power. During this sleep period, the AP queues up the packets for the destined client. On wakeup, the client triggers a request to the AP to deliver the queued up packets.



Comprehensive Security Network-Wide

Security is justifiably a key concern for WLAN systems. Summit WM series controllers 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. Figure 4 provides some examples of link security options.

Summit WM series controllers offer a complete range of privacy options ranging from unencrypted communication for guests, shared key for phones and PDAs, to WPA and WPA2. 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 controller offers unique and powerful enhancements to basic network access control. Using information exchanged between the Summit WM controller and the RADIUS server, administrators can design sophisticated access control solutions that tailor access rights to specific locations, users or roles. Summit WM, for example, supports Layer 3 filtering of IP addresses and Layer 4 filtering by port number or type of traffic (TCP/UDP). 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.

The Summit WM solution provides additional level of security by registering only those APs that have been authenticated using 802.1X authentication protocol.

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 APs that are used for wireless connectivity support (see Figure 5). If a rogue device/network is found, it is reported on the management console

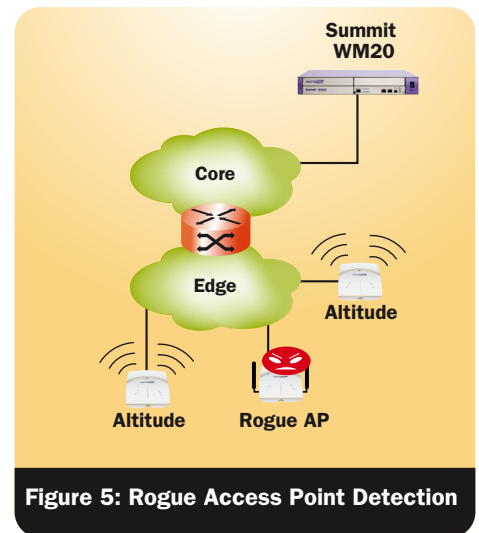


Figure 5: Rogue Access Point Detection

Integration Security Solutions from Extreme Networks

In addition to strong wireless link security, Summit WM can be installed in conjunction with Extreme Networks switching and/or security products to offer more comprehensive security capabilities. For example, ExtremeXOS®-based switches from Extreme Networks offer many complementary Layer 1 – 3 security features in the areas of MAC address security, Network Login, host integrity checking, Denial of Service attack mitigation, IP address security, IP Telephony security, Layer 3 virtual switching for internal firewalls, and secure routing.

Extreme Networks also has network security products that interoperate with Summit WM to provide wireless—in addition to wired—security enforcement. One example is the Sentriant® AG endpoint integrity checking solution. Sentriant AG can be installed with Summit WM to enforce endpoint integrity check before allowing access to the network.

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 SPA-PSK	Guest	None	Factory Floor	Application Network
Corporate Access Sensitive Users and Applications	EAP-TTLS, EAP-TLS, PEAP, EAP-MD5	Up to WPAv2 with AES	Guest	None	Anywhere	By User

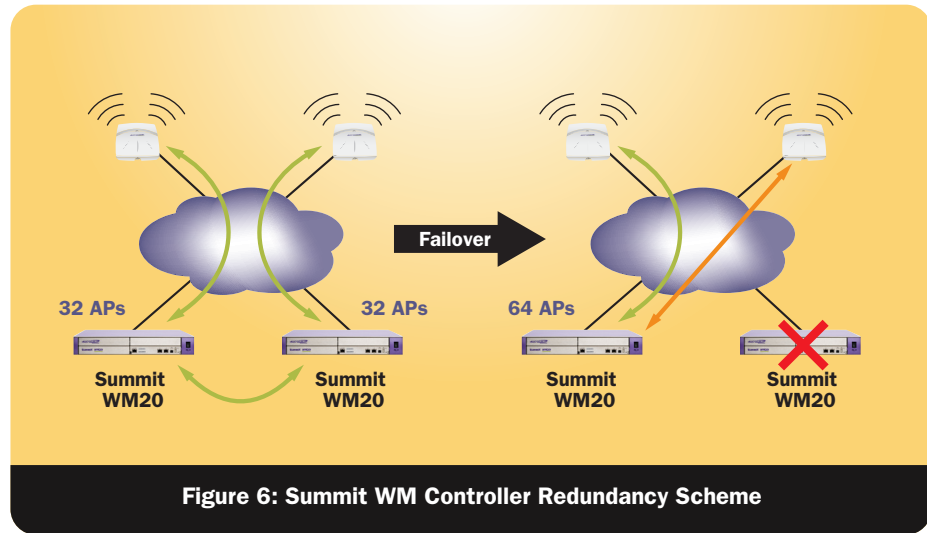
Figure 4: Three Examples of Link Security

High Availability

With increased access to mission critical applications, enterprise users expect wireless service reliability to be at the same level they have experienced with wired access. All aspects of the Summit WM solution provide enterprise-grade high availability.

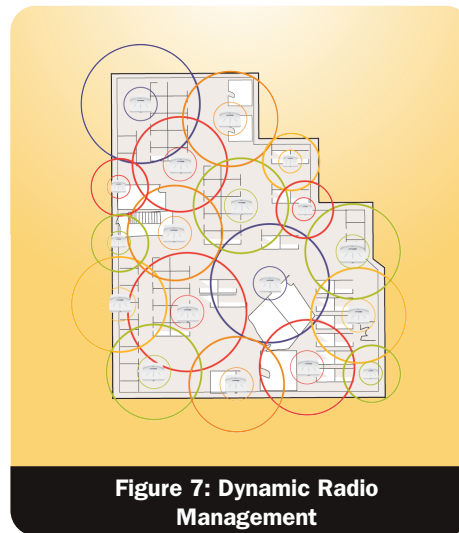
Cost-effective Controller Redundancy

Summit WM controllers can operate in a load sharing redundant mode that enables both the primary and backup controllers to be actively servicing traffic during normal operation. Controllers are paired so each can assume the load of the other during a failure. Should either controller fail, its Altitude APs connect to the backup controller (see Figure 6) without the need for additional AP licenses that competing solutions require. In a failover situation a controller can support up to double the number of APs. So for example, a Summit WM20 can support an additional 32 APs in a failover situation, for a total of 64 APs.



Self-healing Radio Network

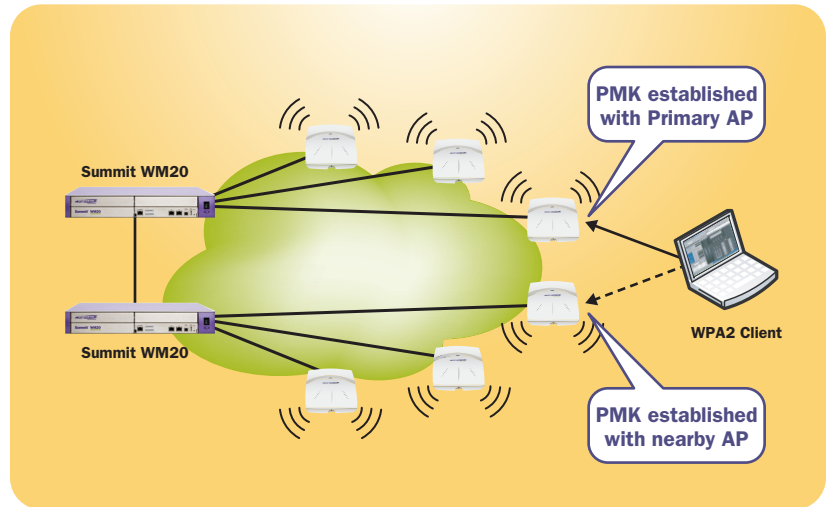
Summit WM offers self healing capability for the radio network. At the radio level, DRM will detect AP failures and boost the power output of the neighboring APs to compensate for the gap in coverage (see Figure 7). This eliminates middle of the night support calls when an AP fails.



Target Applications

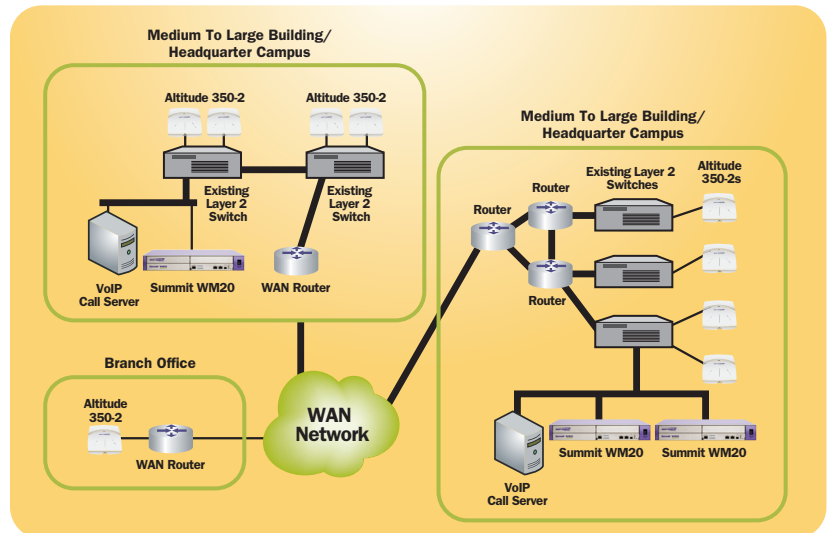
Support for High-Performance Applications Such as Voice over WLAN

Summit WM series controllers 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. Summit WM has Pairwise Master Key (PMK) caching which allows the roaming client to pre-authenticate with nearby APs. This is ideal for voice handsets or roaming applications such as a wireless device mounted on a warehouse forklift.



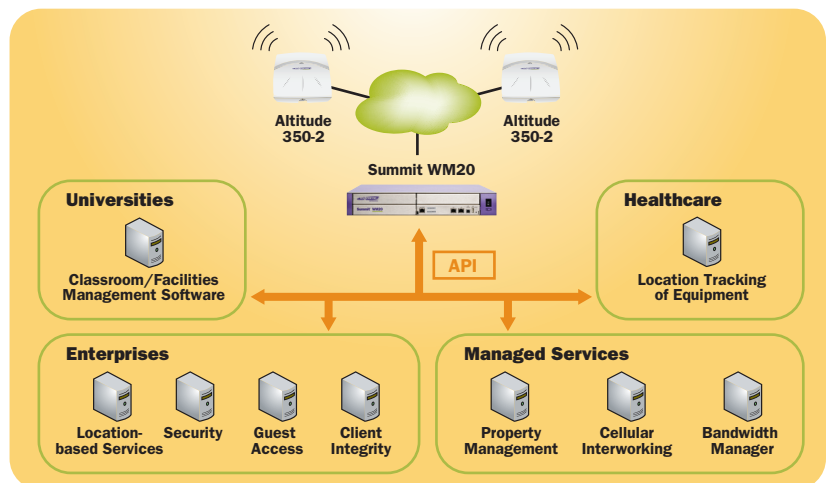
Deployments Requiring Distributed Wireless Connectivity with Plug-and-Play Installation and Centralized Support

Summit wireless mobility is ideal for multi-site enterprise deployments with a centralized Summit WM controller 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 controller. 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 controller.



Guest Access Applications

The Internal Captive Portal feature of the Summit WM controller allows for an optional authentication scheme. A simple configurable login web page is offered to the client upon association. The Summit WM controller also provides an API for integration with external third-party Guest Access applications. These applications can be customized for various sectors including universities, enterprises, healthcare and managed services.



Technical Specifications

Scalability and Performance

Maximum number of managed access points

- 32 in Normal mode
- 64 in Failover mode

Maximum number of users per controller: 512

Maximum number of Access Domains: 8

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 791 – IPv4
- RFC 1812 – Minimum Router Requirements
- RFC 793 – Transport Control Protocol (TCP)
RFC 768 – User Datagram Protocol (UDP)
- RFC 792 – Internet 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
- RFC 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 SNMP
- RFC 959 – File Transfer Protocol (FTP)
- RFC 2660 – The Secure HyperText Transfer Protocol (HTTPS)
- RFC 2474 – Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- RFC 2030 – Simple Network Time Protocol v4
- RFC 1191 – Path MTU Discovery
- RFC 3576 – Dynamic Authorization Extensions to RADIUS
- Internet Draft – Secure Shell v2 (SSHv2)
- Internet Draft – EAP-TTLS
- Internet Draft – EAP-PEAP
- Internet Draft – CAPWAP Tunneling Protocol (CTP)

IEEE Standards

- 802.1D – MAC bridges
- 802.1Q – Virtual LANs
- 802.1X – Port based network access control
- 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)
- 802.11a – Specifications for WLAN in 5GHz band
- 802.11b – Specifications for WLAN in 2.4GHz band
- 802.11g – Specifications for WLAN in 2.4GHz band
- 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 – MAC extensions for enhance security and authentication mechanisms
- 802.11e – MAC extensions for enhanced Quality of Service
- 802.11 MIB – Management information base for 802.11

Physical

Unit Dimensions

Length 36.5 cm (14.4 in)
Width 44 cm (17.3 in)
Height 6.8 cm (2.7 in) – 1.5U
Weight 7.2 kg (15.9 lbs)

Packaging Specifications

Length 53.5 cm (21.1 in)
Width 53.5 cm (21.1 in)
Height 18.5 cm (7.3 in)
Weight 10.4 kg (22.9 lbs)

LEDs: 4

- Activity
- Status
- HDD status
- Hot swap

Storage & Transportation

- Temperature -40° C to 70° C (-40° F to 158° F)
- Relative Humidity 10 – 93% (Non-Condensing)
- Shock* 180 m/s² (18g), 6ms
- Random Vibration* 5 – 20 Hz @ 1.0 ASD w/-3dB/oct. from 20 – 200 Hz
- Sinusoidal Vibration* 5 – 62Hz @ Velocity 5mm/s, 62 – 200 Hz @ .2G
- Drop* at 39.5" (100cm)

Mounting Requirements

- 1.5U Rack Mount Configuration fitting standard 19" rack
- I/O cabling at front of unit; power cabling on back

* Short term test condition

General Specifications

Management Ports

- 1x 10/100/1000 BASE-T Ethernet
 - 1x USB Control port as console port
- Require USB A/B cable and USB/Serial software driver

Data Ports

- 2x 10/100/1000 BASE-T Ethernet

Power Supply

- Nominal Input: 100 – 240V, 1A
- Voltage Range: 90 – 264V~
- Frequency Range: 47 – 63 Hz
- Power (max): 250 Watts
- Input Connector: IEC 60320 C14
- Heat (max): 850 BTU/hr
- In-rush Current Limit: 40A

Input Power Cord

- 1 North American Power cord provided
- Power cord outside of N.A. – Country specific certifications required
- Power Supply Input Socket IEC 320 C14
- Power Cord Input Plug IEC 320 C13
- Power Cord Wall Plug Country Specific
- Minimum Wire Size / Cord Set 18 AWG (.82mm²) copper stranded / 15ft (5m)

Operating Specifications

- Temperature 0° C to 40° C (32° F to 104° F)
- Relative Humidity 10 – 90% (Non-Condensing)
- Altitude 0 – 3000 meters (9,850 ft)
- Shock* (Rack Mounted) 30 m/s² (3g), 11ms
- Acoustic Noise 36.4 dBA Sound Power per ISO 7779

- 5.0 belsA Declared Sound Power per ISO 9296

* Short term test condition

Safety Standards

North American Safety of ITE

- UL 60950-1:2003 1st Ed., Listed Device (U.S.)
- cUL per CSA 22.2#60950-1-03 1st Ed. (Canada)

European Safety of ITE

- EN60950-1:2001+A11
- GS Mark TUV-R
- 73/23/EEC Low Voltage Directive

International Safety of ITE

- CB Report & Certificate per IEC 60950-1:2001+ Country Deviations
- ANATEL Resolution 238 (Brazil)
- NOM/NYCE (Mexico)

