

Design Guide for Pervasive Wireless Networks

This document describes how to design and install a pervasive wireless network based on the Meru Networks Wireless LAN (WLAN) System.

A pervasive wireless network is defined as one that is intended to provide wireless coverage with voice over IP and data application support over all or a significant portion of a building or campus, entailing tens if not hundreds of IEEE 802.11 access points. The number of users may reach the thousands, with areas such as conference rooms or auditoriums experiencing very high densities of users. Multiple types of users (i.e. employees, guests, contractors) must be supported with appropriate levels of security for each group.

Meru Wireless LAN System Overview

While others have created WLAN switch architectures, they focus primarily on ease of deployment and central management of AP configuration parameters. Solving this problem is both important and necessary, but it is not enough. The key challenge in a pervasive wireless LAN deployment is managing contention, interference and Quality of Service in a dense Wi-Fi environment. Meru has done just that with its WLAN System.

Meru Wireless LAN Controller

The Meru Wireless LAN Controller provides centralized management and control of Meru Access Points. Meru Wireless LAN Controllers intelligently manage the RF spectrum to deliver a wireless LAN network that is as reliable as the wired network. Intelligent management of client access ensures the highest performance for dense voice and data applications, delivering a true converged voice and data WLAN network.



- Simple deployment with E(z)RF for fast, simple WLAN configuration without complex channel planning
- Centralized configuration and management
- Multi-layer security approach
- RF aware with self-healing properties in event of interference or reconfiguration
- Integrates easily with existing infrastructure including firewall and intrusion prevention solutions

Meru Access Points

Meru Access Points provide leading Wi-Fi performance for 802.11b, 802.11g and 802.11a clients. Deployed wherever Wi-Fi coverage is required, they work in conjunction with Meru Controllers to deliver the highest toll quality voice over Wi-Fi service, excellent data client performance, self-healing and rogue access point prevention.



- E(z)RF installation and self-healing
- Toll quality voice over Wi-Fi with zero handoff between access points
- Ten-fold increase in client density
- Automatic AP discovery, configuration and RF channel and power assignment
- Intelligent load balancing
- Dramatically improved 802.11g performance in mixed 802.11b environments

Meru Radio Switch

The Meru Radio Switch provides up to twelve simultaneous AP channels from a single device. Based on multiple high performance 802.11a/b/g radios with a patent-pending omni-directional antenna, a single Radio Switch *simultaneously* delivers up to twelve Wi-Fi channels. For sites where multiple Radio Switches are required to provide more pervasive high-density 802.11 coverage, the Meru Controller provides a single interface for WLAN management, security, and Quality of Service.



- Configure any combination of three 802.11b/g and twelve 802.11a channels from a single device
- Create blankets of high capacity coverage with multiple Radio Switches
- Automatic load balancing of clients among channels
- Deliver performance levels near Ethernet
- Perfect for branch or remote offices

Planning the Pervasive Wireless LAN

Site Survey

Site surveys are typically performed for two reasons:

- 1) To ensure complete RF coverage of the desired area at a specified data rate

- 2) To minimize channel overlap which will cause interference and degrade wireless LAN performance

For a Meru wireless LAN, this traditional site survey method is not necessary, saving significant time, resources and money. The next two sections discuss the traditional method and how Meru's patented Air Traffic Control technology and virtual cell capability allows Meru APs to be quickly and easily deployed.

Access Point Spacing

Access points transmit at multiple data rates, with the rate decreasing as the client distance from the access point increases.

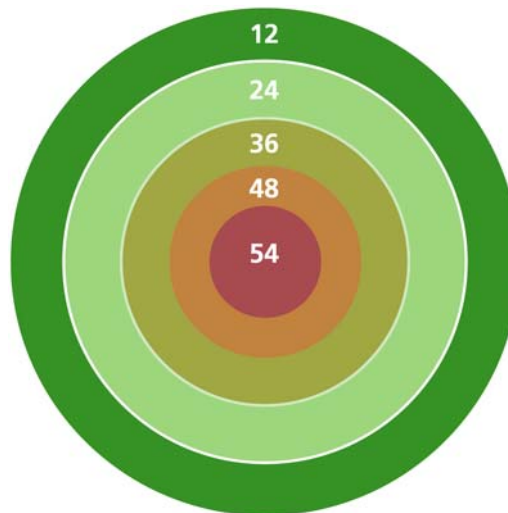


Figure 1: 802.11 data rate decreases with distance from the Access Point

Maintaining a desired overall data rate (i.e. 24 Mbps) throughout the coverage area is dependent upon both the spacing of the access points as well as the access point data rate setting. The traditional method for determining the spacing is to physically place an access point in one area and then using the wireless client, walk away from the access point until the desired lowest data rate is just lost. Measuring the distance away from the access point gives an approximate radius at that particular data rate. The access point is replaced, and the process is repeated. This ensures complete coverage, but is extremely time consuming.

An alternate method, Meru recommends spacing the access points at approximately 60' intervals to provide comprehensive coverage and high throughput. After initial deployment, any coverage holes can be addressed by adding an access point in that specific area. For other systems, adding an access point requires a complete new channel plan, reconfiguring the entire AP network. Because Meru's Air Traffic Control™ (ATC) technology eliminates the need for complex channel planning, this method is much less time consuming and the relative costs of a few additional access points more than outweigh the time involved to do a comprehensive site survey for a large campus with multiple multi-story buildings using a system that lacks ATC technology.

Channel Planning

Traditional WLANs require a second portion to the site survey process, which is a particularly onerous one particularly in the 2.4 GHz band where there are only three non-overlapping channels. With only three channels, a pervasive WLAN deployment is quite challenging to implement as the co-channel interference from the many access points causes performance degradation. Significant effort is usually spent plotting or measuring RF coverage of each access point to minimize channel overlap. This is further aggravated with a pervasive wireless LAN deployment as access point spacing is typically minimized to support higher densities of users. Decreased access point spacing creates more overlap between access points on the same channel. In addition, for wireless VOIP deployments, the decreased access point spacing will increase handoffs between APs. Unless there is zero handoff technology in the wireless LAN system, voice quality will suffer greatly.

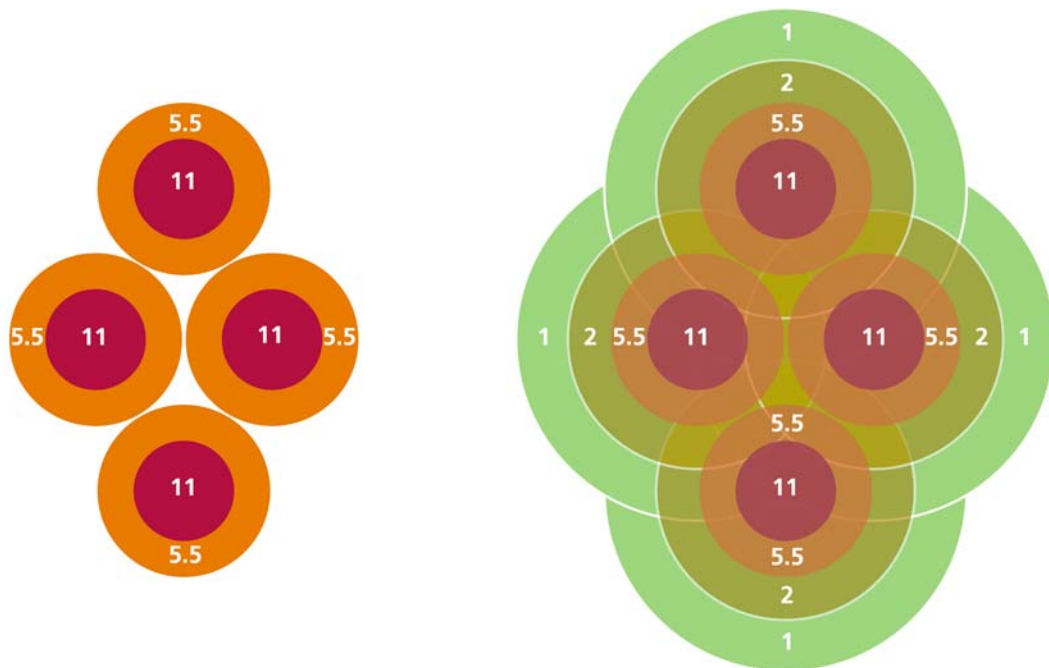


Figure 2: With a denser deployment of access points, significant overlap of channels occurs, necessitating complex planning to mitigate co-channel interference.

Meru's Wireless LAN System eliminates channel planning through creation of a Virtual Cell. With virtual cell mode, all access points are set to the same channel, thus eliminating the need for channel planning. And Virtual Cell automatically assigns the BSSIDs for each AP, so no manual configuration is needed. Issues with co-channel interference are eliminated through Air Traffic Control™ (ATC) technology. ATC deterministically schedules client access to the medium both within a single access point cell as well as across multiple cells, thus mitigating contention and the ensuing performance degradation. And, because the Meru Wireless LAN System employs zero handoff technology, voice calls roam seamlessly among access points, no matter the spacing, ensuring toll quality.

For increased capacity, multiple virtual cells can be 'painted' over the same area. With three independent channels in the 2.4 GHz spectrum, up to three times the capacity can be created in a single area.

Access Point Data Rate and Mode Setting

It is recommended that a high, or highest, data rate available from the access point be set rather than using the defaults which allow the access point to transmit all the way down to the lower rate. I.e. in an 802.11b only network, setting the access point to only transmit at 11 and 5.5 Mbps and not transmit at 2 and 1 Mbps. There are several reasons for this including:

- Broadcast and multicast packets are sent at the lowest data rate to ensure that all clients can see them. This reduces the throughput of the WLAN as all traffic stops until these frames are processed.
- Clients farther away from the access point will transmit at slower data rates, decreasing overall WLAN throughput as the slower rates are serviced.

Data rate setting requirements can also vary by client type. Meru uniquely compensates for this by allowing data rate setting per ESSID. This allows each client type to be supported in an optimum way, without suffering the 'lowest common denominator' problem.

The access point mode must also be set. Meru Access Points support 802.11a, 802.11b only, 802.11g only and 802.11b/g. Meru recommends that most deployments should be configured for a mixed 802.11b and 802.11g environment due to high likelihood that 802.11b clients will be present and to support voice clients, which are 802.11b based. Even in a completely new deployment where the clients are all 802.11g, it is advisable that the system be set for 802.11b/g mode due to the presence of neighboring 802.11b networks. If there are neighboring 802.11b networks, the 802.11g clients and APs must be able to signal to the 802.11b network using RTS/CTS that they are present to ensure that high throughput for the 802.11g network is maintained.

In addition, the Meru WLAN system is also intelligent enough to disable CTS temporarily if no 802.11b transmissions are heard after a period of time, allowing an 802.11g network to operate at its peak performance level. If 802.11b traffic does become present at a later time, the system will automatically revert to using CTS. CTS is used to prevent the 802.11b clients from transmitting during an active 802.11g transmission since the 802.11b client adapters cannot decode/understand 802.11g frames.

Meru Dual-Speed 802.11b/g Technology

In 802.11b/g mode, most wireless LANs penalize the faster 802.11g clients due to having to take much more time to transmit to the slower 802.11b clients. The Meru WLAN System uniquely solves this problem with dual speed mode. Dual speed mode is the default for Meru Access Points and is based on fair time on the channel, not fair access for 802.11b and 802.11g clients. In this mode, 802.11g clients perform up to five times faster than in standard wireless LAN systems.

Implementing Security

Wireless LAN security should be an extension of wired network security policies. Within the wireless LAN network, there are multiple levels of security that can be implemented, depending upon network infrastructure and client type.

WPA and WPA2/IEEE 802.11i

WPA and WPA2 provide the highest levels of security through strong over-the-air encryption and mutual authentication between the client and the network infrastructure. The original IEEE 802.11 security method, WEP, provided no user authentication and was proved to be quite weak as an encryption method. Wi-Fi Protected Access (WPA) user authentication is implemented using 802.1X and the Extensible Authentication Protocol (EAP). Together, these technologies provide a framework for strong user authentication. This framework utilizes a central authentication server, which employs mutual authentication so that the wireless user does not accidentally join a rogue network.

WPA is an interoperability certification granted by the Wi-Fi Alliance to a vendor's equipment based on successfully passing a series of interoperability tests. WPA uses TKIP for the encryption method and IEEE 802.1x for mutual authentication. WPA2 is based on the IEEE 802.11i standard and is a recent Wi-Fi Alliance certification. WPA2 increases over-the-air security by using AES, a stronger form of encryption, however, WPA has never been cracked. WPA has some advantages for legacy 802.11b deployments in that some vendors 802.11b infrastructure was upgradeable to WPA.

For both WPA and WPA2, a RADIUS server is required to provide authentication services. The RADIUS server must support WPA or WPA2. Currently a variety of vendors provide WPA or WPA2-compatible RADIUS servers including Funk Software and Meetinghouse. An EAP type must also be selected. Several EAP methods are available including EAP-TLS, EAP-TTLS and EAP-PEAP. All of these EAP methods are open and not proprietary. EAP-TLS requires a certificate on both the client and the network infrastructure, making management and support more burdensome. Both EAP-TTLS and EAP-PEAP eliminate the need for a certificate on the client and rely on username/password. For PEAP, the inner authentication protocol can include one of MS-CHAPv2 (username/password), EAP-GTC (Generic Token Card) or EAP-SIM (Subscriber Identification Module). Support for TTLS and PEAP varies with operating system and will largely depend upon your mix of clients.

Meru Networks Wireless LAN System supports the stringent security requirements and is WPA Certified™ by the Wi-Fi Alliance. Meru Access Points are transparent to EAP type and fully support EAP-TLS, EAP-TTLS and EAP-PEAP.

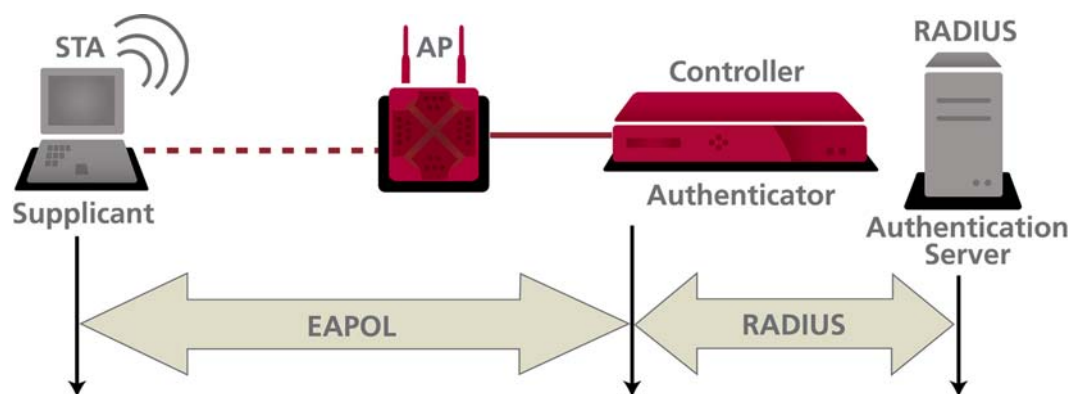


Figure 3: The Meru Wireless LAN System supports WPA for the most stringent enterprise security.

WEP, MAC Address Control Lists and VPNs

Certain types of specialized business devices (i.e. printers, bar code scanners, Point of Sale terminals, voice clients etc) may not support WPA or WPA2. Securing these types of devices is possible, but requires different methods. If the device is capable of supporting a VPN, this is the best choice. VPNs provided similar security levels to WPA and WPA2, however will potentially require additional infrastructure and administration. A VPN server will be required along with VPN software on each client device. Each client device must be configured to communicate with the VPN server. Some wireless LANs experience difficulty supporting VPN security when the clients roam, as the handoff between the access points may terminate the connection. This causes the user to have to re-authentication to reestablish a tunnel. This is annoying at best, and may be unusable for certain applications or work flows. With the Meru Wireless LAN System, zero handoff eliminates this problem as IP connectivity is maintained during roaming, thus ensuring that the VPN session stays active.

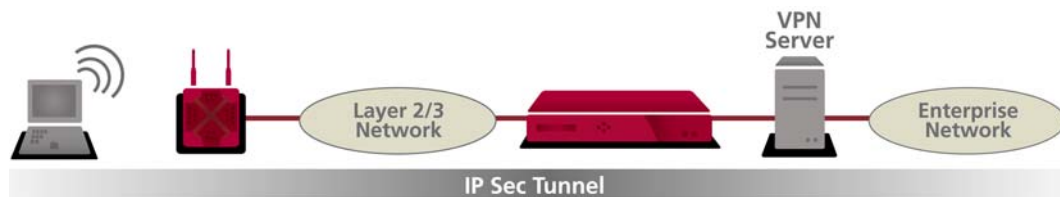


Figure 4: Clients that cannot support WPA security can be secured through a VPN. Meru seamlessly supports VPN overlays and ensures no loss of connectivity when IPSec clients roam with zero handoff.

However, many specialized devices may not support a VPN either. In this case, a combination of WEP and MAC Address Control Lists can provide a meaningful security level. Some encryption level is better than nothing at all. And, security can be increased by rotating the WEP key at regular intervals. In addition, the access points can be configured to only accept users with specific MAC address lists. In this case, if someone were to determine the WEP code, they may still be blocked from accessing the network due to an unauthorized MAC address.

Meru Networks Wireless LAN system supports 40, 64 and 128 bit WEP as well as MAC Address Control lists. MAC address filtering can be done locally using the Controller database, or via a RADIUS server. VPNs can be overlaid on the Meru Wireless LAN infrastructure with seamless support for client roaming.

Restricting Network Resource Access with Virtual LANs

In addition to the above methods, the use of virtual local area networks (VLANs) can significantly enhance network security. VLANs allow multiple clients to be grouped within the same broadcast domain regardless of physical location. This concept can be extended to the wireless LAN as well. Based on SSID, the access point can segment traffic to different VLAN ports. Further more, security settings can vary by SSID. The table below provides an example within an enterprise where full time employees, contractors, legacy business devices and guests all use the same infrastructure.

User Type	SSID	VLAN Port	Security Method
Full time employee	Company	20	WPA
Contractor	PartTime	30	WPA
Legacy Business Device	Voice	40	WEP, MAC Address Control List
Guests	Guest	50	Open Authentication/ No security

Meru Access Points support up to 64 separate SSIDs each with a different security configuration. Each SSID can be mapped to a specific VLAN port, providing enhanced security by restricting network resources based on user type and application. VLANs only need to be configured on the Ethernet port the controller connects to, eliminating time consuming configuration of the switches that the access points are connected to.

Guest Access through a Captive Portal

Many enterprises now wish to accommodate guests and partners desire to access email or other corporate network services. To do so securely requires that the corporate network not be accessed and that complicated security procedures be avoided (i.e. providing each guest with a temporary encryption key). A VLAN can be set up to direct users of the 'Guest' SSID to a separate VLAN port providing access only to the Internet. To audit the use of this network, the Meru Wireless LAN system supports a Captive Portal function. Any guest that opens their browser will automatically be redirected to a secure SLL-based login page before being allowed access to the Internet. The interface of the login page can be customized by the enterprise. This allows the enterprise to audit use and provides an authentication method which universally works without requiring configuration of the wireless security settings to match the corporate network.

Preventing Rogue Access Points

Rogue access points are a serious threat to enterprise security. Rogue access points are typically low cost, consumer-grade APs brought in by employees. Typically, no security is enabled when they are attached to the network. Once behind the firewall, they leave the enterprise network open to loss of confidential data or malicious hacking if an unauthorized client within range of the AP's is able to connect.

The Meru Wireless LAN System proactively searches and prevents rogue access points. Through scanning of all 2.4 and 5 GHz channels, the Meru Wireless LAN System can identify unknown and non-authorized access points, alerting IT administrators. A client attempting to associate with a rogue access point can be automatically blocked, preventing all access to the Enterprise network unless through an authorized access point. As this mitigation is over the air, rogue access points do not need to be connected to the same wired infrastructure as the Meru Access Points in order for the prevention to be effective.

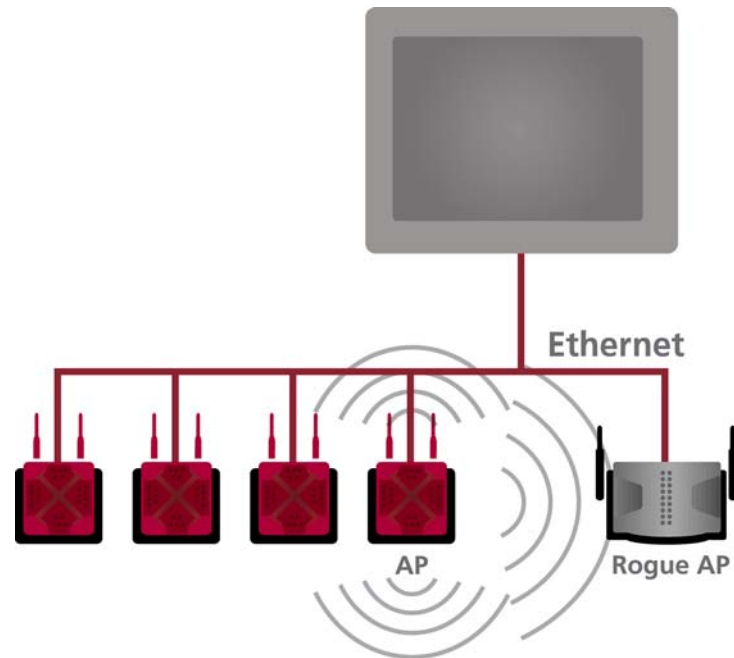


Figure 6: The Meru Wireless LAN System automatically scans all 2.4 and 5 GHz channels for rogue access points and automatically blocks all clients that try to connect, protecting enterprise network security.

Supporting Voice and Data Applications Simultaneously

Supporting voice applications adds complexity to the overall wireless LAN design and implementation. Voice traffic is jitter and latency sensitive, and when mixed with data traffic, requires Quality of Service settings to provide toll quality performance. Jitter and latency are common problems in wireless networks as 802.11 is a shared medium and unlike wired hubs, the transmitting devices cannot detect a collision until they complete their entire packet transmission. This is quite different from wired networks where collisions can be detected shortly after starting transmission. Quality of Service classification is available on the wireline network through IEEE 802.1q via 802.11p and DiffServ. Only recently has a new standard been adopted that translates wired Quality of Service settings to the wireless medium.

WMM Quality of Service (or IEEE 802.11e EDCF) provides prioritization based on traffic classification from the wireless LAN access point to the client as well as from the client to the access point. The IEEE 802.11e standard provides for four levels of quality of service: voice, video, best effort data traffic and best effort background traffic. This provides prioritized channel access on the upstream direction however does not scale up with large numbers of WMM voice clients. WMM essentially shortens back off times to give certain clients priority. By shortening the back off time, the belief is that if there is a collision between a voice client and a data client, it will get access to the channel sooner than the data client, enabling it to meet delay and latency requirements for good quality voice. However, in a high-density voice deployment, the lower back offs actually *increase* the chance of a collision.

Therefore, with high numbers of active WMM voice flows, this will create contention that impacts voice quality. Voice clients will collide and back off, introducing latency and delay. Current norms

for acceptable voice over IP quality put a total one-way delay budget at 150 ms¹. Delay is caused by a variety of factors in the end-to-end system, including the codec, propagation through the network, queuing in routers and switches, the jitter buffer and congestion. Allowing for the other portions of the network, the wireless LAN can contribute approximately 15 ms of delay to the entire system. Additionally on the downstream direction, since the access point would fall into the same WMM priority with lower back offs for the voice flows it will be contending equally with all of the voice clients that are sending upstream traffic. And, furthermore WMM does not address collisions from clients in neighboring cells nor co-channel interference. All of this contention will increase delays from the wireless LAN beyond 15 ms, causing poor voice quality.

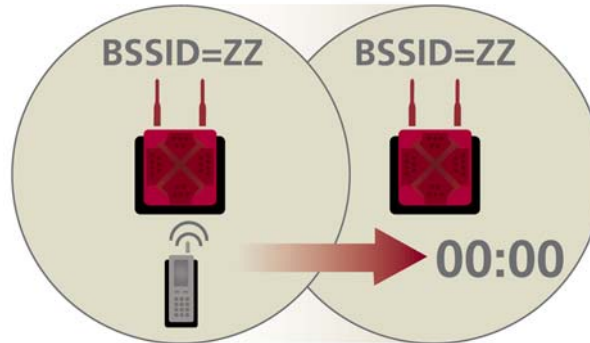
Handoffs among APs also impact voice quality. As voice applications are extremely latency sensitive, the long delays associated with disassociation and re-association to a new access point can severely degrade voice quality. Adding security to a voice device can increase handoff time. Several phones on the market today support IEEE 802.1X, providing much greater security than simply WEP. However, the longer re-authentication times and need for the access point to verify with the RADIUS server that the device is authenticated causes additional delay. This delay can lead to packet loss, and thus reduced voice quality, during handoff. Currently, no IEEE standard addresses the need for fast, secure roaming for latency sensitive devices like voice clients.

To address these issues, the Meru Wireless LAN System uses Air Traffic Control™ technology to manage client contention and create true upstream and downstream quality of service. The Meru Wireless LAN System automatically recognizes voice flows including H.323, SIP, Spectralink SVP, Cisco SCCP and Vocera ensuring high priority for these protocols. Prioritization is passed from the wireless side up to the wireline network through support of 802.1e via 802.1p and Diffserv. Air Traffic Control technology manages client access to the medium to reserve bandwidth over the air, ensuring high performance for high densities of voice and data clients. ATC also enables inter-cell coordination, a cellular coordination algorithm between APs analogous to the cellular telephone network's operation, to mitigate interference from clients in neighboring cells and co-channel interference.

Inter-cell coordination also eliminates handoffs by allowing all APs to be on the same channel and allowing the network to be in full control of the connection. With guaranteed zero handoff, voice clients will maintain toll quality while roaming among access points, including those that are on different IP subnets. Zero handoff is independent of security context, so even phones that use IEEE 802.1X will roam seamlessly without any call interruption. In addition, the Meru Wireless LAN System also supports Call Admission Control. This means that if the network resources upper limit has been reached, new calls are rejected with a busy tone instead of allowing the call to enter and reduce quality for all the voice users. This is a unique Meru Wireless LAN feature, and provides a similar user experience to wired telephony networks.

¹ ITU G.114

Virtual AP Architecture



Zero-handoff with no loss

Figure 5: Meru's cellular coordination enables zero hand-off ensuring toll quality wireless VoIP.

A Wireless LAN Case Study

The following is a typical large enterprise example. The enterprise has one headquarters office with 7 branch offices in Europe and Asia. Headquarters includes approximately 2000 employees with office space and light manufacturing. Branch offices range from 10 to 50 employees with office space only. Some of the branch offices are in office buildings where other wireless LANs may be in operation. The headquarters facility is a multi-story building.

Employees use laptops and in the light manufacturing areas some business specific devices such as barcode scanners and portable printers are used. Spectralink SVP phones are used in the light manufacturing areas as well. The enterprise expects to adopt wireless VOIP capability for office areas within the next 12 months.

The IT department is located at the headquarters site with the branch offices managed remotely. The network is IP based and has Quality of Service enabled. Remote employees access network resources through IPSec VPNs.

Customer Requirements

The customer requires that all applications supported on the wired network be supported on the wireless LAN network. In the corporate office, the wired network is not being replaced, but augmented with the wireless network as an extension. In the branch offices, the wireless network will be primary. Some of the smaller branch offices are expecting significant growth and are expected to change locations. Reducing complexity of adding new employees and anticipating the move is fueling the enterprise's desire for the speed and flexibility of a wireless network for the branch offices. Additional requirements are:

- Support for Windows 2000 and XP laptops
- Support for wireless barcode scanners, portable printers and Spectralink phones in manufacturing areas
- Support for wireless VOIP phones using SIP in the next 12 months
- Rogue AP mitigation

- Support for guest access at the headquarters location

Equipment Selection

As the headquarters desires wireless as an extension to the wired network, the Meru Wireless LAN Controller and Access Points are the appropriate devices. The Meru Access Points are dual radio and can provide 802.11b/g and 802.11a support.

For the branch offices where wireless will be the primary network, the Meru Radio Switch will deliver the high capacity wireless coverage needed. As the Meru Radio Switch is available in 4, 8 or 12 radio versions, each branch office can select a Radio Switch with an appropriate number of radios. The Radio Switches can be managed remotely from headquarters via the Meru WLAN Controllers used to manage the Meru Access Points.

Equipment Deployment

The headquarters site is approximately 2,000,000 square feet. Branch offices range from 25,000 to 100,000 square feet. Instead of a detailed site survey, the enterprise will deploy access points approximately every 60 feet. Because the enterprise intends to add voice clients in the near future, the Meru WLAN System will be configured to support Virtual Cell mode, meaning that all access points will be on the same channel. At a later time, when voice clients are in use, they will be able to move among access points with zero hand off, assuring toll quality voice. A quick walkthrough with a handheld analyzer or laptop with Wi-Fi client will allow the IT administrator to determine if any coverage holes exist. If so, an additional AP will be added. As the System is using Virtual Cell, there is no time consuming channel planning needed to add an additional AP. This method will significantly reduce deployment costs. Meru WLAN Controllers will be deployed in wiring closets at appropriate points within the enterprise. There is no restriction on layer 2 or layer 3 hops from the Access Points. Clients will be able to roam seamlessly among all Access Points, even across subnet boundaries.

Security

As the majority of the enterprise wireless devices are laptops, the recommendation is for an 802.1x authentication method. WPA or WPA2 should be used and will easily integrate with the enterprise's Microsoft Active Directory infrastructure. The enterprise should choose between EAP-TLS, EAP-TTLS or EAP-PEAP based on its assessment of authentication needs.

As the wireless barcode scanners, portable printers and Spectralink phones support WEP only, they should be segmented from employee laptop access by using a different SSID and different VLAN. This allows the partitioning of clients with different security capabilities.

For guests, the enterprise will make use of the Captive Portal and will redirect traffic on the 'Guest' SSID to a separate VLAN that is outside the corporate firewall with access to the Internet only.

Voice and Quality of Service

One of the key reasons the organization chose Meru's WLAN System is due to its desire to integrate pervasive wireless VOIP in the short term. When the organization desires to roll out voice clients, little to no changes will need to be made to the wireless network. If using a SIP, H.323 or Cisco 7920 phone, the Meru WLAN System is already configured to automatically recognize voice flows and reserve bandwidth for it to ensure toll quality voice. If another type of voice device is chosen, the Meru WLAN System can be easily configured to recognize it and provide the same level of performance. No special SSID or wireless VLAN separation is required for the voice clients if they can support the same security levels as the laptops. The Meru WLAN System will automatically

differentiate Quality of Service based on the application type and its dynamic bandwidth requirements, not the SSID.

If other applications require Quality of Service, they can be configured to have reserved bandwidth or prioritized quality of service. QoS is applied with reserved traffic being allocated the first portion of total bandwidth, followed by fixed priority levels, and finally by the best-effort (default) traffic class. For priority-based QoS, you can specify one of eight levels of priority.

Rogue AP Mitigation

The enterprise also desires rogue AP mitigation. The Meru Access Points will be configured to scan as well as provide client services. As the Meru APs support both 802.11b/g and 802.11a, all channels can be scanned ensuring rogue access points of all types are discovered. Automatic rogue AP mitigation will also be enabled as the branch offices do not have local technical support and any security threat must be stopped immediately. In addition, an SNMP alarm can also be sent to the IT staff at corporate headquarters so that they are alerted of these security incidents at the remote sites.

Management

The Meru WLAN System supports SNMP and will easily integrate into the enterprise's existing HP OpenView management system. The Meru WLAN Controller provides centralized management and configuration for all Meru Access Points and Radio Switches.

In addition, Meru Access Points uniquely capture packets of every Wi-Fi device within range over the air. The packet capture data can be uploaded into a packet sniffer of the enterprise's choosing, allowing fine grained connectivity and performance troubleshooting to be done, even remotely.