White Paper

The Benefits of Centralization in Wireless LANs via the Cisco Unified Wireless Network

This paper addresses the benefits of 802.11 wireless LAN centralization via the Cisco Unified Wireless Network. It discusses how centralization of wireless LANs (WLANs) delivers advanced features and benefits that are easy to deploy, scale, and manage. These benefits include ease of deployment, ease of upgrades, reliable connectivity through dynamic RF management, optimized per-user performance through user load balancing, guest networking, Layer 3 roaming, an embedded wireless Intrusion Detection System (IDS), location services, voice over IP, lowered total cost of ownership (TCO), and wired and wireless unification.

CHALLENGE

Perspective is everything—consider maps. Before high altitude photography, maps were not accurate; they were made of estimates scaled to the mapped geography. High altitude photography gave cartographers something that they didn't previously have—perspective. This perspective has revolutionized the way that we travel; how we view distance, and ultimately how our civilization evolved.

Traditionally, wireless LANs have had a lack of perspective—because each access point operates as a separate node, autonomously configured with channel and power settings from a static RF plan (generally an RF prediction). While these autonomous access points hear a nearby access point operating on the same channel, the autonomous access point has no way of determining if the adjacent access point is part of the same network or a neighboring network. Also, because autonomous access points are "nodal", scaling to large contiguous, coordinated wireless LANs and adding higher-level applications presents some challenges.

Consider the wireless requirements and solutions developed for autonomous access point deployments as outlined in Table 1. In some instances, the implementation of a WLAN using autonomous access points places limitations on the WLAN.

Table 1. Wireless Requirements and Solutions for Autonomous Access Point Deployments

Requirement	Description	Autonomous Solution
Layer 2 Fast Secure Roaming	Seamless client roaming within subnets across access points and virtual LANs (VLANs)	Add a wireless domain services (WDS) device (access point or switch module) to facilitate roaming
Layer 3 Fast Secure Roaming	Seamless client roaming between subnets across access points and VLANs	Not available in an autonomous access point. Requires a centralized solution to facilitate roaming
Upgrade Costs	Time to deploy additional management capabilities and push new images to access points	Deploy a centralized management station or use management scripts
Intrusion Detection System (IDS)	Ability to detect access point impersonation, attacks, and unauthorized access	Use a WDS-based IDS or add an overlay WLAN solution
Location Services	Visualization into received-signal-strength-indication (RSSI) information changes and location of Wi-Fi devices	Use a site survey solution or an overlay WLAN
Dynamic RF	Immediate, dynamic adaptation to RF environment	Use systems-level application appliance or a Simple Network Management Protocol (SNMP); RF information is available for manual review and action

Requirement	Description	Autonomous Solution
Load Balancing	Auto-balance client loads between adjacent access points	Individual access points advertise load, but load is not automatically spread between access points
Guest Networking	Ability to provide customers, vendors, and partners with controlled access to the WLAN while keeping the network secure	Implement specialized trunk VLANs into each access point and propagate them across the enterprise
Voice Over WLAN	Cost-effective, real-time voice services using the existing wireless infrastructure	Implement access point-based Call Admission Control (CAC); control is on a per-access point basis and not coordinated across multiple access points
Management	Cost-effective, simplified WLAN management and deployment	Implement scripts or SNMP solution to configure WLAN management and individually configure each access point

SOLUTION

First-generation wireless LANs using autonomous access points were convenience networks. Much has changed since the early adoption of WLANs. Today, basic connectivity is not enough. Enterprises need ubiquitous wireless coverage throughout their buildings. Their WLANs must support mobility services like voice, guest access, location and enhanced Wireless Intrusion Prevention Systems (WIPS), while also providing simplified deployment, management, and scalability. Enterprises need WLANs that do not have the limitations outlined in Table 1.

To implement these capabilities and remove these limitations, a unified WLAN is needed—one that is centralized and based on lightweight access points connected to wireless LAN controllers. Organizations need the Cisco® Unified Wireless Network.

Scalability: A WLAN Necessity

The need for scalability and advanced services over a wireless network is not new. In fact, cellular network providers have already overcome many of the challenges of scaling wireless networks. Originally, cellular wireless networks were an amalgamation of cellular towers that provided basic coverage. There were protocols for managing phone calls from tower to tower, but these protocols were not reliable—calls that weren't dropped were the exception.

Cellular operators needed a solution that allowed users to maintain their calls while roaming, as well as a platform for deploying advanced services. The solution was a new network element called a base station controller.

The base station controller, for cellular networks, coordinated a group of radio towers. As cellular users roamed from tower to tower, the base station controller coordinated the roaming. This allowed cellular calls to become more stable, with fewer dropped calls.

The concept of the cellular base station controller can be applied to 802.11 WLANs. Instead of managing multiple autonomous access points, operators manage lightweight access points via a centralized device called a wireless LAN controller.

WLAN Centralization

Following the path of cellular networks, Cisco Systems® pioneered WLAN centralization, and delivered the industry's first unified platform for advanced wireless LAN services. The key to Cisco's unified architecture, called the Cisco Unified Wireless Network, is the delivery of data from a lightweight access point, through the network to a wireless LAN controller.

Cisco offers many wireless LAN controllers that enable centralization of wireless LANs. Enterprise-class standalone wireless LAN controllers that fully integrate into the network infrastructure are available such as Cisco 4400 Series Wireless LAN Controllers and Cisco 2000 Series Wireless LAN Controllers, as well as wireless LAN controllers that are unified with the wired network such as the Cisco Catalyst 6500 Series Wireless Services Module (WiSM) and Cisco Wireless LAN Controller Module (WLCM) for Integrated Services Routers.

Developing a New Wireless LAN Centralization Protocol

To transport data and facilitate communication between lightweight access points and a wireless LAN controller, a new protocol was needed. This protocol needed to address the following requirements:

- **Ease of deployment**—Instead of trunking VLANs to the centralized controller(s), the protocol had to be able to cross subnet boundaries.
- **Deployment security**—Just because an access point is plugged into the network doesn't mean that it should have full access to the network. The protocol needed to provide a way of authenticating all access points connected to the network.
- **Real-time control of the access point**—Once the access point is deployed, authenticated, and connected to the controller, the protocol needed to provide real-time control of the access point for management and deployment of mobility services.
- **Protocol extensibility**—The protocol needed to work across a myriad of platforms, from chassis-based modules in large Ethernet switches, to stackables, to routers, and any other network elements.
- **Transport extensibility**—Although networks generally run over Ethernet, the protocol had to be capable of running across low-speed WAN links and even over the air (for applications like wireless mesh networking).

Cisco explored many options to address the needs for developing the new communications protocol. The Generic Routing Encapsulation (GRE) protocol was considered, but GRE does not support visibility into native Layer 2 packets, which is a necessity for secure WLANs. SNMP was considered since this protocol provides command and control of the access point, but its bulkiness made it less than ideal.

After considering other protocols, Cisco decided to develop a new protocol—Lightweight Access Point Protocol (LWAPP) that supported both Layer 2 and Layer 3 packet information.

What Is LWAPP?

LWAPP is a draft Internet Engineering Task Force (IETF) standard, authored by Cisco Systems, that standardizes the communications protocol between lightweight access points and WLAN systems such as controllers, switches, and routers. Its goals are to:

- Reduce the amount of processing within access points, freeing up their computing resources to focus exclusively on wireless access instead of filtering and policy enforcement
- Enable centralized traffic handling, authentication, encryption, and policy enforcement for an entire WLAN system
- Provide a generic encapsulation and transport mechanism for multivendor access point interoperability, using either a Layer 2 infrastructure or an IP-routed network

The LWAPP specification accomplishes these goals by defining:

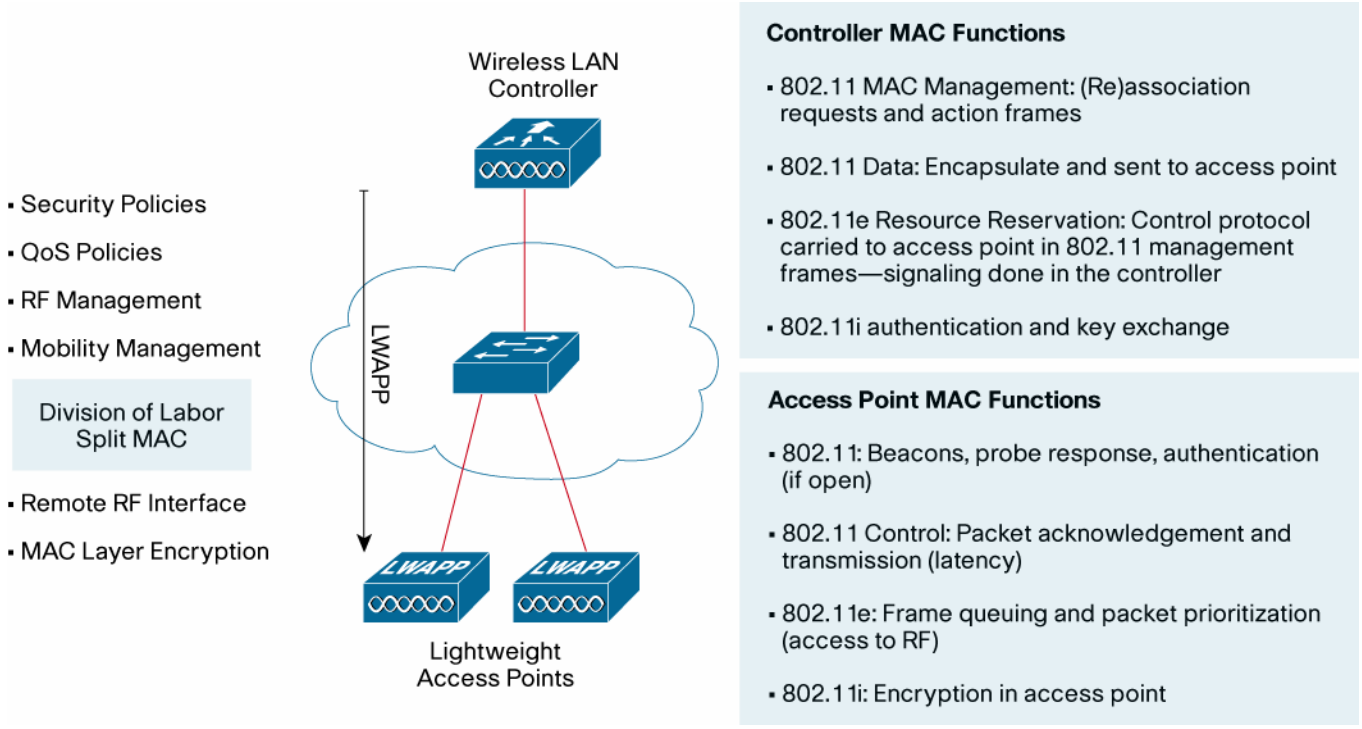
- Access point device discovery, information exchange, and configuration
- Access point certification and software control
- Packet encapsulation, fragmentation, and formatting
- Communications control and management between access points and wireless controllers

Learn more about LWAPP by reading the Understanding the Lightweight Access Point Protocol (LWAPP) white paper.

How Does LWAPP Work?

LWAPP splits the media access control (MAC) of a lightweight access point between the wireless LAN controller and the lightweight access point. Timing-critical functions such as the subatomic handshake and emitting beacons to the access point are managed at the access point. Other network-critical functions such as mobility management, authentication, VLAN segregation, RF management, wireless IDS, and packet forwarding are managed at the wireless LAN controller. (Figure 1)

Figure 1. Split Media Access Control Functions



There is a many-to-one relationship between lightweight access points and wireless LAN controllers—a single wireless LAN controller can manage and operate a large number of lightweight access points. In addition, the wireless LAN controller can coordinate and collate information across a large wireless network and even across a WAN. The controller has a holistic view of the entire network in much the same way a satellite has a complete view of an expansive geography.

Once a protocol was standardized upon and platforms were available for unification, the real benefits of WLAN centralization became apparent.

Benefits of Centralization and Unified WLANs

The numerous benefits of WLAN centralization and unified WLANs are presented below.

Ease of Deployment

When autonomous access points are deployed in an enterprise, each access point is individually configured. This configuration can be performed on a per-access-point basis or via a systems-level application or appliance. Once the autonomous access point is configured, each access point can be configured to support VLANs that allow segmentation of user groups and differentiation of LAN policies and services, such as security and quality of service (QoS), for different users and user groups. These VLANs extend into the access layer of the network. Depending upon the size and scope of deployment, VLANs can be trunked and extended across multiple switches.

When centralization using lightweight access points and a wireless LAN controller is introduced into a network, resubnetting and VLAN trunking into the access layer is not required. Instead, VLANs are trunked into a centralized wireless LAN controller, and the controller breaks users and WLANs into VLANs. This simplifies WLAN deployment and management.

Centralization Enables Ease of Deployment

When centralization is used, a lightweight access point only needs to find out the IP address of a wireless LAN controller—when deployed in Layer 2 mode. (When deployed in a remote subnet, the access point needs an IP address, subnet mask, and default gateway information.) The lightweight access point can also receive the wireless LAN controller IP address from a standard Dynamic Host Control Protocol (DHCP) server.

After the lightweight access point contacts the wireless LAN controller, the controller programs all RF policies and wireless LAN policies onto the lightweight access point. Because all packets from the access points are placed into an LWAPP tunnel and subsequently sent to the wireless LAN controller, there is no need to extend special VLANs to individual access points.

Ease of Upgrades

A low cost of operation makes an organization more capital-efficient. The question is: how are low-cost operations implemented?

Centralization Makes Upgrades Simple

With the Cisco Unified Wireless Network, all lightweight access point images are embedded in the controller image. When a controller image is upgraded, it upgrades all of the access points that are associated with it. There is no need to deploy a specialized script, or create a special job on a centralized management station.

Another benefit of the Cisco Unified Wireless Network's low-cost access point image upgrades is that interoperability between lightweight access points and controllers has been thoroughly tested and certified by Cisco's quality assurance team.

Reliable Connectivity Through Dynamic RF Management

Wireless networks using autonomous access points are traditionally deployed using a static RF plan, where each access point has its channel and power statically set. This is done according to an RF prediction, which estimates an access point's coverage area using a computer simulation of the RF environment, taking into account the access point's antenna transmit power. The goal of RF prediction is to deploy access points for optimal coverage with minimal channel overlap. However, since RF predictions are created on a computer with minimal accounting of what actually happens in the RF environment after deployment, they are only estimates of the actual RF environment.

For instance co-channel interference from a neighboring network, an office reconfiguration, a door opening or closing, microwave oven interference, or other sources of interference cannot be accurately accounted for predeployment when RF prediction is used.

Centralization Delivers Dynamic RF

Wireless LAN controllers have a built-in understanding of the signal strength that exists between lightweight access points within the same network. These controllers can use this information to create a dynamic optimal RF topology for the network. Wireless LAN controllers deliver dynamic RF in a unique fashion.

When a Cisco LWAPP-enabled access point boots up, it immediately looks for a wireless LAN controller within the network. After it finds a wireless LAN controller, the LWAPP-enabled access point sends out encrypted "neighbor" messages. These neighbor messages include the MAC address and signal strength of any neighboring access points. In a single wireless LAN controller network, the controller uses this neighbor information to determine the relative spatiality of the access points in the network. The controller then tunes each access point channel and optimal signal strength for optimal coverage and capacity.

When there is a cluster of wireless LAN controllers (i.e. many controllers deployed in a single network) in the network a default controller is chosen, and all of the controllers feed the default controller information for their lightweight access points. The default controller correlates information for all of the access points in the network, and then pushes out the optimal channel and power for every access point on the network.

The algorithms built into the Cisco Unified Wireless Network architecture help to ensure that the network does not “flap”, or needlessly change. The result is a dynamic wireless network that adapts to changing RF conditions in real time.

Optimized Per-User Performance Through User Load Balancing

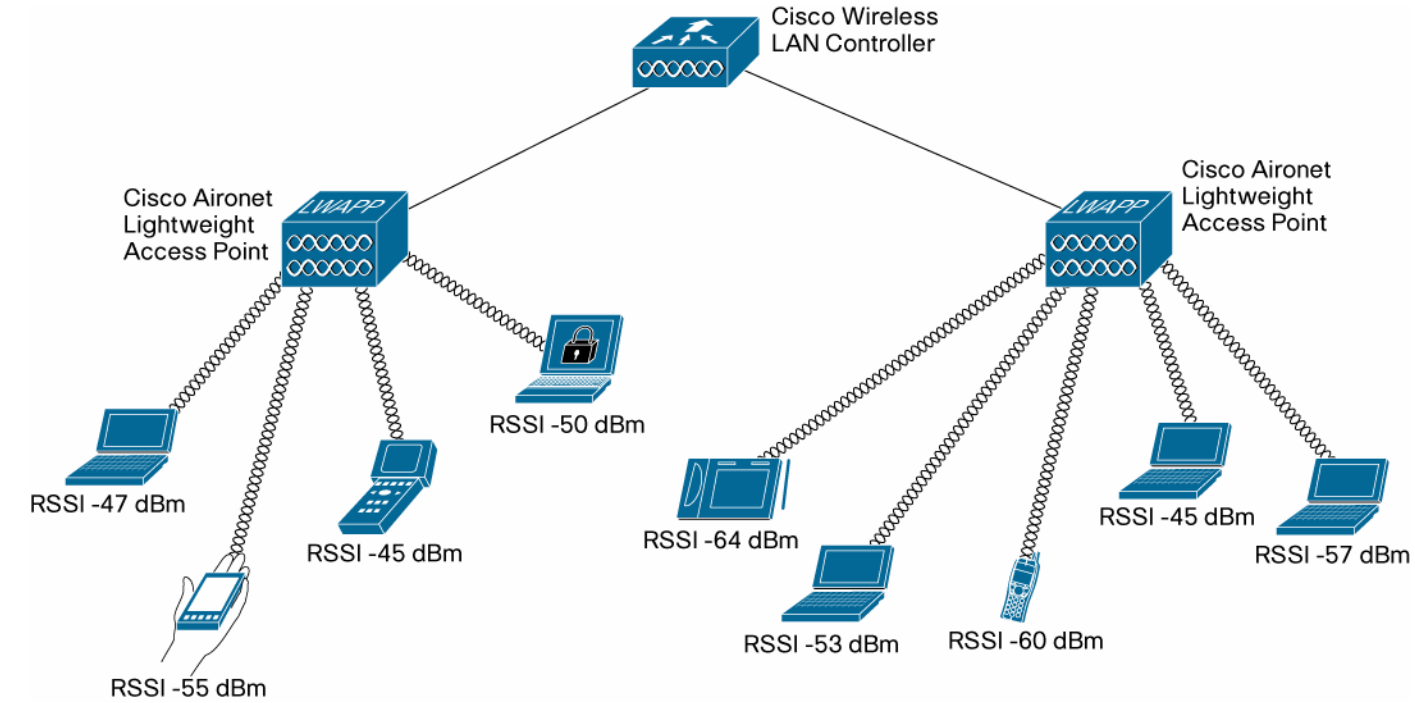
The 802.11 protocol makes it difficult to predict and guarantee user performance and throughput. Because 802.11 gives each network element equal access to the air, each client decides which access point it will roam to next. When client devices enter a coverage area, they may roam to the access point with the strongest signal. Likewise, each client device has as much access to the RF medium as the access point that they are associated with. Therefore, RF throughput for all clients can be potentially reduced—all clients may associate with the same access point. This is commonly called the “meeting room effect”.

Load balancing optimizes throughput for all clients by constantly optimizing user associations to give each client optimal throughput. This improves the throughput for each client and dynamically balances the client load for the network.

Centralization Load Balances Users

Cisco wireless LAN controllers and modules have a holistic view of the network. Through encrypted over-the-air messages, these controllers have an understanding of the signal strength between access points. In addition, when a client probes for an access point (a part of the 802.11 standard wherein a client looks for any access point advertising the WLAN name it is looking for), the controller hears the probe from each access point that hears the client’s probe. The controller then chooses which access point will respond to the client’s probe, taking into account the client’s signal strength and signal to nose ratio. For example, an adjacent access point may provide an equivalent service but at a lower signal strength. The controller will decide which access point should respond to the client’s probe based on its signal strength (RSSI). (Figure 2)

Figure 2. Wireless LAN Controllers Decide Which Access Point Should Respond to a Client's Probe



Guest Networking

Guest networking has evolved from a luxury to a business requirement. Guest networking allows organizations to keep their wireless networks secure while providing their customers, vendors, and partners with controlled access to their WLANs. It allows consultants and visitors to collaborate quickly, accelerating the velocity of business.

Today, the question is not whether an organization is going to deliver guest networking, but how it is going to deliver it? With autonomous access point deployments, administrators provide guest networking by extending "guest" VLANs into the network. These VLANs have security policies that are different from normal network traffic. These VLANs can be sources of misconfiguration and potential security holes.

Centralization Enables Simplified Guest Networking

In the Cisco Unified Wireless Network, each wireless LAN controller has a captive Web portal feature that allows organizations to customize the WLAN for their specific business needs. For example, network managers can place controllers into the DMZ to act as a guest anchor. When a guest wireless LAN is deployed in a network, all traffic from the guest WLAN is tunneled through the network to the guest controller. Unlike a wireless LAN with autonomous access points, Cisco's solution using lightweight access points and wireless LAN controllers does not require any modifications to the underlying VLAN architecture.

Layer 3 Roaming

With the Cisco Unified Wireless Network using lightweight access points, when Layer 3 roaming is introduced into a network, administrators do not have to extend VLANs to all of the access points in the network in an effort to keep a flat wireless subnet. This is not the case with networks using autonomous access points that extend VLANs to enable roaming and in turn introduce large broadcast domains, which are not scalable.

Implementing Layer 3 roaming without VLANs as is done by the Cisco Unified Wireless Network simplifies the network and makes it ready for real-time applications such as voice and video over wireless.

Centralization Enables Layer 3 Roaming

With the Cisco Unified Wireless Network, lightweight access points are deployed in a network's normal subnet infrastructure and are given an IP address that is local to the subnet to which they are deployed. All traffic that comes from wireless clients is placed into an LWAPP packet that is tunneled through the underlying network to the wireless LAN controller. Client devices receive their IP addresses from a subnet that is connected to the controller—not the subnet of the area of a building where they reside. The underlying subnet infrastructure is hidden from the client. The controllers manage all roaming and tunneling between one another to help ensure protocols such as Mobile IP are not required.

Embedded Wireless IDS

Security is a concern for network administrators, and wireless security is a concern of security professionals. One significant concern is the threat of a rogue access point creating a hole in a wired or wireless network. Introducing a wireless IDS system into the network provides an added layer of protection and security into the network. A wireless LAN IDS reduces the threat of hackers or malicious users gaining access to critical network resources.

Centralization Enables Wireless IDS

Cisco lightweight access points and wireless LAN controllers simultaneously act as data-serving devices and IDS sensors. This is possible through the LWAPP's unique split-MAC architecture, wherein some capabilities are in the access point, and other capabilities are in the controller. The LWAPP split MAC allows lightweight access points to scan channels without interruption to data services. Access points and controllers have a robust library of attack signatures that are used to detect wireless threats, which could be rogue access points, ad-hoc networks, or malicious people trying to find a weakness in the wireless network. Lightweight access points can detect attacks on the same channel that they are operating on, as well as threats such as rogues and ad-hoc networks operating on channels that they are not operating on.

In addition, because the Cisco Unified Wireless Network lightweight access points and wireless LAN controllers ship with X.509 certificates, they can detect an unauthorized access point that is spoofing a trusted access point (acting as a honeypot*) in the network.

The Cisco Unified Wireless Network also mitigates threats presented by rogue access points through its powerful rogue containment feature, which helps to ensure that clients cannot associate with a rogue access point.

Location Services

Location services are an absolute requirement for next-generation wireless networks. Location services support the simultaneous tracking of thousands of Wi-Fi devices from directly within the WLAN infrastructure. These services are used for critical applications such as high-value asset tracking, IT management, security, and business policy enforcement. Other applications include:

- e911 and voice over wireless LAN
- Client troubleshooting and correlating a client's location with client connectivity issues
- Asset tracking and management to support tracking of any device that has 802.11, including assets with 802.11 RFID tags
- Location-based security

* An authorized access point deployed by a network administrator to detect and mitigate unauthorized network access.

Enabling Location Services

In much the same way that wireless LAN controllers have an understanding of the path loss and signal strength between lightweight access points, they also gain information about client signal strength from the LWAPP-enabled access points that are available in the network.

Cisco wireless LAN controllers forward received client signal strength information onto the Cisco Wireless Control System (WCS) and Cisco Wireless Location Appliance, where intensive RF fingerprinting calculations are made that take into account building material type, multipath, and reflection to determine the location of the 802.11 or active RFID device. This information is available in real time. LWAPP is the control and transport protocol that enables location services.

Voice over WLAN

Voice over WLAN (VoWLAN) offers the benefits of voice over IP (VoIP) such as toll bypass, but with the additional benefit of mobility. Administrators looking for VoWLAN capabilities are looking to reduce or eliminate expensive cell phone usage in buildings by using their 802.11 data network for voice capabilities.

Centralization Enables High-Performance VoWLAN

Voice over 802.11 for autonomous solutions uses the same underlying protocol as regular data traffic, plus additional capabilities by using 802.11e, which runs between an autonomous access point and a voice terminal. Unfortunately, autonomous access points operating on the same channel have no way to coordinate their Call Admission Control (CAC) capabilities. Also, all devices that can hear one another operating in the same channel are subject to co-channel interference and autonomous access points cannot easily address this issue.

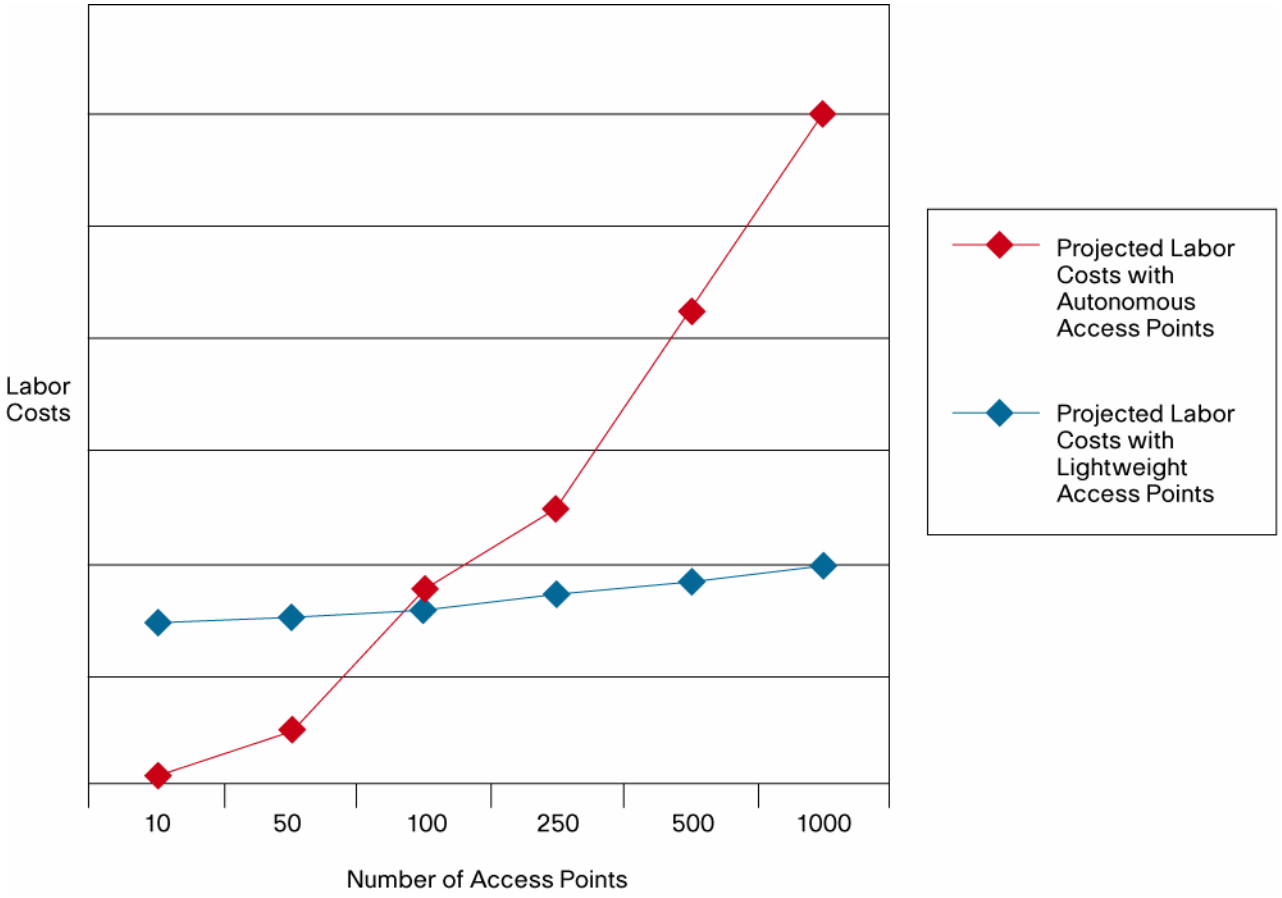
With the Cisco Unified Wireless Network, wireless LAN controllers enable predictable CAC for the network. In this unified network, the controller has a holistic view of all of the clients in the network, along with the total available call capacity between all access points on the same channel. This capability helps to ensure that when a VoWLAN call is admitted into the Cisco Unified Wireless Network, there is enough voice capacity across all access points. The result is more predictable, reliable voice performance.

Lower Total Cost of Ownership

A low total cost of ownership (TCO) allows organizations to deploy solutions without adding additional staff, ultimately leading to a reduced burden of deploying and maintaining the network. This improves the bottom line for an organization. With autonomous access point deployments, time is spent installing and initially configuring access points, reconfiguring access points, and upgrading access points.

In an autonomous access point network with 100 access points, if 30 minutes are spent a year per autonomous access point, this is equivalent to 3000 person minutes or 50 person hours a year. Over a five-year depreciation cycle, this is more than one month spent on autonomous access point administration—exclusive of troubleshooting client problems and other components of the network.

Figure 3. Projected Labor Costs Per Configured Access Point



Centralization Reduces TCO

With the Cisco Unified Wireless Network, instead of configuring 100 network elements, users only need to configure the wireless LAN controller. The controller in turn configures all access points in the network. In addition, instead of upgrading the software on each access point in the network, an administrator simply upgrades the wireless LAN controller software, and all lightweight access points are simultaneously upgraded.

Because the wireless LAN controller is able to look across the entire wireless network, it can coordinate information and use advanced capabilities like location to aid in troubleshooting client connectivity problems. These capabilities keep the TCO for a large wireless network low, while reducing the cost of troubleshooting and managing the network.

Wired and Wireless Unification

Integration of the wired and wireless network is critical for unified network control, scalability, security, and reliability. Systemwide wireless LAN functions, such as security policies, intrusion prevention, RF management, QoS, and mobility, must be available to support enterprise-class wireless applications. A WLAN using lightweight access points and wireless LAN controllers readily supports unification of the wired and wireless LAN because controller capabilities can be integrated into Cisco switching and routing platforms.

Unification Provides Investment Protection and Streamlines Costs

The Cisco Unified Wireless Network delivers a complete end-to-end solution that is unified and innovative. It provides solid investment protection that helps ensure a secure, mobile, cost-effective interactive workplace for the wired and wireless network. This unified network infrastructure, using lightweight access points and wireless LAN controllers, can be deployed with standalone or modular wireless LAN controllers integrated into a range of Cisco switching and routing platforms.

Customers can realize significant TCO, streamline support costs, and reduce planned and unplanned network downtime by adding a modular wireless LAN controller such as the Cisco Catalyst 6500 Series WiSM or Cisco WLCM for Integrated Services Routers.

The Cisco Unified Wireless Network also supports Network Admission Control (NAC) and Cisco Compatible Extensions client devices. NAC for WLANs provides security threat protection by enforcing device security policy compliance when WLAN clients attempt to access the network. The Cisco Compatible Extensions program ensures the widespread availability of client devices that are interoperable with a Cisco WLAN infrastructure and take advantage of Cisco innovations for enhanced security, mobility, quality of service, and network management.

SUMMARY

The Cisco Unified Wireless Network reduces the complexity of deploying and managing a wireless network; enables advanced services like voice, location, and guest networking; and helps to ensure that the cost of operating the wired and wireless network is manageable. The idea of network centralization and unification is not new—it was first considered by cellular network operators and then carried forward into 802.11 networks. It is through centralization and unification that wireless networks will be able to scale to large enterprise deployments and provide reliable connectivity and mobility to users.

FOR MORE INFORMATION

Contact your local account representative or visit the locations below for more information.

For more information about the Cisco Unified Wireless Network, please visit: http://www.cisco.com/go/unifiedwireless

For more information about Cisco wireless products, please visit: http://www.cisco.com/go/aironet

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA C11-60008-00 02.06