How Cisco Deployed Wireless Access Points Worldwide

Cisco Aironet deployment improved employee productivity, mobility, and network security.

Cisco IT Case Study / Wireless / Wireless Local Area Network: This case study describes Cisco IT's internal deployment of wireless LANs within the Cisco network, a leading-edge enterprise environment that is one of the largest and most complex in the world. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

> "From the start Cisco saw the benefits of wireless networking across the enterprise and the potential productivity it would offer."
> **– Oisin Mac Alasdair, program manager, Cisco IT Global Wireless Program**

BACKGROUND

In 2000, Cisco® IT began developing a consistent and supported wireless networking architecture. During this process, IT recognized a growing number of non-IT deployments throughout the company, led by user demand for the benefits offered by wireless networking. These WLANs were purchased, deployed, and supported by local teams without IT support or supervision. This resulted in inconsistent deployments, often with poor security and sometimes involving ready-to-use wireless solutions with no security features enabled. Most of the WLANs used Cisco Aironet® access points, but wireless products from other manufacturers were also identified. When the same products were used, often software versions and configurations were different. Security was IT's primary concern. In some circumstances WLANs were implemented without any security.

The question for Cisco IT was not whether WLANs should be deployed, because Cisco Systems® had long since identified the many benefits offered by the technology, but rather how could Cisco cost-effectively maintain control, reduce overall support costs, and still provide benefits to Cisco employees? The IT staff realized WLANs would deliver productivity benefits. Additionally, Cisco already had a highly mobile workforce where almost every employee (in excess of 34,000) was issued a laptop computer. The potential mobility was limited, however, because laptop users were restricted to their desks because of an Ethernet wired network connection. Cisco IT looked to its own Cisco Aironet WLAN technology to increase employee flexibility, mobility, and time savings; generate higher productivity enterprise-wide; foster more effective and efficient employee, partner, and customer collaboration; and provide users with a more dynamic and reactive workplace, unlimited by physical constraints.

CHALLENGE

Cisco IT's challenge was to provide secure, reliable, consistent, high-performance, and cost-effective wireless services worldwide.

Network Security

Network security issues inherent in deploying WLANs had to be addressed. Wireless technology is a shared medium, and can pass through protected secure walls with ease. The fundamental nature of a WLAN lies in its use of RF as a transport medium that, by definition, is not as secure as a wired environment. Unlike traditional wired networks, there is no physical security and WLAN transmissions can be intercepted by any adaptor within range. A solid security framework was essential to protect corporate traffic, yet without introducing unwieldy or overly complex security requirements for end users. Excessively strong security measures would complicate and discourage use by employees, while too little security could increase potential vulnerabilities. A carefully balanced, user-friendly, yet secure architecture was required.

Reliability

Because WLANs use RF as the transport medium, they are, by nature, highly susceptible to interference and subject to attenuation and environmental conditions. Cisco IT set a goal to overcome these variables and deliver a reliable WLAN service that would be widely accepted and used by Cisco employees.

Performance and Scalability

In 2000, Cisco IT needed to maintain optimal network performance while scaling the network to support new WLAN standards, additional access points, and client devices as needed. Because WLANs are a common shared medium (a single “collision domain”), end users share bandwidth among all wireless devices in a particular cell. Cisco IT needed to create an architecture to meet the performance requirements of all users sharing this finite bandwidth currently and in the future as standards evolved. In 2000, the standard wireless technology was 802.11b, which provided a data rate of 11 Mbps, producing an effective throughput of approximately 6 Mbps. Cisco IT designed the original Cisco wireless network based on the 802.11b standard. Today, additional standards such as 802.11a and 802.11g are available and are being used in Cisco WLANs. These new standards offer data rates of up to 54 Mbps and effective throughput of 22 Mbps for 802.11g and 30 Mbps for 802.11a. In addition, as new users are added to the network and new buildings are added to Cisco campuses worldwide, this WLAN design and Cisco Aironet products easily facilitate scaling the network to meet current and future WLAN needs.

Consistency

As with all enterprise-class networks, Cisco IT required a standard design and implementation of its WLAN networking technology. Cisco staff also expected a homogenous environment where user experience is identical irrespective of physical location. Furthermore, global standards were needed to help ensure ease of deployment, support, and maintenance and to reduce operational expenditures. Finally, the use of a standard set of architectural, procedural, and user standards allowed easy outsourcing of both physical deployment and frontline support (where appropriate).

Global Deployment

Early on, Cisco made a decision to deploy the wireless network to all Cisco offices, supporting all Cisco staff. This called for the installation of more than 3000 access points at approximately 280 sites in more than 85 countries, serving at least 35,000 active users.

Cost-Effectiveness

Deploying a wireless network in all Cisco offices worldwide was an expensive undertaking and cost-effectiveness was an important consideration. Not only did design and deployment costs need to be controlled, but ongoing support and maintenance expenses, operational overhead, and potential outsourcing costs had to be kept to a minimum, while maintaining a high standard of service. At first Cisco IT attempted to control costs by turning the WLAN deployment into a customer-funded project, asking each business group within Cisco to pay a portion of the total cost of purchasing and deploying access points. This effort failed because groups sharing floors frequently did not pay for what Cisco IT perceived as their share of the costs, and relied on other groups to pay for the entire floor. A continuation of this effort would have resulted in an inconsistent and incomplete deployment, and increased the likelihood of groups continuing to build their own nonstandard, unsecured wireless subnetworks. To prevent this from occurring, IT received the funding to deploy a companywide wireless network with access points on all floors in all buildings, allowing maintenance of a worldwide Cisco WLAN standard.

Investment Protection

Cisco wanted to deploy a wireless network that supported upgrades and provided a migration path to future features and new IEEE 802.11 technologies. Cisco Aironet access points and Cisco Aironet client devices met this need. These products supported automatic or user-initiated firmware, driver, and utility upgrades that were well documented by the Cisco Aironet product team. They also supported several operating systems including Windows 98, 2000, XP, and CE; Mac OS; Linux; and DOS.

Today, Cisco Aironet products support modular deployment that allows upgrading of the radio module to 802.11a and 802.11g standards and new encryption standards such as 802.11i. The introduction of the Cisco Compatible Extensions program in 2003 further helped to ensure investment protection by facilitating the easy addition of client devices to the WLAN using laptops with built-in radios, without having to distribute and manage individual client cards.

SOLUTION

Cisco IT formed an Architecture team to define business and user requirements, global architecture standards, support plans, and an ongoing management framework for the WLANs. The team established five principles to guide them in their efforts:

- WLANs should be productivity tools, enabling greater mobility for Cisco employees
- Every Cisco employee should have access to the global wireless network
- Ease of use and a common user experience were essential for widespread usage
- The WLANs should be built on global, scalable standards providing a single, worldwide wireless network
- IT must design a secure architecture that did not rely upon the then-prevalent, yet insecure, static Wired Equivalent Privacy (WEP) shared-key framework
- Cisco IT identified additional security principles, including:
- WLANs should support both privacy and access control through enterprise-class authentication and encryption capabilities
- Network attacks must be mitigated
- Rogue access points must be detected and remediated

Cisco Aironet Access Points

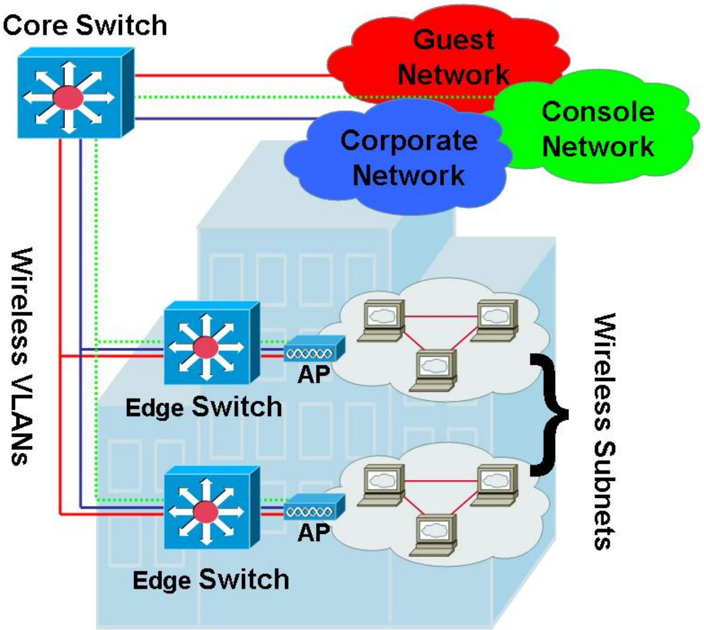
The Cisco Aironet 350 Series Access Point was selected as the standard access-point device for global WLAN deployment. At the time it was chosen, the Cisco Aironet 350 Series was the most advanced, fully featured wireless access point available. It supported the 802.11b protocol standard (the most advanced at that time), which provides data rates of up to 11 Mbps. As the product line evolved, new features helped to improve the WLANs, both in deployment and in sustainability. The Cisco Aironet 350 Series also supported inline Power over Ethernet (PoE), which greatly simplifies installation and reduces costs by eliminating the need for separate, dedicated power cabling to the main supply.

PoE allows the access point to draw power through its Ethernet cable, from the switch to which it is connected. The Cisco Aironet 350 Series also offered an industry-leading radio capable of 100-milliwatt (mW) transmission power with power-management capabilities for excellent throughput and range. It supported load balancing, hot-standby redundancy, and beginning in 2003 Cisco IOS® Software features. Today Cisco IT is expanding and enhancing its initial Cisco Aironet 350 Series deployments by installing Cisco Aironet 1100 Series and Aironet 1200 Series access points (Figure 1). These access points support new 802.11 standards and additional feature enhancements and options for modular and flexible WLAN deployments.

Figure 1. Cisco Aironet 1100 Series and Aironet 1200 Series Access Points

In 2000, the architecture standard called for Cisco Aironet 350 Series access points to be connected to the nearest access-layer switch (Figure 2). A separate cable provided console access to each access-point device, in the event of a loss of network connectivity—a practice that Cisco IT has standardized on for all network devices.

Figure 2. Cisco WLAN Network

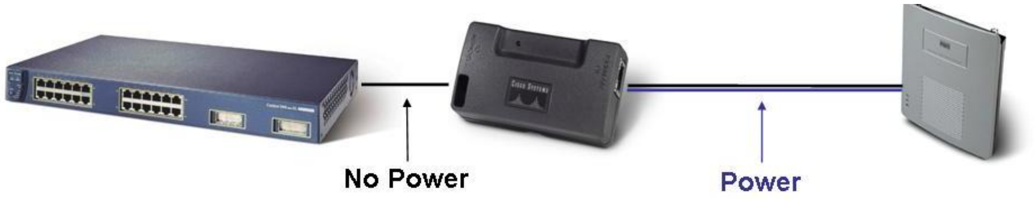


The WLAN Architecture team initially considered locating access points within wiring closets and connecting them via coaxial cable ("pigtail") to the antennas closer to the end users at appropriate locations throughout the floor. This would have placed the access points close to the access-layer switches and main power supply and secured them in a locked data closet. However, because this would require the use of expensive, plenum-rated coaxial cable from the access point to the antennas, it was deemed too costly. (Cabling used in the plenum area, the interstitial space above a drop ceiling or under a raised floor, must be specially rated as fire-retardant per U.S. fire safety regulations.) The architecture team decided to place the access points at the location defined by the Site Survey (IT engineers would do a site survey of each building to determine the best locations for each access point in a site survey, described below). At U.S. sites, deployment teams mounted the access points in the ceiling, and relied upon certified plenum-rated metal enclosures for fire safety compliance. Outside the United States, access points generally were mounted on walls, below the ceiling, where plenum rating was not required.

Access Point Power Requirements

The next challenge was providing power to the access points. But as with the plenum-rated cable between access points and antennas, the cost of running AC power to ceiling-mounted access points was cost-prohibitive. Instead Cisco IT used inline power adaptors that provided DC over the existing Category 5 (Cat5) network cable. (This same technique is used to power Cisco IP phones.) Cisco Aironet access points supported 48 volts direct current (VDC) PoE, as did most of the access-layer switches to which they were connected. In those locations where access switches were not equipped with the PoE blade, or so many IP phones were being powered that there was insufficient power available for the access points, power injectors were used to inject power into the network cable from an electrical outlet (Figure 3)

Figure 3. Power Injectors



802.11 Wireless Networking Standards

At the time that the Architecture team was defining global standards, the only widely deployed standard was the 2.4-GHz 802.11b standard providing throughput rates of up to 11 Mbps, and the team selected this standard. Today, Cisco also is deploying 802.11a, 802.11b, and 802.11g Cisco Aironet access points and client devices in its WLANs. 802.11g has data rates of up to 54 Mbps in the 2.4-GHz band and 802.11a has data rates of up to 54 Mbps in the 5-GHz band. These additional bands provide Cisco employees with increased capacity and performance for bandwidth-intensive applications and in areas with dense user traffic.

Access Control: IEEE 802.1X and Extensible Authentication Protocol

In 2000, the 802.11 protocols used a basic encryption technology known as Wired Equivalent Privacy (WEP) to provide security. WEP encrypts traffic using a fixed key of 40 or 128 bits in length. The major drawback to WEP is that the key is static; that is, it never changes. Not only did this make key management (the distribution and maintenance of static WEP keys to thousands of access points and tens of thousands of clients) a major challenge, but security analysts and network intruders had also developed several methods of easily cracking static WEP keys. Cisco IT deemed WEP both unwieldy and insufficiently secure for enterprise deployment.

In an effort to make this encryption standard more secure, Cisco developed Cisco LEAP, which was based on the Extensible Authentication Protocol (EAP) framework, part of the IEEE 802.1X specification. The development of Cisco LEAP increased the security capabilities by introducing dynamic key management for mutual authentication between the user and the authentication server through the access point. Cisco adopted the IEEE 802.1X standard using Cisco LEAP. This solution is made up of three separate services, each with a vital role in the EAP process:

Supplicant—client

Authenticator—access point

Authenticator server—authentication, authorization, and accounting (AAA)

In 2004, Cisco IT started migrating to EAP-FAST (described in “Next Steps”).

Data Privacy: Temporal Key Integrity Protocol and Advanced Encryption Standard

In 2001 Cisco IT further strengthened its internal WLANs by implementing the Cisco Wireless Security Suite. This suite introduced several important additions to Cisco Aironet security capabilities. Perhaps the most significant of these was the Temporal Key Integrity Protocol (TKIP). The TKIP increases WEP security by addressing its well-known weakness to “weak IV” attacks. These attacks exploit WEP’s predictable reuse of particular initialization vectors (IVs). If a sufficient number of WEP-encrypted packets are captured, it is possible to reverse-engineer or derive the underlying WEP key. This enables network intruders to gain access to the WEP-encrypted WLAN. TKIP mitigates this attack by replacing WEP’s reliance upon static keys with a dynamic, *per-packet* key generated from about 500 trillion possibilities. Effectively, each and every packet is encrypted with a unique key, which prevents intruders from capturing sufficient packets with the same key in an attempt to crack the wireless encryption scheme.

Furthermore, Cisco Wireless Security Suite also introduced the message integrity check. The message integrity check uses a mathematical function to validate the contents of each packet. Because both the sender and receiver independently perform the message integrity check, either of them can detect if a packet has been intercepted, modified, and resent—mitigating “man in the middle” attacks.

Finally, Cisco Wireless Security Suite also introduced Broadcast Key Rotation (BKR), which allows the common broadcast key to be recalculated on a regular basis.

Collectively these three enhancements address the known weaknesses of static WEP encryption and, at the time of writing in October 2004, retain this status. Additionally, versions of TKIP and MIC have been implemented in the cross-industry WiFi Protected Access (WPA) protocol.

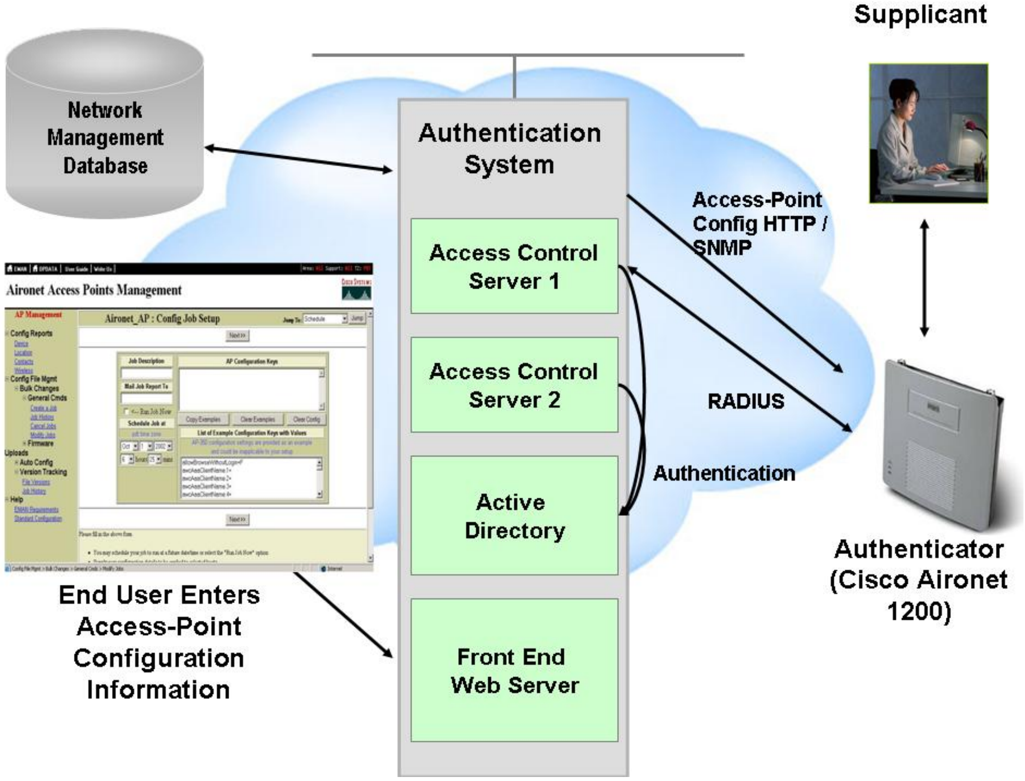
Today, Cisco WLANs include WPA, which supports a variety of EAP types for per-user mutual authentication as well as TKIP for encryption. In 2004 Cisco Aironet products will support WPA2, which uses Advanced Encryption Standard (AES) encryption. Where applicable, Cisco WLANs will be upgraded to include support for WPA2.

Cisco Secure Access Control Server

Users must be authenticated against the authentication server when they log on to a network. The AAA server performs this authentication function. The Architecture team standardized on the Cisco Secure Access Control Server (ACS) to perform this task for WLAN users. The team deployed pairs of Cisco Secure ACSs at strategic locations worldwide. The value of using a globally distributed AAA architecture instead of a single AAA server was highlighted by the WLAN deployment. In a wired network environment, employees are authenticated by the nearest AAA server once or perhaps twice a day. In a wireless environment, users are authenticated by the AAA server several times a day as they roam throughout a building. Because each connection to a new access point required a new authentication event, it was critical to keep authentication latency low, and to make sure that the authentication server was available at all times.

Cisco IT deployed Cisco Secure ACS pairs using the same architecture it had used for deploying RADIUS servers and Active Directory servers: in server cabinets in 13 hub locations worldwide. This meant that end users experienced less latency because they connected to the nearest Cisco Secure ACS. It also meant that authentication services were always available, because end users were redirected to the next-nearest Cisco Secure ACS when a Cisco Secure ACS pair became unavailable.

Figure 4. Access Point and Cisco Secure ACS Provisioning


Supplicant
Network Management Database
Authentication System
Access Control Server 1
Access Control Server 2
Active Directory
Front End Web Server
Access-Point Config HTTP / SNMP
RADIUS
Authentication
Authenticator (Cisco Aironet 1200)
Aironet Access Points Management
End User Enters Access-Point Configuration Information

The team also decided to integrate the WLAN into the Microsoft Active Directory domain structure, enabling a single sign-on (SSO) capability. Because the Cisco Aironet Client Utility supported SSO, users could authenticate easily with the WLAN. Effectively, their NT user credentials were not only used for access to their laptops, but also to provide transparent authentication to the wireless network. SSO greatly reduced the client impact for users, and helped ensure a common and user-friendly experience across platforms and transport media. Users had only to remember their normal ID and password for access to their laptop, the wired network, and the wireless network; and only had to enter their credentials once each session regardless of which transport medium was being used.

Network Topology

Early in the planning stage, the Architecture team decided that the WLAN would be a secondary network complementing the existing wired network (that is, a separate "overlay" network). Each large building would use a single Layer 3 domain across all floors to help ensure session integrity for wireless devices moving within or between floors. In smaller buildings with less than 20 or 30 users, wired and wireless users would share a common virtual LAN (VLAN).

User-to-Access-Point Ratio

The Architecture team had to determine how many users of a shared medium could effectively use an access point at the same time without performance issues. One of the team members conducted traffic-analysis tests and determined that a ratio of 25:1 would prove adequate performance. It was unlikely that all 25 users would be logged on at the same time, and even more unlikely that they would all be simultaneously sending or receiving large amounts of data. Because the WLAN was an overlay network, those users who needed to use bandwidth-intensive applications like network backups or video streaming were encouraged to use the wired network and not depend on the wireless network for these functions.

Even with the limitation of the 802.11b data rate of 11 Mbps (or actual throughput of 6 Mbps), performance has not been adversely affected. Comments from users have been overwhelmingly positive. Some buildings in Cisco use predominantly wireless connectivity for all their needs, including network backups, software downloads, video unicast, and Cisco IP Communicator (a software IP phone), in addition to standard Web browsing, e-mail, and calendars. "With quality of service now supportedover wireless, I've been taking all my phone calls over the wireless network using Cisco IP Communicator, and it's been working perfectly," says Rich Gore, Cisco project manager.

Signal Strength

Like radio stations, WLANs broadcast signals into the surrounding area. Any signals extending beyond the building can increase security risks posed by network intruders. Cisco Aironet access points can broadcast up to 100mW (depending on the regulatory domain), potentially reaching out into parking lots and public areas. After conducting tests, the Architecture team established standards that call for using minimum power to reach all areas within buildings, and never exceeding 20mW. In some instances, directional antennas were used to more narrowly focus the signal, reducing the power required to achieve full coverage. If necessary, rather than increasing transmit power to exceed 20mW, additional access points were installed to cover "dead" spots.

Roaming

Most buildings require multiple WLAN antennas and transmitters to help ensure coverage in every area: to the far corners of each floor, and to multiple floors. These "cells" must touch or overlap slightly to provide complete coverage. Like cell-phone users whose motion causes them to leave one cell and move to another, WLAN users within or near the intersection of two cells will associate with one transmitter and then switch, or roam, to another when certain thresholds are met. If the radio architecture is not well designed, the user can switch back and forth between transmitters, seeking the strongest signal.

Each time the user switches from one access point to another, connectivity is momentarily lost, necessitating reauthentication. Numerous reauthentication requests can increase load on the authentication server, which can adversely affect service.

The Architecture team resolved this issue by creating guidelines for cell overlap and locking in transmission rates. If cells overlap by too much, continual switching is much more likely. The team found that an overlap of about 15 percent (roughly 10 feet in most buildings) minimized frequent user reassociation to a new access point. In addition, configuring the wireless Cisco Aironet Client Utility application on the laptop PC to only scan for a better access point when the current signal strength has dropped below a specified threshold also reduces the tendency to reassociate to a new access point.

Another cause of flipping to a new access point is signal degradation over distance. As the user moves farther from the WLAN transmitter, the signal's ability to carry data diminishes as noise and interference increase. As with traditional dial-up modems, the IEEE 802.11b standard allows wireless transmitters to "step down" to a lower bandwidth rate to compensate for this noise and interference; for example, from 11 Mbps to 5.5 Mbps to 2 Mbps, and then to 1 Mbps. But as the user moves away from a cell, rather than transferring to the other access point, the wireless device may try to continue communicating with the first access point at 5.5 Mbps, which could cause greater cell overlap and more jumping to new access points. To minimize this problem, the Architecture team locked the data rate at 11 Mbps. This means that the user's wireless connection will never "step down," but rather will associate to a different access point when it is far enough away from the original access point. This controls the roaming and avoids flipping between access points.

Access points that support 802.11g offer speeds greater than 11 Mbps. Cisco IT created a policy for these access points and clients that disallows the connection to "step down" *below* 11 Mbps. However, if an 802.11g client is close to an access point that supports 802.11g, it can transmit and receive data at the higher rates offered by that standard. The policy for 802.11g networks is to permit data speeds as high as possible, but never less than 802.11b (11 Mbps).

Global Naming Standards

Keeping track of thousands of WLAN access points is essential to proper management of the worldwide wireless network. Adopting a global naming standard for all access points enables network engineers to recognize access points and their location—including city, building, floor, and location on the floor. A naming convention also helps to eliminate duplicate device names, which could complicate support. As such, all access points were given host names in compliance with existing defined global-naming standards. Cisco IT has found that a consistent naming standard allows for easier management.

Pilot Deployments

Prior to global deployment, pilot WLANs were deployed in each region (the Americas, EMEA, Asia Pacific, and corporate headquarters) to validate design criteria developed by the Architecture team. This phase of the process spanned approximately two months in 2000 and the pilots successfully validated the chosen architecture.

Deploying the WLAN Companywide

With design issues tested and resolved, the next challenge was how to quickly deploy hundreds of sites and thousands of access points in more than 80 countries. Cisco IT assembled a Global Program Management team under the direction of a global program manager. Representatives were selected from each of the four regions worldwide.

Responsibility for deployment within each region was delegated to a regional project manager and local team. Region-specific project managers determined and managed an implementation schedule within their own region. Local teams communicated progress at a weekly global deployment meeting. Several sites were deployed concurrently across and within regions. Serial installation by one global team might have taken years. Instead, almost all sites were deployed within a 4-month timeframe in 2000, with the exception of India, which was delayed due to local regulatory issues with 802.11 standards.

The Global Program Management team recognized that using Cisco employees exclusively to perform WLAN installation tasks was not the most cost-effective use of resources. Instead, vendors were hired for the bulk of the work. These vendors had to meet a minimum set of requirements established by the Global Program Management team. The local contractors had to be trusted, were required to have an existing relationship with Cisco, and had to be wireless certified. An emphasis on competitive bidding helped to minimize capital investment. Each local team selected their contractors based on their familiarity with the local market.

Site Survey

The Global Program Management team established a guideline for the deployment process to be followed worldwide. The first step in deployment was the site survey. The purpose of a site survey is to determine placement of access points and antennas to maximize coverage throughout a building and minimize “dead spots.” Each building is unique. Structures that appear similar can behave and interact differently with radio signals due to differences in metal composition, conduction, environmental factors, elevators, interference, etc. A formal and well-defined site survey was, and remains, critical to a successful WLAN deployment.

In many locations, trusted vendors performed the site surveys, while in some locations, such as San Jose, Cisco IT employees participated in the process. Using a floor plan, the site survey teams estimated the location of each access point on each floor. Then, using a laptop loaded with the Cisco Aironet Client Utility, the team physically measured signal strength, coverage, and cell overlap throughout the space.

Cabling

After the site survey was complete, local contractors (different from the site survey firm) installed the cabling and physically placed, secured, and connected the Cisco Aironet access points. Each access point was provided with two cables: one for data connectivity and one for console access.

Access-Point Configuration

With the access points connected to the network and powered up, it was time to configure them. In actuality, the access points were preconfigured with a “generic” configuration that allowed Cisco IT to communicate with them and “push” the final production configuration. This configuration was in compliance with the global design specifications established by the Architecture team. Most critical were the IP address, channel assignment, and transmit power settings. Assigning the wrong channel, setting the transmit power too high, or assigning a duplicate IP address could all create performance problems. Using generic and standardized access-point configurations helped to ensure consistent access-point settings across the entire deployment, simplified troubleshooting, and provided Cisco IT with greater control of individual access points.

Testing

Following configuration, the same contractor that performed the site surveys returned to conduct post-installation acceptance tests on the WLAN in each building. Dummy user accounts with limited access rights were provided, which enabled the contractors to test basic WLAN authentication and services. The globally consistent and clearly defined acceptance tests included the ability to roam from access point to access point and transfer a file at a minimum designated speed. Tests also helped to ensure the correct overlap between access-point cells and that there were no dead spots.

Distribution of Wireless Network Cards and Instructions

At the time of the global WLAN deployment, distribution of Cisco Aironet 802.11b WLAN client adapters (wireless cards) presented a unique challenge. Cisco had to smoothly distribute more than 35,000 wireless cards in a timely and controlled manner. Not only did the cards represent a significant percentage of the total program cost, but Cisco IT needed to update each card with the latest firmware before delivering it to each user. Furthermore, it was important that the cards were not distributed to users until their sites were completed and had successfully passed the post-installation acceptance test.

In most locations, the task of inventorying, verifying firmware level, and distributing cards and operating instructions to users was given to the same vendor that performed acceptance tests. Cards were shipped to the local vendor’s distribution center where the correct firmware level would be verified or updated as appropriate. When vendors went out to perform acceptance tests, they recorded serial numbers, assigned cards to a local user ID, and passed the cards out to users at the local site. At the same time, the vendor distributed user fact sheets (frequently asked questions, technical tips, etc.) and instructions on how to contact technical support if necessary. Setting user expectations and providing comprehensive information were critical to minimizing support calls.

Today, Cisco uses both Cisco Aironet access points and Cisco Compatible client devices in its network. Cisco Compatible client devices include laptops, personal digital assistants (PDAs), Wi-Fi phones, and other devices with built-in wireless antennas. Using these devices provides Cisco employees with a variety of licensed Cisco infrastructure innovations and enhancements for its WLANs including advanced enterprise-class security, extended air RF management, and enhanced interoperability.

Managing the WLAN

To date, more than 3100 Cisco Aironet access points have been deployed worldwide, supporting more than 35,000 users. This requires a robust management capability. Because a management device was not available in 2000, the

Cisco wireless network was managed through Enterprise Management, an internally developed Web-based enterprise-management framework.

Today, Cisco IT also uses the CiscoWorks Wireless LAN Solution Engine (WLSE), a Cisco appliance for managing WLAN deployments. CiscoWorks WLSE, released in 2002, is a component of the Cisco Structured Wireless-Aware Network (SWAN). Cisco SWAN provides WLAN network, host, and radio management, assisted site surveys, interference detection, self-healing, and rogue access-point detection capabilities. Cisco SWAN extends "wireless awareness" into important elements of the network infrastructure, providing the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations have come to expect from their wired LANs. Cisco SWAN is a component of the Cisco Self-Defending Network strategy.

Rogue access points are of particular concern for all WLAN deployments. All rogue access points create an unsecured WLAN connection that puts the entire wired network at risk. Cisco and all companies with WLAN deployments need to be able to detect both employee and malicious rogue access points. Cisco has made a strong effort to emphasize to its employees that they should not install their own access points. Like Cisco, many companies are finding that employee-installed rogue access points are becoming more common as the demand for wireless networking increases, the cost of access points decreases, and access-point installation becomes easier. Deploying a corporate-sanctioned WLAN helps to reduce and in many cases to eliminate unauthorized, employee-installed access points. It is worth noting that the number of rogue access points detected has decreased significantly since Cisco IT deployed WLAN s worldwide. Malicious rogue access points, while much less common than employee-installed rogue access points, are also a security threat. Malicious rogues present an even greater risk and challenge because they are intentionally hidden from physical and network view.

CiscoWorks WLSE continually scans the Cisco wireless network for rogue access points through persistent security-policy monitoring and enforcement of WLAN security best practices. Whenever rogue access points are detected, CiscoWorks WLSE issues an alert and shuts down the switch port to which the access point is connected. Also, because Cisco IT uses Cisco Aironet and Cisco Compatible client devices that can participate in scanning the RF environment for rogue devices, the Cisco WLAN is more likely to find rogue access points than a WLAN deployment that is not engaging client devices to participate in air or RF monitoring.

Cisco Service and Support Levels

Network devices, systems, and applications on the Cisco global network are managed according to levels of impact to the business. Service or support levels fall into four categories:

Priority 1 (P1) —Immediate and severe business impact: revenue loss (actual not postponed); or inability to make or ship product; or inability to develop code or product; or inability to meet contractual, legal, or government-imposed processing deadlines; or impact to external Cisco customers, partners, or supplier processes with negative implications to relations, market perception, or revenue; or engineering groups unable to work on a critical customer build or fix or other critical account issue.

Priority 2 (P2) —Adverse business impact: inability of an organization (or organizations) within Cisco to perform daily operations such that it is essentially idle; or direct and critical impact to executives within the company, or to development, test, disaster-recovery, or staging environment for a P1 service or system.

Priority 3 (P3) —Low business impact: inability of multiple users to perform their daily tasks such that they are essentially idle; or impact to a single user under an approved, documented SLA requirement, or to a development, test, disaster-recovery, or staging environment for a P2 service or system.

Priority 4 (P4) —Minor or no business impact to Cisco: a question or new service request, or a problem that keeps one employee from performing part of a job function.

Within this support-level structure, Cisco secure access control servers (ACSs) are managed as a P2. The wireless network itself was originally managed as a P4 because it was considered a secondary network to the wired network. However, due to widespread adoption and usage within Cisco—more than 25 percent of employees now use wireless connectivity as their primary or only means of connection to the network—support for the WLAN has become equivalent to P2.

RESULTS

Cisco WLANs are now fully deployed worldwide. More than 3100 Cisco Aironet 1300, Aironet 1200, Aironet 1100, and Aironet 350 series access points have been installed at more than 280 sites in 85 countries. The network has more than 40,000 Cisco Aironet and Cisco Compatible wireless clients and more than 35,000 users—every Cisco employee.

Adoption has been much greater than anticipated. According to a Voice of the Client survey conducted in 2002, 97 percent of Cisco employees use wireless on a regular basis, at least once a day, and 25 percent use it as their primary or only method of access.

In spite of more than 35,000 users and 40,000 clients associated with the wireless network, the Global Technical Assistance Center (Cisco IT's internal technical-support division) receives an average of just 1000 WLAN-related calls per month; the equivalent of just 0.35 calls per employee per year. This low number is credited to a concerted effort to properly set user expectations from the beginning through user training. Based on this figure, total annual support costs per user average a mere US$19.00.

Cost Benefits and Productivity Gains

The Cisco wireless network is enabling users to gain productive time, be more responsive, and increase collaboration throughout the workday and everywhere they work. Some of these user productivity-enhancing scenarios include the following:

- Instant network connectivity while away from their desk (and in other buildings)
- Ability to turn any area, any chair, or any table into a work place if needed at any time
- Having access to online data during meetings
- Ability to work after arriving early to meetings and before meetings start
- Ability to work during portions of meetings that are not relevant to each attendee
- Ability to poll people not attending a meeting using instant messaging (IM) to help in decision making
- Network connectivity for large groups in one room without having to set up a network hub or switch
- Network access in communications rooms without disturbing active equipment
- More effective and efficient employee, partner, and customer collaboration with extended access to critical business applications

Cisco IT has attempted to quantify the global productivity benefits of the WLANs. A custom study released in November 2003 entitled "2003 Wireless LAN Benefits Study" (see http://newsroom.cisco.com/dlls/hd_111203b.html for more information) conducted for Cisco by independent research firm NOP World Technology confirms that WLANs substantially increase productivity. The study queried end users and IT network administrators from more than 400 medium-sized and large organizations in the United States using WLANs. Most notably, end users in the study reported that using WLANs increased their productivity by as much as 27 percent, largely because they can stay connected to the network on average 3.75 hours more hours per day and gain 1.5 hours in productivity. This equated to US$14,000 savings per year per employee.

However, Cisco IT undertook its own cost-benefit estimate. It was assumed that just 10 minutes of productive time would be saved per day per employee. Given 230 seven-hour work days per year, or 96,600 work minutes per year, at an average fully loaded cost of each employee of US$120,000 per year, the average cost per work minute equals US$1.24. Therefore, 10 minutes saved multiplied by US$1.24 multiplied by 230 work days equals US$2852 per employee, and multiplied by 32,500 employees totals US$92,690,000 in companywide savings per year.

10 minutes saved x $1.24 x 230 work days = $2852 per employee x 32,500 employees = US$92,690,000

But not all employees might gain 10 minutes per day, so Cisco IT took an even more conservative approach. Rather than assuming users saved 10 minutes per day, Cisco IT safely estimates a figure of 10 minutes per user per week**.** This provides for an annual productivity benefit of US$18,358,000 in companywide savings. [1]

In calculating the financial benefits of the WLAN, the underlying costs of providing the service must be figured in to determine the true net benefit. These include the cost of deploying the WLAN, the cost of client devices—for example, wireless network interface cards (NICs or wireless-ready laptops), the cost of managing the WLAN, and the cost of securing the WLAN. Cisco calculated the total cost of providing WLAN service to each employee is about US$0.72 per day. Compare that to the cost per employee per minute of about US$1.25 and it can be seen that Cisco achieves a payback in less than one minute of productivity gain per employee per day.

LESSONS LEARNED

Over the past four years, Cisco IT has gained first-hand experience in deploying and maintaining WLAN technologies worldwide. Following are some of the lessons learned in that effort and new features and capabilities implemented since initial deployment.

Network Security

Security issues impacting the WLAN arose in 2002 with new attacks known as the Fluhrer, Mantin, and Shamir attacks designed to crack WEP, the link-layer security protocol for 802.11 networks. A research team at Rice University, using a passive attack, was able to recover the 128-bit secret key used in a production network by exploiting a design failure in the WEP standard. Cisco IT perceived that, even with dynamic keys used in Cisco LEAP, network intruders might be able to penetrate the Cisco wireless network by snooping a sufficient number of packets. After WEP keys are known, network intruders can gain access to the network.

To improve the security of the WLAN, the Cisco Wireless Networking Business Unit developed the Cisco Wireless Security Suite. This solution focuses on access control and privacy and is a component of the Cisco Self-Defending Network strategy. Robust WLAN access control, also called authentication, prevents unauthorized users from communicating through access points. Strong WLAN access-control measures help ensure that legitimate client stations associate only with trusted access points rather than rogue or unauthorized access points. The privacy of transmitted WLAN data is protected when that data is encrypted with a key that can be used only by the intended recipient. Encrypting data helps ensure that it remains uncompromised throughout the sending-and-receiving transmission process.

The Cisco Wireless Security Suite provides robust wireless security services that closely parallel the security available in a wired LAN. It supports IEEE 802.1X authentication using Extensible Authentication Protocol (EAP) types and Temporal Key Integrity Protocol (TKIP) encryption. TKIP includes message integrity check, per-packet key hashing, and Broadcast Key Rotation (BKR). Implementations of these new technologies are included by the Wi-Fi Alliance under the Wi-Fi Protected Access (WPA) certification and in the IEEE 802.11i standard.

TKIP defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV), a counter that increments with each frame in encrypted packets, to deduce the encryption key. TKIP hashes or encrypts the IV before it is used to create a new encryption key. The packet-encryption key changes for every new IV (each new

[1] For an even more conservative approach, if only half of the users were to gain 10 minutes per week, the savings would total $9,179,000 per year. Cisco IT believes the real savings are somewhere between the $18.358 and $9.179 million estimates.

frame). This removes the predictability that an intruder relies on to determine the encryption key by exploiting IVs. (For a definition of TKIP, see http://www.devx.com/wireless/Door/11455. For more information on TKIP read the Cisco Aironet Wireless LAN Security Overview http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html or SAFE: Wireless LAN Security in Depth—Version 2 http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a008009c8b3.shtml.)

Message integrity check prevents bit-flipping and replay attacks. During these attacks, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The message integrity check adds a few bytes to each packet to make the packets tamper-proof. Message integrity check is similar to cyclical redundancy check (CRC) and can detect if a network intruder has intercepted and changed a packet between its source and destination.

Broadcast Key Rotation enables the network administrator to set the shared broadcast key to time out, causing a new broadcast key to be generated. This procedure mitigates passive attacks attempting to determine the broadcast key from weak initialization vectors.

Cisco IT has also implemented a policy to require long, complex passwords with a mixture of upper and lower case, numeric, and extended characters. Cisco recommends that all WLAN deployments implement a secure password policy. Read more about strong passwords in section 5.2.2 of the 802.11 Wireless LAN Security White Paper at http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b469f.shtml.

Site Surveys

From the beginning, Cisco IT had established a policy requiring a site survey for every building with a WLAN. But some buildings received either cursory or no site surveys because a number of buildings on the San Jose campus and other locations appeared to have the same footprint and floor layout. To save time and reduce costs, the local WLAN deployment team used a uniform approach to place access points. Ultimately, the assumption that this approach for WLAN deployment could effectively replace site surveys was incorrect. More time and effort was spent after deployment to adjust the WLAN in each individual location than would have been spent performing a proper survey for each individual building initially. Cisco recommends that each location perform a site survey to reduce installation costs and ongoing maintenance requirements.

Better diagnostic tools to identify sources of radio interference would have further eliminated much of the post-installation fine-tuning. Even though site-survey tests had indicated adequate signal strength, client devices were unable to associate with access points in some isolated circumstances. The cause was later determined to be either rogue access-point devices or malfunctioning laptops transmitting signals that created interference. Today, Cisco IT uses Cisco SWAN and its management device, the CiscoWorks WLSE, to pinpoint sources of interference and rogue devices.

As a result of experience gained over the first two years of operating the WLAN, new site-survey guidelines were adopted. The new design standard calls for smaller cells to allow for a higher density of access points. For example, in San Jose, according to the 2000 deployment guidelines, the typical building had six access points per floor. The new 2004 standard calls for eight per floor. This provides better coverage “at the corners” where so many Cisco conference rooms are located. Cisco IT is also evaluating even higher-density deployments and now recommends a user-to-access-point ratio of approximately 10:1 to support new services (such as voice and video), and provide more available bandwidth to users. Also in some locations, additional high-speed 802.11a or 802.11g networks are being deployed.

Provisioning Tools

In the original deployment guidelines, Cisco IT planned to manually configure each of the 3000+ access points. As early as the pilot deployment, IT realized that manually configuring access points and providing firmware and software updates was not an efficient, scalable methodology. The large-scale deployment of the WLANs required automated provisioning. In 2000, Cisco IT adapted the capabilities of Enterprise Management to automate the provisioning process. Today, the CiscoWorks WLSE is used for this task.

Cisco Secure ACS Remote Authentication

When originally deployed, each Cisco Secure ACS contained AAA information for users within the local domain, and there were four domains worldwide. If a user from San Jose traveled to Australia and attempted to log on to the WLAN, the local Cisco Secure ACS server would have no record of that user. The request would have to be sent over the WAN to the San Jose Cisco Secure ACS for authentication. Long delays in the delivery of an authentication request could result in a time-out, which could trigger a new authentication request (again over the WAN), and the process could repeat. This would only repeat itself for a short time before the client would time out its request, leaving the user with no network connectivity. Furthermore, similar requests from other users could collectively generate an authentication storm, overburdening the Cisco Secure ACS and impacting other users trying to log on to the WLAN.

Cisco IT solved the timeout problem by collocating Active Directory domain servers with each Cisco Secure ACS. The entire authentication process can now occur in one location, eliminating the need to go over the WAN to the remote server. The authentication-storm problem was solved by implementing an authentication back-off algorithm. Rather than repeatedly attempting to authenticate every second or two, if the authentication is unsuccessful the first time, the system waits 10 seconds on the second attempt, and 30 seconds on the third attempt.

Cisco Secure ACS Failures

During the initial deployment, and with older versions of Cisco Secure ACS software, users occasionally experienced authentication failures. When investigated, the AAA architecture appeared to be functioning perfectly, yet users were still unable to log on. Detailed analysis showed that the Cisco Secure ACS RADIUS service was failing, yet the server remained fully functional. The solution was to create a synthetic Cisco LEAP transaction process, initially on Enterprise Management, but now also part of CiscoWorks WLSE. There are now two monitoring processes. The network-management system confirms that the Cisco Secure ACS is online and responding to network pings, and the synthetic LEAP transaction process confirms that authentications are functioning correctly.

Setting User Expectations

Since global WLAN deployment, Cisco IT has striven to educate users about both WLAN capabilities and restrictions. For example, WLAN service does not extend coverage outside of buildings. This improves security, yet requires users to reauthenticate when traveling from one building to another. On occasion, when a large number of WLAN users are crowded together in a small area, such as a conference room or cafeteria, some users find it difficult to log on, while others find performance is reduced. Users are encouraged to avoid multigigabyte file transfers, such as hard-drive backups, over the 802.11b wireless network, because they can negatively impact the performance level for every other user sharing the same access point. Wireless voice over IP (VoIP) works well, with only minor delays in crowded areas where many users share the finite bandwidth, or while large files are being simultaneously transferred on the WLAN.

As with all WLANs, performance depends on signal strength and quality, which can vary within a few feet in some areas. Because the 802.11 standards work in unlicensed RF band, free-to-use spectrums, situations exist where interference from other nearby 2.4-GHz devices may affect signal strength. This not only includes other wireless networks installed by neighboring companies or users, but also several common household devices such as microwave ovens, wireless telephones, Bluetooth devices, or even baby-monitors. Interference is not usually an issue in locations with 802.11a 5-GHz deployments. Helping users to understand these constraints as well as implementing new policies, such as the increased access-point density and reduced users-to-access-point ratio, has helped users worldwide to have a very positive experience with the Cisco WLANs.

New WLAN Features

Since 2002, when the wireless network was completed, several new products, services, and capabilities have been added that dramatically enhance the WLANs and provide new services for Cisco employees and guests. These new enhancements include the Cisco Wireless IP Phone 7920 using quality of service (QoS), Cisco IP Communicator (a software-based IP phone often called SoftPhone), wireless networking for guests, and the implementation of wireless VLANs.

The Cisco Wireless IP Phone 7920 is an easy-to-use IEEE 802.11b wireless VoIP phone that provides comprehensive voice communications in conjunction with Cisco CallManager and Cisco Aironet access points. As of October 2004, there are more than 1200 Cisco Wireless IP Phone 7920 users worldwide. The Cisco Wireless IP Phone 7920 requires QoS. QoS is critical to voice and video because, unlike data, any packets lost have a negative impact on voice quality, and can even terminate the call in extreme circumstances. QoS poses a number of challenges for Cisco IT because QoS voice standards for WLANs are still under development by the IEEE 802.11e working group. Cisco IT has managed this issue by creating a separate VLAN for voice devices and has implemented a prestandards QoS. After 802.11e is ratified, Cisco IT will adopt this standard and will support the new Wi-Fi Multimedia (WMM) certification introduced in September 2004.

Cisco IP Communicator is a software-based application that delivers enhanced telephony support through personal computers. Cisco IP Communicator has the features and functions of a full-featured Cisco IP phone, including the ability to transfer calls, forward calls, and conference additional participants to an existing call.

Cisco IT is deploying a global, scalable architecture based on a Cisco Broadband Building Service Manager (BBSM) model to provide wireless networking for guests. Cisco BBSM is an authentication, authorization, and accounting router, built on Microsoft Windows 2000 technology, that controls access to the Internet for building-centric applications such as hotels, apartments, and multitenant offices. Cisco currently provides guest WLANs to visitors at its Executive Briefing Centers. This access will be extended to all Cisco locations, so that guests visiting Cisco at any global site can obtain secure wireless connectivity to the Internet and their corporate resources through VPN.

Today, Cisco Aironet access points support up to 16 VLANs in single-mode or dual-mode operation. This has allowed Cisco IT to differentiate LAN policies and services—such as security and QoS—for different users. For example, some locations use different VLANs to segregate employee traffic from guest traffic, and further segregate those traffic groups from high-priority voice traffic. Cisco IT is using multiple VLANs to segregate traffic to and from wireless clients with varying security capabilities with differing security policies. Implementing VLAN segmentation has dramatically increased WLAN manageability and security.

NEXT STEPS

Cisco IT has been at the forefront in deploying WLANs and, in doing so, has learned through first-hand experience what worked and what needed to be modified. Following are some of the lessons learned in the deployment of the global Cisco wireless network:

- Adoption of Cisco SWAN, CiscoWorks WLSE, and the Cisco Catalyst 6500 Series WLSM
- Cisco Centralized Key Management
- EAP-FAST
- Migration to Dual-B and 802.11a or 802.11g
- Home Wireless Deployments
- Pocket Office
- Wireless IP Handsets
- Next-Generation Workspace

- Adoption of Cisco SWAN, CiscoWorks WLSE, and the Cisco Catalyst 6500 Series WLSM

Cisco IT has adopted Cisco SWAN, which provides the framework to integrate and extend wired and wireless networks to deliver the lowest possible total cost of ownership for companies deploying WLANs. Cisco SWAN extends “wireless awareness” into important elements of the network infrastructure, providing the same level of security, scalability, reliability, ease of deployment, and management for WLANs that organizations have come to expect from their wired LANs. Cisco SWAN is an important step to achieving an intelligent network that easily combines today’s separate wired and wireless networks.

One of the important components of Cisco SWAN is CiscoWorks WLSE, a centralized, systems-level solution for managing the entire Cisco Aironet WLAN infrastructure. The advanced RF and device-management features of the CiscoWorks WLSE simplify everyday operation of WLANs, support smoother deployments, enhance security, and maximize network availability, while reducing deployment and operating expenses. CiscoWorks WLSE enables Cisco IT to provide radio management and radio-based rogue access-point detection, self-healing WLAN capabilities, and enhanced support. CiscoWorks WLSE will give Cisco IT an end-to-end view of the WLAN beyond the access point.

Another important component of SWAN is the Cisco Catalyst® 6500 Series Wireless LAN Services Module, which provides secure, campuswide, Layer 3 roaming capabilities for large sites with multiple Layer 2 domains that require roaming. The module also simplifies wireless network management and deployment, supports up to 6000 WLAN users and 300 Cisco Aironet access points, and extends Cisco Catalyst 6500 Series rich, intelligent network services to the wireless edge.

Cisco Centralized Key Management

Cisco IT plans to implement Cisco Centralized Key Management (Cisco CKM), which provides fast, secure roaming. This feature will be particularly important for wireless voice and video services such as wireless IP phones. Cisco CKM-authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. Using Wireless Domain Services (WDS), an access point on the WLAN network or the Cisco Catalyst 6500 Series Wireless LAN Services Module acts as a subnet context manager (SCM) and creates a cache of security credentials for Cisco CKM-enabled client devices on the subnet. The SCM’s cache of credentials dramatically reduces the time required for reassociation when a Cisco CKM-enabled client device roams to a new access point.

EAP-FAST

Cisco IT is migrating from Cisco LEAP to a new and improved EAP mechanism known as Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), which addresses the weaknesses of Cisco LEAP that were inherited from its use of Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2). (See Cisco Response to Dictionary Attacks on Cisco LEAP at http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html) Cisco developed EAP-FAST to support customers who cannot enforce a strong password policy and want to deploy an 802.1X EAP security type that does not require digital certificates, supports a variety of user and password database types, supports password expiration and change, and is flexible, easy to deploy, and easy to manage. Support for EAP-FAST is provided in client adapter firmware and the AAA server. With EAP-FAST, a username, password, and shared secret are used by the client adapter to perform mutual authentication with the RADIUS server through an access point.

Migration to Dual-B and 802.11a or 802.11g

In 2005, Cisco will replace all existing 11-Mbps 802.11b access points with Cisco 1130a or 1130g tri-mode access points. It is important to note that 802.11g networks that contain 802.11b radios will force the network to work at a reduced rate from 54 Mbps. This rate reduction accommodates the 802.11b devices because 802.11g packets must add information to the headers when 802.11b access points are simultaneously used with 802.11g access points.

Home Wireless Deployments

As part of the Enterprise Class Telecommuter (ECT) program, Cisco IT will implement a fully managed, end-to-end wireless solution that includes home WLANs. Up to now, wireless services for telecommuters have been self-managed. Cisco IT is already deploying a standard secure router to users' home offices to support secure VPN access to corporate resources for multiple devices. Initially this will be for PC access, but will incorporate access for wireless access points and for IP phones in the near future.

Pocket Office

Cisco is adopting a framework, unofficially known as the Pocket Office, to provide a secure, scalable, and sustainable support model for smart wireless Cisco Compatible handheld devices (smart phones, PDAs). Connecting such devices in the past has been an improvised process with no definitive standards or guidelines. This will change rapidly as Cisco IT develops standards for securing wireless PDAs, and for supporting secure communication between PDAs and e-mail servers. This will allow PDAs to be used to retrieve and respond to e-mail, as well as to browse corporate Websites and the public Internet for critical and fast-moving corporate information.

Wireless IP Handsets

Cisco IT will continue to deploy the latest generation of Cisco WLAN handsets. These devices are especially useful for employees who move between buildings or have no particular fixed office space to support a wired IP phone. Many executives, who spend more time in meetings than in their offices, have found these wireless IP phones extremely useful.

Next-Generation Workspace

Cisco IT has already deployed a proof-of-concept, next-generation workplace with higher access-point densities, as the trial cost-saving use of space and reliance on wireless as the primary or sole network-access technology. Reliance on wireless for both data and voice streams more than doubles the number of people using each access point. This proof of concept is a test of various technologies and creative use of flexible workspaces; it encourages collaboration and reduces real-estate costs by supporting shared workspaces that are not assigned to individuals but rather are used as needed. The reliance on wireless as the primary access technology has not only saved in real-estate costs but also has reduced infrastructure-cabling costs.

Cisco IT routinely provides about two to three access points per quarter-floor of its San Jose buildings; in the flexible workspace proof of concept, IT has deployed 10 access points, for the following reasons:

There are more than twice the number of employees per 1000 square foot in this trial environment.

Employees are encouraged to cluster in small areas, which can increase the density.

Many employees are using Cisco IP Communicator, a PC-based software telephone, over the same PC wireless connection. This requires additional wireless bandwidth to accommodate the two data streams.

IT tries to ensure that there are only about six to eight employees at one time associated with any access point. Today this is monitored manually by taking “snapshots” of the number of associations on each access point; Cisco IT is planning to install a CiscoWorks WLSE to automatically track the number of associations.

During the trial period, employees clustered in one corner where there were windows on both walls and the access points in that area were experiencing heavy loads. Employees complained of poor performance in that area, and IT engineers looking into those access points found more than 30 laptops associated with the access points there. IT responded by adding an access point to that area.

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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