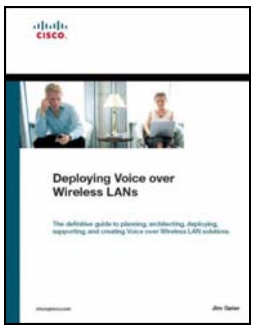
Chapter 2, VoWLAN System Components

Author: Jim Geier

Principal Consultant, Wireless-Nets, Ltd.

Email: jimgeier@wireless-nets.com



This chapter is a sample from the book *Deploying Voice over Wireless LANs*, written by Jim Geier and made available with permission from Cisco Press.

Wireless Nets, Ltd.

Independent Consulting Services

www.wireless-nets.com

Objectives

Upon completing this chapter, you will be able to

- Identify the primary components of a VoWLAN system.
- Describe specific applications of alternative VoWLAN components.
- Differentiate the benefits of traditional “thick” access points and wireless switched solutions.

CHAPTER 2

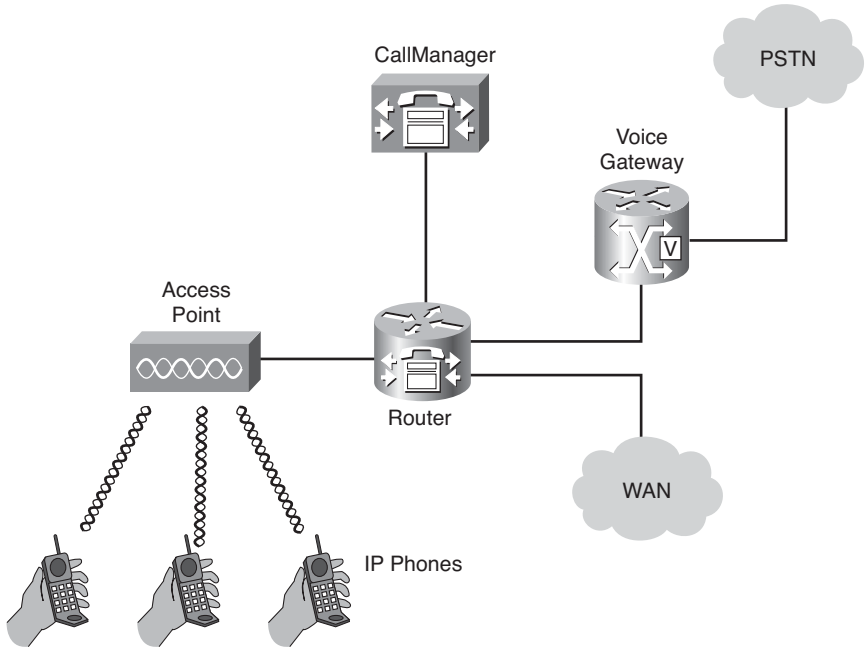
VoWLAN System Components

This chapter defines the components that are part of a VoWLAN system, such as phones, client software, call managers, and so on. Examples of actual components are given, with emphasis on Cisco products. Descriptions of how VoWLAN integrates with existing systems found in enterprise settings are also given.

VoWLAN System Overview

A general VoWLAN system architecture consists of components that provide mobile phone usage throughout a facility or campus. Figure 2-1 illustrates the interconnection of these components.

Figure 2-1 *Primary VoWLAN System Components*



The following is a brief description of each primary component of a VoWLAN solution:

- **Wireless IP Phone**—This appliance is similar to a cell phone; however, it includes a wireless LAN adapter that interfaces with a wireless LAN for connectivity to the telephone system. The user can place calls directly to another user, similar to an office telephone system, or make calls external to the facility through the Public Switched Telephone Network (PSTN). The Cisco 7920 is an example of a wireless IP phone.
- **Call manager**—The call manager on a Voice over Internet Protocol (VoIP) network takes the place of a traditional private branch exchange (PBX). It processes calls on the network and handles functions such as registering IP phones, administering dial and route plans, and managing voice mail. The Cisco CallManager and CallManager Express are examples of a call manager.
- **Voice gateway**—This device interfaces Internet Protocol (IP) telephony to other types of networks and systems. For example, a gateway can interface a VoIP network to the traditional PSTN. This can provide a path for primary communications between internal IP phones and users of standard phones. And the gateway connection to the PSTN can act as a backup in case the wide-area network (WAN) becomes unavailable.
- **Wireless LAN infrastructure**—A wireless local-area network (LAN) handles the transport of wireless VoIP calls throughout the facility. As a result, telephone users can freely move about their workspace. The Cisco 1200 and 1300 access points are popular wireless LAN infrastructure components.

The wireless LAN adapter in the user's wireless IP phone must connect to an access point on the network before the user can make calls. When a user initiates a call, the request travels through the access point and across the wired network to the call manager, which processes the request. For example, if User A is calling User B, the call manager rings User B's phone and then makes a connection between the two users. To provide mobility, the wireless LAN adapter in the wireless IP phone of the roaming user reassociates with other access points throughout the facility as needed. The call between the two users continues uninterrupted, assuming that the transition (roaming delay) between access points is less than 100 milliseconds. If the delay is more, calls generally drop.

If a user is dialing an external phone number, the call manager forwards the call to the PBX or the Internet, which completes the external call. If the PBX is not equipped to handle IP traffic directly, an intermediate VoIP gateway is needed to translate the VoIP traffic into analog signals. The PBX directs external calls coming into the facility to the call manager, which then forwards the call using VoIP signaling to the applicable wireless IP phone.

Cisco 7920 Wireless IP Phone

The Cisco 7920 Wireless IP Phone, shown in Figure 2-2, interfaces with Cisco access points and works with Cisco CallManager. The 7920 has similar features as office phones and wireless smartphones, such as directory of incoming calls, call waiting, call transfer,

conference calling, voice message indication, local phone book, and multiple ring tones. It is compatible with Cisco CallManager Version 4.1, 4.0, 3.3 and later, and CallManager Express Version 3.2, using the Skinny Client Control Protocol (SCCP).

Figure 2-2 *Cisco 7920 Wireless IP Phone*

The following is a summary of the 7920 features:

- **IP address assignment**—This is done through Dynamic Host Configuration Protocol (DHCP) or is statically configured by an administrator.
- **Firmware updates**—After it is connected to an access point, a company can perform firmware updates over the wireless LAN by using the Trivial File Transfer Protocol (TFTP) server and the Cisco web interface.
- **VLAN support**—The 7920 implements IEEE 802.1q (virtual LAN) configuration and Cisco-proprietary virtual local-area network (VLAN) technology Interswitch link protocol.
- **Site survey functions**—Using a 7920 when performing Radio Frequency (RF) site surveys is possible. This feature takes into consideration the specific wireless LAN adapter, antenna, and physical construction of the handheld device.
- **Security**—The 7920 implements a variety of security protocols, including IEEE 802.1X Cisco LEAP authentication, 40- and 128-bit static Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA Pre-shared Key (PSK), Cisco Centralized Key Management (CCKM), Temporal Key Integrity Protocol (TKIP), and Message Integrity Check (MIC). Users can also utilize an optional phone unlock password.

- **Wireless technology**—The wireless adapter inside the 7920 implements IEEE 802.11b, direct sequence with automatic rate or static data rates of 1, 2, 5.5, or 11 Mbps (megabytes).
- **Transmit power**—The wireless LAN adapter transmits at 1, 5, 20, 50, or 100 milliwatts, depending on configuration settings.
- **Range**—The 7920 can communicate successfully at ranges of 500–1,000 feet from the connected access point, but the actual range depends on the environment.
- **Access point support**—The 7920 interfaces with Cisco Aironet access points, including the 1300, 1200, 1130, 1100, 1000 Lightweight, 350, and 340 series. The access point must be set to support 802.11b-only or mixed 802.11b/g mode. Other configuration parameters, as discussed in detail in Chapter 8, "Installing, Configuring, and Testing a VoWLAN System," are necessary to ensure effective operation of the phone.

NOTE Several other manufacturers offer wireless IP phones. For example, Linksys also has SIP phones, the WIP 300 and WIP 330, which integrate directly into Cisco CallManager. Also, Vonage offers a Wi-Fi phone for users to make calls from Wi-Fi hotspots.

Case Study: Acme Furniture Users Make Use of Cisco 7920 Wireless IP Phones

Brian, a division head of the Acme Furniture's manufacturing plant, is given a Cisco 7920 Wireless IP phone for making phone calls via the company's new VoWLAN system. The IT department has already configured the phone with the proper SSID, security settings, and extension number, but Brian can personalize the phone. He first sets the ring tone to sound unique to distinguish his phone from others. Brian uses the phone for the first time while on the manufacturing floor. After talking with the line supervisor, he learns that a change in the design of a new rocker requires some additional input from the design group before production can move forward. So Brian immediately uses his 7920 to locate the phone extension of the rocker's lead designer, Evan, and places the call. Evan is currently in a staff meeting, but he hears his unique ring tone and answers the call on the second ring. The problem in manufacturing has priority over the staff meeting, and he arrives on the manufacturing floor within a couple minutes. While en route, Brian and Evan continue discussing possible fixes for the issues. Brian then recalls the past, when extensive telephone tag due to fixed wired phones resulted in hours before they could mitigate a problem like this.

Cisco IP Softphone

The Cisco IP Softphone, shown in Figure 2-3, is a Microsoft Windows–based application that is an alternative to using the 7920 handset. Softphone installs on a laptop equipped with a wireless LAN card and enables a user to place calls over the VoWLAN system. You

can use Softphone as a standalone phone end station or in conjunction with a Cisco IP Phone. The software allows connections to the phone system when the laptop has an online connection to the Internet. This feature makes it handy to check voice messages and place calls from anywhere within the signal coverage of the VoWLAN system or just about anywhere you are online with the Internet. Using a phone headset with this configuration can be beneficial, especially if your laptop or PC does not have a microphone and speakers. The Softphone integrates with Lightweight Directory Access Protocol 3 (LDAP3) directories, which allows placing calls by looking up people by name or e-mail address. A drag-and-drop capability makes placing calls and scheduling conference calls relatively easy.

Figure 2-3 *Cisco IP Softphone Main Screen*

Case Study: Researcher Makes Use of Cisco IP Softphone

A chemical company located in the southwestern U.S. has a Cisco VoIP system and equips each employee with a wired VoIP desk phone. Before the company implemented the system, it found that mobility requirements were limited. The company did, however, deploy wireless LANs to provide coverage in several remote locations, such as conference rooms and laboratories. To provide mobile phone coverage in these remote places, the company equipped its staff with Cisco IP Softphone on their laptops to facilitate calls. This solution was preferred over purchasing 7920 Wireless IP Phone handsets for everyone because all employees have laptops. This configuration also takes advantage of the call forwarding function. Calls made to someone's desk phone (his or her primary phone number) simultaneously ring both the desk phone and the Softphone on the laptop. If the

person is sitting at his desk, he can answer the desk phone. When working somewhere else, the person can answer the Softphone. The call forwarding function makes this capability possible. To illustrate the versatility of this approach, Shanna, a researcher for the company, is working in a lab and finds that she needs to call an associate, Jared, to discuss a testing procedure that she is getting ready to commence. She does not have time to go track down Jared. Shanna uses her laptop to call Jared. Jared is working in an associate's office with his laptop. Shanna does not know this, so she calls Jared's primary phone number (his desk phone). Jared's desk phone and Softphone both ring, and he immediately answers her call from his Softphone and offers some tips on performing the test procedure.

Cisco CallManager

Cisco CallManager is a software-based call-processing component and extends traditional enterprise telephone system features and functions to packet telephony to IP phones. CallManager installs on Cisco 7800 series media convergence servers (MCS) and selected third-party servers. CallManager runs on a variety of operating systems. The older versions of CallManager run on Windows platforms, but CallManager 5 is Linux-based. CallManager Express runs on Cisco's Internetworking Operating System (IOS).

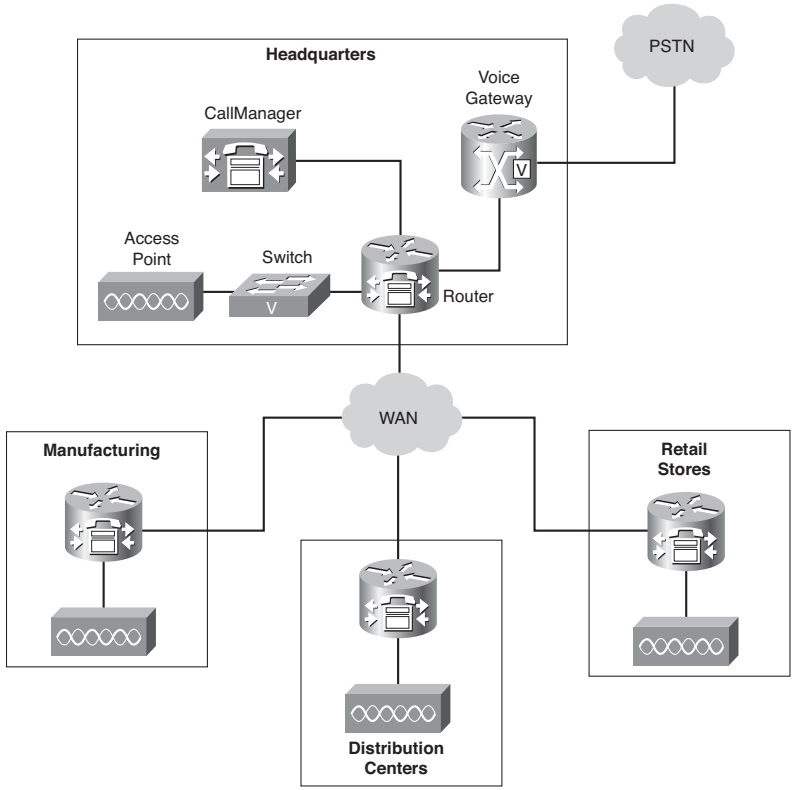
A company can deploy multiple Cisco CallManager servers and manage them as a single entity. Cisco CallManager clustering enables scalability from 1 to 30,000 IP phones per cluster. Security features verify the identity of the mobile devices and servers that they communicate with to ensure the integrity of data they are receiving. Encryption offers privacy of communications.

Case Study: Acme Furniture Chooses Cisco CallManager for Handling VoIP Calls

Acme Furniture, the hypothetical company introduced in Chapter 1, needs to select components for its voice IP telephony solution. The company has 750 employees located in corporate headquarters, a manufacturing plant, and multiple retail stores and distribution centers spread throughout the U.S. A WAN, which has plenty of capacity for the expected VoIP calls, interconnects all sites.

Debbie, the IT manager for Acme Furniture, chose Cisco's CallManager to provide call processing for users equipped with Cisco 7920 wireless IP phones. This choice enables a scalable solution that can fulfill the number of initial users and satisfy future growth. Acme will interconnect calls between its distributed sites through its existing wide-area network (WAN). Figure 2-4 illustrates the system component interconnections.

Figure 2-4 *Acme Furniture Voice Telephony System*



This system enables wireless VoIP communications among all of Acme Furniture's facilities. In addition, users can place and receive telephone calls from the Cisco 7920 IP Phones with standard telephone users via a gateway connection to the PSTN.

Cisco CallManager Express

To satisfy requirements for small offices, Cisco offers CallManager Express. This version of CallManager is simpler to deploy, administer, and maintain. It can handle from 24 to 240 users.

Case Study: Chemical Company Chooses Cisco CallManager Express for Handling VoIP Calls

A chemical company located in the southwestern U.S. consists of 120 employees located inside a single three-floor building. The company does not expect to grow the workforce. The company has been using a relatively old PBX for handling internal and external calls from standard analog telephones. To reduce costs associated with adds/moves and long-distance phone service, the company decided to deploy a mix of wireless and wired IP telephones to replace the existing analog system.

The company chose Cisco's CallManager Express because it can easily support the total number of users. In addition, the internal IT staff can easily install, configure, and manage the solution. CallManager Express handles all internal call processing and interfaces with the external world through a connection to the PSTN.

Linksys Wi-Fi Video Cameras

The Linksys Wireless-G Internet Video Camera, shown in Figure 2-5, captures and sends live high-quality video and sound over an 802.11g wireless LAN. The unit operates independently and does not require a connection to a PC. The video signals are sent directly over the wireless LAN.

Figure 2-5 *Linksys Wireless-G Internet Video Camera*

The following is a summary of the Linksys Wireless-G Internet Video Camera specifications:

- **Integrated web server**—Makes viewing captured video from web browsers possible.
- **Motion detection**—Automatically begins capturing video and sends an e-mail notification.

- **MPEG-4 compression**—Significantly reduces load on the network.
- **640 × 480 pixels resolution**—Good quality for most applications.
- **128-bit WEP encryption**—Encrypts the video contained within 802.11 data frames.

NOTE Keep in mind that even though the camera is wireless, it still needs to connect to electrical power. In addition, you may need to install the camera in a protective enclosure.

Case Study: Chemical Company Monitors Processes with Wireless Video

A chemical company located in the southwestern U.S. uses a Linksys Wireless-G Internet Video Camera to remotely monitor chemical mixing in one of its chemical plants. Telemetry instruments continually measure temperature and pressure of the processes, but having a human eye watch over the mixing process from time to time is also valuable. So, the company installed the wireless video camera at a good vantage point within the mixing room. This solution avoids needing to have one of the engineers personally monitor the process.

The wireless video camera connects over the wireless LAN to the nearest access point. System operators located in different buildings can occasionally view the process using a web browser on their PC. They point the web browser at the camera's IP address, and the video signals travel through the wireless LAN and over the company's wired network to the person's PC.

NOTE In addition to Linksys, consider using Wi-Fi video cameras from Axis Communications for applications where better quality is necessary.

NOTE Vocera Communications Systems offers a solution that includes users wearing Vocera Communications Badges and centralized Vocera System Software residing on a server that is attached to the network. This solution provides immediate communication between people wearing Vocera Communications Badges, which provide voice-controlled communication over an IEEE 802.11b wireless LAN. The badge includes a microphone, speaker, and display for showing caller ID or a text message. Vocera System Software runs on a standard Windows server and controls and manages call activity. Optional Vocera Telephony Solution Software enables users to make and receive telephone calls through their Badge.

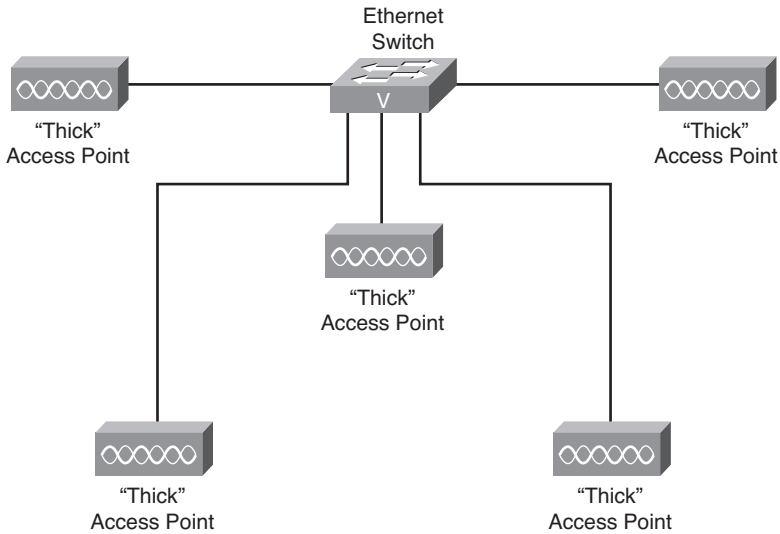
Wireless Network Infrastructures

A wireless voice telephony system requires an effective wireless network infrastructure. You can take advantage of traditional access points or make use of the newer wireless switches. However, ensuring that enough capacity exists and that roaming delays are short enough to avoid dropped calls is very important.

Traditional Access Point Networks

The customary approach for deploying wireless LANs includes the installation of multiple intelligent ("thick") access points that interconnect via a conventional Ethernet switched network, as shown in Figure 2-6. This distribution system provides coverage throughout a facility while enabling connections with servers and the Internet residing on the wired portion of a company's network. Companies have been deploying wireless LANs having this type of architecture for more than a decade.

Figure 2-6 *Cisco Traditional Access Point Network*



The access points implement functions of the 802.11 standard, such as medium access and association procedures. As users roam throughout the facility, their wireless client devices reassociate with an access point having the strongest beacon. Because the access points are the only wireless LAN devices on the network, the access points must contain a significant amount of intelligence to meet the essential elements of a wireless LAN that the 802.11 standards do not provide. The access points implement security and management functions in addition to basic radio connectivity.

When deploying VoWLAN solutions, a company may choose to use an existing access point network, which is usually the traditional "thick" access point architecture. This

certainly reduces the initial capital expenses for hardware. This sort of access point solution, however, can be costly to scale up in terms of coverage and performance because the access points are relatively expensive. For example, a company will likely pay $500 per access point to increase coverage by 30,000 square feet. In addition, more than one access point may be necessary to increase performance in the same area. For large implementations, the cost of access points becomes a major part of the total cost of ownership (TCO). Thus, the use of an existing access point solution may not be the best long-term option, especially if the company plans to scale up the network in the future to support more users.

The "thick" access point approach may also be costly to migrate to newer technologies. For example, a company may deploy an 802.11b/g network now and find that 802.11a or something else is necessary in three years to support higher-end applications. A company may experience a lower TCO if it needs to replace expensive access points with new ones in the future.

Access points within a traditional solution generally interconnect using standard switched Ethernet, the predominant type that supports wired connections in companies worldwide. A switch connects one user, such as an access point, to another without blocking access of other users. The switch improves throughput as compared to a shared hub because of the smaller resulting collision domains. Users do not have to wait until others are finished before sending data. A switch is necessary with VoWLAN systems to maximize performance.

Handoffs from one "thick" access point to another may be too slow to support VoIP applications when users roam. The problem here is that the combination of the access points and traditional Ethernet switches in this type of solution are not fast enough. For example, someone using a wireless LAN phone will likely experience a dropped call when roaming from one access point to another. Before depending on an existing wireless LAN for supporting voice applications, you should test the roaming delays, and they should be less than 100 milliseconds to minimize dropped calls.

The "thick" access point approach requires decentralized management to support the remote functions that the access points implement. Even if the "thick" access point manufacturer provides a centralized management system, the wireless LAN must handle the additional overhead traffic necessary to communicate regularly with the access point. This traffic may reduce the capacity of the wireless LAN, which precludes the deployment of some applications that could have provided additional benefits and resulting lower TCO.

Cisco has a complete line of traditional wireless LAN hardware that supports voice applications and addresses needs for enterprises, public networks, and homes. The following identifies currently available Cisco Aironet access points:

- **Cisco Aironet 1300 Series**—The Cisco Aironet 1300 Series Outdoor Access Point/Bridge is a multifunctional component that provides access point, bridge, and workgroup bridge functionality for network connections within an outdoor campus area. The 1300 series supports the 802.11b/g standards.

- **Cisco Aironet 1230AG Series**—The Cisco Aironet 1230AG Series has dual antenna connectors for extending range with optional antennas for enterprise solutions.
- **Cisco Aironet 1200 Series**—The Cisco Aironet 1200 Series includes a dual-slot architecture that allows flexibility when configuring radio cards for enterprise solutions. For example, a 1200 Series access point can include any combination of radio card technology, such as 802.11a and 802.11g.
- **Cisco Aironet 1130AG Series**—The Cisco Aironet 1130AG Series includes integrated antennas and dual 802.11a/g radios for enterprise solutions.
- **Cisco Aironet 1100 Series**—The Cisco Aironet 1100 Series offers an easy-to-install, single-band, 802.11b/g access point for enterprise solutions.
- **Cisco Aironet 350 Series**—The Cisco Aironet 350 Series is designed for small and medium-sized businesses. The Cisco Aironet 350 Series access point provides an ideal solution for customers who desire a nonupgradeable IEEE 802.11b solution. The 350 series supports the 802.11b standard.

All the access points can support IOS. The Cisco Aironet 350 can also support Vxworks.

Case Study: Warehouse Uses Existing Wireless LAN for VoWLAN Solution

A warehouse located in the northeastern U.S. has an existing wireless LAN that supports warehouse logistics functions. For example, warehouse clerks use wireless bar code scanners to perform inventory management. The wireless LAN consists of three Cisco Aironet 1200 access points, implementing IEEE 802.11b technology. A wireless site survey was completed a couple years ago to ensure a minimum of 15dB signal-to-noise ratio (SNR) signal coverage throughout the warehouse floor. The bar code application traffic over the network occupies only 5–10 percent of the overall capacity.

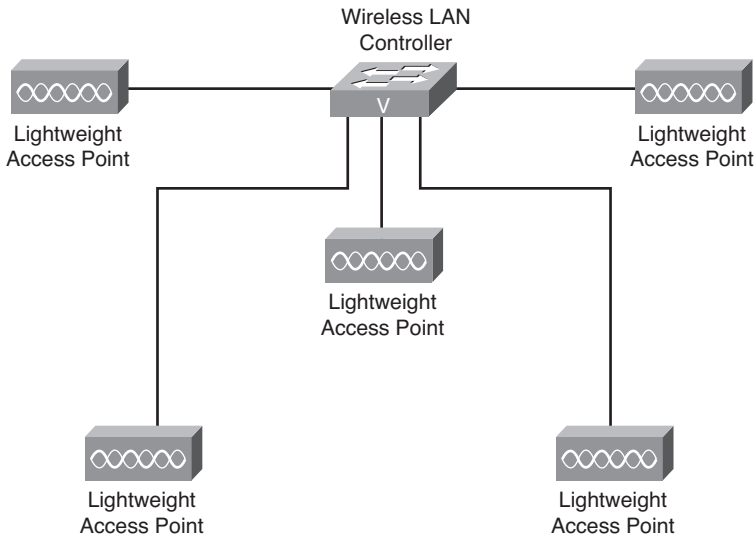
Because plenty of capacity is left to support voice traffic, the warehouse manager, Evan, decided to deploy a VoWLAN solution using the existing access points. Only five warehouse clerks will carry Cisco 7920 IP phones, which connect to the nearest access point. It is likely that only three of the clerks will be making calls at the same time, and they will probably be connected to different access points. Each access point can support up to three simultaneous callers, so there is no problem with capacity.

The minimum 15dB SNR throughout the facility is fine for supporting bar code applications, but it is not good enough for voice applications, which require a minimum of 25dB SNR. As a result, Evan scheduled a company to perform another wireless site survey and consider increasing the gain of the antennas and possibly add a fourth access point to improve the signal strength.

Wireless Switched Networks

As an effective alternative to traditional "thick" access point infrastructures, consider the use of wireless switched networks, as shown in Figure 2-7. The main idea here is to have "thin" access points focus on reliable and high-performance radio technology. The access points merely implement the 802.11 protocol, whereas the switch provides intelligence necessary to offer effective security, management, and performance. This feature results in a solution that effectively satisfies voice applications and significantly reduces TCO for most applications.

Figure 2-7 *Cisco Wireless Switched Network*



The switched wireless solution is less costly to scale up coverage and performance due to relatively inexpensive access points. The lack of intelligence in the access points makes offering access points at relatively low prices possible. The overall system is still intelligent, however, because the central switch shares the intelligence in a cost-effective and efficient manner with the access points. The smarts of the system only need to reside on one central hardware device, which reduces costs of the access points. Also, less overhead is sent over the wireless LAN when managing access control.

An intelligent wireless switch, such as that offered by Cisco, provides roaming handoffs much faster than conventional wireless LAN solutions. This enables effective support of VoIP applications. Wireless phone users are able to roam smoothly throughout the facility while reassociating with different access points.

Because the access points are less expensive, a "thin" solution is overall less costly to implement and support. Again, the sharing of the wireless intelligence in the switch results

in lower TCO. The overall hardware costs are lower, and migrating to newer technologies is less expensive because of lower replacement costs.

The wireless switch implements effective rogue access point detection. If an employee or hacker plugs in a rogue on the wired side of the switch, the switch disallows access via the rogue access point to the network. The wireless switch containing all security configurations can also be kept in a locked server room, which prevents hackers from fiddling with the configurations to their advantage.

In addition to better security, a compelling reason to deploy the thin access point solution is centralized management. Administrators can maintain, monitor, and upgrade multiple access points and user access configurations through the central switch, enabling efficient management because of integrated support functions. Furthermore, this approach relieves a significant amount of overhead on the wireless LAN, which increases capacity and utility.

Another benefit of the switched wireless solution is that it is better understood by IT personnel. Wireless technologies are very new to most companies, and existing IT personnel are not familiar with the radio characteristics of wireless LANs. The switched wireless approach has less focus on radio waves and more emphasis on the switch, which is familiar territory for administrators.

Cisco offers the following wireless switch components:

- **Cisco 1000 Series Lightweight Access Points**—Formally an Airespace product, the Cisco 1000 Series Lightweight Access Point is an 802.11 a/b/g dual-band, zero-touch configuration and management access point for enterprise solutions. It works in conjunction with a Cisco Wireless LAN Controller and optional Cisco Wireless Control System (WCS) to support real-time intrusion monitoring in addition to data traffic.
- **Cisco 4100 Series Wireless LAN Controllers**—The Cisco Wireless LAN Controllers work in conjunction with the Cisco 1000 Series Lightweight access points and the Cisco WCS to provide systemwide functions, such as intrusion detection, RF management, and security policy management. Ideal for medium to large enterprise facilities.
- **Cisco 2000 Series Wireless LAN Controllers**—Similar to the 4100 Series, except the 2000 Series is best for small to medium enterprise facilities.

Case Study: Acme Furniture Selects Cisco's Wireless Switch Solution for Corporate Offices

Acme Furniture has existing Cisco wireless LANs in retail stores, distribution centers, and manufacturing plants. To deploy a complete VoWLAN solution, Acme Furniture must install a wireless LAN in its corporate headquarters. Headquarters consists of a two-story

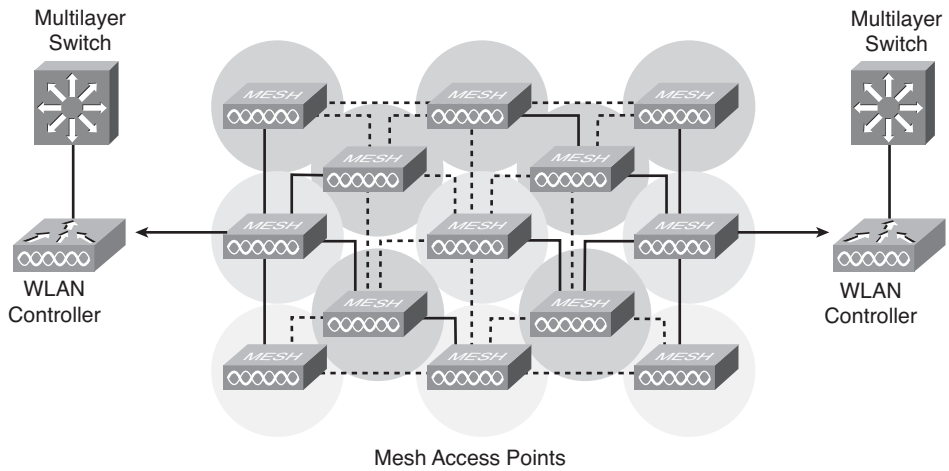
building with approximately 50,000 square feet. Based on preliminary analysis, 12 access points are needed to provide adequate signal coverage for wireless VoIP.

Because the company is installing a new wireless LAN in this area, it wants to take advantage of the benefits of wireless switches. So, Acme Furniture decided to install Cisco 1000 Series Lightweight Access Points and a 4100 Series Wireless LAN Controller. Doing so provides the company with an optimal solution for both voice and data traffic. Over time, the company will migrate existing traditional wireless LANs in retail stores, distribution centers, and manufacturing plants to the wireless switched network.

Mesh Networks

Many municipalities, such as Philadelphia, San Francisco, New York City, and a host of others, are deploying mesh networks that offer citywide Wi-Fi access. In general, mesh networking replaces traditional wireless LAN access points with "backhaul nodes" that are entirely wireless, except for the electrical cord. Figure 2-8 illustrates the Cisco wireless mesh network architecture. One side of the node interfaces with Wi-Fi users, typically using 802.11b/g. The Wi-Fi user associates with the mesh network node just as it does with an access point. The other side of the backhaul node has radios that interconnect the node to other backhaul nodes that make up the mesh network.

Figure 2-8 *Cisco Wireless Mesh Network Architecture*



The operation of a mesh network is fairly straightforward. For example, the URL request from a Wi-Fi user enters the mesh network at the backhaul node that the user associates with using Wi-Fi protocols. Then it hops from one node to the other until it reaches the node that connects to the Internet service provider (ISP). In some cases, the data packets may hop only a couple of nodes, but a greater number of hops may be necessary in larger networks.

Thus, the time taken for the corresponding web page to return to the user varies, depending on the layout of the network.

A mesh network offers multiple paths from source to destination. Intelligent routing algorithms allow each node to decide on which path to forward packets through the network to improve performance. If the link between a pair of nodes along one of the paths is clogged, for example, the algorithms establish another path that avoids the congested link. Also, if a node goes down, an alternate route is chosen based on the routing algorithms.

This feature makes mesh networks suitable for areas where installing a traditional wireless LAN consisting of access points is not feasible. For example, a mesh network approach makes sense to consider for residential and citywide Wi-Fi networks. The deployment of cabled access points over larger, open areas is a daunting task because of the massive amount of data cabling that requires installation and the countless permissions that you must receive. Other places where installation is difficult include convention centers, college campuses, stadiums, marinas, parks, and construction sites. Simply plop in the backhaul nodes where coverage is necessary, and automatic mechanisms connect the node into the network.

A mesh network is also worthwhile when installing a temporary wireless network because the backhaul nodes are faster to install and there is less to remove. For example, emergency crews can quickly establish a mesh network when working at a disaster site. Enterprises can also benefit from mesh networks when they need network connectivity in temporary work areas.

Another good fit for mesh networks is within buildings that do not have existing data cabling for access points. Instead of access points, the company installs mesh nodes. The costs of installing cable are relatively high, especially when requirements exist for conduit for enclosing the cabling, which is commonly the case. The conduit alone generally doubles the cost of installing access points. In this case, the deployment of a mesh network can save hundreds of dollars per access point.

The mesh network solutions on the market today differ widely. As a result, you must carefully analyze each solution and ensure that it satisfies requirements before moving forward. Latency, for example, may vary significantly, depending on the number of users and hops that are necessary for moving packets through the backhaul network. Roaming and routing delays may cause performance issues, especially for VoIP applications. Even if the data rate between the user and the local backhaul node is kept high, which many of the mesh network vendors claim, the delays across the network may be substantial. A mesh network in your application, though, will likely deliver much better performance than existing cell phone systems.

In some cases, the benefits of a mesh network far outweigh the issues. If you need a robust Wi-Fi solution where running cable to access points is not feasible, a mesh network is the answer. Lower installation costs because of less cabling and increased utility in difficult-to-wire areas make mesh networks shine. There are a few wrinkles to iron out with the standards and better provisions for VoIP, but mesh networks certainly have a permanent home in the wonderful world of wireless. Keep in mind, however, that without mesh network standards, you must install mesh nodes from the same vendor, such as Cisco.

The Cisco wireless mesh network solution includes the Cisco Aironet 1500 Series access point ("mesh node"):

- **Adaptive Wireless Path Protocol**—This patent-pending protocol dynamically forms optimal traffic routes between nodes. If RF interference occurs, the protocol automatically selects an alternate path.
- **Radio redundancy**—Each access point has two 802.11a/b/g radios for data integrity and throughput. One radio is dedicated to wireless communications between access points. The other radio can be dedicated to a specific application for segmentation or set to optimize performance of all users.
- **Security**—The solution offers a variety of security mechanisms, such as hardware-based Advanced Encryption Standard (AES) between access points and 802.11i, Wi-Fi Protected Access 2 (WPA2), and WEP for wireless clients. X.509 digital certification prevents unauthorized devices from joining the network.
- **Multiple SSIDs**—Each access point supports up to 16 SSIDs that can map into separate VLANs to support different wireless ISPs and private applications.

The Cisco mesh solution also includes wireless LAN controllers that implement the Cisco WCS, which offers scalable management, security, and support tools to manage a mesh network.

Case Study: City of Hope Chooses Cisco's Wireless Mesh Solution to Offer Wi-Fi Connectivity

Evan, the mayor of the city of Hope, learned about the benefits of wireless VoIP while golfing with Bob, president of Acme Furniture. Bob's company is deploying a wireless voice telephony solution. Evan liked the idea and envisioned similar applications for city employees. After researching citywide wireless networks, Evan realized that many other cities, such as Philadelphia and San Francisco, are deploying citywide Wi-Fi networks for both public and private applications. Hope is a medium-sized city with hundreds of employees (firefighters, police, and other staff) mobile throughout the city. The use of Wi-Fi for supporting voice communications would definitely enhance operations and save money. The city of Hope could not afford to install the mesh hardware, so arrangements

were made with a local ISP to offer public, fee-based Wi-Fi access to the city's numerous business and vacation visitors.

The city of Hope decided to install a Cisco wireless mesh solution using Cisco Aironet 1500 Series access points and associated controllers. The city scheduled a preinstallation site survey to determine the presence of RF interference that might significantly impair the operation of the network. In addition, the site survey will include RF propagation tests to analyze impacts of buildings and other obstacles on RF signal coverage. These results are crucial for providing a basis for determining the required density of access points necessary for voice applications.

Chapter Summary

When building a wireless voice telephony system, you must include several components that are not typical of a standard data-only wireless LAN. For example, users need wireless IP phones to utilize voice services. The phone operates very similar to a cell phone, except that calls are made over a wireless LAN using VoIP signaling. In a wireless voice telephony system, a call manager replaces the traditional PBX. The resulting system can interconnect users in different facilities and cities using digital circuits, such as the Internet.

A key element of the wireless voice telephony system is a wireless LAN infrastructure, which routes calls to and from mobile users. A company's existing traditional ("thick") access points can support voice calls, assuming that the signal coverage and delays between access points are adequate. However, a wireless switched network using "thin" access points offers superior performance for voice applications. For example, the switch reduces the security issues resulting from someone connecting a rogue access point to the switch.

Cities can also deploy wireless mesh solutions to offer citywide voice services to employees and public users. Mesh networks can also be used indoors to reduce requirements for interconnecting access points with Ethernet cabling.

Chapter Review Questions

1. What are the primary components of a VoWLAN solution?
2. What are the two main Cisco wireless IP phone approaches?
3. What functions does a call manager have on a VoWLAN system?
4. What is the purpose of a voice gateway?
5. Why is a wireless switched network better for supporting voice applications?

6 Why would an existing "thick" access point solution not be the optimum solution for supporting voice applications?

7 What are examples of Cisco's traditional "thick" access points?

8 What Cisco access point is used with a wireless switch?

9 Why might a wireless mesh network not provide adequate performance for voice applications?