Intel and Cisco WLAN Deployment Guide for Healthcare

Table of Contents

1. Introduction

Mobile technologies have demonstrated maturity in large enterprises, empowering workers and boosting productivity by greatly increasing access to tools and information. Adoption of mobile technologies continues to increase, with wireless networks becoming nearly ubiquitous in Fortune 500[1] campus environments.

Many forward-looking healthcare provider organizations are deploying mobile solutions to help improve quality of care, patient satisfaction, staff efficiency, and clinical outcomes. These include mobile point-of-care (MPOC) solutions that combine mobile devices, mobilized applications, and wireless infrastructure to support delivery of healthcare to the patient. As populations continue to age, wireless technologies are expected to facilitate more home-based monitoring and long-term care.

Healthcare organizations are already realizing the benefits of mobile and wireless technologies:

- It has been demonstrated that providing mobile access to clinical information systems can produce significant time and resource savings.[2]
- Automation of routine data collection and elimination of manual entry processes can reduce errors and dependency on paperwork. This is underscored by a recent Institute of Medicine report suggesting that many common medical errors can be avoided with better communication and computing links.
- Real-time information can be captured and instantly made available to care providers. Access to patient information, test results, records, and medical reference sources at the point of care helps accelerate evaluation and improve diagnostic accuracy.
- Wireless handheld devices and patient bracelets employing radio frequency identification (RFID) make it possible to track the location and status of patients throughout a hospital campus. Real-time location systems (RTLSs) are used for accurate asset tracking and location, driving cost savings and workflow productivity gains.

All of these benefits are ultimately dependent on the successful deployment of wireless infrastructure and clients. Wireless implementation in a healthcare facility requires many steps and decisions. The purpose of this deployment guide is to educate prospective adopters of WLANs on the most important considerations involved.

More specifically, this guide walks through the six stages of a WLAN deployment—Prepare, Plan, Design, Implement, Operate, and Optimize. These are steps that Intel's own IT organization has taken since 2003 to deploy wireless capabilities across its worldwide corporate IT environment. Most recently, Intel IT used the same process to evolve its wireless capabilities with a Cisco® unified wireless infrastructure and Intel® Centrino® processor technology-based clients for 6000 employees in its Jones Farm Campus in Hillsboro, Oregon. This network design is now being widely deployed at Intel facilities. Intel's wireless network availability, bandwidth, and redundancy requirements may serve as an appropriate reference for wireless deployments in acute care facilities.

Intel and Cisco have a long cooperative relationship in the design and deployment of WLANs. This guide refers exclusively to Intel and Cisco technologies and equipment. Intel Centrino processor technology wireless clients seamlessly integrate into the Cisco Unified Wireless Network with support for a jointly produced set of features called the Business-Class Wireless Suite (BCWS). For more information on the specific features of the BCWS, please refer to Appendix B and the Cisco Intel Alliance site at www.ciscointelalliance.com.

[1] Other names and brands may be claimed as the property of their respective owners.

[2] Queensland Health brings the productivity advantages of technology, including MPOC solutions, to hospital staff. See *Queensland Health: Checking Vital Signs of IT Infrastructure at Herston Hospitals*, Intel case study, 2004, www.intel.com/cd/services/intelsolutionservices/asmo-na/eng/success/casestudies/179115.htm.

1.1 Summary of Wireless Deployment Steps

The wireless deployment cycle comprises six main phases:

- **Prepare**—Understand the various challenges and requirements of a wireless infrastructure deployment and identify roles and types of usage.
- **Plan**—Determine the requirements of the wireless infrastructure and clients by investigating the targeted usages, applications, environment, network performance, security, and management.
- **Design**—Become familiar with key wireless architectural choices and their impact on the entire network.
- **Implement**—Execute the plan based on design decisions made in the previous step.
- **Operate**—Deploy various methods for providing optimum service to end users.
- **Optimize**—Understand how to continuously monitor the performance and reliability of the network to make optimal changes.

2. Prepare

Before starting the planning process, some preparation is necessary to identify user needs and determine the challenges and requirements of the specific site where the WLAN will be deployed.

2.1 User Expectations and Bandwidth Needs

An important part of preparation is to determine user expectations of the WLAN. What benefits are they seeking? This information is needed when planning the bandwidth, layout, coverage, and client management for the WLAN. Be sure to answer the following questions:

- What are the primary usage models (for example, campus-wide access to the wireless network, bedside use of wireless PDAs, wireless patient monitoring, or asset tracking)?
- Where is coverage needed—not only in rooms, but also in traffic areas such as hallways, elevators, and stairwells?
- What applications will run on the WLAN and how much bandwidth do they require?
- Do these applications have latency and authentication considerations?
- Will any of the applications require service as the user is in motion around the facility—will subnet roaming need to be accommodated?
- What kinds of clients will be used on the WLAN (for example, desktop PCs, tablet PCs, laptops, PDAs, voice handsets, inventory/location tracking devices, or medical devices), and what connecting software will they be using?
- What 802.11 radios will be used by the clients? (See section 3.3.1 for more information.)

When documenting expected benefits, it is helpful to keep in mind some special needs typical of healthcare settings. Computers often have more than one user or new users at each shift change, so authentication must be considered. The authentication process may be complicated by the fact that some of the equipment does not have a user interface. Battery recharge stations should be conveniently located to help ensure that low-battery conditions do not interfere with delivery of care.

Setting realistic expectations with users and stakeholders is important during the preparation phase. Signal strength and throughput variations can occur in a WLAN, and it may not be practical to extend wireless connectivity to every part of a facility. Look for “mobilized” applications—those able to work in both connected and disconnected mode—to deal with situations in which connectivity may be disrupted as the user roams from one area to another.

2.2 Challenges and Requirements

Use of WLANs and mobile devices constitutes a significant milestone in the evolution of a fully integrated digital hospital. At the same time, WLAN implementations in healthcare settings present a number of challenges. It is important that these WLANs remain highly available as part of mission-critical systems—that is, business or operational processes that cannot be interrupted for business continuity reasons. They must also provide a high level of security, including interference notification and detection of rogue access points.

The nature of radio frequency (RF) brings another set of challenges to the medical environment. The WLAN must not give off any signal that will interfere with medical systems (see section 3.4). Wireless installations are also complicated by the fact that healthcare facilities are often built using a combination of different materials, and RF behavior in these varying environments cannot always be reliably predicted. Additionally, there are areas surrounded by shielding or other substances that RF signals have difficulty penetrating.

2.2.1 Importance of Conducting a Site Survey

For all of the reasons cited above, it is absolutely essential to conduct a site survey as part of the preparation for deploying a WLAN. Without a properly completed site survey, a WLAN will very likely perform inconsistently and frustrate both IT and clinical users. Proper site surveys will be guided not only by form and structure, but also by the anticipated usage of the wireless infrastructure.

Medical environments frequently use equipment that shares the unlicensed RF bands that 802.11 WLAN devices occupy. When a healthcare facility is being surveyed for a wireless installation of an 802.11a/b/g wireless infrastructure, it is recommended that a full RF spectrum analysis also be conducted.

2.2.2 Surveying the RF Environment

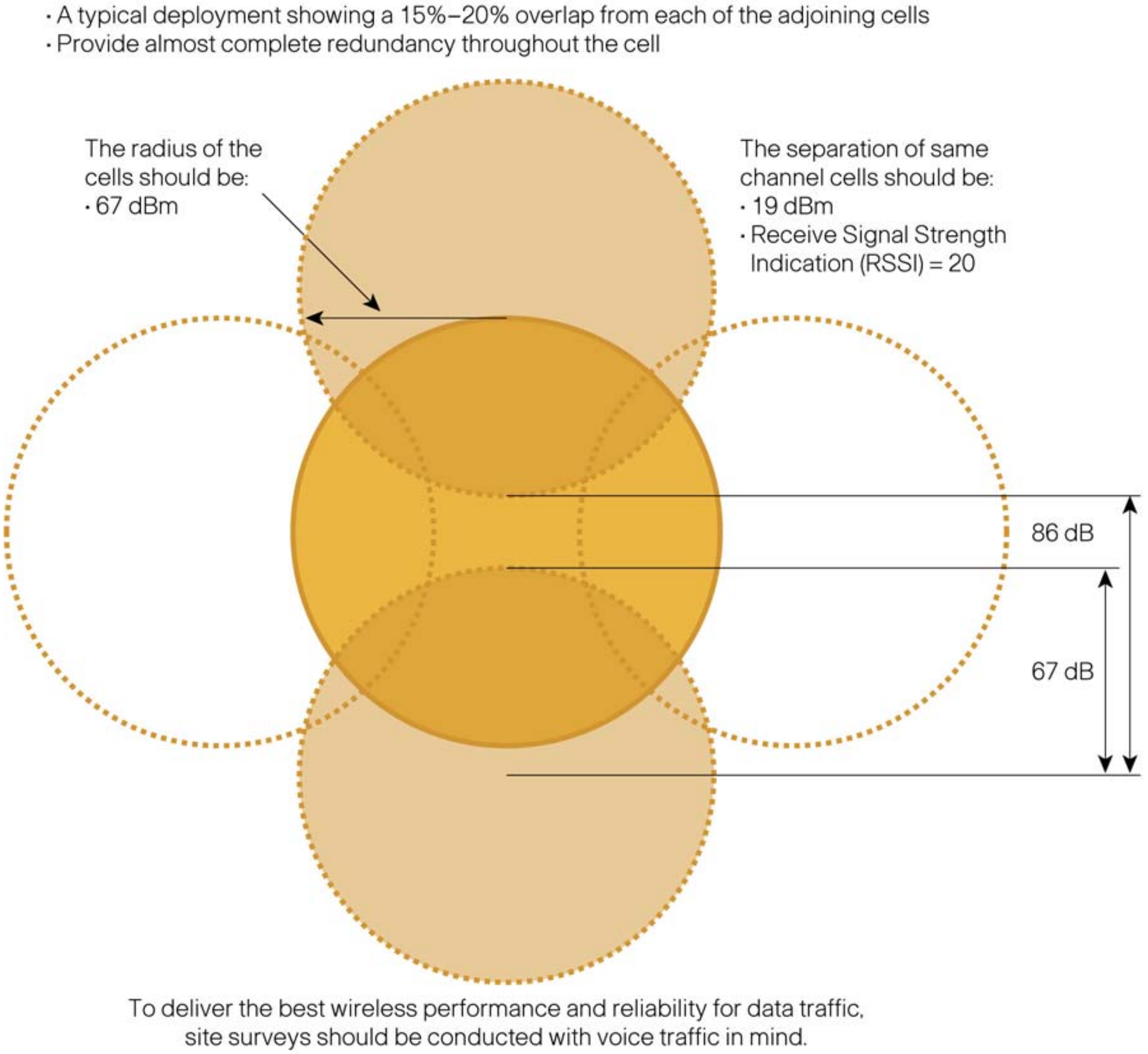
The performance of the WLAN and its equipment depends on its RF environment. Surveyors should check for adverse environmental variables using tools such as the Cisco Spectrum Expert Wi-Fi. Adverse variables in the environment may include:

- 2.4-GHz and 5-GHz cordless phones
- Walls fabricated from wire mesh and stucco
- Filing cabinets and metal equipment racks
- Transformers
- Heavy-duty electric motors
- Fire walls and fire doors
- Concrete
- Refrigerators
- Elevators
- Sulfur plasma lighting (fusion 2.4-GHz lighting systems)
- Air conditioning ducts
- Areas with tight aggregation of medical devices
- Other radio equipment
- Microwave ovens

2.2.3 Surveying for Access Point Requirements

Based on the variability in environments, a site survey is also highly recommended to determine the number of required access points (also called cells) and their optimal placement. Figure 1 shows a typical deployment that can serve as a guideline for conducting the initial survey.

Figure 1. Deployment Example Showing Overlap in Requirements


· A typical deployment showing a 15%–20% overlap from each of the adjoining cells
· Provide almost complete redundancy throughout the cell
The radius of the cells should be:
· 67 dBm
The separation of same channel cells should be:
· 19 dBm
· Receive Signal Strength Indication (RSSI) = 20
86 dB
67 dB
To deliver the best wireless performance and reliability for data traffic, site surveys should be conducted with voice traffic in mind.

A good rule of thumb for access point density (for 802.11a/b/g and 802.11n access points) is one access point per 5000 square feet for a data-only network, or one per 3000 square feet for an environment capable of supporting voice traffic or hand-held devices. It is typically recommended to use the higher access point density to provide for devices such as phones and handhelds. Proper coverage should not be sacrificed for economy.

If an RTLS system is to be implemented, different access point densities and access point placement schema may be required. With a typical non-RTLS WLAN deployment, it is common for access points to be placed centrally in the building (along hallways, for example). With RTLS, access points are placed along the perimeter of the desired coverage area. This provides for signals from multiple angles, which are required by RTLS systems for location determination. With some RTLS systems, non-WLAN access points or monitors can be utilized to enhance location accuracy. The RTLS vendor should be able to provide specific deployment recommendations.

Performing access point surveys in healthcare environments includes special considerations. For example, hospitals may have management spaces (basically another floor between floors) that are used to run various patient support systems to bed locations. Another special consideration is that radiology departments commonly have containment shielding for systems such as MRIs, and extensive steel or concrete support structures. Such design features will alter survey findings if they are not recognized at the beginning of the activity.

2.3 High Availability

In spaces where greater numbers of wireless applications will be used or where more personnel will be concentrated, Intel and Cisco recommend deployment of multiple access points within the overlapping cell coverage area to provide better management of bandwidth, traffic, and downtime.

This approach also helps keep sterile spaces clean and uncontaminated to prevent the spreading of disease. If an access point fails in one of these areas during clinical activity, other access points located in the area will still function, enabling the hospital to put off non-sterile technical work until a less critical time. During the preparation phase, survey the facility to identify all of the areas that require multiple access points for high availability and/or infection control.

Designing a secondary wireless network as failover protection can provide additional high availability. High availability can also be achieved by the adoption of the proper wireless protocols. These topics are addressed in more detail in section 3.3.

2.4 Security Assessment

A complete assessment should be made during the preparation stage to understand any security vulnerabilities that exist, including authentication and encryption methods already deployed. Legacy systems may be using outdated and ineffective measures that can affect security if they are incorporated into the new WLAN.

Since August 1996, healthcare providers have been required by law to comply with Health Insurance Portability and Accountability Act (HIPAA) regulations for medical information privacy (see section 3.4.3 for more information). Be prepared to meet HIPAA requirements and help ensure confidentiality.

Network planners must understand and be prepared to mitigate both passive and active WLAN attacks. A passive attack involves an unauthorized user gaining access to the network but not modifying any network resources. During the attack, the unauthorized person may analyze WLAN traffic or eavesdrop on transmissions through packet capture methods. In an active attack, the unauthorized user may modify or disrupt network resources.

A number of tools and techniques are available to mitigate such threats. Wireless security solutions are discussed in section 4.6.

2.5 Access Types

Much like wired networks, WLANs must provide access to a diverse population of users encompassing clinical staff, administrative staff, guest physicians, business guests, patients, and even medical equipment. Each user type requires a unique level of privileges, so it is important during the preparation phase to determine all of the access types that fit the user base.

Most hospitals use multiple virtual WLANs to control access. For example, a service set identifier (SSID)/virtual LAN (VLAN) might be established for guests, while other SSID/VLANs are created for staff only. Each VLAN is isolated from the other, and provides unique access privileges to the Internet or the hospital’s internal private network. Devices with limited security mechanisms may need to be on the network, so be prepared to establish SSID/VLANs for this equipment as well.

Medical facilities with independent physicians may require a “physician guest” class of users. These doctors usually need access beyond a simple connection to the Internet, often requiring access to the private network for hospital applications and databases. Because these physicians are not necessarily employees, they are likely to use a variety of uncontrolled client devices.

Emerging business requirements are also creating a “business guest” class of users—for example, vendors supporting equipment over the Internet and business affiliates accessing their company intranets. When these individuals visit the healthcare organization premises as part of their jobs, it is expected that they will be able to access their company networks using virtual private networks (VPNs) or be able to securely access the Internet. This can be achieved by establishing service areas for these guests and using SSID/VLAN technology to logically segment the traffic.

A final category of guest user consists of patients and visitors who request Internet access while at the medical facility. This type of guest privilege should be strictly limited to Internet access and is most easily accomplished via a WLAN running on a VLAN and through the medical facility’s firewall. For more information on the security design considerations for guest access, see section 4.6.3.

3. Plan

Achieving the greatest return on the wireless investment requires a well-considered, long-term strategic deployment plan. A healthcare IT organization must plan its wireless infrastructure to support present and future usage models and devices. For example, although an organization may initially be interested only in providing data connectivity to laptops or PDAs, the organization should plan its wireless infrastructure to support future uses, such as voice and video traffic over wireless.

The IT organization should begin by planning its wireless infrastructure to support all of the device form factors identified during the preparation phase, such as tablet PCs, PDAs, voice-over-IP (VoIP) handsets, and wireless telemetry monitors. Each device has different RF characteristics and requirements. Some devices may have stronger signal transmission strength or more sensitive reception compared to other devices.

Voice traffic is sensitive to wireless network performance and robustness, so it is a best practice to make plans based on the requirements of a VoIP solution. This helps the healthcare organization to ensure a robust wireless experience for data and hand-held devices, as well as allowing flexibility for new applications in the future.

3.1 Service-Level Agreement

The next step is to define a service-level agreement (SLA) based on the applications, devices, workflow scenarios, and user expectations gathered during the preparation phase. This includes the amount of bandwidth the applications need and the locations where they must be accessible. Many requirements from users will be general in nature, and a study may be needed to characterize the actual demands on network resources.

A practical approach is to negotiate acceptable service levels in various areas of the facility. For example, users may agree that certain areas, such as elevators, cannot be expected to maintain a reliable connection even though it is technically possible. Return on investment may be a limiting factor in non-mission-critical situations.

Now is also the time to draft requirements for IT support of the WLAN:

- What parameters does the IT staff need to monitor? (See section 6.2 for suggestions.)
- How do they want to be able to monitor the WLAN?
- How and where do they need to access WLAN configuration and control?
- What do they need to monitor and control for security compliance?
- What are the security requirements?

3.2 Hardware and Software Version and Configuration Control

Strong hardware, firmware, and software change control policies and enforcement are a must for all components of the WLAN infrastructure and clients. Start by determining change control requirements, including the needs of stakeholders who may not directly use the service but could be affected by others' use of the WLAN. This can be critical for ensuring there will be no interference with vital equipment and for mapping exceptions if the 802.11 spectrum is already in use by existing equipment. A variety of commercially available packages provide change control mechanisms.

On the client side, a wireless client administration tool such as Intel® PROSet/Wireless Administrator Tool is recommended to manage version and configuration control of Intel Centrino mobile processor-based wireless clients. This tool enables IT administrators to centrally configure and manage wireless clients.[3]

3.3 Density, Capacity, and Connecting Devices

Since WLANs use a radio spectrum that is potentially shared with other devices, bandwidth is limited and latency-sensitive applications such as voice must be prioritized. This is especially important in a healthcare setting.

Each access point covers a limited area, so the healthcare facility will need many of them, with fast handoff between cells to support latency-sensitive applications. Consider using one of the site survey planning tools that are commercially available to help plot out access point locations. The Cisco Wireless Control System along with the Cisco Wireless Control System Navigator can be used for WLAN planning, configuration, and management especially for large-scale deployments such as hospitals. After the WLAN goes live, the same tools can be used to study congestion patterns to continuously optimize the physical and performance characteristics of the infrastructure.

[3] For more information, see *Managing Wireless Clients with the Administrator Tool*, Intel white paper, 2006, www.intel.com/network/connectivity/products/whitepapers/admin_tool_wp.pdf.

3.3.1 Radio Frequency Spectrum Management

The WLAN spectrum may be shared with other technologies, such as smartphones, Bluetooth* devices, and even microwave ovens, so there is potential for interference. WLANs use two possible radio spectrum bands: the 2.4-GHz band, used by 802.11b and 802.11g protocols, or the 5-GHz band, used by the 802.11a protocol. 802.11n, the newest protocol, utilizes both 2.4-GHz and 5-GHz bands and is compatible with existing 802.11a/b/g.

For the most robust system operation and performance, healthcare IT organizations should deploy 5-GHz band with 802.11a and 802.11n protocols as the primary WLAN data handling technology. The healthcare IT organization should deploy 2.4-GHz band with 802.11b and 802.11g for existing devices and medical equipment. Hospitals with electronic medical records, clinical information systems, and bandwidth-intensive applications such as medical imaging should consider a 802.11a or 802.11n wireless network to deliver the highest throughput and reliability. Typically, this will result in data traffic and notebook computers being placed on the 802.11a and 802.11n WLAN, and non-802.11a or non-802.11n-capable devices, such as VoIP phones and handhelds, being placed on the 802.11g WLAN.

The 5-GHz band 802.11a and 802.11n standards offer the following advantages compared to 2.4-GHz band 802.11b/g:

- High data throughput that is not reduced by other technologies (throughput of 802.11g-based devices decreases by 30 to 60 percent when 802.11b-based devices share the same frequency channel)
- Reduced contention with other WLAN devices
- Reduced interference from non-802.11 wireless devices
- Improved performance in RF-reflective environments
- Larger number of nonoverlapping channels (typically 21 for 802.11a; 9 for 802.11n, compared to three for 802.11b/g), resulting in less co-channel interference (CCI) for a higher density of access points
- High data throughput via channel aggregation (for instance, combining two 20-MHz channels to create a 40-MHz channel can effectively increase data throughput because of the greater number of channels available in the 5-GHz band)
- Higher aggregate WLAN capacity to support more users per cell or more data-intensive applications (for example, in the United States, 11 channels of 802.11n at 300 Mbps per channel provides more than 3300 Mbps capacity, while three channels of 802.11g at 54 Mbps per channel provides only 162 Mbps capacity)

A summary of the 2.4-GHz and 5-GHz band 802.11a/b/g/n technologies is presented in Table 1.

Table 1. Summary of the 802.11 Technologies

	802.11b	802.11g	802.11a	802.11n
Max Data Rate (Mbps)	11	54	54	300
Actual Throughput (Mbps)*	5	20 ~-30% with 11b present	22	146[1] ~-10% with legacy present
Number of Available Channels**	3	3	12	3 in 2.4 GHz 11 in 5 GHz
WLAN Capacity (data rate x channels) (Mbps)	33	162 ~-30% with b present	648[2]	1200[3]-1500[4]-at 5 GHz ~-10% with legacy present
Interference Probability/Impact	High	High	Low	Low
Difficult Environment Handling	Poor	Good	Better	Best
Compatibility	802.11b	802.11b/g	802.11a	802.11a/b/g/n
Spectrum	2.4	2.4	5	2.4 and 5
Channel Aggregation	No	No	No	Yes
Security	WPA/WPA2	WPA/WPA2	WPA/WPA2	WPA/WPA2

* Number of Available Channels is subject to country-specific regulations. Please consult your local authorities as these regulations are subject to change without notice.

** Actual Throughput results are from controlled laboratory environments. Actual results in an enterprise environment may vary.

[1] Results achieved with Intel® Next-Gen Wireless N technology enabled by 2x3 Draft N implementations with 2 spatial streams. Actual results may vary based on your specific hardware, connection rate, site conditions, and software configurations. See http://www.intel.com/performance/mobile/wireless/index.htm for more information.

[2] Achieved using twelve 5-GHz channels at 54 Mbps per channel.

[3] Achieved using four pairs of 20-MHz-bonded channels in the 5-GHz spectrum at 300 Mbps per bonded channel-pair.

[4] Achieved using four pairs of 20-MHz-bonded channels in the 5-GHz spectrum at 300 Mbps per bonded channel-pair, one remaining available 5-GHz band at 150 Mbps, and three channels in the 2.4-GHz spectrum at 54 Mbps per channel.

The comparison between the various 802.11 protocols suggests that healthcare enterprises should adopt the 5-GHz-band technologies, 802.11a or 802.11n, for their primary wireless network for data traffic and 2.4-GHz band technologies, using 802.11n or 802.11g, for VoIP traffic.

For completely new Greenfield WLAN deployments, healthcare IT organizations should deploy 802.11n-based access points and clients as the best investment in performance and extended equipment lifecycle. For healthcare environments with existing 802.11a/b/g environments, migration to 802.11n will improve wireless networking performance and reliability. Such a migration can be performed gradually.

With the advent of compatibility and certification testing of 802.11n draft 2.0 devices, healthcare enterprises can begin planning the migration to 802.11n. Corporate laptops with dual-band (2.4-GHz and 5-GHz) 802.11n adapters are available today and should be the purchase option of choice in current and future client deployments. The acceptance of 802.11n in the healthcare enterprise environment is expected to occur rather quickly. Adopting 802.11n devices during the lifecycle of today's client systems will allow healthcare enterprises to take full advantage of 802.11n benefits when devices based on the final 802.11n ratified specification become available in 2010. 802.11n devices are completely compatible with existing 802.11a, b, and g access points and will interoperate with existing devices and infrastructure. Planning the infrastructure migration to 802.11n requires technical and business needs planning.

Why should I adopt 802.11n when the standard has yet to be ratified?

Even though the 802.11n technology is still under development by the IEEE standards body, products based on the 802.11n draft 2.0 standard are now widely available. These include the Cisco Aironet® 1250 Series access point as well as an Intel® Centrino® Processor Technology-based notebook clients.

Draft 2 802.11n devices are designed to deliver up to five times the performance of 802.11a/b/g networks,[4] effectively supporting higher capacity and improved predictability and reliability for enterprise WLANs. In instances where the client devices are based on 802.11a/b/g standard, deploying 802.11n access points can still result in an aggregate increase in overall client performance due to the benefits of the radio enhancements and multiple-input multiple-output (MIMO) antenna technology supported by the access points.

The 802.11n standard is expected to be ratified in 2009.[5] Although the benefits are clear, many enterprises are understandably concerned about adopting the 802.11n draft 2.0 prior to final ratification of the standard. Cisco and Intel have taken measures to help ensure the investment protection of their customers. In addition to leading the IEEE standards process and being the benchmark against which all other draft 802.11n products are Wi-Fi certified, both companies have conducted extensive joint interoperability testing between Intel clients and Cisco's wireless infrastructure.

Given the significant improvements in throughput, reliability and predictability offered by 802.11n networks, all of which are important in a healthcare environment, any healthcare facility interested in the new technology should understand the site survey implications of Draft- 2 802.11N devices for RF spectrum analysis. Following the survey, it is recommended that healthcare organizations plan a deployment approach that takes into account the RF environment and the bandwidth intensive applications that will benefit from this technology. Where relevant, an incremental migration plan may work where in the new access points can be installed to supplement existing coverage in cases where additional capacity is required. To conduct a comprehensive analysis of the RF spectrum, IT should use tools such as the Cisco Spectrum Expert Wi-Fi that can analyze the frequency to detect non–Wi-Fi interference sources.

For more information on Cisco's Next-Generation Wireless Solutions, please refer to 72Hhttp://www.cisco.com/go/nextgen-wireless.

For more information on Draft-2 802.11N and Intel® Next-Gen Wireless-N, please refer to 73Hhttp://www.intel.com/go/wifi.

Tight control of all radios in the hospital environment must be implemented and stringently enforced. There should be one centralized control point established for the RF spectrum. It is suggested that no RF devices be allowed in the environment without having first been tested, validated, and cleared for usage. Proper RF spectrum monitoring tools should be put in place to aid troubleshooting and ensure adherence to policies.

[4] For more information, see www.intel.com/performance/mobile/index.htm.

[5] The formal ratification date of the IEEE 802.11n standard is subject to change without notice.

At an appropriate time, the hospital's biomedical engineering department should be involved in testing the prototype WLAN in a controlled environment with sources of electromagnetic interference (EMI). It is the responsibility of this department to test devices and define the policies and procedures relating to these devices and their usage. Most biomedical engineering departments have a standard test set.

3.3.2 Capacity Planning

With a WLAN, capacity planning is critical. Even though the 5-GHz band provides more channels than the 2.4-GHz band, the number of nonoverlapping channels is still limiting, and each channel provides low overall throughput compared with wired networks. In addition, CCI limits the available bandwidth.

One key aspect of capacity planning is deciding how many clients each access point should support and by clearly understanding the client applications. This issue is complex. With WLANs, throughput is greatest near the access point, and decreases as devices get farther away, as shown in Table 2. But placing access points too close together increases the potential for CCI.

Table 2. WLAN Throughput with Distance from an Access Point

	802.11b	802.11g/b	802.11g	802.11a	802.11n
Data rate 40 to 50 feet from access point	11 Mbps	54 Mbps	54 Mbps	54 Mbps	300 Mbps
Data throughput 40 to 50 feet from access point	6 Mbps	13 Mbps (802.11b present)	20 Mbps	24 Mbps	145 Mbps

Options for Migrating Existing WLANs to 802.11n

A couple of options exist for healthcare IT organizations to migrate to 802.11n wireless networks.

1. Replace individual existing access points with 802.11n access points as budget allows and user demand for additional capacity and throughput dictates. This gradual migration can be accomplished over a planned period of time or as the need arises. This migration method would have the new 802.11n access point operate on the same channel of the existing access point it replaced. The new 802.11n access point would support both 802.11n clients and existing 802.11a/b/g clients. Operating in a mixed mode, the new 802.11n access points provide investment protection for the existing clients and headroom for new 802.11n clients deployments.
2. Reassign the channels of selected legacy access points to free a set of channels that can be allocated for 802.11n use exclusively. As budget allows and demand dictates, new 802.11n access points can be *added* to the existing WLAN, operating simultaneously in overlapping areas with the legacy access points. This method allows the new 802.11n access points to support only 802.11n devices and provide the greatest benefits of the new standard by not having to contend with existing devices that will increase channel contention. Once the last existing client is retired, the existing access points can also be retired.

3.3.3 High-Availability Example

Intel IT planned for 20 to 25 users per 802.11a cell for its Jones Farm Campus. Each cell is an access point, and planning for 20 to 25 users requires each access point to sustain a minimum connection speed of 36 Mbps to meet the service agreement. The Intel IT organization assumed 20 users and 36 Mbps per cell for its high-availability WLAN, yielding the following requirements:

- Estimated throughput of more than 5 Mbps for each client, with a guaranteed minimum of 1.2 Mbps
- Ability of each access point to support approximately seven concurrent voice calls
- Enough capacity to enable a third of the users supported by each access point to make simultaneous voice calls

Based on the 802.11a data throughput measurements outlined in Table 2 and the requirements just listed, access points must be placed no farther than 80 to 100 feet from each other. With this relatively high access point density, CCI can become an issue even with 12 nonoverlapping channels. CCI reduces the available throughput in a cell, because the cell may be considered busy because of transmissions in a neighboring cell using the same frequency. Cisco radio management features can adjust dynamically to minimize CCI. For more information, see www.cisco.com/en/US/products/hw/wireless.

It is important to keep in mind that each environment is unique. With differing user capacity, density, and bandwidth requirements, healthcare IT managers can nonetheless adopt a similar methodology to plan for high availability in an acute care environment.

3.3.4 Process and Network Prioritization

Applications such as voice are highly sensitive to packet loss and delay. To avoid poor quality, it will be necessary to guarantee these applications the right quality of service (QoS) priority.

Client-based policy agents can ensure applications requiring network QoS have their packets marked appropriately, using tagging based on 802.11e and Wi-Fi* Multimedia (WMM). Also, soft phone applications are available that use the Intel and Cisco BCWS voice application programming interface (API), which supports admission control and simple packet marking.

3.3.5 Handoff and Roaming

To function as a primary access method, the WLAN needs to support all applications currently carried over the wired network. These applications should be supported as appropriate by each of the various clients that will be used. Some of these clients are highly mobile, requiring fast handoff to avoid disruption as users roam between cells. Roaming requirements vary according to the client and the usage/workflow characteristics:

- Desktops generally do not need handoff or roaming support.
- Laptop users may roam while using applications, and laptops are sometimes mounted on carts for computer-on-wheels mobility, requiring roaming support.
- Tablets, PDAs, and other highly mobile devices will need application continuity while on the move.
- Voice applications and phones are the most demanding, with a preferred handoff time of about 50 ms or less.

Until IEEE completes work on 802.11r and other specifications to provide a standard way to support fast handoff, it is advisable to use Cisco Compatible Extensions devices with Cisco Centralized Key Management*. When coupled with the smart access point selection feature of the BCWS developed by Intel and Cisco, this provides the required handoff and roaming times.

For more information on the Cisco Compatible Extensions and business-class wireless solutions, see Appendix B.

3.3.6 Reliability and Redundancy

In a healthcare setting, the WLAN must be highly reliable, especially if it will provide the primary access method. The characteristics of WLANs can be used to create a robust network architecture.

With WLANs, each access point supports multiple clients. Theoretically, a single access point failure could create an outage for multiple users. However, unlike a wired LAN, a WLAN client connection to an access point is virtual. A client can dynamically switch from one access point to another, as long as the second access point supports the same service with adequate signal strength.

One approach is to use this capability to create a redundant design in which a floor or building with multiple access points is divided into interspersed grids. Each grid is connected to a different LAN access switch or access point controller. If one entire grid fails, the other grid will still be able to provide complete RF coverage. As a result, clients will be able to seamlessly reconnect to the second grid, although potentially with reduced throughput.

3.3.7 Management

WLANs enable organizations to service many more clients at lower cost than traditional LANs, since many fewer switches are needed. Instead of a large number of expensive switches, WLANs involve a large number of less expensive access points. Managing all these access points and combining the management of wired and wireless networks are challenges that should be addressed at the planning stage. A poorly planned and managed WLAN can result in inconsistent service delivery.

To be able to install, upgrade, and manage this environment while providing the required service levels, a lightweight access point or controller based architecture, such as the Cisco Lightweight Access Point Protocol (LWAPP), is recommended. In this architecture, access points do not handle management directly. Instead, management is off-loaded to dedicated wireless controllers that each coordinate and manage multiple access points.

Deploying a lightweight access point architecture in medium-sized to large enterprise environments requires a centralized wireless control system that allows IT managers to design, control, and monitor enterprise wireless networks to simplify operations and reduce total cost of ownership. Cisco Wireless Control System (WCS) is an optional network component that works in conjunction with Cisco LWAPP to enable those capabilities. For more information on the Cisco Wireless Control System, visit: www.cisco.com/en/US/products/ps6305/index.html

3.4 Compatibility and Compliance in the Medical Environment

Wireless equipment must meet a variety of standards and regulations. Before a radio product is placed on the market, regulations require it to be evaluated for electromagnetic compliance, per the various national standards of the host country. On the wireless side, radios are also tested for compliance based on the applicable national radio standard.

As part of the approval process, Intel and Cisco radios are thoroughly tested and certified per international regulatory standards that are applicable for 802.11a, 802.11b, and 802.11g wireless devices and labeled accordingly. Testing and certification is also applicable to any current and future 802.11n devices. Individual country guidelines and regulations for privacy and security may vary, and investigation is required on the part of the healthcare IT organization to understand country-specific requirements.

3.4.1 Medical Electromagnetic Compatibility Standards

It should also be determined whether equipment needs to meet the electromagnetic compatibility (EMC) and safety requirements for implanted medical devices used to provide direct patient care or peripheral support. Compatibility means that any equipment used in proximity to such devices should not cause harmful interference, but must be able to accept harmful interference, including that which disrupts service. To adhere to EMC standards, Intel and Cisco equipment must operate on a non-interference basis.

Wireless devices operating in a healthcare setting are required in the EU and recommended elsewhere to be compliant with International Electrotechnical Commission (IEC) 601-1-2 standards. Similar requirements also exist in Japan. Compliance requires that the device be tested to ensure it meets the CISPR 11 emission requirements. However, if the device has been tested to ensure it meets the requirements of CISPR 22, the product does not need to be tested for CISPR 11 compliance as well.

3.4.2 Safety of Radio Frequency Emissions

Questions have been raised from time to time regarding the effects of RF emissions on human health. This topic has been studied for many years, and based on the opinions of scientific experts, there is no reason to believe that low-powered wireless networks such as WLANs cause any adverse health effects.

A recent fact sheet from the World Health Organization[6] states: “From all evidence accumulated so far, no adverse short- or long-term health effects have been shown to occur from the RF signals produced by base stations. Since wireless networks produce generally lower RF signals than base stations, no adverse health effects are expected from exposure to them.”

Generally, the transmission power of WLAN devices is considered low relative to the expected immunity levels of equipment in healthcare environments. In addition, the operational frequencies of 802.11b/g and 802.11a radios normally are not used by patient monitoring systems. However, guidelines are recommended for the safe implementation, use, and management of all wireless devices in healthcare environments. These guidelines include establishing specifications for the required immunity of all electronic devices used in a particular healthcare setting, a program for the identification and training of responsible personnel (for example, clinical and biomedical engineers), and a management program for all wireless devices.

Organizations sometimes express concerns that WLAN devices may interfere with hearing aids or pacemakers. Tests have shown that interference is possible with some wireless portable devices, though not specifically ones related to WLANs. For example, some studies have suggested that when some digital cellular phones are placed very close to implanted cardiac pacemakers, interference with the pacemaker's normal delivery of pulses can occur. As a result, the Center for Devices and Radiological Health of the U.S. Food and Drug Administration (FDA) recommends keeping the phone about six inches or more from the implanted pacemaker.[7]

With regard to WLANs and implanted devices, there has been limited study. General industry consensus is that 802.11 radios have very little risk of creating EMI. A Mayo Clinic laboratory study of non-implanted pacemakers and defibrillators found no interference with PDAs in close proximity to the medical device served by an 802.11b radio.[8]

[6] *Electromagnetic Fields and Public Health*, World Health Organization Fact Sheet No. 304, 2006, www.who.int/mediacentre/factsheets/fs304/en/index.html.

[7] *Electromagnetic Compatibility—Cellular Phone Interference*, FDA publication, 1995, www.fda.gov/cdrh/emc/pace.html.

[8] “Potential for Personal Digital Assistant Interference with Implantable Cardiac Devices,” article by Jeffrey L. Tri, Jane M. Trusty, and David L. Hayes, *Mayo Clinic Proceedings* 79: 1527–30, 2004, www.mayoclinicproceedings.com/pdf%2F7912%2F7912a7.pdf.

Another study, published in Telemedicine and e-Health, determined WLAN RF not to be a significant cause of EMI and thus of extremely low risk to medical equipment. The study conservatively suggested maintaining a distance of one meter between WLAN devices and medical equipment.[9] Such a separation is not a required practice, but healthcare IT organizations should always refer to sensitive medical equipment documentation for further information on potential EMI issues.

Additional information on this subject is available from:

- Guidance on Electromagnetic Compatibility of Medical Devices for Clinical/Biomedical Engineers—Part 1: Radiated Radio-Frequency Electromagnetic Energy, Association for the Advancement of Medical Instrumentation (AAMI) TIR18:1997, 1997, webstore.ansi.org/ansidocstore/product.asp?sku=AAMI+TIR18%3A1997
- *Radiofrequency Interference with Medical Devices*, IEEE Committee on Man and Radiation (COMAR) Technical Information Statement, 1998, www.ewh.ieee.org/soc/embs/comar/interfer.htm
- *Electromagnetic Compatibility—FDA/CDRH Recommendations for EMC/EMI in Healthcare Facilities,* FDA publication, www.fda.gov/cdrh/emc/emc-in-hcf.html

3.4.3 HIPAA Compliance in the United States

As an aid to planning, the following is a partial list of HIPAA requirements. It is not totally inclusive of all the requirements—this document should not be used as a checklist for HIPAA compliance.

You must reference the applicable government documents directly for the latest and most complete information.

A variety of technologies and services are available from Intel, Cisco, and their partners to help IT organizations meet the requirements.

1. Implement policies and procedures to prevent, contain, and correct security violations.
2. Identify the security official who is responsible for the development and implementation of the policies and procedures required.
3. Implement policies and procedures to ensure that all members of the workforce have appropriate access to electronic protected health information, and to prevent workforce members who do not have access from obtaining access to electronic protected health information.
4. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with other applicable requirements.
5. Implement a security awareness and training program for all members of the workforce, including management.
6. Implement policies and procedures to address security incidents.
7. Establish and implement policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.
8. Perform a periodic technical and nontechnical evaluation in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which a healthcare organization's security policies and procedures meet all requirements.
9. Permit a healthcare employee to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the information will be appropriately safeguarded.
10. Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. Ensure that line-of-sight positioning does not lend itself to wireless eavesdropping.
11. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.
12. Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

[9] "Wireless Technologies and Patient Safety in Hospitals," article by Justin Boyle, *Telemedicine and e-Health* 12: 373–82, 2006, e-hrc.net/pubs/papers/pdf/RP-JB-tech-review-wireless-tech-patient-safety.pdf.

13. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility as well as the movement of these items within the facility.
14. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to persons or software programs that have been granted access rights.
15. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
16. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
17. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
18. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

In addition, healthcare organizations are governed by the following organizational guidelines:

1. All contracts between the healthcare organization and its partners must meet HIPAA requirements.
2. A covered entity is not in compliance if it knew of a pattern of an activity or practice that constituted a breach of these requirements, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, (a) terminated the contract or arrangement, if feasible; or (b) if termination is not feasible, reported the problem to the proper authorities.
3. The organization must implement reasonable and appropriate policies and procedures. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and implemented in accordance with HIPAA requirements.
4. The healthcare organization must maintain the policies and procedures implemented in written or electronic form, as well as records of all actions, activities, or assessments.

Outside of the United States, other patient data privacy and security laws will apply. Individual country guidelines and regulations for privacy and security may vary, and investigation is required on the part of the healthcare IT organization to understand country-specific requirements.

4. Design

Now that the planning process has been completed, it is time to begin making design choices. This requires gaining familiarity with key wireless architectural considerations and their impacts on the overall network.

4.1 Access Point Coverage

At this point, WLAN planners should have in hand a thorough site survey and the results of their capacity planning efforts. As the design process goes forward, testing, resurveying, and replanning access point locations might be required in some cases.

In multistory buildings such as office towers, hospitals, and university classroom buildings, it is advisable to check the cell overlap between floors, since the 2.4-GHz and 5-GHz signals can pass through floors, ceilings, and walls. With 2.4-GHz WLANs in particular, take care to avoid overlapping cells not only on the same floor, but also on adjacent floors. Even with only three channels, overlapping can be minimized through careful three-dimensional planning.

For an 802.11n migration, the placement and spacing of the 802.11n access points remains the same as before for 802.11a/b/g access points.

4.2 Data Rate Selection

It’s important to consider a number of factors that can affect WLAN coverage, including the selected data rate, which is affected by the physics of radio wave interference, reflection, and refraction. When radio waves experience RF noise, bounce off walls or equipment, and scatter when penetrating floors, the integrity and reliability of the signals is reduced. To compensate for those effects, 802.11a/b/g/n radios will send redundant signals on the wireless link, allowing data to be more easily recovered from noise. Higher redundancy in the signal results in lower data throughput and increased reliability.

The number of symbols sent out for a packet at the 1 Mbps data rate is greater than the number of symbols used for the same packet at 11 Mbps. This means that sending data at the lower bit rate takes more time than sending the equivalent data at a higher bit rate. The data rate settings are used to choose transmission rates. The wireless device always attempts to transmit at the highest possible data rate as configured in the access point interface. If RF rates are insufficient to support the highest rate, the wireless device steps down to the highest rate that supports reliable data transmission.

Data throughput experienced by the user is also affected by the bandwidth of the wired connection between the access points and the wired infrastructure. A network is only as fast as its slowest component. Therefore it is critical to provide at least 100Mbps Ethernet wired connections to 802.11a and 802.11g access points since their maximum data wireless rates are 54 Mbps.

For 802.11n access points, maximum data throughput can exceed 145 Mbps per radio (300 Mbps for dual radios) and therefore require 1 Gbps Ethernet connections to the wired infrastructure. This will help ensure ample headroom for users to achieve maximum data throughput as well as allow for future upgrade headroom. A migration from 802.11a/b/g to 802.11n access points may require an upgrade of edge switches and switch aggregation links.

4.3 Antenna and Channel Selection

For a given data rate and location, the designer can alter the power level or elect to use a different antenna to change the coverage area or shape. Multiple wireless antenna designs are available, each with its specific strengths and purposes. It is highly recommended to investigate the various types of antennas (omnidirectional, directional, and distributed) to help ensure the best coverage according to the site survey requirements.

Antenna concerns for healthcare include the following:

- It is important to remember that third-party antennas often need enclosures in healthcare settings for infection containment.
- Installers should ensure that all antennas are beyond the reach of patients or other passersby.
- A misaligned antenna could result in poor coverage and performance.

Channel selection depends on the frequencies that are permitted for a particular region. The channels should be allocated to the coverage cells as follows:

- Adjacent cells should use nonoverlapping channels.
- Channel reuse should be implemented to minimize CCI.
- For 802.11n implementations, it is possible to aggregate two adjacent nonoverlapping 20-Mhz channels in the 2.4-GHz and 5-GHz range into 40-MHz channels to effectively double the throughput. Note: within the 2.4-GHz frequency, only a single 40-MHz channel can be created, effectively limiting the benefits of 40-MHz channels in 2.4-GHz.

For more detailed information on the types of antennas, please visit:
www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a00807f34d3.shtml.

4.4 WLAN Design

There is no one-size-fits-all template for the majority of healthcare requirements and environments. The following section begins with general principles and then focuses on the Cisco Unified Wireless Network and the high-availability WLAN that Intel implemented based on the Cisco architecture. As previously noted, the Intel WLAN can serve as a reference for consideration in the design of a WLAN for a medium-sized to large acute care facility.

4.4.1 Typical WLAN Configuration

Generally speaking, the network architecture will consist of service areas or SSIDs on the wireless side, mapping to a VLAN or mobility groups on the wired side that allow multiple models to coexist on the same WLAN.

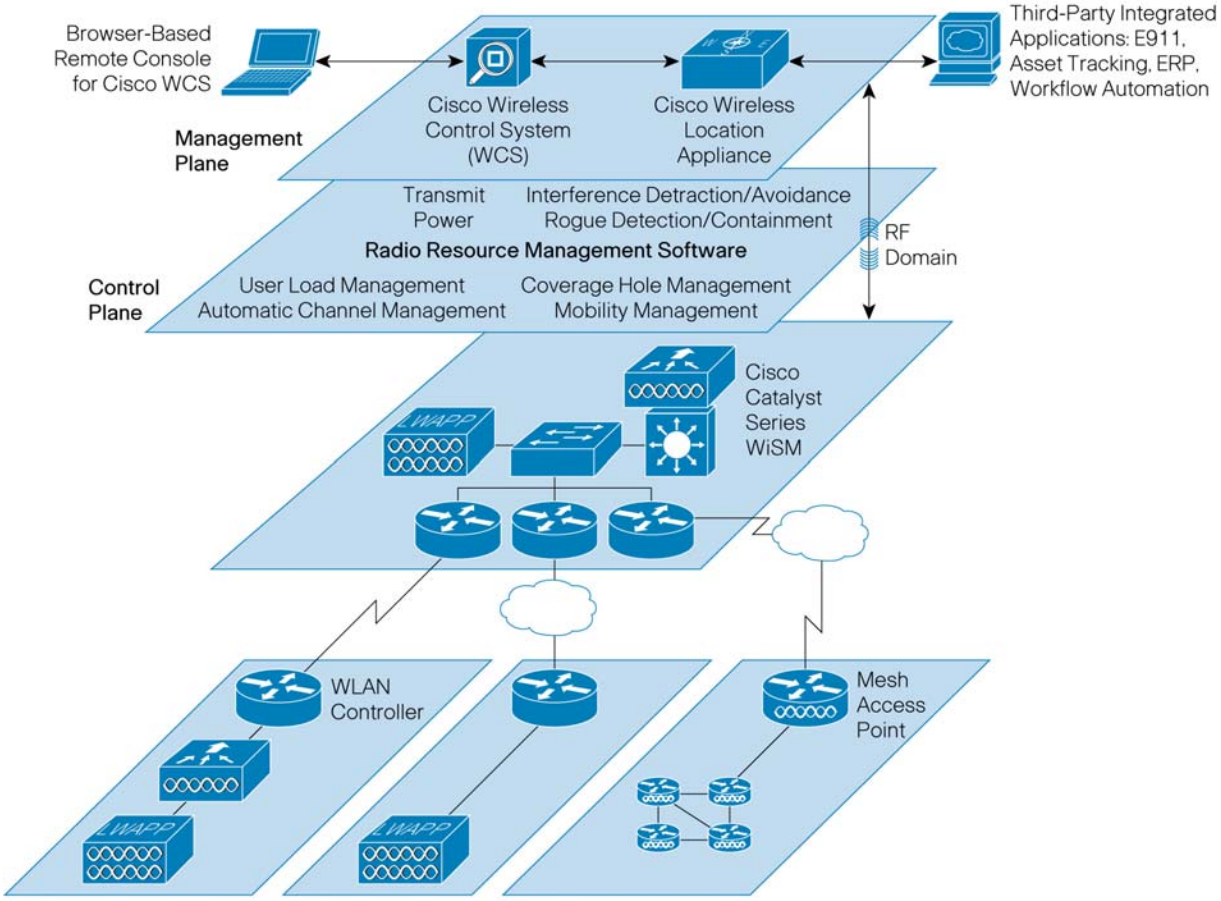
In a typical WLAN configuration, clients communicate through an access point, and the basic service set (BSS) is the coverage area provided by that cell. To extend the BSS, or to add wireless devices and extend the range of an existing wired system, another access point can be added, creating an extended service set (ESS) coverage area. Roaming from BSS to BSS occurs within the ESS coverage area. Typically, each access point attaches to the Ethernet backbone and allows communication between all devices on the backbone and in the cell area.

802.11 ad-hoc peer-to-peer connections are not recommended for hospital applications because of the security concerns they raise.

4.4.2 Cisco Unified Wireless Network

The Cisco WLAN infrastructure product offering is the Cisco Unified Wireless Network (see Figure 2). The architecture is based on the centralization of management and control using WLAN controllers to deliver business-class reliability and scalability. As part of the Cisco Unified Wireless Network, access points can be deployed in standalone or centralized mode. Access points deployed in centralized mode deliver the greatest breadth of mobility services. After considering a number of different possibilities, the Intel IT department decided to base its high-availability campus WLAN on the Cisco Unified Wireless Network architecture.

Figure 2. Architecture of the Cisco Unified Wireless Network



Browser-Based Remote Console for Cisco WCS
Cisco Wireless Control System (WCS)
Cisco Wireless Location Appliance
Third-Party Integrated Applications: E911, Asset Tracking, ERP, Workflow Automation
Management Plane
Transmit Power
Interference Detraction/Avoidance
Rogue Detection/Containment
Radio Resource Management Software
RF Domain
Control Plane
User Load Management
Automatic Channel Management
Coverage Hole Management
Mobility Management
LWAPP
Cisco Catalyst Series WiSM
WLAN Controller
LWAPP
LWAPP
Mesh Access Point

This architecture is recommended by Intel and Cisco because it is relatively easy to deploy and can deliver high levels of security, reliability, and management. It is also scalable to meet the needs of growing healthcare facilities, enabling dozens or thousands of access points to be managed from a centralized console. Organizations with an existing WLAN are encouraged to consider an upgrade to the Cisco Unified Wireless Network architecture. Many of the standalone access point models can be upgraded to work with the Cisco Unified Wireless Network system, thereby reducing financial and reinstallation requirements. For additional information on understanding how to migrate your standalone network to a controller-based architecture please refer to the Guidelines and Tools for Migrating to the Cisco Unified Wireless Network.

The Cisco Unified Wireless Network is composed of a number of interconnected elements that work together as building blocks to deliver a unified, enterprise-class wireless solution. It includes Wi-Fi-enabled client devices, radio resource management capabilities, the Cisco Aironet family of access points based on 802.11a/b/g and now 802.11n connectivity, systemwide network unification and management, and mobility services.[10]

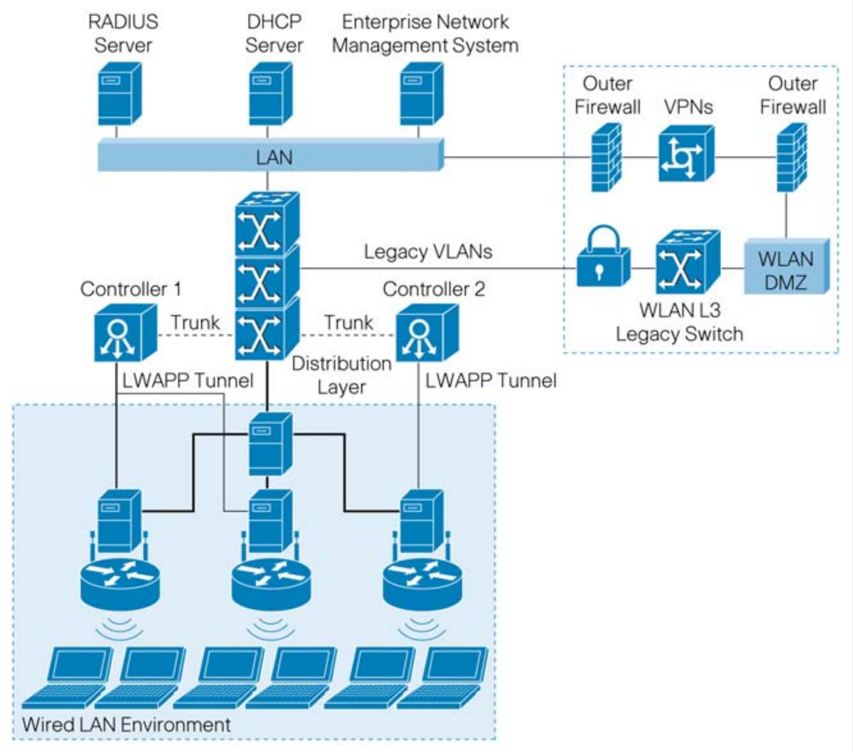
Because of the mission-critical nature of some wireless devices, it is imperative that a level of traffic prioritization be implemented at the VLAN level. Each environment, with its own unique mix of client devices, will require a full evaluation of the applications supported by the wireless network. This data can then be developed into a wireless QoS/class of service (CoS) policy that integrates with the QoS policies of the associated LAN.

[10] *Cisco Unified Wireless Network*, Cisco solution overview, 2007, www.cisco.com/application/pdf/en/us/guest/products/ps430/c1031/ccmigration_09186a0080184925.pdf.

4.5 Case in Point: Intel High-Availability Design

The Intel IT organization designed a campus WLAN based on the Cisco Unified Wireless Network and Intel Centrino processor technology-based notebook computers, which support Cisco Compatible Extensions devices. A high-availability environment, it supports a minimum connection speed of 36 Mbps during normal operation and 24 Mbps if half of the redundant network fails. The environment is designed to support all client types, including desktops, laptops, PDAs, and Wi-Fi phones. Figure 3 shows the logical design of the Intel network.[11]

Figure 3. Logical Design for a Redundant, High-Availability WLAN



This environment is also structured to allow easy installation and control of access points. Management servers allow IT staff to track users and detect and mitigate a wide variety of security offenses. Access points are divided into interspersed grids, as suggested in section 3.3.6. Each grid is connected to a different LAN switch, which supplies the access points with both network connectivity and Power over Ethernet (PoE).

The access points are connected to dedicated, building-level management VLANs. They receive their addresses dynamically from Dynamic Host Configuration Protocol (DHCP) directory servers, and automatically detect a controller available on the appropriate VLAN. An access point will then create LWAPP control and data tunnels to the controller. The controller then automatically configures the access point based on templates. This provides the access point with the correct operating system release, security settings, and other services.

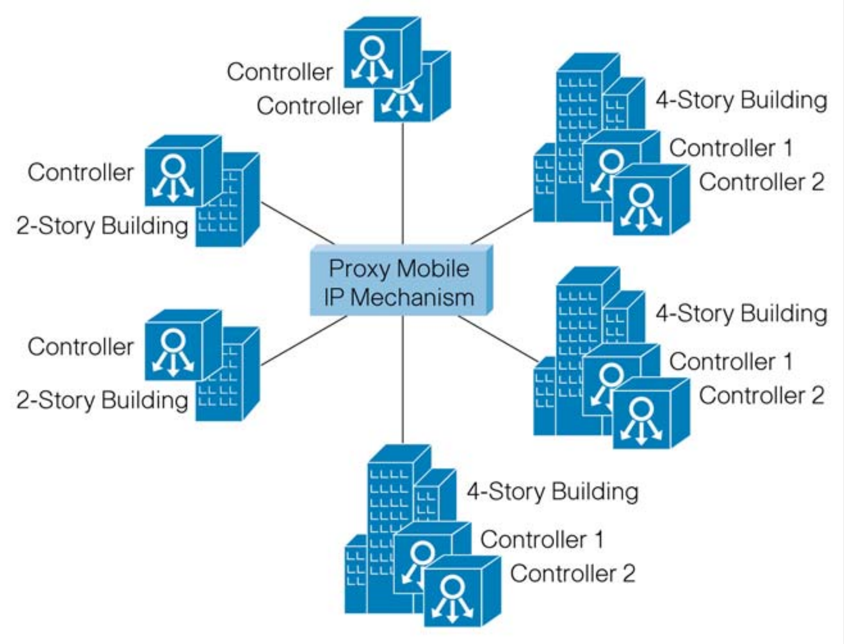
Each access point is assigned a primary controller, a failover controller, and sometimes also a tertiary controller. This provides another level of redundancy, allowing the access point to remain active even if its primary controller becomes unavailable. Full 802.11i encryption is used to provide security for the WLAN. Remote Authentication Dial-In User Service (RADIUS) servers that are shared between LAN and WLAN perform user authentication.

The primary wireless service is available on the 5-GHz 802.11a band only, with legacy services supported on the 2.4-MHz 802.11b and 802.11g band. These include a legacy WLAN, which uses older security that mandates use of a Layer 3 VPN. These services are still provided for users who need them, and go through on-site demilitarized zone (DMZ) firewalls for added security.

[11] Architecture and Design of a Primary Wireless Network, Intel white paper, 2006, http://www.intel.com/it/pdf/architecture-design-of-pwn.pdf.

Campus controller distribution is a critical element of the design. An example installation of this design is shown in Figure 4. It includes three four-floor buildings and two smaller buildings. Each large building uses two controllers to manage the large number of access points. The two smaller buildings have one controller each and are grouped together into a single logical building.

Figure 4. Campus Controller Distribution



With this design, the entire campus becomes a single mobile environment. Clients can roam freely anywhere on campus, with no interruption to applications, as they transition between access points or controllers. In a healthcare setting, this can be essential for enabling campus-wide physician access to decision support systems and other applications that assist clinicians in making treatment decisions.

Within each building, the two controllers share a VLAN, and clients roaming between access points within the building remain on the same IP network. When clients move between buildings they retain their IP address, despite moving into a “foreign” network, through a proxy mobile IP mechanism.

4.6 Security in the Mobile Environment

With patient data traversing the WLAN, security is a vital concern. Robust encryption, authentication, and other standards-based security measures are essential.

4.6.1 Common Security Issues

It is widely known that mobile security cannot rely on basic Wired Equivalent Privacy (WEP) encryption. Stronger security measures must be put in place by the healthcare organization. Examples include Wi-Fi Protected Access (WPA and WPA2), Extensible Authentication Protocol (EAP), and 802.1X protocols. For legacy support of medical or nonmedical devices that require WEP encryption, it is a best practice to keep these devices on their own segregated VLAN.

Another security issue is that the shared key authentication feature of a WLAN can open the network to attack. The access point challenges the WLAN user to ensure possession of a valid encryption key. However, the challenge takes place in a cryptographically flawed manner that enables an attacker to obtain the key stream during the process. The shared key authentication feature is therefore not recommended for deployment.

Many attacks can be easily detected and contained with common rogue access point detection mechanisms. Risk can also be mitigated with cryptographic binding of authentication exchanges.

Media Access Control (MAC) and IP address spoofing are both possible in WLANs. An outside attack via IP address spoofing can be mitigated if encryption is turned on (where DHCP messages are encrypted between the client and the access point). The station still effectively spoofs the MAC address, but it does no good since network access is prevented. EAP/802.1X authentication, in which a unique encryption key is derived per user, is also effective against spoofing.

Denial-of-service (DoS) attacks are critical considerations when implementing primary WLANs. DoS threats can be classified into physical layer and MAC layer threats. From an architecture perspective, DoS threats can be handled by an additional infrastructure overlay, or protection can be embedded into the production WLAN infrastructure. For the Intel high-availability WLAN, Intel IT used the production infrastructure with dedicated access points to detect DoS threats, as well as a separate location-based server to locate and track multiple threats such as rogue devices in real time.

4.6.2 Architecting Security for the WLAN

The basic requirements for providing WLAN security include:

- Encryption to ensure data privacy, using the Temporal Key Integrity Protocol per-packet keying (TKIP-PPK) or Advanced Encryption Standard (AES)-Counter with Cipher Block Chaining Message Authentication Code (CBC-MAC) algorithm
- Message integrity, to ensure that data frames are tamper-free and truly originate from the source address, based on Temporal Key Integrity Protocol-Message Integrity Check (TKIP-MIC) or Advanced Encryption Standard (AES)-Counter with Cipher Block Chaining Message Authentication Code (CBC-MAC)
- An authentication framework that facilitates authentication messages between clients, access points, and the authentication, authorization, and accounting (AAA) server, based on the EAP/802.1X protocols
- An authentication algorithm to validate client credentials, such as Protected EAP Transport Layer Security (PEAP TLS) or EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)

It is a best practice to use 802.1X protocols to authenticate devices and derive keys to secure controller-to-access-point traffic. The Intel IT department’s WLAN architecture incorporates the 802.1X authentication framework with RADIUS authentication severs.

Intel uses the 802.11i encryption process. The 802.11i four-way handshake includes the creation of a Transit Master Key (TMK) for encrypting Unicast messages and a Group Master Key (GMK) for encrypting multicast and broadcast messages. This process also includes the mutual authentication of the client and associated access point.

Other best practices include mapping wireless security policies to the wired network and assigning user and device groups to wired access policy via SSIDs, VLANs, identity, and RADIUS. Some of the advanced security features on wired switches are especially applicable to wireless, including rate limiters to prevent DoS attacks using “bogus” traffic and TCP Intercept to prevent flooding attacks.

Determining which EAP type to utilize (or the need to implement multiple EAP types) can be a complex question.[12] A detailed review of existing and future client device capabilities and requirements, existing AAA servers, and related factors must be accomplished. Table 3 provides a feature and capability summary of common EAP/802.1X types.

Table 3. EAP/802.1X Features and Capabilities

	TLS	TTLS	PEAP	FAST	LEAP
Client-side certificate required	Yes	No	No	No (PAC)	No
Server-side certificate required	Yes	No	Yes	No (PAC)	No
Rogue access point detection	No	No	No	Yes	Yes
Authentication attributes	Mutual	Mutual	Mutual	Mutual	Mutual
Deployment difficulty	Difficult (because of client certificate deployment)	Moderate	Moderate	Moderate	Moderate
Wireless security	Very high	High	High	High	High when strong passwords are used

[12] For more information, see Cisco Wireless LAN Security, Cisco solution overview, 2007.

TLS, while very robust, requires client certificates to be installed on each wireless workstation. Maintenance of a public key infrastructure (PKI) requires administrative expertise and time in addition to that for maintaining the WLAN itself. Tunneled TLS (TTLS) addresses the certificate issue by tunneling TLS, thus eliminating the need for a certificate on the client side, often making this a preferred option. TTLS is primarily promoted by Funk Software and Certicom, and there is a charge for supplicant and authentication server software.

Cisco LEAP has the longest history, and while it was previously proprietary to Cisco and worked only with Cisco wireless adapters, Cisco has licensed LEAP to a variety of other manufacturers through the Cisco Compatible Extensions program. A strong password policy should be enforced when LEAP is used for authentication. EAP-FAST is now available for enterprises that cannot enforce a strong password policy and do not want to deploy a full PKI system for authentication. Cisco has licensed EAP-FAST to a variety of other manufacturers through Cisco Compatible Extensions.

The more recent PEAP works similarly to EAP-TTLS in that it does not require a certificate on the client side. PEAP is backed by Cisco and Microsoft, and is available at no additional cost from Microsoft. If the IT organization desires to transition from LEAP to PEAP, the Cisco Secure Access Control Server (ACS) authentication server will run both.

4.6.3 Guest Access Design

The WLAN will be the primary means of allowing guests to access network services. The design must comprehend the security and service consumption implications of having users on the WLAN who are not employees of the medical facility.

Security policy is the starting point for developing the guest Internet access portion of the WLAN design. Examples of security considerations are:

- Legal liability
- Access controls
- Ability to deactivate clients if required
- Level of logging and accounting needed per legal and security requirements

Generally, legal liability includes ensuring that guests accept a Terms of Use policy for using the provided network and agree to be liable for any activities or security incidents that may result from inappropriate use of the resources.

Guest Internet access should be as controlled as possible. For example, it is recommended that no access be allowed to the internal network and resources of the healthcare organization. Access to the Internet on specific ports and protocols, and to the VPN back to the clients' home networks, are examples of "allowed" network access. If there is a business requirement for patients or visitors to access any internal data, this should be protected using the appropriate controls for authentication and authorization as required by information security and regulatory guidelines. The initial sign-on page for guests may include instructions via a "walled garden," detailing any steps required to gain access to protected internal data.

Auditing requirements should be used to guide the level of logging and accounting for the access. As part of the logging information, regulatory and legal considerations should be addressed—for example, it may be necessary to state that no personal identifiable information is collected, or if it is, how it may be used. This can be part of the Terms of Use policy.

While providing guest Internet access is often an important business requirement, the network must be designed so that guests do not overwhelm the available resources or interfere with business functionality. Based on access requirements, designers should implement QoS or bandwidth controls to protect WLAN and back-end network resources for internal use.

Implementation includes setting aside an SSID with an appropriate name such as "Guest Network" and assigning it to a VLAN that is completely isolated from other SSID/VLANs available from the WLAN network infrastructure. This provides a level of isolation at the access layer that can be used to further implement controls at the network back end. For example, the "Guest Network" VLAN can be routed only to network devices that implement the network bandwidth controls.

Internet connectivity can be provided in a distributed or centralized manner, depending on the network architecture used for other services. As an example, if each facility has an Internet access point, the guest traffic can be routed to the Internet at each site. Or, if there is a centralized Internet connection supporting multiple sites and locations, the guest traffic can be routed to the central location for Internet access.[13]

4.6.4 Security on the Client Devices

The preceding sections describe security considerations with respect to authentication and encryption of the wireless transmission. Another important consideration, although out of immediate scope of this document, is worth briefly mentioning here: client security is equally important for securing the content. IT organizations must be able to remotely monitor system health and conformance to IT security policies beyond the version and configuration control provided by the Intel PROSet/Wireless Administrator Tool.

The introduction of Intel Centrino Pro processor technology and enabled management solutions allow IT staff to manage wireless clients remotely. Systems can be provisioned wirelessly with new software and driver updates; software agents can be reinstalled or reactivated; and alerts can be generated for IT staff when issues arise. This can be achieved even when the client's operating system is disabled. For more information, please refer to www.intel.com/go/centrinopro.

The implementation of WLAN and client-side security measures will help ensure the maximum level of security for the healthcare IT environment.

4.7 Quality of Service

Hospital management and IT need to develop a common policy to guide QoS traffic prioritization. This policy should be developed from the organization's mission and goals, as well as regulatory requirements. The IT organization will then use the policy to prioritize packets as they pass over the wired and wireless portions of the network. The policy should help drive application decisions, network design, deployment, and operations.

Designers should consider a migration strategy to allow the number of classes to be smoothly expanded as future needs arise. The number of specific QoS classes required to be implemented will vary from one organization to the next. The hospital WLAN may need to support:

- Voice (as VoIP) real-time operations
- Videoconferencing (as VoIP and video over IP) real-time operations
- Biometric data (may be Layer 2 tunneled) critical data operations

4.7.1 Delivering Voice Quality

For its high-availability campus WLAN, Intel uses a client software package to ensure resource allocation and prioritize packets transmitted from the client. This approach, used together with a robust infrastructure and prioritization over the network, can significantly improve voice quality.

To prioritize traffic within the wired LAN, the IEEE 802.1p standard defines eight priority queues. The WLAN equivalent of 802.1p is 802.11e, which has recently been certified but is not yet extensively supported. In the near term, expect to use the interim IEEE solution, WMM, which is becoming widely available.

With WLANs, unlike switched wired LANs, clients have to share the bandwidth provided by each access point. This requires that the MAC layer handle medium-access prioritization. The priority is set by altering the expected amount of time a station waits for medium access, depending on the traffic service type. This is a called a contention window. WMM defines four access categories, or service levels, where the top category—voice—has the shortest contention window, and therefore the best statistical chance of transmitting frames first.

In case of an 802.11n deployment, for clients to realize 802.11n speeds, it is imperative to enable the WLAN with Wi-Fi Multimedia (WMM) (set to either allowed or required, depending on your needs and client support). Also, 11n *requires* that AES cryptography be performed on all encrypted links.

[13] For detailed information on designing guest access, see *Achieving Business Goals and Enhancing Customer Relationships with a Secure Guest Access Wi-Fi Network*, Cisco white paper, 2006, www.cisco.com/application/pdf/en/us/guest/products/ps6366/c1244/cdccont_0900aecd8047180a.pdf; and *Cisco Wireless LAN Access Planning and Design Service Bundle*, Cisco data sheet, 2005, www.cisco.com/application/pdf/en/us/guest/products/ps2738/c1262/cdccont_0900aecd80358b6d.pdf.

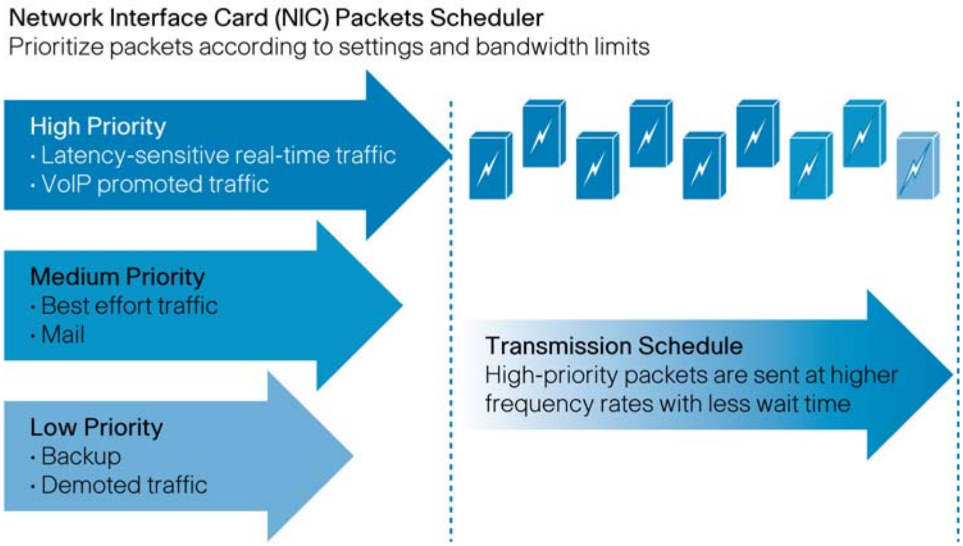
Wireless networks require stringent signal strength and coverage characteristics to deliver quality voice over WLAN (VoWLAN). For healthcare organizations that would like to take advantage of their existing Cisco Unified Wireless Network infrastructure for voice applications, Cisco offers a new VoWLAN Readiness Tool[14] that facilitate fast and simple visualization of design guideline compliance for voice over Wi-Fi. Wireless network degradations are rapidly identified and addressed, helping maintain user satisfaction. Operations and maintenance are simplified because VoWLAN calibration can be quickly assessed.

4.7.2 Client Package

The client package selected by Intel IT prioritizes transmitted packets and helps ensure that adequate client resources are reserved for voice. Intel uses a service that exploits the Microsoft Windows* traffic control API to prioritize traffic for transmission. It defines traffic flows and filters traffic based on the transport layer ports used by different applications, assigning matching packets to specific flows.

Two flows are defined: promoted and demoted. The promoted flow is used for latency-sensitive, real-time traffic such as voice. The demoted flow is for backup and other lower-priority applications. Bandwidth floors and ceilings are set for each flow. All traffic that does not match these filters is treated by default as normal best-effort traffic and becomes a medium-priority flow, as shown in Figure 5.

Figure 5. Packet Prioritization on the Client


Network Interface Card (NIC) Packets Scheduler
Prioritize packets according to settings and bandwidth limits
High Priority
· Latency-sensitive real-time traffic
· VoIP promoted traffic
Medium Priority
· Best effort traffic
· Mail
Low Priority
· Backup
· Demoted traffic
Transmission Schedule
High-priority packets are sent at higher frequency rates with less wait time

For handheld 802.11 Wi-Fi phones, the device marks the packets using WMM and the infrastructure grants all of its packets voice-type service. This QoS approach meets the requirements for wireless voice over the campus network. However, as Intel IT moves forward to deploy this architecture more widely, it is expected that a broader approach will be required to impose more fine-grained, application-level control over quality and to achieve end-to-end QoS.

Plans call for the current QoS package to be expanded so that it can track any connection opened by an application process and use the socket information unique to that process to generate a specific rule for handling by the packet scheduler. This will enable prioritization of traffic based on the application that created it.

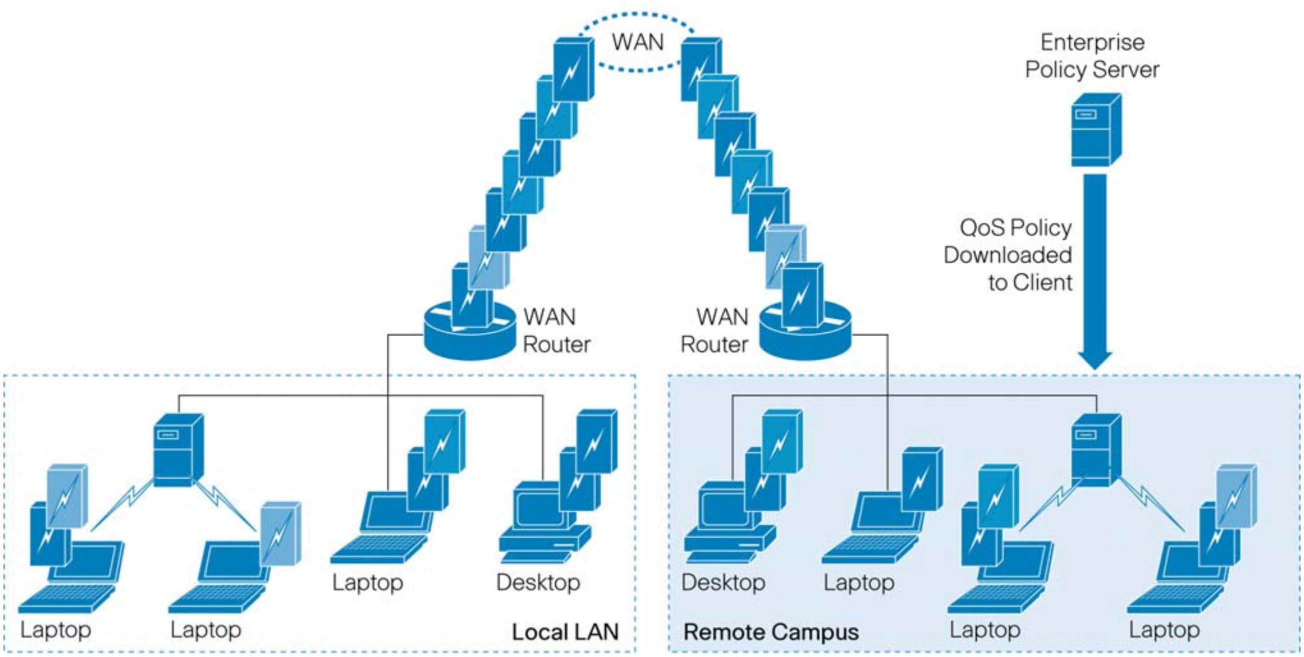
[14] Learn more about the voice services enhancements supported by Cisco Unified Wireless Network Software Release 4.2 and 4.1 by reading the Feature Brief-Voice over WLAN Solutions Using Cisco Unified Wireless Network Software Releases 4.1 and 4.2.

4.7.3 Central Policy Control

Moving from an initial campus WLAN to a broader deployment will require a toolset that allows easy deployment and central administration of client agent software and QoS policies.

Ideally, this would involve a single QoS policy agent on the client, handling resource management and packet prioritization according to corporate policy and operating outside the user's control. This agent should be controlled and monitored from a central policy server and integrate with other corporate security and policy mechanisms. Figure 6 shows one potential arrangement, with end-to-end prioritization of packets according to policies set at an enterprise policy server.

Figure 6. Packet Prioritization Using an Enterprise Policy Server



4.8 Power Outage Recovery

To ensure business continuity a wireless deployment in a healthcare environment should be designed for the possibility of a natural disaster or other occurrence that causes power failure. When primary power and ground-based telecommunications are unavailable, hospital facilities must continue to operate via auxiliary power and alternate forms of communications. Limited operations should be made possible during a facility evacuation.

During a widespread power outage, auxiliary power to the wireless network is also a key design consideration. Unlike traditional voice traffic that is dependent on powered regional hubs or base stations, communication within the healthcare facility is possible with an auxiliary powered WLAN. Ensuring an auxiliary power supply to both the wired and wireless infrastructure will help clinical and extended staffs maintain mobile access to the electronic medical record, clinical information, and communication systems during a disaster.

Wireless networks should be able to resume service faster using power over Ethernet (PoE). Hospitals should consider whether or not they would like to take advantage of this faster time to disaster recovery.

Current 802.11a/b/g access points operate using PoE that provides 15 watts of DC power over the cat 5 Ethernet cable. For 802.11n access points, more than 15 watts of power is required due to the multiple antennas inherent to the 802.11n standard. The IEEE PoE standard (IEEE 802.3at) stipulates 30 watts of DC power for 802.11n access points.

Migrating from 802.11a/b/g to 802.11n requires planning for this higher power requirement. One way is to provide power via the Ethernet switch the access point is connected to. Healthcare organizations should evaluate Ethernet switches that can deliver adequate power from a single switch port to fully power dual-mode 11n access points. A second option is to utilize an inline power injector which connects between the switch and the access point and provides the power for the access point.

Hospitals wishing to have Wi-Fi VoIP accessibility during power or land-based communications outages should design their network so that Wi-Fi phones will not fail to authenticate with the AAA server. The AAA server should also be able to operate via auxiliary power. Otherwise, the Wi-Fi phones will not be useful because they will not be granted access to network resources.

4.9 WLAN Management

The complexities of the RF spectrum and EMI, along with the diversity of mobile devices and users in a wireless environment, require a WLAN management system.

The Cisco Wireless Control System (WCS) is a Cisco Unified Wireless Network management tool that adds to the capabilities of the Web user interface and command-line interface (CLI), moving from individual controllers to a network of controllers. WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level, and adds a graphical view of multiple controllers and managed access points.

Cisco and Intel recommend a level of wireless Intrusion Protection System (IPS) to protect against wireless threats such as rogue access points and denial-of-service attacks. The Cisco Unified Wireless Network offers several wireless IPS deployment modes to meet the varying needs of the enterprise. Access points can be deployed to serve clients and scan for wireless threats, or deployed as dedicated air monitors only.

5. Implement

Once design decisions have been made and approved, the implementation phase can proceed. This phase includes procurement, deployment planning, and execution.

5.1 Procurement

All of the components and resources should be ready prior to execution. Lack of a key component or resource can prevent the deployment from moving forward as planned. This is particularly important for controllers and control systems. In addition, the IT organization should have installation resources lined up to perform the work of installing the hardware, connecting it to the network, and installing and connecting access points. Best practices for procurement include the following:

1. Order fiber gigabit interface converters (GBICs) not only for any new switches, but also for the old switches to which they will be connected—an easy item to miss.
2. If you are unsure about antenna types, Intel has almost exclusively deployed omnidirectional 2.2-dB dipole antennas with good results.
3. Access point density in cafés, conference rooms, and auditoriums will often need to be higher than the standard density of one per 3000 to 5000 square feet because of the higher density of people and clients. Likewise, high-traffic areas such as emergency rooms and intensive care units will require additional access points. One procurement technique is to order 5 to 10 percent more access points than planned, to use later as any coverage holes emerge.

5.2 Deployment Planning and Execution

Deployment planning should include a step-by-step list such as the following:

1. Order equipment.
2. Install cabling can be started while waiting for ordered equipment to arrive).
   - Run cabling in the ceiling with terminal outlets located every 60 feet in a grid pattern. This permits the cabling to be installed before the access points are located and allows flexibility for future changes. The access points do not have to be located immediately adjacent to one of the terminal outlets, only within 30 feet of an outlet.
   - Confirm the planned location of access points using software such as the Airmagnet Site Survey Planner or WCS Airwave Planning software.
   - Order fiber patch cables for deployment between switches.
   - Ensure adequate cabling between buildings and switches to connect all parts of the network.
3. Inventory equipment as it arrives.
4. Mount access points to the ceiling.
5. Connect controllers to switches and perform initial configuration to ensure they are accessible.
6. Configure switches and VLANs to support management and users.

7. Configure RADIUS to accept EAP sessions from controllers (to act as network access server devices).
8. Configure Domain Name System (DNS) for all devices (assign static IP addresses)—does not include access points, as they use DHCP.
9. Configure DHCP scopes for access point management VLANs and client VLANs.
10. Configure all controllers.
11. Connect access points to switches so that they can auto-discover controllers.
12. Verify configurations.
13. Enable radio on one access point to test connectivity.
14. Perform acceptance testing in various locations—testing signal strength and throughput.

In environments with extensive concrete and metal, or hard walls such as those in healthcare facilities instead of soft cubicle walls, access point locations will need to be tested to verify good coverage. Be sure to test the coverage of the access points with room doors open as well as closed, as that can have a significant effect on coverage. For healthcare environments, which can be difficult to characterize, the physical site survey is considered the best tool available.

The use of a centralized controller greatly simplifies the deployment process for access points. In the past, each access point had to be manually adjusted to select a unique channel, name, IP address, and power setting before it could be placed in the ceiling. Technicians might spend hours configuring the 100 or more access points for a typical building.

With a centralized architecture such as the Intel WLAN, all of those access points can be configured at once using the controller. Technicians can simply remove the access points from the box and connect them to the switch. The access points discover their controller, download the right firmware, and then download their configuration.

It is highly recommended to start with installation in two locations—for example, two different buildings or floors—and run in pilot mode with a few users for several weeks to validate that the WLAN design works as planned. A pilot is ideal for tuning the WLAN configuration and performing validation. In phase 1 of the pilot, WLAN and client performance should be quantitatively measured against specific criteria (see section 6.2). Phase 2 of the pilot should validate usage under worst-case scenario conditions.

Once all validation requirements are met, the pilot is complete and technicians can proceed with deployment throughout the facility. Formal user acceptance of the wireless solution per SLAs should be performed before the WLAN is moved to production status. A best practice is to operate the WLAN in a steady state, meeting all performance criteria for a period of time, before declaring it ready for full production.

6. Operate

During the operation phase, the IT organization must support the WLAN, monitor performance, and continue to make any necessary adjustments.

6.1 Training and Certification

For the IT organization to provide quality support, training is imperative. An inventory of current training levels should be conducted among personnel who will be administering the WLAN, and a program established to meet the organization's training objectives. Certification can be made a part of the training program to provide tangible objective milestones and to demonstrate results to management.

A variety of vendor-specific, vendor-neutral, and combination training courses are available, including:

- **Cisco Wireless Network**—Cisco provides WLAN and product training in an instructor-led environment. There are two categories of training leading to the Cisco Qualified Specialist designation, one for design and one for implementation. Intel and Cisco highly recommend this training. Certification is valuable because it allows in-depth and measurable understanding of the wireless network.
- **Certified Wireless Network Professional (CWNP)**—This vendor-neutral training is suggested for organizations desiring technical training that is not vendor-specific or extends beyond the scope of vendor training.
- **WLAN Diagnostic Tools**—IT organizations will need to use multiple tools to deploy and maintain the WLAN, and formal training is required to properly use them and get the most out of the tool investment. Otherwise, design and implementation may not be successful. Training is available from each of the tool vendors.

Several excellent publications are available as a supplement to training or to help prepare individuals for certification testing. Intel recommends the following reading list:

- ***Wireless Certification Official Study Guide (Exam PWO-050),*** **by Tom Carpenter**—If you are new to wireless or want an overview of a variety of wireless technologies, this is an easy-to-read book. Topics discussed include Wi-Fi, Bluetooth, WiMAX, infrared, RFID, and VoWLAN. This publication is designed as a study guide for the PWO-050 level Certified Wireless Network Administrator (CWNA) exam.
- ***Certified Wireless Network Administrator Study Guide (Exam PWO-100),*** **by David D. Coleman and David A. Westcott**—This book is intended as a study guide for the CWNA PWO-100 exam. If the individual is new to 802.11, this is essential reading.
- ***Cisco Wireless LAN Security (Networking Technology),*** **by Krishna Sankar**—A good overall source of information on wireless security, this book provides Cisco specifics but is not limited to Cisco technology.
- ***CWAP—Certified Wireless Analysis Professional Official Study Guide (Exam PWO-205),*** **by Planet3 Wireless**—Ideal for those who are experienced and knowledgeable about 802.11, this book looks at details "under the hood" covered by the PWO-205 exam. It discusses WLAN analysis, including the inspection of a WLAN and the assessment of performance, security, RF coverage, and root causes of problems.

6.2 Performance Monitoring

Monitoring and managing the WLAN is an ongoing task that requires defined metrics and goals tied to intended usage and workflow scenarios. Some suggested monitoring parameters are as follows:

- **Concurrent users per access point (Intel threshold: <20)**—This parameter is the number of users that simultaneously transmit or receive data to or from the access point. A threshold example might be that an access point should have 20 or fewer connected users at any one time.
- **Access point utilization (Intel threshold: <90 percent)**—This is the percentage of time the access point is actively transmitting or receiving packets. There must be enough headroom so that the access point can handle random bursts of simultaneous activity. Allowing 90 percent utilization (or, in other words, 10 percent idle time) provides a buffer for this purpose.
- **Controller microprocessor utilization (Intel threshold: <50 percent)**—The back-end controller that directs traffic to and from access points, dynamically controlling signal strength or roaming handoffs, must not be overwhelmed. A substantial buffer should be maintained to handle sudden bursts of activity.
- **Controller free memory (Intel threshold: >50 percent)**—As with controller microprocessor utilization, a buffer should be maintained for controller free memory. There must be enough free space to handle the routing of packets during peaks of high activity.
- **Interference (Intel threshold: <20 percent on 802.11b/g, <10 percent on 802.11a)**—This metric relates to CCI. The 802.11 packets that are inadvertently received from other cells, and interfere with data reception, must be kept below an acceptable limit.
- **Noise (Intel threshold: <10 percent)**—Any RF energy that is not an 802.11 packet is considered to be noise. Noise levels should be less than 10 percent; otherwise the environment has serious noise problems that will affect wireless performance.
- **Poor signal-to-noise-ratio clients (Intel threshold: <10)**—The signal-to-noise ratio enables noise to be understood as a baseline to assess the relative strength of the active signals. Intel IT sets a low threshold for poor-performing clients.
- **Channel changing frequency**—The frequency of channel changes of a lightweight access point can affect the ability to re-associate properly or maintain continuous connectivity for client devices such as laptops, PDAs, and wireless-enabled medical equipment. Specific parameters for channel changing frequency are not defined. Each healthcare facility should investigate its environment to determine the threshold to ensure optimal coverage and security.

Numerical values listed for each metric are specific to the Intel campus WLAN and are shown for illustrative purposes.[15] In general, they are in line with thresholds recommended in healthcare facilities. However, each healthcare IT organization should conduct their own analysis based on their design specifics, goals, and requirements.

The Intel IT organization gathers most WLAN monitoring information directly from the controllers, storing it in a data warehouse. Other data is collected from clients, servers, and back-end devices such as VoIP, authentication, and IP management servers. Management of the RF environment focuses on finding a balance between WLAN capacity and fidelity. Tracking client data enables IT staff to see the network from the user's perspective.

[15] For more information, see *Managing and Monitoring a Primary Wireless Network*, Intel white paper, 2007, www.intel.com/it/pdf/Managing-and-Monitoring-a-Primary-Wireless-Network.pdf.

Analysis is performed and reports are generated based largely on the thresholds set for the various parameters. These thresholds are continually refined based on experience.

7. Optimize

Troubleshooting and fine-tuning are essential activities during the optimization phase. The following are best practices for healthcare IT organizations to consider in designing their own optimization programs.

7.1 Software and Driver Updates

For consistency of service, it is best to keep the client environment as homogeneous as possible. Ideally, this means the same hardware, connectivity client software, and drivers should be deployed throughout the environment. Software, driver, and firmware updates are frequently made available to address known issues.

It is a best practice to always update clients and infrastructure hardware with the latest software stack and device driver whenever an issue is observed, before investing time and resources in troubleshooting. Once a problem has been identified, installing the latest software release may well solve the problem. Prior to contacting any technical support organization, it is best to have installed and tried the latest software release, and to have the most recently tried version number available.

To find the latest public software availability for Intel wireless products, visit: support.intel.com/support/wireless/wlan/sb/cs-010623.htm.

7.1.1 Access Points and Firmware Updates

Most access point manufacturers release regular firmware upgrades to address compatibility and other connection issues. The healthcare IT organization should ensure that they have the latest firmware on all of the applications. The fact that an access point is new does not ensure that it is running the latest firmware. In fact, off-the-shelf access points typically do not have the latest firmware installed. Many access point issues can be improved or resolved with a firmware upgrade.

In the case of lightweight access points such as Cisco LWAPP, firmware maintenance for each individual access point is unnecessary due to the centralized control and management by the backend controller. This is a significant benefit of a unified wireless architecture.

7.1.2 Testing for Client and Infrastructure Upgrades

For all new software releases, thorough testing on clients should be performed before release to the general user population. Testing on a representative sample of all clients running in the environment will root out most issues before those problems affect users and support staff. This best practice also applies to the WLAN infrastructure software, to ensure that all critical equipment and applications will behave normally when upgrades are deployed.

7.1.3 User Support

Updates and upgrades can catch some WLAN users off-guard. A key to keeping customer support incidents low is to find a way to deliver training to users quickly and effectively. A short 15-minute orientation on new capabilities with wireless devices and software can save hours of support time and user frustration.

7.1.4 Client Troubleshooting

It is recommend that the IT organization always examine problems holistically and refer to the vendors’ latest troubleshooting guidelines.

7.2 Optimization Tools

Due to the underlying complexities of today’s WLANs, it is imperative that proper tools are available for the installation, ongoing maintenance, and optimization of a WLAN. A best practice is to keep a set of software diagnostic tools on site that are WLAN specific. Key assets for network optimization include:

- WLAN analyzer
- RF spectrum analyzer
- RF site survey tool
- Protocol analyzer for 802.11

WLAN analyzers allow the technician to see into the WLAN at a detailed level. Channel usage, throughput, and a variety of other parameters are readily available. Additionally, many WLAN analyzers include an 802.11-specific protocol analyzer.

RF spectrum analyzers allow the technician to see the non-WLAN items in the RF environment in detail. This allows for the easy identification and isolation of interference sources for the WLAN. A hospital environment is rich in potential sources of interference, from medical diagnostic equipment to telemetry monitors. There is simply no other way to readily diagnose and resolve interference issues than a spectrum analyzer.

RF site survey tools allow the technician to define access point placement before installation or verify coverage after the installation. Site survey tools can also be used for ongoing troubleshooting efforts and for monitoring environments as changes are made.

Protocol analyzers allow users to observe, analyze, and diagnose the behavior of installed networks. The technician can actually see in detail what is occurring within frame exchanges. Often an on-site technician may be asked to provide a protocol trace to help the IT organization solve a problem, and a protocol analyzer is ideal for this task.

A variety of client analysis packages are available commercially. When combined with network analysis, client analysis allows the technician to view a complete picture of LAN and WLAN traffic. This can be very helpful for optimization and troubleshooting. Client analysis packages are able to focus on either application performance or network performance. A tool that can be used to log and understand the network traffic generated by client applications will prove to be a valuable asset.

8. Conclusion

In summary, by using a centralized architecture combined with a strong emphasis on monitoring performance and network health, IT organizations should be able to mitigate the bandwidth and service-level challenges of WLAN management, providing users with dependable service and many valuable benefits.

Those benefits include greatly increased access to tools and information. In healthcare settings, a WLAN can ultimately lead to improvements in quality of care, patient satisfaction, staff efficiency, and clinical outcomes. Intel and Cisco see significant opportunities for healthcare organizations to reap the benefits of mobile technology, and are ready to help healthcare IT departments successfully complete the six-step process described in this document.

This guide is intended to help healthcare IT departments become familiar with the principal considerations behind a wireless infrastructure and client deployment. Additional documents are available from Intel and Cisco that provide more detailed information on various aspects of WLAN technology, validation, design, and implementation.

For more information, please visit:

Intel at www.intel.com/it/mobility-wireless

Cisco at www.cisco.com/en/US/products/hw/wireless

Or contact your local Intel or Cisco representative.

Bibliography

(In order of reference)

Queensland Health: Checking Vital Signs of IT Infrastructure at Herston Hospitals, Intel case study, 2004, www.intel.com/cd/services/intelsolutionservices/asmo-na/eng/success/casestudies/179115.htm

Managing Wireless Clients with the Administrator Tool, Intel white paper, 2006, www.intel.com/network/connectivity/products/whitepapers/admin_tool_wp.pdf

Electromagnetic Fields and Public Health, World Health Organization Fact Sheet No. 304, 2006, www.who.int/mediacentre/factsheets/fs304/en/index.html

Electromagnetic Compatibility—Cellular Phone Interference, FDA publication, 1995, www.fda.gov/cdrh/emc/pace.html

"Potential for Personal Digital Assistant Interference with Implantable Cardiac Devices," article by Jeffrey L. Tri, Jane M. Trusty, and David L. Hayes, *Mayo Clinic Proceedings* 79: 1527–30, 2004, www.mayoclinicproceedings.com/pdf%2F7912%2F7912a7.pdf

"Wireless Technologies and Patient Safety in Hospitals," article by Justin Boyle, *Telemedicine and e-Health* 12: 373–82, 2006, e-hrc.net/pubs/papers/pdf/RP-JB-tech-review-wireless-tech-patient-safety.pdf

Guidance on Electromagnetic Compatibility of Medical Devices for Clinical/Biomedical Engineers—Part 1: Radiated Radio-Frequency Electromagnetic Energy, Association for the Advancement of Medical Instrumentation (AAMI) TIR18:1997, 1997, webstore.ansi.org/ansidocstore/product.asp?sku=AAMI+TIR18%3A1997

Radiofrequency Interference with Medical Devices, IEEE Committee on Man and Radiation (COMAR) Technical Information Statement, 1998, www.ewh.ieee.org/soc/embs/comar/interfer.htm

Electromagnetic Compatibility—FDA/CDRH Recommendations for EMC/EMI in Healthcare Facilities, FDA publication, www.fda.gov/cdrh/emc/emc-in-hcf.html

Cisco Unified Wireless Network, 2007, Cisco solution overview, www.cisco.com/application/pdf/en/us/guest/products/ps430/c1031/ccmigration_09186a0080184925.pdf

Architecture and Design of a Primary Wireless Network, Intel white paper, 2006, www.intel.com/it/pdf/architecture-design-of-pwn.pdf

Achieving Business Goals and Enhancing Customer Relationships with a Secure Guest Access Wi-Fi Network, 2006, Cisco white paper www.cisco.com/application/pdf/en/us/guest/products/ps6366/c1244/cdccont_0900aecd8047180a.pdf

Cisco Wireless LAN Access Planning and Design Service Bundle, Cisco data sheet, 2005, www.cisco.com/application/pdf/en/us/guest/products/ps2738/c1262/cdccont_0900aecd80358b6d.pdf

Managing and Monitoring a Primary Wireless Network, 2007, Intel white paper, www.intel.com/it/pdf/Managing-and-Monitoring-a-Primary-Wireless-Network.pdf

Appendix A: Supplemental Reading

(Alphabetical order)

Certified Wireless Network Administrator Study Guide (Exam PWO-100), by David D. Coleman and David A. Westcott

Cisco Wireless Control System (WCS), www.cisco.com/en/US/products/ps6305/index.html

Omni Antenna vs. Directional Antenna, www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a00807f34d3.shtml

Cisco Wireless LAN Security (Networking Technology), by Krishna Sankar

CWAP—Certified Wireless Analysis Professional Official Study Guide (Exam PWO-205), by Planet3 Wireless

Wireless Certification Official Study Guide (Exam PWO-050), by Tom Carpenter

Appendix B: Intel and Cisco Product Details

Intel PROSet/Wireless Software

The Intel® PROSet/Wireless Software works in conjunction with Intel® PRO/Wireless Network Connection 2200BG, 2915ABG, 3945ABG and Intel® Wireless WiFi Link 4965AGN hardware to connect your notebook or desktop computer to a wireless LAN.

As Figure 7 and Table 4 show, Intel® PROSet/Wireless Software offers rich features for easy use and deployment of wireless clients.

Figure 7. Intel PROSet/Wireless Software

Ease of Use

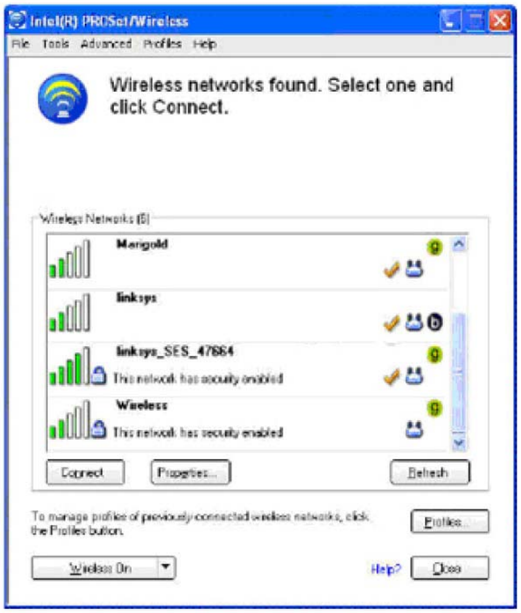
- Simplified user interface
- Auto-detection of access points
- Profile management
- Intel Wireless Troubleshooter
- Wi-Fi Protected Setup

Security

- IEEE 802.11i/WPA/WPA3
- 802.1x authentication
- Auto security detection
- Single Sign-On (SSO)

Management

- Administrator Tool
- Business-Class Wireless Suite
- Intel Active Management technology



Wireless networks found. Select one and click Connect.

This network has security enabled

To manage profiles of previously-connected wireless networks, click the Profiles button.

Table 4. Intel PROSet/Wireless Software Compatibility and Features

Features	v10.1	v10.5	v11.5
Hardware	Intel® PRO/Wireless 2200BG, 2915ABG and 3945ABG	Intel® PRO/Wireless 2200BG, 2915ABG, 3945ABG, 4965ABG	Intel® PRO/Wireless 2200BG, 2915ABG, 3945ABG, 4965ABG
Operating system support	Microsoft Windows 2000*, Microsoft Windows XP* Linux‡ v2.6	Microsoft Windows 2000*, Microsoft Windows XP* Linux‡ v2.6	Microsoft Windows 2000*, Microsoft Windows XP*, Microsoft Windows Vista* Linux ‡ v2.6
EM64T$^{\Phi}$ (64-bit support)		Yes	Yes
802.11 standards	Yes	Yes	Yes—adds 11n
Wi-Fi Alliance* certifications	Yes	Yes	Yes
Cisco Compatible Extensions*	v2, 3, 4	v2, 3, 4	v2, 3, 4 (except Vista)
Single sign-on (SSO)	Yes	Yes	Yes (except Vista)
Intel® Smart Wireless Solutions	Yes—v1	Yes—v1 v2	Yes—v1 v2
IT Administrator Tool	Yes—v2	Yes—v2	Yes—v2
ISV applications	Yes–adds management, VoIP	Yes–adds Pmode	Yes
Wake on WLAN	Yes	Yes	Yes
Enhanced power management and performance	Yes	Yes	Yes

Features	v10.1	v10.5	v11.5
Business-Class Wireless Suite	Yes—v1	Yes—v1	Yes—v2
Simple configuration		Yes—Legacy operating system	Yes—Legacy operating system
Intel® AMT^			Yes

For the latest feature, configuration, and usage details, visit the Intel® PROSet/Wireless Software Website: www.intel.com/network/connectivity/products/wireless/proset/proset_software.htm.

Cisco Compatible Extensions

Intel is a lead collaborator in the Cisco Compatible Extensions program. The Cisco Compatible Extensions program enables the WLAN client adapter to make best use of a Cisco WLAN infrastructure and its features. Vendors submit their adapters for compliance testing to earn the Cisco Compatible Extension certification.

Initiated several years ago, the Cisco Compatible Extensions program has gone through four versions to date. Each successive version includes the features of previous versions. Figure 8 provides an overview of the feature progression.

Figure 8. Cisco Compatible Extensions Feature Evolution

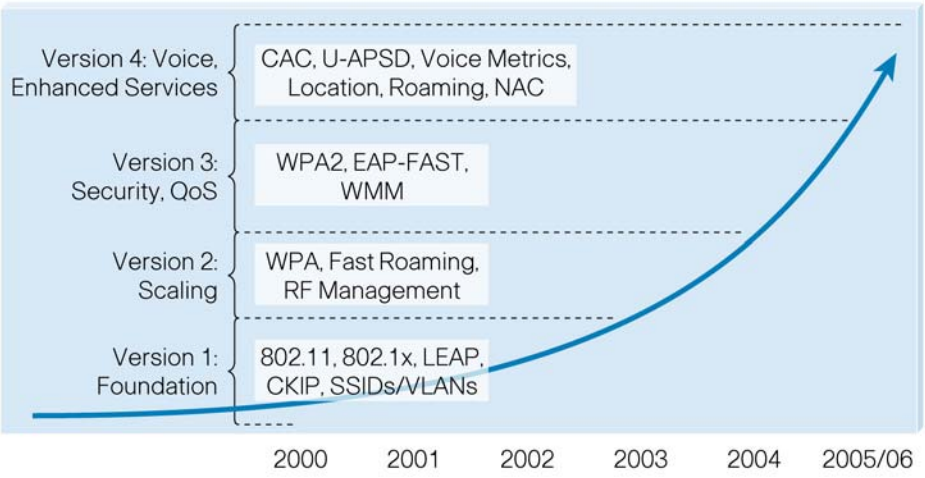
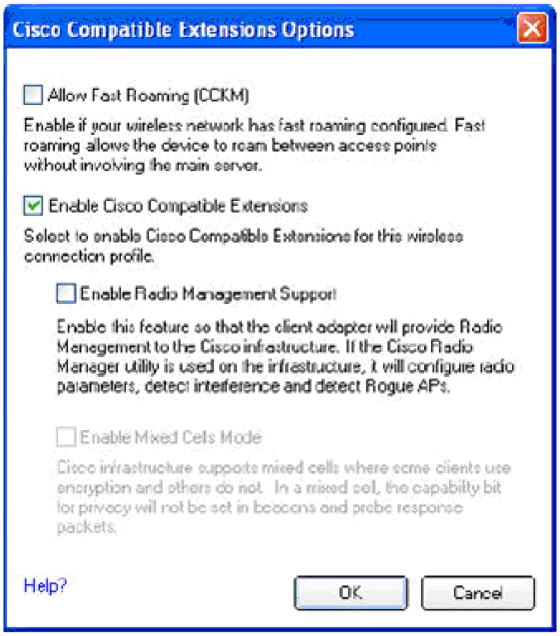

Version 4: Voice, Enhanced Services
CAC, U-APSD, Voice Metrics, Location, Roaming, NAC
Version 3: Security, QoS
WPA2, EAP-FAST, WMM
Version 2: Scaling
WPA, Fast Roaming, RF Management
Version 1: Foundation
802.11, 802.1x, LEAP, CKIP, SSIDs/VLANs
2000
2001
2002
2003
2004
2005/06

Table 5 shows the evolution of the Cisco Compatible Extensions certifications and their relationships to Intel PRO/Wireless Network Connection models. Figure 9 shows how to configure Intel wireless adapters to enable Cisco Compatible Extensions.

Table 5. Intel Wireless Adapters/Cisco Compatible Extensions Certifications

		Intel PROSet/Wireless Software version			
		7.1.4	9.x	10.0.1	11.5 XP/2K only
Intel PRO/Wireless Network Connection model	2100	Version 2 Version 3 EAP-FAST	N/A	N/A	N/A
	2200/2915	N/A	Version 3	Version 3	Version 3
	3945	N/A	N/A	Version 4	Version 4
	4965	N/A	N/A	N/A	Version 4

Figure 9. Intel PROSet/Wireless Security Page/Cisco Options



Cisco Compatible Extensions Options

☐ Allow Fast Roaming (CCKM)

Enable if your wireless network has fast roaming configured. Fast roaming allows the device to roam between access points without involving the main server.

☑ Enable Cisco Compatible Extensions

Select to enable Cisco Compatible Extensions for this wireless connection profile.

☐ Enable Radio Management Support

Enable this feature so that the client adapter will provide Radio Management to the Cisco infrastructure. If the Cisco Radio Manager utility is used on the infrastructure, it will configure radio parameters, detect interference and detect Rogue APs.

☐ Enable Mixed Cells Mode

Cisco infrastructure supports mixed cells where some clients use encryption and others do not. In a mixed cell, the capability bit for privacy will not be set in beacons and probe response packets.

Business-Class Wireless Suite

The Intel and Cisco Business-Class Wireless Suite provides extended capabilities between Intel clients and a Cisco WLAN infrastructure. Intel and Cisco have worked closely together to enhance the delivery of data, video, and voice wirelessly. Business-Class Wireless Suite provides:

Enhanced VoIP Technology

- Support for 802.11e QoS
- Wideband codecs
- Enhanced voice quality
- Access point to client QoS statistics
- API extensions for third-party soft phone vendors

Optimal Access Point Selection

- Access point assisted roaming
- Enhanced load balancing
- QoS flow enhancements

Table 6 shows which Business-Class Wireless Suite version works with the various Intel PRO/Wireless Network Connection models.

Table 6. Intel Wireless Adapters/Business-Class Wireless Suite

		Business-Class Wireless Suite	
		Version 1	**Version 2****
Intel PRO/Wireless Network Connection model	2100	N/A	N/A
	2200/2915	N/A	N/A
	3945	Yes	Yes
	4965	Yes	Yes

** Requires Cisco Unified Wireless Network infrastructure

For additional information on the Business-Class Wireless Suite, visit: www.ciscointelalliance.com/about/about.aspx

* Brand names and trademarks may be claimed as the property of others.

Φ 64-bit computing on Intel architecture requires a computer system with a processor, chipset, BIOS, operating system, device drivers and applications enabled for Intel® 64 architecture. Processors will not operate (including 32-bit operation) without an Intel 64 architecture-enabled BIOS. Performance will vary depending on your hardware and software configurations. Consult with your system vendor for more information.

^ Intel® Active Management Technology (Intel® AMT) requires the platform to have an Intel AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/technology/manage/iamt/.

For more information contact:

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
www.cisco.com

Intel Corporation
2200 Mission College Blvd
Santa Clara, CA 95052
www.intel.com