Wireless Network Design Process

Contents

Introduction ................................................................. 1-5
Terminology ................................................................. 1-5
Assess Customer Needs ..................................................... 1-6
Identify the Purpose of the Wireless Installation .............. 1-6
   User Access .......................................................... 1-6
   Wireless Bridging ................................................... 1-7
Conduct a User Survey ..................................................... 1-7
Identify User Types ........................................................ 1-7
   Employees ............................................................. 1-8
   Temporary Workers ............................................... 1-8
   Guests ................................................................. 1-8
Determine Usage Habits ................................................... 1-9
   Time of Day ......................................................... 1-9
   Applications ......................................................... 1-9
   Data ................................................................. 1-9
Estimate User Density .................................................... 1-9
Identify User Equipment .................................................. 1-10
   Laptops ............................................................... 1-10
   Wireless VoIP Phones ............................................ 1-10
   Handhelds .......................................................... 1-11
   Specialty Devices ................................................ 1-11
Determine Roaming Requirements ..................................... 1-12
### Wireless Network Design Process

#### Contents

- Assess Security Needs .................................................. 1-13
- Determine Risk Tolerance .................................................. 1-13
- Observe Applicable Regulations ........................................... 1-14
- Determine Access Control ................................................ 1-16
- Conduct the Preliminary Site Survey .................................. 1-18
  - Define Space Types ...................................................... 1-18
  - Identify Obstacles ...................................................... 1-18
    - A Note About Ceilings .............................................. 1-19
  - Identify RF Interference .............................................. 1-20
    - FHSS Systems ....................................................... 1-20
    - Other Wireless Systems in the WLAN Range .................. 1-22
    - Non-Interfering Wireless Systems ............................... 1-23
  - Evaluate the Existing Infrastructure .............................. 1-24
  - Locate Power Outlets and Switches ................................. 1-25
- Plan the Equipment Layout ............................................. 1-26
  - Select a PHY Layer .................................................... 1-26
  - Choose the Architecture ............................................. 1-27
    - Standalone Architecture .......................................... 1-27
    - Coordinated Architecture ....................................... 1-29
  - Select the Equipment ................................................ 1-30
    - Access Points ..................................................... 1-30
    - Wireless Edge Services Modules ................................ 1-33
    - External Antennas .................................................. 1-35
    - Switches ............................................................. 1-36
    - Wireless NICs ........................................................ 1-36
  - Choose a Management Solution ..................................... 1-37
- Plan Coverage and Capacity .......................................... 1-38
  - Using PMM ............................................................. 1-39
  - Planning Without PMM .............................................. 1-40
  - Multi-Level Coverage ................................................. 1-42
- Create a Security Plan .................................................. 1-44
  - Plan Physical Security ............................................... 1-44
  - Designate Access Zones ............................................. 1-45
    - Public Access Zone .................................................. 1-45
    - Private Access Zone ............................................... 1-45
Wireless Network Design Process

Contents

Use MAC Lockout .................................................. 1-84
Employ De-Authentication on the AP 530 ......................... 1-84
Use NIM to Detect and Respond to Threats ...................... 1-85
Enforce Endpoint Integrity ........................................ 1-85
Provide High Availability .......................................... 1-86
Create Redundancy Groups for the Wireless Module .......... 1-86
Install Redundant Wireless Services Modules .................... 1-86
Create a Redundancy Group ....................................... 1-87
Choose Active or Standby Mode .................................. 1-88
Adopt the RPs ....................................................... 1-89
Implement the Wireless Module’s Self-Healing Features ....... 1-90
Neighbor Recovery .................................................. 1-90
Interference Avoidance ............................................. 1-91
Use Adaptive Transmit Power Control on the AP 530 ........... 1-91
Introduction

Designing a wireless network is a complex process, but meticulous planning and management will greatly simplify the task and prevent problems in the later phases of deployment. The process entails assessing a company’s needs, completing an initial site survey, planning radio frequency (RF) coverage, installing devices and applying configurations, and then completing the final site survey. You will then need to monitor the wireless network and make adjustments to the RF coverage as needed.

This design guide cannot provide step-by-step instructions that take into account all the variables in your particular environment. A wide range of variables go into the creation and functioning of wireless networks, and every site presents its own unique needs and challenges. However, this guide can provide a general process that serves a starting point for designing a wireless network. You will have to rely on your own judgment and experience to implement these steps, and in some cases, you will need to modify, omit, or add steps.

Terminology

In this design guide, access device will be used as a generic term to describe access points (APs) and radio ports (RPs). Per Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards literature, station describes a wireless device such as a wireless-enabled laptop or personal digital assistant (PDA) that connects to an access device.
Assess Customer Needs

As an IT professional charged with establishing a wireless network, your first step should be to define the intended purposes of the wireless network and the needs of those who will use it. You should know whether the wireless network is intended to extend the network into new areas, to provide network access to new or temporary users, or simply to enable mobility. Define the purposes and needs in as much detail as possible. Sufficient care at this step can prevent significant setbacks later. For example, you would not want to begin ordering and installing equipment only to learn that you had overestimated the intended reach of the wireless network.

During this part of the design process, you will ask various questions: some questions you can answer immediately, perhaps even before visiting the installation site; other questions might need to wait for the site survey for a final answer.

Give each issue as much or as little thought as seems useful before the site survey, and remember to continually return to these questions as you conduct the survey.

Identify the Purpose of the Wireless Installation

There are two basic purposes for a wireless installation:

- user access
- wireless bridging

User Access

The most common purpose of a wireless installation is to provide a wire-free alternative to the traditional local area network (LAN). A wireless LAN (WLAN) permits users to access network resources using radio transmissions instead of copper wire.

The IEEE 802.11 family of WLAN standards specify radio frequencies as the PHY layer and use a specialized MAC layer that closely resembles Ethernet. Wireless 802.11 frames encapsulate IP packets that are identical to those delivered by wired Ethernet. A wireless access device bridges the wireless frames into the wired network by reencapsulating the IP packet within an Ethernet header. (See “IEEE Family of Wireless Standards” in Appendix B, “Appendix B: Reference Tables.”)
Wireless Bridging

Wireless bridging is typically used to connect areas separated by a space over which connections are not available or feasible to create, such as two buildings or areas within a large warehouse.

These bridges are typically dedicated, one-to-one links between APs, though you might need to deploy a one-to-many link. To boost the signal between one AP and another, specialized antennas are employed, typically a Yagi or directional antenna.

The primary factors to take into consideration with wireless bridging are the distances involved between the two points and the amount of traffic the bridge will handle.

Conduct a User Survey

You will need to conduct careful surveys of users and IT managers of the future wireless network to better understand their needs and expectations. Simple worksheets or questionnaires such as those found in Appendix C, “Appendix C: Site Survey Forms and Tables” can help you gather as much detail as possible about the needs and usage patterns of those who will use the wireless network.

These interviews or surveys should allow you to anticipate with reasonable accuracy the capacity and coverage needs of wireless network users. Remember to ask multiple-choice questions rather than open-ended questions so that you can more easily compile and analyze the results.

Identify User Types

It is helpful to identify users according to their relationship to the organization. For example, you might start with these common groups:

- employees
- temporary workers
- guests
Employees

For employees, you might further group users by role or function. For example, you could group users by department, rank, or specialty:

- Marketing_executives
- Marketing_associates
- Marketing_graphics
- Sales_executives
- Sales_associates
- Sales_trainees
- Engineering_electrical
- Engineering_mechanical
- Engineering_software

While creating these categories, you should keep in mind the other criteria that you will be considering, such as bandwidth needs and degree of mobility. You might need to further break down your categories to reflect unique needs. For example, you could divide the mechanical engineering group into “Engineering_mechanical CAD” and “Engineering_mechanical_testing” to distinguish between those who will spend most of their time at their workstations using CAD software and those who will spend most of their time in the testing lab.

Temporary Workers

Temporary workers can be on-site contractors, employees on loan from a different branch of the company, or seasonal workers. You will need to account for their locations, bandwidth needs, and mobility as well. If appropriate, you can put them in the same categories as those you created for regular employees.

Guests

Guests represent a group with limited needs in limited locations. Typically, these users need only Internet access and basic print services. Their bandwidth needs are therefore lower than for the other groups, and their mobility can vary, depending on the nature of the guest’s visit.
Determine Usage Habits

“Usage habits” refers to the ways in which the network is used.

Time of Day

You should know when users typically log on to the network and when they log off. Find out if some users access the network after business hours or if there is more than one shift per day. You need this information to determine whether network traffic is expected to fluctuate severely at certain times or if it is more or less constant.

Applications

Knowing which applications users intend to access gives you a rough sense of throughput requirements. It is particularly important to distinguish the different types of traffic: Will users be transmitting time-sensitive traffic such as voice over IP (VoIP) and video streaming, somewhat more lag-tolerant traffic such as the Internet, or background traffic such as File Transfer Protocol (FTP)?

Data

You should understand in general the typical content of data they want to access from a wireless connection. For example, if the wireless network will transmit credit card numbers or other personal information, it is all the more crucial to encrypt traffic using a highly secure encryption method. Consult your organization’s management to determine the extent of your organization’s legal or contractual obligations for securing data.

Estimate User Density

To plan for coverage and capacity, you must know, on average, how many users will access the wireless network in a given area at any given time. You also should find out where wireless coverage should not extend. Does your organization have areas open to the public that should not receive wireless coverage?

Unlike wired networks, where you can determine ahead of time how many users will connect to a particular switch, users will “decide” by their locations which access device to connect to. Theoretically, hundreds of users can associate with one access device at the same time. However, the more users...
who share the access device, the slower the data throughput rate. When a large enough number of users associates with a single access device, the wireless network can become functionally inaccessible.

For this reason, you must estimate the number of users that will occupy a space at any given time, keeping in mind that the number could fluctuate during the day.

Identify User Equipment

The types of devices that will be accessing the wireless network constitute another important factor because the various types of devices have different capabilities, different bandwidth demands, and sometimes different frequency needs.

Typically, the types of devices fall into one of these groups:

- laptops
- VoIP phones
- handhelds
- specialty devices

**Note**

In the 802.11 standard, the devices that are used to access the wireless network are referred to as stations—no matter what type of devices they are.

**Laptops**

Usually, most of the wireless stations in an organization are laptops with wireless network interface cards (NICs), although other workstations can also include a wireless NIC and use a wireless connection. These stations tend to demand the highest amount of wireless bandwidth because they use the same applications and network services that users access from a wired connection.

**Wireless VoIP Phones**

These telephones use WLAN technologies as their PHY and MAC layers and therefore transmit over the same frequencies as WLANs, unlike cellular or some cordless telephones. Voice over WLAN (VoWLAN) phones use relatively little bandwidth, are highly likely to roam, and are not tolerant of interruptions in the data stream.
Handhelds

Handheld devices range from wireless-enabled PDAs to smart phones to PC tablets. The amount of bandwidth that they use depends on the OS, the applications that they are running, and the network resources that they access.

Specialty Devices

In environments such as warehouses, hospitals, or manufacturing floors, wireless devices are often used to perform highly specialized tasks: scanning barcodes, monitoring patient vital signs, or tracking inventory. Bandwidth demands vary with the application type.

Many employees and temporary employees use devices that are provided by the company. In this case, you should know the devices’ capabilities. You should know if the devices support:

- 802.11a, 802.11b/g, or both
- Wi-Fi Protected Access (WPA) or WPA2 (or Wired Equivalent Privacy [WEP] only)
- Temporal Key Integrity Protocol (TKIP) or Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) Advanced Encryption Standard (AES)
- 802.1X supplicants

If the users’ wireless devices support TKIP or CCMP/AES and have an 802.1X supplicant, you can implement the strongest security possible for a wireless network—802.1X with WPA/WPA2.

Some VoWLAN phones and PDAs may not support 802.1X. (The Apple iPhone lacks an 802.1X supplicant as of January 2008.) If you want to support such devices, you will have to factor them in when you design your WLANs.

You will not be able to control what type of equipment guests will use, and you will not know if their devices support any of these capabilities. You should therefore plan for the lowest common denominator in the security solution: an Internet browser and 802.11b/g support. (See “Choose the Security Protocols” on page 1-50 for more information.)
Determine Roaming Requirements

The primary purpose of wireless networking is to free people from Ethernet cables and allow them to move freely from place to place. But because access devices do not have an infinite range, a moving wireless device may need to disassociate from one access device and reassociate with another to maintain connectivity.

As the network administrator, you cannot explicitly control the mechanism by which a NIC decides when and whether to roam to a new access device: the roaming algorithm for each NIC is proprietary, and the manufacturers do not release that information. Instead, you can plan for roaming by plotting likely roaming paths throughout the site and ensuring that places such as corridors are adequately covered.

Keep in mind that an access device must offer a roaming NIC an adequate signal-to-noise ratio (SNR) to persuade it to associate with it. If the access devices are spaced too far apart, the NIC might not find an adequate signal before it drops out of range of the access device to which it is currently associated. The result could be a dropped network connection, which would require the user to reconnect to the network.

In addition, remember that a wireless NIC bases its data rate on the SNR. A roaming NIC cannot associate to a new access device until the SNR is strong enough to support the data rates required by the new access device. This might pose a problem if the access device has been configured to require high data rates. Access devices must be spaced more closely so that a roaming NIC receives a strong enough SNR from a new access device to support the required data rates before the NIC moves out of range of its current access device.

You should also keep in mind that some wireless clients are less tolerant of signal interruptions others. The Windows client, for example, has been known to disconnect rather easily between access device coverage areas, whereas Macintosh clients can maintain the connection during signal interruptions.

Most users want what they would call “seamless roaming,” but you will have to carefully determine what they mean. Specifically, where do users want to roam? Do they expect to maintain uninterrupted access to applications as they roam, or do they just want to be able to log on to the network from any location?
Assess Security Needs

Given the nature of the wireless medium, security can be more difficult to provide than with wired networks. An intruder needs no more than an antenna to pick up your WLAN traffic, and if you have not taken precautions to prevent it, the intruder can break into your network over the wireless medium.

Before deciding which security strategies to implement on your wireless network, you should consider the amount of risk your organization can tolerate and the regulations to which your organization may be subject.

Determine Risk Tolerance

An important part of implementing security on a wireless network is evaluating your organization’s risk tolerance. What type of data does your organization store, and what are the consequences if a hacker breaches your network security and steals or damages that data?

The more valuable your network assets are, the more severe the consequences if network security is compromised. Because organizations today rely heavily on their networks to run their businesses, nearly every organization’s network stores confidential customer information and proprietary organization information. However, some customer information—such as credit card numbers—is particularly valuable.

When you evaluate the information stored on your network, you must ask yourself a few questions. What is the information worth to your organization and its customers? How much effort will hackers make to steal this information? If you are storing credit card numbers, for example, hackers have a strong motivation for infiltrating your network. On the other hand, do not assume that your network is safe from attack if you are not storing credit card information. For example, information stored about employees as a matter of course can be quite attractive to identity thieves. Do you collect and store information about customers? Your organization has an obligation—perhaps a very real legal obligation—to protect that data. No network is immune from attack.

You must also estimate the cost of downtime if systems are damaged and employees or customers cannot use the network. How will downtime affect your organization’s productivity? Can your organization continue to operate without impacting service to customers?

Damage is higher, of course, if the attack is made public. As part of a study of 475 companies, the IT Policy Compliance Group “conducted benchmarks focused on the expected financial losses associated with data losses and thefts”
that are publicly disclosed.” The compliance group concluded that the “expected financial consequences” were “changes in the price of stock for publicly traded firms,” “customer and revenue losses,” and unspecified “additional expenses and costs.” (Why Compliance Pays: Reputations and Revenues at Risk, a Benchmark Research Report, July 2007, p. 10. You can download this report at http://www.itpolicycompliance.com/research_reports/spend_management/.)

According to that report, a company’s stock price could decrease between “7.9 and 13.6 percent,” depending on the size of the organization. In general, the larger the organization, the more the stock price would decrease. (Why Compliance Pays, p. 11.)

Once you know the importance of your organization’s network assets, you can determine its risk tolerance. If your organization stores customers’ credit card numbers, it has a low risk tolerance. That is, if a hacker stole these credit card numbers, your organization would not easily recover: it might be liable to customers, which means that they could seek reparation for damages.

The organization’s reputation might also be irreparably damaged, resulting in a loss of both existing and new customers.

Observe Applicable Regulations

In your evaluation, you should factor in your organization’s legal obligations to provide a certain level of network security. Countries worldwide have enacted privacy laws or reinforced existing ones to improve security standards for organization networks.

The following are some examples of U.S. regulations:

- **Sarbanes-Oxley Act of 2002 (SOX)**—SOX was enacted to improve the accuracy and reliability of corporate disclosure, which in turn protects investors. SOX dictates that companies establish a public organization accounting oversight board, which monitors auditor independence, corporate responsibility, and enhanced financial disclosure. It also provides a way to review the dated legislative audit requirements.

- **Health Insurance Portability and Accounting Act (HIPAA)**—HIPAA addresses healthcare dangers, such as waste, fraud, and abuse in health insurance and healthcare delivery. HIPAA also prohibits companies that use electronic transactions and the Internet from publishing personal health information. (Before HIPAA, some companies were transferring or selling such information for commercial gain.)
Wireless Network Design Process  
Assess Customer Needs

- **Gramm-Leach-Bliley Act (GLBA)**—GLBA requires companies to store personal financial information securely, advises consumers of their policies on sharing personal financial information, and gives consumers the option to opt out of some sharing of personal financial information. And while it ended regulations that prevented the merger of banks, stock brokerage companies, and insurance companies, it also mitigates the risks of these mergers for the consumer.

- **Federal Information Security Management Act of 2002 (FISMA)**—FISMA is the primary legislation governing U.S. federal information security. Passed as part of the Homeland Security Act of 2002 and the E-Government Act of 2002, FISMA requires every government agency to secure information and the information systems that support its operations and assets. If the government uses commercially developed security products, those products must offer advanced and effective information security solutions and work in concert with government policies, procedures, and guidelines.

- **Family Educational Rights and Privacy Act of 1974 (FERPA)**—FERPA was enacted to protect student educational records and personal information from unlawful disclosure. The penalty for violating FERPA is loss of all federal funding, including grants and financial aid.

- **Payment Card Industry Data Security Standard (PCI DSS)**—To combat breaches and identity theft dangers, all major credit card companies agreed upon PCI DSS as an industry-wide data-security standard. PCI applies to all members, merchants, and service providers that store, process, or transmit cardholder data, as well as any network component, server, or application included in, or connected to, the cardholder data domain. Companies must use firewalls, message encryption, access controls, and antivirus software. PCI also requires frequent security audits and network monitoring and forbids the use of default passwords.

As the member states of the European Union (EU) began to legislate electronic privacy protection in the 1980s and 1990s, the European Commission soon realized that countries had diverging data protection laws, which would impede the flow of data, and therefore the flow of trade within the EU. In 1995 the European Commission proposed the Directive on the Protection of Personal Data (Directive 95/46/EC), which specifies how personal and sensitive data should be handled.

Although the majority of the directive focuses on the explicit reasons for which an entity can collect and store personal data, it also includes the specification that stored data must be secured, protected against accidental loss, and kept for a limited amount of time. Meeting these specifications necessitates a highly secure and organized network infrastructure.
Wireless Network Design Process
Assess Customer Needs

Many countries have passed regulations, such as:

- **Germany**—Bundesdatenschutzgesetz (Federal Data Protection Act)
- **United Kingdom**—Data Protection Act of 1998
- **France**—Law 78-17 (revised)
- **Canada**—Personal Information Protection and Electronic Documents Act (PIPEDA)
- **Australia**—Private Sector Provisions of the Privacy Act 1988 (Cth)
- **Japan**—Personal Information Protection Law

Determine Access Control

If your network stores particularly sensitive information, you should seriously consider implementing a full-service access control solution. An access control solution combines authentication methods, access policies, and endpoint integrity to help ensure that unauthorized users cannot access those network resources to which they are not entitled.

Network access control (NAC) is the process of controlling who has access to which network resources under what conditions (the time, location, and means of access).

An access control security policy addresses these questions:

- Who should access the network?
- What data, services, and other resources on the network should these users access?
- What conditions should alter the level of access granted to a particular user?

You can think of access control as granting many different types of users—employees, both temporary and permanent; guests; and customers—the level of access that is appropriate to their needs.

For example, it is appropriate for doctors and nurses in a hospital to access patient records; receptionists at the front desk, on the other hand, do not require such access. However, the receptionists should have access to other network resources such as appointment databases and scheduling software. And the only resource appropriate for patients and visitors might be the Internet.
The third question raises another important issue: factors beyond a user’s identity can affect the appropriate level of access. For example, daytime manufacturing workers might require network access during normal working hours from computers near their assembly stations, but not from computers in the marketing department or at night.

The means by which the user connects to the network can also be relevant. Wireless connections are sometimes more vulnerable to eavesdropping than wired, so a user that is normally allowed to access sensitive data might be prohibited from viewing that same data over a wireless connection. Furthermore, mobile users might inadvertently call up sensitive information in public areas. For example, a banker could call up customer account numbers on her laptop while she sits in the lobby, exposing the information to anyone who cares to look over her shoulder.

Endpoint integrity adds another component to an access control solution: users can only connect to your network using equipment that meets your standards for security. For example, the endpoint integrity policy might test the security settings for the Internet zone used by the endpoint’s Internet Explorer (IE). The policy enforces the security setting, such as Medium, for that zone; unless the endpoint’s setting is at or above Medium, the endpoint fails the test and cannot connect to the network.

For more information about setting up access controls for both wired and wireless access, see the ProCurve Access Control Security Design Guide and the ProCurve Access Control Security Implementation Guide.
Conduct the Preliminary Site Survey

After conducting the user surveys, you should conduct a preliminary site survey. Go to the site with one or more copies of the site’s floor plan and make note of anything that can potentially interfere with your WLAN installation.

Define Space Types

First, identify the types of spaces in each building so that you can estimate how the space will affect signal propagation. Use the following three categories:

■ **Open area**—This category includes warehouses, large retail spaces, arenas, and outdoor locations that are relatively unobstructed but rarely entirely empty. For example, many warehouses have large metal shelves, which are significant sources of obstruction for radio signals, and in an outside courtyard, trees can cause attenuation.

■ **Normal office space**—This category includes rooms with many partitions such as cubicles or movable walls. Such spaces can include more portable machinery or other obstructions than a closed environment, and you should be aware of the potential for substantial and regular changes to this kind of environment.

■ **Dense office space**—This category includes homes or offices that have floor-to-ceiling walls and permanent doors.

Identify Obstacles

Every building contains obstacles that will attenuate a radio frequency (RF) signal to some degree. Most construction materials such as drywall, glass, brick, wood, and cinder block will attenuate the signal only a little.

Following is a list of items and building materials that can cause significant interference with RF signal propagation:

■ specialty glass—tinted, bullet-proof, energy-efficient, wire mesh, silvered (conventional mirror), or half silvered (two-way mirror)

■ load-bearing interior walls or pillars made from concrete or reinforced concrete

■ ceiling-mounted sprinkler heads closer than 60 cm (2 ft) to the antenna

■ walls that are shielded with lead, copper, or other metal for rooms where high-energy electromagnetic radiation is generated
Wireless Network Design Process
Conduct the Preliminary Site Survey

- uninterruptible power supplies or surge protectors
- ceramic tile with metal content (backing or mounting mesh)
- dense foliage or pine trees with needles that are near wavelength or half wavelength (wavelength is roughly 12.5 cm for 802.11b/g radios and 6 cm for 802.11a radios)
- large heat-producing machines or chambers
- water—aquariums, organic inventory, hot-water tanks
- fluorescent, mercury vapor, or sulfur plasma lighting
- high-voltage power lines
- metal shelving or scaffolding
- human bodies: large crowds
- overhead cranes or conveyors
- paper in dense rolls or stacks
- elevator shafts or stairwells
- heavy-duty motors, transformers, or other devices with substantial lead content, strong magnets, or high current
- lead paint
- marble and other stone facing

A Note About Ceilings

Best practices suggest that you mount your access devices either on the ceiling itself or high on a wall. Unfortunately, ceilings can be cluttered with various obstacles, or their construction can pose special problems for access devices.

Obstacles. Sprinkling systems—both the metal heads and the plumbing—can pose problems for RF generation. Fluorescent lights can also disrupt signals because of their flickering radiation and their metal housings. Make sure that you note any other metal objects that occupy the area near the ceiling such as pipes, pulleys, exit signs, or scaffolding.

Ceiling properties. A “false” ceiling consists of acoustic tiles in a metal grid that is suspended a few inches or feet below the true ceiling. Organizations often use the gap between the tiles and the true ceiling to run wiring or to conceal the ventilation system. In some cases, you can mount an access device inside the false ceiling.
However, a particular kind of false ceiling is a “plenum” ceiling, which means that the gap is explicitly engineered as part of the building’s ventilation system. Building codes forbid placing anything inside a plenum ceiling that is not plenum rated, because toxic fumes from smoldering equipment could be spread quickly through the plenum into other areas of the building.

If the building has a plenum ceiling, you must select products that are plenum rated (including any cabling or power sources), or you should plan on mounting the access devices outside the plenum.

Identify RF Interference

Because the 2.4 GHz and 5 GHz bands are designated as “industrial, scientific, and medical” (ISM) bands, many wireless systems have been developed that use the ISM frequencies. Some of those systems were developed before WLAN technologies became widespread, and you can expect to find those legacy systems in warehouses, laboratories, hospitals, and manufacturing floors.

Determine which wireless systems the organization is using that transmit on the 2.4 GHz or 5 GHz bands and take them into consideration when planning a WLAN network that will occupy the same physical space. In some cases, the existing systems will have a negative effect on WLAN performance. Some examples of competing technologies that use the WLAN frequencies follow.

FHSS Systems

One of the PHY layers that was specified for IEEE 802.11b employs Frequency-Hopping Spread Spectrum (FHSS), in which the signal jumps from one narrow frequency to another in a sequence known only to the sending and receiving stations. The other PHY is Direct-Sequence Spread Spectrum (DSSS), in which the signal is encoded and spread over a wide range of frequencies, albeit at a lower intensity. Most WLANs use the DSSS technique because FHSS introduces unacceptable delays in the jump sequence and because the FHSS hardware tends to be more costly.

However, some non-WLAN wireless systems have opted for FHSS, and when they transmit in the 2.4 GHz range, they can interfere with 802.11b/g DSSS systems. (FHSS systems typically do not operate in the 5 GHz range, so they are less a concern for 802.11a systems.)

FHSS systems cannot “understand” DSSS signals (used by 802.11b and 802.11g when transmitting at 1 or 2 Mbps) nor orthogonal frequency-division multiplexing (OFDM) (used by 802.11a and high-speed 802.11g) signals. Therefore, while there is no risk of crosstalk between data streams, the two systems will often send data packets at the same time, resulting in bit errors and frame...
retransmissions. This will cause more problems for the 802.11b/g system than for the FHSS system, so you can expect throughput rates for the 802.11b/g system to drop while the FHSS system remains relatively unaffected.

You will need to determine whether the rate loss is acceptable. The 802.11 default limit for frame retransmission is three, so if a particular packet fails to arrive at its destination more than three times, the radio will drop the packet.

If the data loss is unacceptable, you should consider using a 5 GHz system in those areas where an FHSS system is transmitting. It is not sufficient to find an “optimal” channel on a DSSS system, because the FHSS system will hop from one narrow frequency to another in the same range as the wider-spread DSSS signal.

Following are some systems that use FHSS at WLAN frequencies:

**Medical Monitoring Devices.** “Medical telemetry” systems consist of wireless devices that attach to a patient to record and track vital signs. The device transmits its data to a console at the patient’s bedside or at a nurses’ station. Some of these systems transmit at 2.4 GHz using FHSS. However, many other medical monitoring devices use Wireless Medical Telemetry Service (WMTS) frequencies, which do not overlap 802.11 frequencies. (See Table 1-2 on page 1-24.)

**Cordless Telephones.** Cordless telephones (as opposed to cellular telephones) are licensed to broadcast on a variety of frequencies, including 2.4 GHz and 5.8 GHz. FHSS is often used on these telephones, so you will need to find out which PHY protocols are being used by any cordless telephones on your site.

**Bluetooth.** The personal area network (PAN) technology IEEE 802.15 operates at short ranges in the 2.4 GHz frequency range and uses FHSS. Most applications of Bluetooth consist of cable replacement for computer peripherals and headsets for mobile telephones. The transmission range of a Bluetooth device varies depending on its class:
Table 1. Bluetooth Classes

<table>
<thead>
<tr>
<th>Class</th>
<th>Power Output</th>
<th>Approximate Range</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100 mW</td>
<td>100 m</td>
<td>Access points</td>
</tr>
<tr>
<td>2</td>
<td>2.5 mW</td>
<td>10 m</td>
<td>PCMCIA cards for PCs, printers, scanners, copiers, fax machines, LCD projectors</td>
</tr>
<tr>
<td>3</td>
<td>1 mW</td>
<td>6 m</td>
<td>Mobile phones, PDAs, cordless phones, CD players, digital cameras, headsets, keyboards</td>
</tr>
</tbody>
</table>

802.15 Variants. ZigBee, based on IEEE 802.15.4, is designed for low data output, low-power applications such as medical data collection, industrial control, embedded sensors, and home and building automation. ZigBee builds on the PHY and MAC layers of 802.15 to supply higher-layer specifications. It transmits in the 868 MHz, 902–928 MHz, and 2.4 GHz ranges.

Wibree, similar to Bluetooth, was also designed to operate in low-power, low data output applications. It transmits in the 2.4 GHz range and is used in wrist watches, wireless keyboards, toys, and sports sensors.

Other Wireless Systems in the WLAN Range

These systems may or may not interfere with your WLAN installation, depending on the specific frequencies that you choose and the extent of the other systems’ installation.

RFID Tags. Radio frequency identification (RFID) tags are growing in popularity and are being used in applications as wide ranging as passports, transportation payments (e-tolls), product and asset tracking, animal identification, and automotive entry systems.

There are three kinds of RFID tags: passive, semi-passive, and active. Passive tags have no power source and communicate with the tag reader through the small electrical current that the reader induces when it scans the tag at close range. Semi-passive tags use battery power to store data but not to transmit; they also transmit with the induction from the reader. Active tags use battery power to send signals to the reader and to power integrated circuits.

Most RFID tags use frequencies other than those used by WLANs (see Table 1-2 on page 1-24), but one standard, International Standards Organization (ISO) 18185, broadcasts at 433 MHz and 2.4 GHz. Other RFID systems use the 2.4 GHz band to take advantage of existing WLAN systems.
Wireless Network Design Process
Conduct the Preliminary Site Survey

**DSRC.** Dedicated Short Range Communications (DSRC), a subset of RFID technology, is a standard that is used primarily in automotive applications to transmit data from the vehicle to roadside stations, such as in electronic toll collection. DSRC transmits in the 5.9 GHz band (U.S.) and the 5.8 GHz band (Japan, Europe). DSRC should not generally interfere with 802.11a unless you have specified WLAN transmissions in the higher ranges of the 5 GHz band.

**Microwave Ovens.** Although microwave ovens operate at 2.45 GHz (the frequency at which water molecules resonate), the radiation from these ovens should not interfere with your WLAN signals unless the oven's shielding has been compromised or the oven is closer than 3 m (10 ft) to the antenna. Because a microwave oven is designed to block RF signals completely, a large group of microwave ovens can be a significant obstacle to RF transmissions.

**HiperLAN.** A European Telecommunications Standards Institute (ETSI) competitor to IEEE 802.11, HiperLAN/1 and HiperLAN/2 transmit in the 5 GHz range. This standard is considered by some to be defunct, but some systems may still exist in Europe.

**WiMAX.** A long-distance, point-to-point technology, WiMAX (IEEE 802.16-2004) transmits in the 2–11 GHz and 10–66 GHz ranges.

**Radar.** Radar systems use a wide range of frequencies, with each band of frequencies licensed for a different use. The radar frequencies between 2 and 4 GHz (“S” band) are set apart for terminal air traffic control, long-range weather, marine radar, and some military applications. The frequencies between 4 and 8 GHz (“C” band) are for satellite transponders.

**Wireless USB.** Operating in the 3.1–10.6 GHz range, this equipment transmits at a short range (3–10 m). It is used in place of wired USB connections such as printers, hard drives, digital cameras, game controllers, and MP3 players.

**Non-Interfering Wireless Systems**

Many wireless systems will not interfere with your WLAN. Below is a list of common systems that transmit at frequencies other than 2.4 GHz and 5 GHz.
Table 1-2. Non-Interfering Wireless Systems

<table>
<thead>
<tr>
<th>System Type</th>
<th>Frequencies</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global System for Mobile Communications (GSM) and relatives (Code Division Multiple Access [CDMA], Time Division Multiple Access [TDMA], Universal Mobile Telecommunications System [UMTS])</td>
<td>900 MHz, 1800 MHz, 1900 MHz</td>
<td>Mobile telephony</td>
</tr>
<tr>
<td>Global Positioning System (GPS)</td>
<td>1227.60 MHz, 1575.42 MHz</td>
<td>Global positioning</td>
</tr>
<tr>
<td>Wireless Medical Telemetry Service (WMTS)</td>
<td>608–614 MHz, 1395–1400 MHz, 1427–1432 MHz</td>
<td>Medical monitoring devices</td>
</tr>
<tr>
<td>RFID</td>
<td>125–134.2 kHz, 140–148.5 kHz, 13.56 MHz, 865–928 MHz, 902–928 MHz</td>
<td>Tracking, inventory, payment systems, animal identification, electronic locks</td>
</tr>
<tr>
<td>AM band</td>
<td>520–1610 kHz</td>
<td>Commercial radio</td>
</tr>
<tr>
<td>FM band</td>
<td>87.5–108.0 MHz</td>
<td>Commercial radio</td>
</tr>
<tr>
<td>UHF band*</td>
<td>300 MHz–3 GHz</td>
<td>Broadcast television</td>
</tr>
<tr>
<td>VHF band</td>
<td>30–300 MHz</td>
<td>Broadcast television</td>
</tr>
<tr>
<td>Infrared</td>
<td>60,000–430,000 GHz</td>
<td>Remote controls</td>
</tr>
<tr>
<td>Near Field Communication (NFC)</td>
<td>13.56 MHz</td>
<td>Interactive advertising, mobile ticketing</td>
</tr>
<tr>
<td>Local Multipoint Distribution Service (LMDS)</td>
<td>26 GHz, 29 GHz, 31.0–31.3 GHz</td>
<td>Point-to-point, “last mile” telephony</td>
</tr>
</tbody>
</table>

* The 2.4 GHz band is a subset of the UHF band.

Evaluate the Existing Infrastructure

Access devices must be connected to the wired infrastructure. The distance limitations inherent in wired networks dictate how close the access devices must be to a switch. For example, a 10/100Base-T (Cat5) cable’s maximum of 100 meters limits the distance between an access device and its edge switch. If you cannot run cable between a switch and an access device, you should consider a wireless bridge between one access device and another that is connected to the wired switch.
You also need to know if the infrastructure can support the additional traffic that the WLAN will bring and if there are enough switch ports to plug in the access devices.

Find out what kind of authentication the network already uses. If you plan to implement 802.1X authentication, you will need at least one Remote Authentication Dial-In User Service (RADIUS) server. (ProCurve access devices have built-in RADIUS servers, if needed.)

Last, you should know if the existing network uses subnetting or virtual LANs (VLANs) to divide up its broadcast domains. Note the logical location of routers or Layer 3 switches. Learn about any firewalls, access control lists (ACLs), or other security measures that protect the existing LAN as well.

**Locate Power Outlets and Switches**

The devices will need a power source. Will they use AC power or Power over Ethernet (PoE)? For RPs, PoE is the only option. If the APs will use AC power, you may need to arrange for additional electrical outlets, because the ideal location for an AP—for example, in an air duct or ceiling space—is not always near a power source. If you are using AC power, you will also need to consider how you will secure the power cord.

In some cases, PoE may be a better option for an AP, to eliminate the expense of moving or adding electrical outlets.

Mark the location of switches and power outlets on the floor plan (not *every* power outlet—just the ones that you might need).