HP ProCurve MultiService Mobility Solutions

Design Guide

HP ProCurve MultiService Mobility Solutions

April 2010
Rev. 10.21

Design Guide

Applicable ProCurve Products

HP ProCurve Manager Plus 3.10	
50-device license-upgrade	(J9173A)
50-device license	(J9174A)
100-device license	(J9175A)
unlimited device license-upgrade	(J9176A)
unlimited device license	(J1977A)
HP ProCurve Identity Driven Manager 3.0	
500-user license	(J9438A)
unlimited-user license	(J9440A)
HP ProCurve Mobility Manager 3.0	
HP ProCurve RF Manager Controller w/50 Sensor License	(J9521A)
HP ProCurve Guest Management software v5.4	N/A
HP ProCurve RF Planner	(J9400A)
HP ProCurve RF sensor license	(J9384A)
HP ProCurve MSM710 Mobility Controller	(J9325A)
HP ProCurve MSM760 Mobility Controller	(J9420A)
HP ProCurve MSM765zl Mobility Controller	(J9370A)
HP ProCurve MSM710 Access Controller	(J9328A)
HP ProCurve MSM760 Access Controller	(J9421A)
HP ProCurve MSM422 Access Point US	(J9358A/B)
HP ProCurve MSM422 Access Point WW	(J9359A/B)
HP ProCurve MSM422 Access Point JP	(J9530A/B)
HP ProCurve MSM410 Access Point US	(J9426A/B)
HP ProCurve MSM410 Access Point WW	(J9427A/B)
HP ProCurve MSM410 Access Point JP	(J9529A/B)
HP ProCurve MSM415 RF Security Sensor	(J9522A)
HP ProCurve MSM335 Access Point US	(J9356A/B)
HP ProCurve MSM335 Access Point WW	(J9357A/B)
HP ProCurve MSM325 Access Point US	(J9369A/B)
HP ProCurve MSM325 Access Point WW	(J9373A/B)
HP ProCurve MSM323 US Access Point	(J3937A/B)
HP ProCurve MSM323 Access Point WW	(J9341A/B)
HP ProCurve MSM323-R Access Point US	(J9342A/B)
HP ProCurve MSM323-R Access Point WW	(J9345A/B)
HP ProCurve MSM320 Access Point US	(J9360A/B)
HP ProCurve MSM320 Access Point WW	(J9364A/B)
HP ProCurve MSM320-R Access Point US	(J9365A/B)
HP ProCurve MSM320-R Access Point WW	(J9368A/B)
HP ProCurve MSM320-R Access Point JP	(J9528A/B)
HP ProCurve MSM313 Access Point US	(J9346A/B)
HP ProCurve MSM313 Access Point WW	(J9350A/B)
HP ProCurve MSM313 Access Point JP	(J9525A/B)
HP ProCurve MSM313-R Access Point US	(J9351A)
HP ProCurve MSM313-R Access Point WW	(J9354A)
HP ProCurve MSM310 Access Point US	(J9374A/B)
HP ProCurve MSM310 Access Point WW	(J9379A/B)
HP ProCurve MSM310 Access Point JP	(J9524A/B)
HP ProCurve MSM310-R Access Point US	(J9380A/B)
HP ProCurve MSM310-R Access Point WW	(J9383A/B)
HP ProCurve MSM317 Access Device US	(J9422A/B)
HP ProCurve MSM317 Access Device WW	(J9323A/B)
HP ProCurve M111 Client Bridge	(J9389A)
HP ProCurve M111 Client Bridge JP	(J9523A)
HP ProCurve MSM31x/MSM32x Power Supply	(J9405A)
HP ProCurve MSM31x and MSM32x Power Supply	(J9405A)
HP ProCurve 1 Port Power Injector	(J9407A)

Trademark Credits

Microsoft, Windows, and Windows XP are U.S. registered trademarks of Microsoft Corporation.

Apple, Mac OS, and QuickTime are registered trademarks of Apple, Inc.

Linux is a registered trademark of Linus Torvalds.

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Hewlett-Packard Company
8000 Foothills Boulevard
Roseville, California 95747
http://www.procurve.com/

Contents

1 Wireless Network Design Process

2 Example WLAN Installation

C Site Survey Forms and Tables

1

Wireless Network Design Process

Contents

Introduction

The purpose of this design guide is to help networking professionals complete one of the following tasks:

- Design a new wireless network
- Upgrade an existing wireless network to 802.11n by replacing some of the access points (APs)

This guide first outlines the process for designing a new wireless network and then describes the process of upgrading to 802.11n. Move to the appropriate section in this guide to find the instructions you need:

- “Designing a New Wireless Network” on page 1-5
- “Upgrading a Wireless Network to 802.11n” on page 1-114.

This document is for HP ProCurve MSM products version 5.3.4 and above.

Terminology

In this design guide, *access point (AP)* is used generically to describe HP ProCurve MultiService Mobility (MSM) Access Points, and the MSM317 Access Device. 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 AP.

Documentation

All HP ProCurve documentation and other resources are available at: www.procurve.com/manuals

Designing a New Wireless Network

Designing a wireless network can be 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.

Because each site presents its own unique needs and challenges, this design guide cannot provide step-by-step instructions that take into account all the variables in your particular environment that may affect the creation and functioning of a wireless network. Instead, this guide provides a general process that serves as 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.

The steps in designing a new wireless network are listed below, with the page number in this design guide where each step is described.

- "Assess Users' Needs" on page 1-5
- "Conduct the Preliminary Site Survey" on page 1-18
- "Plan the Equipment Layout" on page 1-27
- "Plan Coverage and Capacity" on page 1-53
- "Begin Planning Wireless Security" on page 1-59
- "Use the Firewall, MAC Lockout, or Traffic Filters" on page 1-74
- "Perform the Initial Setup" on page 1-103
- "Provide Increased Reliability" on page 1-111

Assess Users' Needs

As an IT professional charged with establishing a wireless network, you should first 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. Careful documentation 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 underestimated the intended reach of the wireless network.

During this part of the design process, you will ask various questions (many of which are listed in the sections that follow). Some questions you can answer immediately, perhaps even before visiting the installation site; to answer other questions, you might need to wait until you complete the site survey.

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

Before you begin planning the wireless network, you must know how it will be used. A wireless installation has two basic purposes:

- Provide users with wireless access to a network
- Create a wireless link between two APs, which can be used to extend the reach of a wireless network or to connect two wired networks

A wireless link between two APs can also be called a wireless bridge or a wireless distribution system (WDS). On the MSM Controllers and APs, this link is called a *local mesh.* (To understand how local meshes are implemented on MSM APs, see “Local Mesh” on page 1-7.) As a result, this guide also uses the term *wireless mesh.*

You can design a wireless network to provide:

- Only wireless access for users
- Only a wireless link between APs
- Both functions

In fact, on MSM APs that support a local mesh, a single radio can be used to provide both functions simultaneously.

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

Just as the wired network is based on standards (such as the 802.3 standards), the wireless network is governed by a set of IEEE standards, collectively referred to as 802.11. You should have a basic understanding of the 802.11

standards before you attempt to design a wireless network. (For a basic summary, see "IEEE Family of Wireless Standards" in Appendix B, "Reference Tables.")

Local Mesh. A local mesh can be used to connect APs when a wired connection is not available or feasible. For example, a company may want to link the networks in two buildings or to provide wireless access in areas within a large warehouse. Two types of local meshes are possible:

- Static
- Dynamic

A static local mesh is a dedicated, one-to-one wireless link between two APs, as shown in Figure 1-1. Each static local mesh can support a single point-to-point link.

Each AP can support six static local meshes, which you can use to create point-to-multipoint configurations.

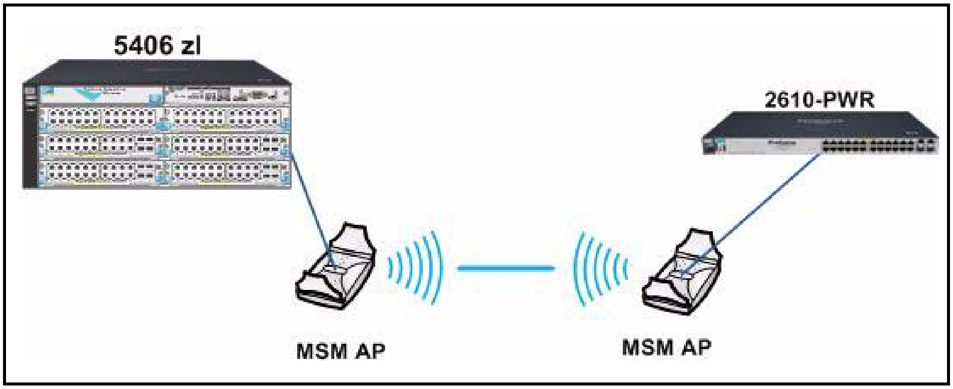


Figure 1-1. Static Local Mesh

A dynamic mesh can provide one-to-one or one-to-many wireless links. In a dynamic mesh, the APs automatically establish wireless links to create a fully connected network. If an AP becomes unavailable, the other APs in the mesh automatically reconfigure the mesh to maintain connectivity, providing high availability for the wireless link.

You can configure a dynamic mesh to operate with a dynamic channel setting. Dynamic Frequency Selection (DFS) allows the AP in charge of the mesh to detect other devices on its channel and switch to a less busy channel. Then all of the APs in the dynamic mesh converge on the new channel.

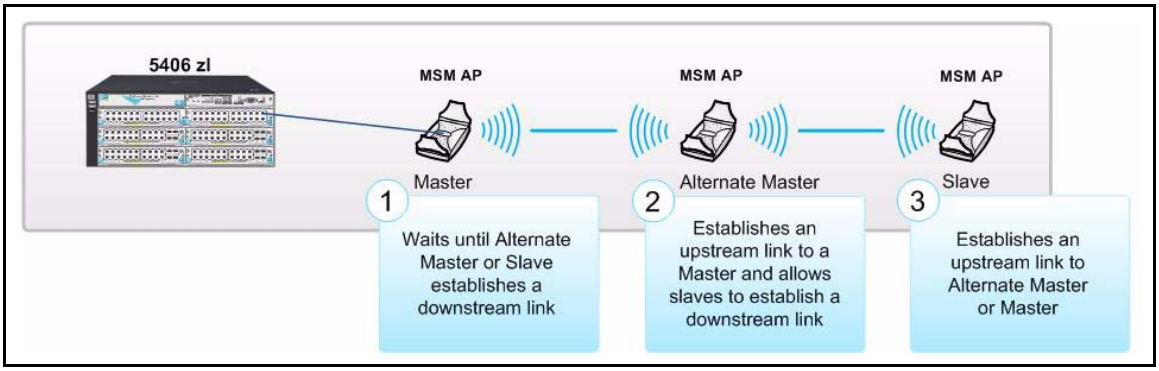

5406 zl
MSM AP
MSM AP
MSM AP
Master
Alternate Master
Slave
1
Waits until Alternate Master or Slave establishes a downstream link
2
Establishes an upstream link to a Master and allows slaves to establish a downstream link
3
Establishes an upstream link to Alternate Master or Master

Figure 1-2. Dynamic Mesh

To boost the signal between APs in a local mesh, specialized antennas are employed; typically a directional antenna, such as a Yagi, is used.

The primary factors to take into consideration when planning a local mesh are:

- Distances between two points
- Amount of traffic the local mesh will need to handle
- High-availability requirements

You will use these factors to determine:

- Type of radios and antennas to use
- Type of local mesh
- Number of wireless links, or hops, required to connect the two end points of the local mesh

Conduct a User Survey

You will need to conduct a survey of wireless users and IT managers to better understand their needs and expectations. Simple worksheets or questionnaires such as those found in 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. When creating user surveys, use multiple-choice questions rather than open-ended questions so that you can more easily compile and analyze the results. You should also have enough potential users complete the survey to make it statistically valid.

Identify User Types

You should start by identifying the users who will access the wireless network. If you are setting up a network that provides public access to the Internet (for a retail company or a hotel, for example), all or most of the users are typically guests. Keep in mind, however, that the organization may have a small LAN and may want their employees to access additional network resources.

If you are setting up a wireless network for a corporation, it is often helpful to identify users according to their relationship to the corporation. For example, you might start with these common groups:

- Employees
- Temporary workers
- Guests

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 using CAD software and those who will spend most of their time in the testing lab.

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 requirements as well. If appropriate, you can put them in the same categories as those you created for regular employees.

Guests represent a group with limited needs in limited locations. Typically, these users need only Internet access and perhaps basic networking services such as print services. Their bandwidth needs are therefore lower than those of other groups. Their mobility requirements can vary, depending on the nature of their visit. For example, guests at a university might want to roam between buildings, in outdoor areas.

Determine Usage Habits

You should also determine usage habits—the way in which the network is used.

Time of Day. You should know when users will typically access the wireless network. Find out if some users will access the wireless 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 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 users will be transmitting:

- Time-sensitive traffic such as voice over IP (VoIP)
- Time-sensitive and high-bandwidth traffic such as video streaming or video conferencing
- High-bandwidth traffic such as Software as a Service (SaaS)
- Lag-tolerant traffic such as HTTP
- Background traffic such as FTP

Data. You should understand in general the typical content of the data that users 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 have wireless coverage?

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

For this reason, you must estimate the number of users who will access the wireless network in each area, keeping in mind that the number could fluctuate during the day.

You should also keep in mind that your estimate is just that, an estimate. After the wireless network is installed, you should check the actual usage. You may want to monitor usage over time because once the wireless network is available, more and more users may begin to access and depend on it.

Identify User Equipment

You must also factor in the types of devices that will be used to access the wireless network because these devices have different capabilities, different bandwidth demands, and sometimes different frequency needs.

Typically, wireless devices fall into one of the following:

- **Laptops**

  Most of the wireless stations in an organization are typically laptops with wireless network interface cards (NICs), although other workstations can also include a wireless NIC and use a wireless connection. Of the stations accessing the wireless network, laptops tend to demand most wireless bandwidth because they can use high-bandwidth applications and network services.

- **VoIP phones**

  VoIP telephones that use WLAN technologies as their Physical and MAC Layers transmit over the same frequencies as WLANs, unlike cellular or some cordless telephones. Although these VoIP phones use relatively little bandwidth, they do not tolerate interruptions in the data stream and are highly likely to roam, and

- **Handheld devices**

  Handheld devices range from wireless-enabled personal digital assistants (PDAs) to smart phones to PC tablets. The amount of bandwidth that handheld devices 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 such as scanning barcodes, monitoring patient vital signs, or tracking inventory. Bandwidth demands vary with the application type.

Note

In the 802.11 standard, the devices that are used to access the wireless network are referred to as *stations*—regardless of device type. When you are identifying user equipment, however, it is important to distinguish among the devices so that you can determine bandwidth needs on both the wireless and the wired networks. In other parts of this design guide, the term *station* is used to describe any device accessing the wireless network.

If you are setting up a public access network or enabling guest access, you will not know what type of devices users will have. However, it is still important to consider the user equipment because you will have to decide which 802.11 standards—802.11a, 802.11b/g, or 802.11n—to support to accommodate the largest number of users. Typically, public access networks use 802.11b/g, but as more consumers begin to purchase 802.11n-compatible wireless devices, some organizations may begin to provide 802.11n for public access networks as well. (Special considerations for using 802.11n and 802.11b/g or 802.11a in the same vicinity are explained in "Select a Physical Layer" on page 1-28.)

If you are setting up a wireless network for a corporation, the IT department may control the devices employees and temporary employees use. In this case, you should list each device's capabilities. You should know if the device supports:

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

Because WEP is so insecure, you should try to replace any device that supports only this encryption method for wireless transmissions. For the highest security, devices should be configured to use WPA2 with AES. In fact, for 802.11n APs support only WPA2 with AES because WEP and WPA with TKIP do not provide sufficient security.

If the users' wireless devices support WPA2 and 802.1X, you can implement the strongest security possible for a wireless network: 802.1X with WPA2.

Some VoIP phones and PDAs may not support 802.1X or 802.11n. If you want to support such devices, you will have to factor them in when you design your wireless network.

Determine Roaming Requirements

The primary purpose of wireless networking is to free people from Ethernet cables and allow them to move without restraint from place to place. As users move from one place to another, their wireless stations may need to roam: they may disassociate from one AP and reassociate with another to maintain connectivity.

In addition to determining where users want to roam, you need to figure out:

- What applications they want to use when they roam
- What they expect to happen when they roam

When you ask users about their roaming requirements, many will say that they want “seamless roaming.” However, this term may mean different things to different users, so you should clarify exactly what users expect. Do they just want to be able to access the wireless network from any location, or do they expect to maintain uninterrupted access to applications as they roam? Will they notice if the wireless client temporarily drops the connection? For example, if they are using voice over WLAN (VoWLAN), delays and loss of signal will not be tolerated, but if users are simply browsing the Internet, they will probably not notice if their wireless client briefly loses its connection and automatically reconnects in the background.

As the network administrator, you cannot directly control the mechanism by which a station’s wireless client determines it should roam to a new AP. The roaming algorithm for each wireless client determines when it roams to a new AP.

Before a wireless client can roam, it must be able to support the required data rates on the new AP before it moves out of range of its current AP. Because a wireless client bases its data rate on the signal-to-noise ratio (SNR), a roaming client cannot associate to a new AP until the SNR is strong enough to support the data rates required by the new AP. This might pose a problem if the APs are spaced too far apart. For example, if the APs have been configured to require high data rates, they must be spaced more closely together.

You should also keep in mind that some wireless clients are less tolerant of signal interruptions than others. This means that slight signal fluctuations or interruptions may cause these wireless clients to drop the wireless connection. Most wireless clients will immediately try to reassociate and reauthenticate to the service set identifier (SSID) without the user's intervention, but if the user is accessing an application, the application may not tolerate the loss of network connectivity—however brief it is. In this case, the user may notice the delay or even need to restart the application.

Assess Security Needs

You must determine the security needs for the wireless network. If you are providing public, or guest, access, security is typically the responsibility of the guest user. If a guest user wants to view or transmit confidential data over the wireless connection, he or she will need to protect the data by using Secure Sockets Layer (SSL) over HTTP or establishing a virtual private network (VPN) with a company network.

If you are providing wireless access for your organization's employees, however, you are responsible for ensuring that the organization's data is protected. With few exceptions, most organizations transmit confidential data over their wireless network and should, whenever possible, use the strongest authentication and encryption possible: 802.1X and WPA2 with AES.

The wireless network must also be secured against legitimate users who might try to use the wireless network to access confidential information that they are not authorized to access. You must ensure that when users are using a wireless connection, they can access only the resources to which they should have rights. For example, marketing employees should not be able to access the virtual LAN (VLAN) that is restricted to finance employees.

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? What type of data will be sent wirelessly, and what are the consequences if a hacker eavesdrops on the data transmission?

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 the organization's proprietary information. 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, other customer information and information gathered about employees can be quite attractive to identity thieves. Your organization has an obligation—perhaps a very real legal obligation—to protect this 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 adversely affecting 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 if its security is breached. (*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 and industries worldwide have enacted measures or reinforced existing ones to improve security and privacy standards for organizations' networks.

The following are some examples of regulations and standards with which businesses must comply:

- **Sarbanes-Oxley Act of 2002 (SOX)**—SOX was enacted to improve the accuracy and reliability of corporate disclosure, thereby protecting investors. SOX dictates that companies establish a public organization accounting oversight board, which monitors auditor independence, corporate responsibility, and enhanced financial disclosure. It applies to all publicly traded companies doing business in the U.S.
- **Health Insurance Portability and Accountability 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.)
- **Basel II**—The Basel Accords are recommendations and standards formulated by the Basel Committee on Banking Supervision. They define acceptable risk and capital management requirements for large banks. The standards are designed to prevent the system of international finance from the damaging effects of the failure of individual institutions. Banks whose investments are higher risk are required to retain larger capital reserves to ensure continued solvency.
- **Gramm-Leach-Bliley Act (GLBA)**—GLBA requires organizations to store personal financial information securely, advise consumers of their policies on sharing personal financial information, and give consumers the option to opt out of some sharing personal financial information.
- **Federal Information Security Management Act of 2002 (FISMA)**—FISMA is the primary legislation governing U.S. federal information security. It requires every government agency to secure information and the information systems that support its operations and assets.
- **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 to 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 DSS also requires frequent security audits and network monitoring, and forbids the use of default passwords.

- **Directive on the Protection of Personal Data (Directive 95/46/EC)**—The European Commission proposed this directive in 1995. It specifies the explicit reasons for which an entity can collect and store personal data. It also requires 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.

There are many additional regulations worldwide, such as:

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

Determine Appropriate Access. If your network stores particularly sensitive information, you should seriously consider implementing a comprehensive security solution to enforce and limit access. Such a 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.

In short, the security solution should be designed to enforce and control *who* has access to *which network resources* under *what conditions* (the time, location, and means of access). While designing this solution, consider 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?

For example, doctors and nurses in a hospital need to access patient records, but 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. The only resource appropriate for patients and visitors might be the Internet.

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, you may not want mobile users to access sensitive information in public areas. For example, a banker could access 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 a security solution. By enforcing endpoint integrity, you can ensure that users can access the network only if they are using endpoints that comply with your security policy. For example, your security policy might require users' workstations to have a certain setting (such as Medium) for the Internet zone in Internet Explorer (IE). An endpoint integrity solution would check this and other security settings on the workstation before allowing it to connect to the network. If the workstation failed the test, it could not connect to the network.

For more information about setting up access enforcement 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 floor plan and make note of anything that can potentially affect the wireless network.

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 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) glass
- 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
- 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 or 6.25 cm for the 2.4 GHz band and 6 cm or 3 cm for the 5 GHz band)
- 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 (in large crowds, for example)
- 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

Mounting APs on Ceilings. Best practices suggest that you mount your APs 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 APs. Some of these factors are listed below.

- **Obstacles**

  Sprinkling systems—both the metal heads and the plumbing—can pose problems for RF generation. Fluorescent lights (including “energy saving” compact fluorescent bulbs) 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 AP 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 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 APs that are plenum rated (including any cabling or power sources), or you should plan on mounting the APs outside the plenum.(HP ProCurve MSM APs are plenum rated, but you must also use plenum-rated cables and attachment hardware.)

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 such systems in warehouses, laboratories, hospitals, and manufacturing floors. However, you will also see some modern systems, such as wireless headsets and handsets, that also use this technology.

Determine if the organization is using wireless systems 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 wireless performance. Some examples of competing technologies that use the WLAN frequencies are listed below.

FHSS Systems. One of the Physical 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 Physical Layer 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 wireless networks 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 of a concern for 802.11a systems and 802.11n in the 5 GHz band.)

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. Such a wireless 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 1-25.)

- **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 Physical Layer 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. Bluetooth is typically used to replace cables for computer peripherals and headsets for mobile telephones. The transmission range of a Bluetooth device varies, depending on its class, as shown in Table 1-1.

Table 1-1. Bluetooth Classes

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

- **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 Physical 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. Some of the other wireless systems may or may not interfere with your WLAN installation, depending on the specific frequencies that you choose and the extent of the other system 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.

  Three types of RFID tags are available:

  - **Passive**—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**—Semi-passive tags use battery power to store data but not to transmit; they also transmit with the induction from the reader.
  - **Active**—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 1-25), but one standard, International Organization for Standardization (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.

- **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 for electronic toll collection. DSRC transmits in the 5.9 GHz band in the United States and in the 5.8 GHz band in Japan and Europe. Generally, DSRC should not interfere with 802.11a, or 802.11n in the 5 GHz band, 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 shielding has been compromised or the oven is closer than 3 m (10 ft) to the antenna. However, a microwave oven is designed to block RF signals completely, so 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. Although some people may consider this standard defunct, some systems may still exist in Europe.

- **WiMAX**

  WiMAX (IEEE 802.16-2004) is a long-distance, point-to-point technology often used instead of cable or Digital Subscriber Line (DSL) in rural areas. WiMAX devices typically transmit in the 2–11 GHz and 10–66 GHz ranges, although in some areas other frequencies are used. Because WiMAX needs to transmit over longer distances, it cannot operate at frequencies higher than 66 GHz.

- **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 applications, marine radar, and some military applications. The frequencies between 4 and 8 GHz ("C" band) are used for satellite transponders.

- **Wireless Cameras**

  Wireless cameras such as Webcams and surveillance cameras operate at high power levels with high-gain antennas in the 2.4 GHz range.

- **Video Senders**

  Video senders transmit video signals from one room to another. For example, if there is one satellite TV decoder in the home, the signal is transmitted to multiple televisions in the home. Video senders use high-powered 10 MHz channels that can obliterate half of an 802.11a/b/g channel and up to one half of an 802.11n (depending on whether there is channel bonding or not).

- **Car Alarms**

  Some manufacturers use the 2.4 GHz frequency for the movement sensors in their security systems. Broadcasting at 2.45 GHz at 500mW, the alarm signals might cause problems with channels 6 and 11.

- **Wireless USB**

  Operating in the 3.1–10.6 GHz range, wireless USBs transmit at a short range (3–10 m). Replacing wired USBs, these devices include printers, hard drives, digital cameras, game controllers, and MP3 players.

- **Existing APs That Are Not Part of Your Network**

  APs that are not part of your network but are physically in the same location are a common source of interference. A retail company or a library, for example, may have a hotspot AP on their premises that belongs to a cellular phone company. In this case, you cannot manage the AP, but it has to be included in your survey and planning.

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

Table 1-2. Non-Interfering Wireless Systems

System Type	Frequencies	Applications
Global System for Mobile Communications (GSM) and relatives (Code Division Multiple Access [CDMA], Time Division Multiple Access [TDMA], Universal Mobile Telecommunications System [UMTS])	900 MHz 1800 MHz 1900 MHz	Mobile telephony
Global Positioning System (GPS)	1227.60 MHz 1575.42 MHz	Global positioning
Wireless Medical Telemetry Service (WMTS)	608–614 MHz 1395–1400 MHz 1427–1432 MHz	Medical monitoring devices
RFID	125–134.2 kHz 140 –148.5 kHz 13.56 MHz 865–928 MHz 902–928 MHz	Tracking, inventory, payment systems, animal identification, electronic locks
AM band	520–1610 kHz	Commercial radio
FM band	87.8–108.0 MHz	Commercial radio
UHF band*	300 MHz–3 GHz	Broadcast television

System Type	Frequencies	Applications
VHF band	30 –300 MHz	Broadcast television
Infrared	60,000–430,000 GHz	Remote controls
Near Field Communication (NFC)	13.56 MHz	Interactive advertising, mobile ticketing
Local Multipoint Distribution Service (LMDS)	26 GHz, 29 GHz 31.0–31.3 GHz	Point-to-point, "last mile" telephony

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

Evaluate the Existing Infrastructure

APs must be connected to some type of wired infrastructure. The distance limitations inherent in wired networks dictate how close the APs must be to a switch. With a 10/100Base-T (Cat5e) or a 10/100/1000 Base-T cable, for example, a maximum of 100 meters limits the distance between an AP and its edge switch. (Switch ports should be 10/100/1000 when using 802.11n.)

If you cannot run cable between a switch and an AP, you should consider using a local mesh to connect the AP to another AP, which is, in turn, connected to a switch.

You also need to know if the infrastructure can support the additional traffic that is transmitted from the WLAN, and if the switches have enough switch ports to connect the APs to the wired network. This is especially important when you will be adding the amount of traffic that is possible with an 802.11n deployment. (See "802.11n" on page 1-30.) Consider the following factors as you assess the readiness of your switches to process additional wireless traffic:

- Which network links and infrastructure devices will be affected?
- How much bandwidth is available on the affected links, how much traffic is on the affected links now, and how much wireless traffic will be sent across the links?
- How much throughput do the infrastructure devices have, how much traffic are they handling now, and how much more can they handle?
- Can they process the wireless traffic without causing a lag in response times?
- Will mobility add users to the network, or will the wireless users be the same users as wired ones?
- Will mobility cause users to access the network more frequently or from different locations? If the users access the network in different locations, are the switches there able to handle the traffic?

- Will mobility cause users (or devices) to access the network in different ways? Will users use more bandwidth-intensive services or the same type of services that they use on wired connections?

Find out what kind of authentication is used on the existing wired network. If you plan to implement 802.1X authentication, you will need at least one Remote Authentication Dial-In User Service (RADIUS) server. HP ProCurve MultiService Mobility Access Controllers provide built-in RADIUS servers.

Finally, you should know if the existing network uses subnets 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 APs will need a power source. Will they use DC power or Power over Ethernet (PoE)? If the APs will use DC 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 DC power, you will also need to consider how you will secure the power cord and power converter.

In some cases, PoE may be a better option for an AP because it eliminates the expense of moving or adding electrical outlets. If your current infrastructure does not provide PoE or if it does not provide PoE 802.3at (PoE+), which some 802.11n devices require, you might consider using a PoE injector. (HP ProCurve MSM422 APs, which support 802.11n, can be powered by standard 802.3af PoE ports.)

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

Plan the Equipment Layout

Once you have finished the user and site surveys, you should have enough information to begin selecting your equipment. First, select the Physical Layer and the architecture. Then, choose the products—including a management solution—that match your choices.

Finally, you should plan where you will install the APs and determine roughly what kind of RF coverage each will provide. HP ProCurve RF Planner provides a site planning tool that helps you complete this step.

Select a Physical Layer

You currently have a choice between four IEEE 802.11 wireless network standards:

- 802.11a
- 802.11b
- 802.11g
- 802.11n

Table 1-3. Wireless Networking Standards

Standard	Frequency (GHz)	Theoretical Data Rates (Mbps)	Probable Maximum Throughput (Mbps)	Channels
802.11a	5	6–54	22	16 non-overlapping
802.11b	2.4	1–11	5	14 overlapping 3 non-overlapping
802.11g	2.4	1–54	22	14 overlapping 3 non-overlapping
802.11n	2.4	1-600	144	14 overlapping* 3 non-overlapping*
802.11n	5	1-600	144	16 non-overlapping*

*If you are not using channel bonding

The legacy standards (802.11a, b, g) operate in only one frequency band. However, 802.11n can operate in two frequency bands. 802.11n also offers the highest transmission rates of any standard.

When selecting a Physical Layer, you must consider both the standard you would like to use and the frequency band in which you want your network to operate. With 802.11a, b, and g, the standard you choose determines the frequency in which the AP operates. The opposite is not necessarily true. If you decide to use the 5 GHz band in your wireless network, you can then choose to use either the 802.11a or the 802.11n standard.

The 2.4 GHz band is currently more crowded than the 5 GHz band, so you should consider using the 5 GHz band if you have other 2.4 GHz radios in the vicinity, including neighboring WLANs. You should keep in mind, however, that the 5 GHz band is highly regulated in each country, so the number of channels available for use varies from county to country.

You may also want to consider using 5 GHz if you plan to support a large number of APs in a small area. In such instances, the channel overlap problem in the 2.4 GHz band can make it more difficult to prevent channel interference.

However, 5 GHz signals do not travel as far as 2.4 GHz signals (or penetrate walls as effectively), so if distance is a factor, 2.4 GHz is a better selection. In addition, some devices are designed to operate using only 2.4 GHz, which might preclude the use of 5 GHz.

When using 802.11n, the 5 GHz band is the better choice because 802.11n has been optimized for use in the 5 GHz band. In addition, most legacy devices operate in the 2.4 GHz band (802.11b/g), so there is less interference in the 5 GHz band.

In addition, you must support the frequency band that the network wireless clients need. For example, if your network supports only 802.11b/g only devices, you must select the 2.4 GHz band.

Channels. Each country regulates how radio signals are used within their boundaries. For example, countries specify the available channels for each frequency band and determine the range of power available for each channel.

As a result, the channels available for wireless networks vary from country to country. This is particularly true of the 5 GHz band, which is more tightly regulated than the 2.4 GHz band. However, regulations for the 2.4 GHz band also vary slightly. Depending on your country, for example, some channels may be restricted to indoor use.

If you set the country code on the HP ProCurve wireless products, they will automatically allow the correct channels and power for the country selected. When a country changes its authorized frequencies, HP ProCurve Networking will release new software to update the country code settings on its wireless products.

To avoid cross-channel interference, you should use non-overlapping channels. For example, in the 2.4 GHz band, there are only three non-overlapping channels. This means that when using this band, you will need to carefully plan channel usage. (See Table 1-4.)

Table 1-4. Non-Overlapping Channels for 802.11b/g

Country	Number of Non-Overlapping Channels	Non-Overlapping Channels
North America	3	1, 6, 11
Europe and Australia	3	1, 7, 13
France and Spain	1	11
Japan	3	1, 7, 13, 14
Rest of world	3	1, 6, 11

802.11n. As next-generation wireless applications emerge, improved WLAN data throughput capabilities are becoming essential. Enterprise-class, bandwidth-intensive applications such as video-conferencing, enterprise resource planning (ERP) and customer relationship management (CRM) systems, workgroup computing applications, and some wireless backhaul applications require throughputs larger than 802.11a/b/g technologies can provide.

In response, the IEEE Task Group N (TGn) and the Wi-Fi Alliance (WFA) drafted a standard for the next generation of WLAN performance. The IEEE 802.11n standard is intended to increase network speed and reliability as well as extend the operating distance of wireless networks.

The 802.11n standard, ratified in September 2009, provides a maximum signal rate of up to 600 Mbps, over 10 times greater than that of 802.11g. Similar to other 802.11n standards, the real-world throughput is significantly less than the maximum signal rate; however 802.11n offers a throughput of up to 300 Mbps, still more than 10 times the speed of 802.11g.

802.11n operates in either the 2.4 GHz or 5 GHz frequency bands—enabling it to provide backward compatibility for 802.11a/b/g devices.

802.11n MIMO. The 802.11n standard is the first to call for multiple-input, multiple-output (MIMO) antenna design. MIMO algorithms in a radio chipset send data out over 2–4 antennas. Signals from each transmitter inevitably reach the target receiver through a unique path, allowing for spatial-division multiplexing (SDM)—that is, sending multiple data streams over the same channel to multiply the throughput of a single stream.

MIMO works best if these paths are spatially distinct, resulting in received signals that are uncorrelated. Thus, while traditional 802.11 networks degrade in the presence of multipath—a propagation phenomenon by which multiple radio signals reach receiving antennas by bouncing off objects along the way—multipath helps decorrelate the 802.11n channels, enhancing the operation of SDM. The signals are recombined on the receiving side by the MIMO algorithms—a process that dramatically improves wireless performance and reliability. The multiple receivers in MIMO systems consistently process each multipath component, thereby eliminating the mixture of out-of-phase components that would normally result in signal distortion.

Because SDM techniques make receivers much more complex, designers usually combine them with Orthogonal Frequency-Division Multiplexing (OFDM) modulation schemes, which are more efficient than Direct Sequence Spread Spectrum (DSSS) or Frequency-Hopping Spread Spectrum (FHSS). The 802.11n OFDM implementation improves upon the implementation employed in earlier standards, using a higher maximum code rate and slightly wider bandwidth.

Aside from using a higher maximum code rate and wider bandwidth, 802.11n also takes advantage of Space-time block coding (STBC), a method for encoding the symbols onto a waveform. STBC permits a receiver to combine all of the copies of a signal to improve data extraction.

Another option is beamforming, which exploits the interference phenomenon to control the strength and direction of the signal. Multiple transmit antennas function as if they were parts of an array, forming a directional antenna. The transmitting antennas use feedback from the receiver to align the waveforms until they achieve “constructive interference,” which results in a stronger signal (as opposed to destructive interference, which degrades a signal). The 802.11n specification allows beamforming when the number of transmit antennas exceeds the number of spatial streams or when the path between the receiver and transmitter is known well enough by the transmitter to enable it to send most of the signal energy in directions that will benefit the receiver.

802.11n Channel Bonding. While MIMO represents the most significant architectural advancement in 802.11n, the standard includes additional feature enhancements designed to boost performance. The most notable improvement is support for 40 MHz radio channels, which have twice the theoretical capacity of existing 802.11 radio channels. A technique called channel bonding combines two adjacent, non-overlapping 20 MHz channels into a single 40 MHz channel. Bandwidth is more than doubled because the guard band between the two 20 MHz channels, used to avoid interference between these channels, can also be removed when they are bonded.

802.11n can also operate using the standard 20 MHz channels; in fact, the specification recommends that 40 MHz channels be used only in the 5 GHz band. When you use channel bonding, each pair of channels must not overlap another pair—a requirement that dramatically reduces the availability of non-overlapping channels. The 2.4 GHz frequency band has only three non-overlapping 20 MHz channels, and therefore, bonding two 20 MHz channels consumes two of these channels.

802.11n Frame Aggregation. To augment throughput at the MAC Layer, 802.11n can aggregate two or more frames into one frame each time it accesses the AP radio. 802.11n can use two types of frame aggregation for unicast transmissions:

- **A-MSDU**—Aggregation of MAC service data units (SDUs)
- **A-MPDU**—Aggregation of MAC protocol data units (PDUs), which requires the use of block acknowledgement (BACK, introduced in 802.11e and optimized in 802.11n)

Compatibility and Protection with 802.11n. Because 802.11n transmits on the same frequencies as legacy 802.11 standards, you must consider how 802.11a/b/g devices will affect an 802.11n deployment. You can support both legacy stations and 802.11n stations by deploying an 802.11n-only radio and an additional 802.11a or 802.11b/g radios, or you can choose to make your cells smaller (more data throughput) by disabling legacy data rates (1, 2, 5.5), when possible. You can also support both types of stations by deploying an 802.11n radio that uses one of the following protection mechanisms.

- **RTS/CTS**—The transmitting and receiving stations transmit conventional request-to-send (RTS) and clear-to-send (CTS) frames prior to sending the High-Throughput (HT) data frame. The RTS/CTS exchange is performed at legacy rates so that legacy stations can decode the signals.
- **CTS-to-Self**—The 802.11n AP sends a CTS frame that is addressed to itself. The frame is sent at a legacy data rate and informs neighboring legacy devices how long before the medium will be clear for transmission.
- **L-SIG TxOP**—Legacy Signal Transmission Opportunity (L-SIG TxOP) permits a device to send multiple MPDUs such that they appear to be a single frame to legacy devices.

Even the most efficient protection mechanism causes a substantial decline in throughput; performance can decrease by as much as 50 percent. (See Table B-3, “Protection Mechanism Overhead” in Appendix B, “Reference Tables.”)

Choose the Architecture

With the HP ProCurve MSM devices, you can choose between two architectures:

- **Autonomous**—Includes one or more HP ProCurve MSM APs.
- **Optimized WLAN**—Includes at least one HP ProCurve MSM Controller that manages multiple MSM APs. In the optimized WLAN architecture, the MSM APs are referred to as controlled APs.

Note

In addition to allowing you to manage controlled APs, an MSM Controller can identify (and link you to the management interface of) autonomous APs. Typically, however, you would only do so to support third-party APs (which must be autonomous).

Whichever architecture you choose, you can create multiple Virtual Service Communities (VSCs) to provide wireless access for users. Each VSC defines settings for one WLAN. By creating multiple VSCs, you can support different services for different wireless users; for example, you can implement different security settings, VLAN assignments, traffic priorities, or other parameters.

Autonomous Architecture. In the autonomous architecture, full-featured APs provide wireless coverage for a specific area. (See Figure 1-3.) These intelligent edge devices can enforce your company’s access policies, securing wireless communications through industry-standard authentication and encryption methods. In addition, autonomous APs can apply sophisticated quality-of-service (QoS) measures and enable Layer 2 roaming (as long as the same VSC is supported in the APs).

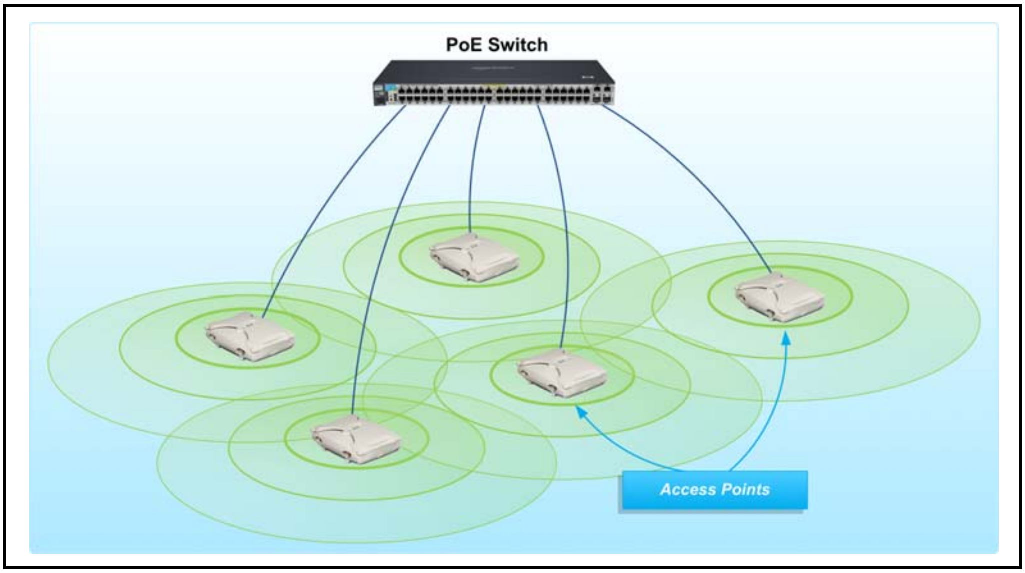


Figure 1-3. Autonomous Architecture

An autonomous architecture is well suited to environments that require:

- Coverage for smaller, isolated areas (such as a small office or a remote site or branch office) requiring only one or a few APs
- Self-sufficient WLAN services, including stand-alone support for WPA/ WPA2-PSK

  An autonomous architecture also provides robust authentication (802.1X) as long as your network also includes a RADIUS server. With HP ProCurve Identity Driven Manager (IDM) managing the RADIUS server, you can implement role-based authentication.
- Static local mesh from one building to another

In small offices, a single AP will often provide more than enough capacity. The limited resources of a small office wired network make an intelligent autonomous AP ideal.

You might also decide to use an autonomous AP to provide wireless access in one area of a medium to large office. For example, you might want to provide wireless access only in conference rooms. Servers and network devices in the existing network already secure and manage wired traffic. You only need to integrate the wireless network with the existing structure and policies.

Public Access Networks (Centralized Access Control). When you want to establish a public access VSC, you must implement centralized access control on that VSC. To implement centralized access control with an autonomous architecture, you must be using one of the following APs:

- MSM313 AP
- MSM313-R AP
- MSM323 AP
- MSM323-R AP

Note These products support software version 5.2.x and below. They do not support subsequent software releases.

At least one AP in your system must be one of these models. The remaining APs can be other models.

When enforcing centralized access control in an autonomous architecture, you configure and manage each AP separately. However, all APs forward authentication and user traffic on the public access VSC to one of the APs listed above, which is configured as the access controller.

The AP acting as an access controller forces wireless users to log in before allowing them to reach resources beyond its Internet port. (Unauthenticated users can access any resources on the LAN port.) The access controller authenticates the users either against its local list or an external RADIUS server. If you want to implement dynamic settings for different users or RADIUS accounting, you must use an external RADIUS server. However, you can configure special settings for all public users on the local list.

Because these products do not offer the full range of features that an MSM Controller offers and because they will not be updated in the future, HP ProCurve recommends that customers update to an MSM710, MSM760, or MSM765zl.

Optimized WLAN Architecture. The optimized WLAN architecture is exactly what the name implies: an architecture that enables you to implement your wireless network so that it is as effective, efficient, and functional as possible in any situation.

The optimized WLAN architecture enables you to centrally manage multiple APs with a controller, which automates deployment and software distribution. The controller also centralizes device configuration and management. Controlling your APs centrally makes your network scalable, reducing the complexity of managing (and the time needed to manage) your wireless network. (See Figure 1-4.)

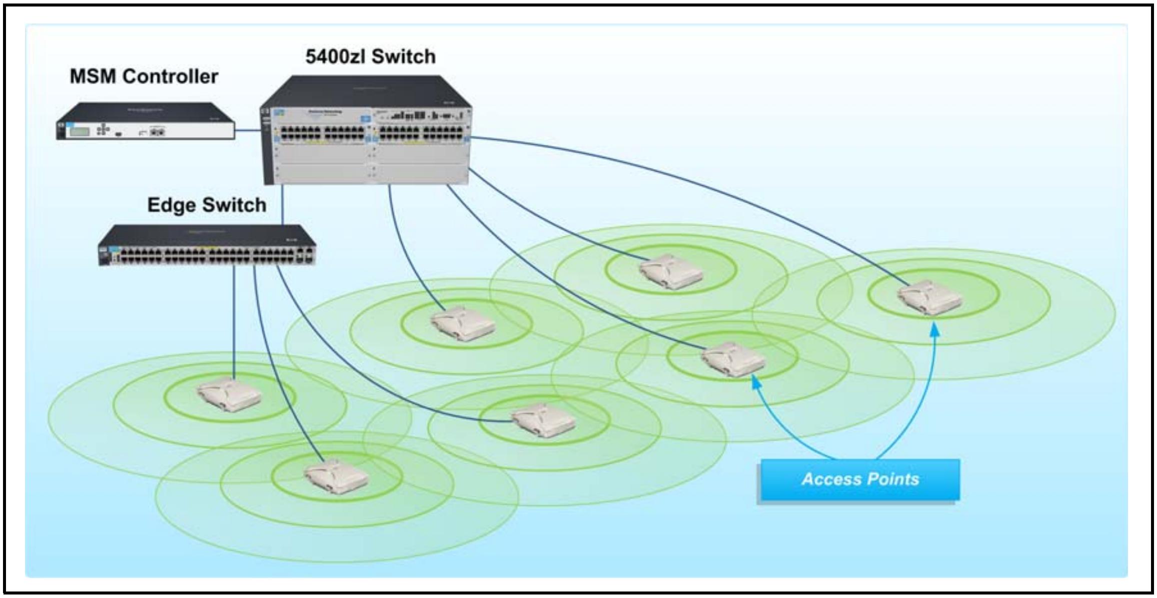


Figure 1-4. Optimized WLAN Architecture

With the 5.4 version of MSM Controller software, you can implement an even more scalable solution for MSM760 and MSM765zl Controllers. You can create a controller team that includes up to five controllers and manage these controllers and their controlled APs from a single interface.

A controller team also provides redundancy. If a controller becomes unavailable, other controllers in the team will discover and manage its APs, eliminating or minimizing the disruption to users.

Centralized Access Control and Distributed Forwarding. In addition to giving you the advantages of centralized management, the optimized WLAN architecture allows you to control how wireless traffic is controlled and distributed on to the wired network. For example, you can have the MSM APs send wireless traffic to the controller for handling, or you can have APs forward traffic directly onto the wired network.

You make this decision for each VSC (or WLAN) that you configure. For some VSCs, the MSM Controller could handle the traffic. For other VSCs, the MSM APs could forward the traffic directly onto the wired network.

If you want the MSM Controller to handle the wireless traffic, you select the **Use Controller for Access Control** option when you create a VSC. This configuration is often referred to as centralized access control because all decisions regarding each user's access are handled by the MSM Controller. The MSM AP forwards the users' traffic to the Controller, and the Controller sends it onto its final destination. (See Figure 1-5.)

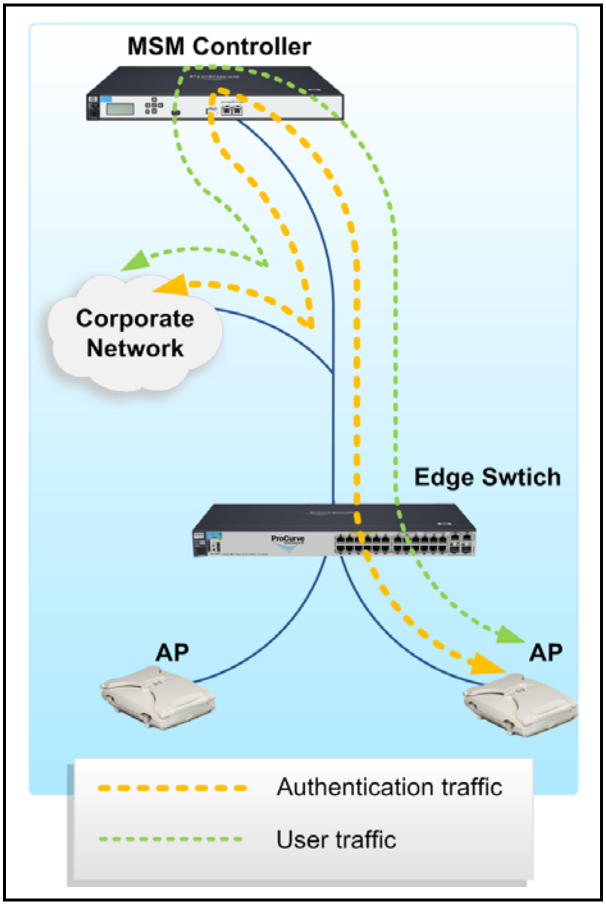


Figure 1-5. Centralized access control

One of the main reasons to implement centralized access control on a VSC is to create a public access VSC, in which users must authenticate through a Web login page before they can access the protected network. Centralized access control enables the controller to act as the gatekeeper to the wired network, enforcing access controls on all wireless user traffic in this VSC.

Centralized access control also benefits networks that require a large coverage but have a limited infrastructure, by providing an integrated firewall, Dynamic Host Configuration Protocol (DHCP) server, and RADIUS server for wireless traffic.

The downside to centralized access control is that the controller processes 100 percent of the wireless user traffic in that VSC. The wireless network thus has a single point of failure, and the traffic detour to the controller adds latency and traffic on the wired network.

In addition, if you are using 802.11n, you may need to evaluate whether or not a single controller with its single uplink can handle the throughput. Determine if the controller must handle a high volume of guest traffic and how much delay guests can tolerate.

Although centralized access control solves many problems associated with giving guests wireless access, it is not usually necessary for VSCs used by employees. When you set up wireless access for employees, you typically want to allow them to access the same or nearly the same resources that are available to them through a wired connection. For these VSCs, you want your intelligent APs to forward wireless traffic directly onto the wired network. This distributed forwarding approach allows you to easily scale performance by combining the benefits of centralized management with the benefits of intelligent APs at the edge. (See Figure 1-6.)

The distributed forwarding approach is ideal for 802.11n deployments, in which high-speed wireless connectivity generates a great deal of traffic. Because each AP forwards traffic independently, the traffic is distributed across multiple points. Your wired network more easily handles the additional traffic, and your users experience the full benefit of 802.11n.

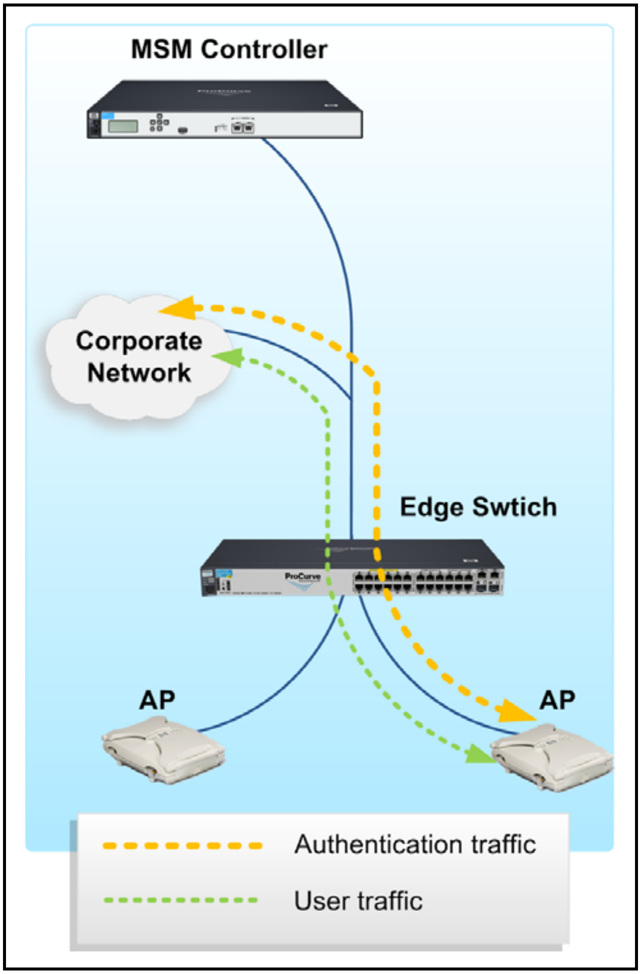


Figure 1-6. Distributed Forwarding

With distributed forwarding, you also have the option to use centralized authentication. With centralized authentication, APs forward all traffic related to the authentication process to the controller for handling. In other words, the controller acts as the authenticator in the 802.1X process. (See Figure 1-7.)

The MSM AP continue to handle the wireless data traffic, transmitting it directly onto the wired network.

You might want to use centralized authentication under the following circumstances:

- You are using the controller's internal RADIUS database to authenticate users.
- You want to simplify the configuration of clients on the RADIUS sever. If the controller is the only RADIUS client for wireless traffic, you only need to configure one client for the wireless network on the RADIUS server, saving you time and hassle.

Although the MSM APs are sending only authentication traffic (which is a relatively small amount) to the MSM Controller, you must still evaluate the impact of that traffic. For example, how will the authentication traffic affect traffic flow on the wired network?

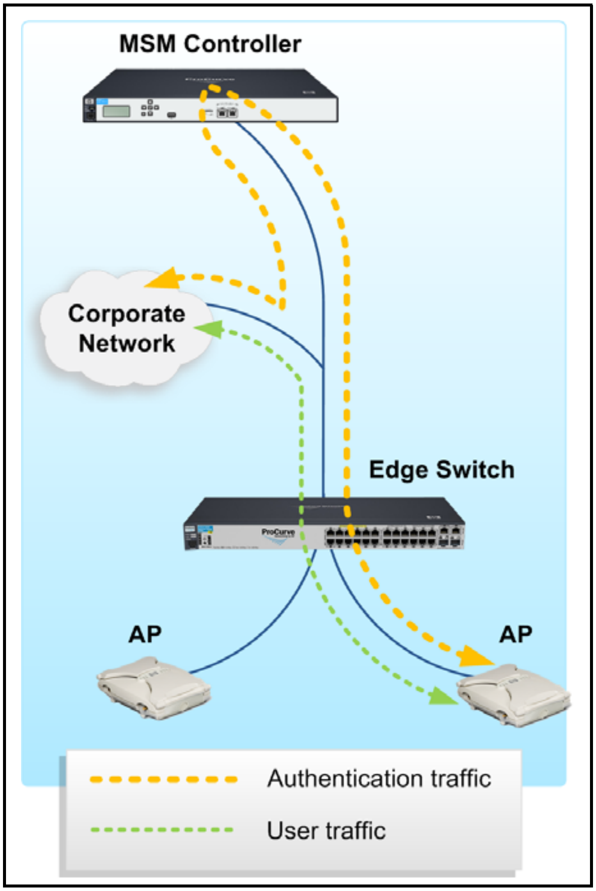


Figure 1-7. Distributed Forwarding with Centralized Authentication

The advantages and disadvantages of each approach for forwarding traffic are summarized in Table 1-5.

Table 1-5. Advantages and Disadvantages to Centralized Access Control and Distributed Forwarding

Approach	Advantages	Disadvantages
Centralized access control	• Effective coverage of large areas • Centralized management of APs with a controller • An integrated firewall, DHCP server, and RADIUS server for wireless traffic (ideal for networks that have a limited infrastructure) • Authentication and access control for the wireless network independent of the wired network • Dynamic meshing across a work space	• Controller must process 100 percent of the network traffic, creating single point of failure • Designed to handle the throughput associated with 802.11a/g standards, it can not easily address the increased performance that comes with 802.11n • No failover mechanism if controller fails • Separate authentication and access control for the wireless network
Distributed forwarding	• Effective coverage of large areas • Centralized management of APs with a controller • Use of the existing corporate network access control system • Dynamic meshing across a work space • Non-blocking architecture capable of delivering full throughput with 802.11n APs • Optional use of the MSM Controller internal RADIUS server (the centralized authentication option)	• No public access network (Web-Auth) • No integrated firewall for wireless traffic

With the optimized WLAN architecture, you can use both centralized access control and distributed forwarding on the same MSM Controller. This means that you can apply the appropriate access control for each group of users and control how traffic is sent onto the wired network.

Combining Autonomous and Optimized WLAN Architectures. When deploying MSM APs, you might use different architectures for parts of your network that have different characteristics. For instance, a large main office might have an optimized WLAN architecture that uses distributed forwarding for employee VSCs and centralized access control for guest VSCs. However, the organization may also have a branch office that is using a couple of MSM APs in an autonomous architecture.

Select the Equipment

This section describes the HP ProCurve MSM devices, starting with the access and mobility controllers and then moving to the APs, client bridge, and antennas.

MSM Access Controllers. HP ProCurve provides the following access controllers, which allow you to centrally control the operation of the wireless infrastructure network:

- J9328A HP ProCurve MSM710 Access Controller (which was formerly called the Colubris MSC-5100)
- J9421A HP ProCurve MSM760 Access Controller.

Both theMSM710 and MSM760 are appliance devices.

These 802.11n-ready MSM7xx Access Controllers allow you to control multiple MSM APs and provision a broad range of identity-based services to ensure consistent QoS and security to stations that use the network. An integral component of HP ProCurve MSM Solutions, the MSM7xx Access Controller pushes QoS and security policies MSM APs at the network edge, where traffic is forwarded directly from source to destination.

MultiService Mobility features include:

- Identity- and roles-based user account profiles using embedded or external AAA services
- Central configuration of VSCs for QoS, authentication, encryption, and VLANs
- Separation of wireless control and data forwarding to maximize delivery of business, voice, and multimedia applications
- Enterprise- and service provider-grade guest access services, fully customizable with Web-based login portal per VSC
- Per-user bandwidth management to ensure fair access to low-bandwidth remote network connections

Management features include:

- Control over MSM APs, ensuring consistent security, QoS, and Layer 2 roaming services from AP to AP

  The controller model number dictates the number of APs that it can control. The MSM710 can control up to 10 MSM APs; the MSM760 can control up to 200. (With a premium license, the MSM760 can be part of a controller team, which can control up to 800 MSM APs.)

- Central management of each MSM AP's wireless operating modes, including APs connected across a local plug-and-play auto-discovery and software installation for easy AP deployment
- Integration with Microsoft Active Directory and external RADIUS services
- RADIUS activity statistics collected per-user for billing by data volume and elapsed session time
- Easy-to-use Web-based administrator interface
- Integration with wired network, leveraging existing Layer 2/Layer 3 infrastructure resources, such as QoS, VLANs, Active Directory integration, and RADIUS servers

Security features include:

- Per-user or per-device security policies
- Authentication based on user credentials (802.1X/EAP), hardware identifiers (MAC address, WEP key), and HTML login (Web-Auth)
- Authentication and authorization through Microsoft Active Directory or internal or external RADIUS servers
- Built-in stateful firewall for secure connection to Internet
- Secure management interfaces, including SSH/SSL access to command-line and Web-based management tools, IPsec-encapsulated SNMP, and XML with digital certificates
- Session tracking to compile a log of user activity for security forensics
- Option for controller-based data forwarding for secure processing of specific applications or services (for example, guest access)
- Access control lists based on IP address, protocol types and port filtering, and DSCP values
- VLAN mapping of guest access traffic for secure passage through corporate network
- Mutual controller/AP authentication using digital certificates to eliminate rogue AP connectivity
- 802.1X supplicant, allowing it to submit its login credentials to an authenticator (typically a switch), which in turn forwards these credentials to the RADIUS server, which verifies them

Table 1-6. Scalability of MSM7xx Access Controllers

	MSM710 Access Controller	MSM760 Access Controller
Scalability	10 MSM APs	200 MSM APs*
Max. simultaneous users	Unlimited	Unlimited
Max. simultaneous guest access users	100	2000**

*Ships with support for 40 APs upgradeable in increments of 40 to a maximum of 200 APs.

**Ships with support for 1000 simultaneous guest access users upgradeable in increments of 250 users per 40 AP license pack to support a maximum of 2000 guest access users.

MSM Mobility Controllers. HP ProCurve provides the following Mobility Controllers.

- J9325A HP ProCurve MSM710 Mobility Controller (formerly called Colubris MSC-5100)
- J9420A HP ProCurve MSM760 Mobility Controller
- J9370A HP ProCurve MSM765zl Mobility Controller

The MSM710 is an Access Controllers with a Mobility license installed, and the MSM760 is an Access Controller with a Premium license installed. (Both the Mobility license and Premium license are sold separately from the Access Controller.)

The Premium license is included when you register and activate the MSM765zl. (You do not have to purchase it separately.) Consequently, the MSM765zl always functions as a Mobility Controller.

The MSM710 and MSM760 are appliances, but the MSM765zl runs on an HP ProCurve ONE Services zl Module, which is installed in an HP ProCurve 5400zl or 8200zl Services Switch. A maximum of four MSM765zl modules can be installed in a single chassis; however, only three can be installed in the 5406zl and 8206zl switches. For more information on the ONE Services zl Module you can go to *www.procurve.com/products/Appliance/HP_ProCurve_ONE_Services_zl_Module/overview.htm*.

The Mobility Controllers provide all the benefits of the Access Controllers, as well as features for roaming, control over wireless traffic, and scalability:

- **WPA2 Opportunistic Key Caching**

  This feature enables fast roaming between APs in a VSC that enforces WPA2 with 802.1X security.

- **Layer 3 Mobility**

  This feature enables users to roam between APs that are connected to different subnets—without requiring the user to log in again or use special client software.

- **Mobility Traffic Manager**

  The 5.4 version of the MSM Controller software includes the Mobility Traffic Manager feature, which allows you to control how wireless traffic is distributed onto the wired network. For example, you may not want to extend user VLANs to the edge where users connect to the wireless network. With Mobility Traffic Manager, you can have the APs tunnel the traffic to the MSM Controller at the network core. The MSM Controller can then distribute the traffic onto the wired network.

  Traffic can be controlled based on a variety of settings including identity-based assignments, making it easy to deploy your enterprise mobility solution no matter what your current network infrastructure. You even have the option to load balance the traffic across multiple VLANs, which might be useful if you have several WAN links that use different VLANs. (For more information about Mobility Traffic Manager, see "Use Mobility Traffic Manager to Control Where Traffic Is Distributed into the Wired Network" on page 1-79.)

- **Controller Teaming**

  The 5.4 version of the MSM Controller software also supports controller teaming, which provides greater scalability and redundancy for large enterprises. Teaming is designed is designed for organizations that:

  - Have more than 200 APs and want to be able to manage them from a single interface
  - Want to implement redundancy for their MSM Controllers

  With teaming, you can configure a group of up to five MSM Mobility Controllers from a single interface, and if one of these controllers fails, its controlled APs can be discovered and managed by other members of the team.

  The teaming feature is available on the MSM760 Mobility Controller and the MSM765zl Mobility Controller. However, it is not available on the MSM710 Mobility Controller.

  (For more information about the redundancy provided by controller teams, see "Redundancy for MSM Controllers" on page 1-111.)

Table 1-7. MSM7xx Mobility Features

	MSM710 Mobility Controller	MSM760 Mobility Controller	MSM765zl Mobility Controller
Additional services	• Fast roaming for 802.1X-controlled VSCs • Roaming across subnets • Mobility Traffic Manager	• Fast roaming for 802.1X-controlled VSCs • Roaming across subnets • Mobility Traffic Manager • 64 VSCs • Teams	• Fast roaming for 802.1X-controlled VCS • Roaming across subnets • Mobility Traffic Manager • 64 VSCs • Teams
Scalability	• 10 MSM APs	• Up to 200 MSM APs with one MSM Controller • Up to 800 MSM APs with a team	• Up to 200 MSM APs with one MSM Controller • Up to 800 MSM APs with a team

*Ships with support for 40 APs upgradeable in increments of 40 to a maximum of 200 APs.

Access Points. To meet the needs of any environment, HP ProCurve offers a variety of APs.

MultiService Mobility (MSM) APs

The HP ProCurve MSM APs bring intelligence to the network edge, providing scalable, seamless wireless access anywhere, anytime. They deliver multiple network services, enforce robust security and deliver high performance client access, unlike “thin” or “lite” access points. An integral component of HP ProCurve MultiService Mobility Solutions, MSM APs support a plug-and-play automatic configuration and ongoing central control by HP ProCurve MSM Mobility and Access Controllers for the highest degree of configurability and ease of management.

RF coverage features include:

- Single-, dual-, and tri-radios
- 802.11a/b/g and 802.11n
- Per-radio software-selectable configuration of the 2.4 GHz and 5 GHz frequency bands
- Plenum-rated or NEMA-rated enclosures for indoor and outdoor wireless coverage
- Self-healing, self-optimizing local mesh extends network availability to areas without an Ethernet infrastructure
- 802.3af Power over Ethernet or external power cord

Management features include:

- Centrally controlled, configured and updated with a Mobility or Access Controller
- Auto-selection of RF channel and transmit power
- Per-client event log of 79 association, security, and DHCP activities for easy diagnosis
- Packet capture on a VSC or LAN interface
- In autonomous mode, SNMP, CLI, and Web-based management interfaces for integration with HP ProCurve Mobility Manager or third-party, standards-based network management systems

Security features include:

- Enforcement of client authorization based on user credentials (802.1X/EAP), hardware identifiers (MAC address, WEP key), and HTML login
- Hardware-assisted encryption using WPA2/AES (IEEE 802.11i), WPA/RC4 and/or WEP
- Dedicated RF sensor and dedicated client access eliminate time-slicing on the MSM325, MSM335, and MSM415.
- Layer-2 client isolation per VSC
- Trusted Network Connect (TNC) network access control for user quarantine
- Protocol filtering per VSC to deny unwanted traffic
- IP filtering per-user and per-VSC to forward traffic to a pre-defined location
- Management communication through SSH/SSL, IPsec, and digital certificates
- Kensington lock for physical security on the MSM335 and MSM422
- Controlled-mode security to prevent data from being recovered from stolen MSM access points

Table 1-8. HP ProCurve MSM AP and Sensor Specifications

Model	802.11 Radios	Enclosure	Ports	Antenna Connectors	Antennas	Power Inputs
MSM310 (US and WW)	1 – a/b/g	indoor plenum-rated	2 – 10/100 (RJ-45)	2 – Reverse-polarity male SMA with diversity	2 – 2 dBi dual-band 2.4/5GHz omni	5 VDC PoE
MSM310-R (US and WW)	1 – a/b/g	outdoor NEMA-rated	1 – 10/100 (RJ-45) waterproof	2 – N-type female with diversity, waterproof	2 – 5.5 dBi 2.4 GHz omni	PoE

Model	802.11 Radios	Enclosure	Ports	Antenna Connectors	Antennas	Power Inputs
MSM320 (US and WW)	2 – a/b/g	indoor plenum-rated	2 – 10/100 (RJ-45)	4 – Reverse-polarity male SMA with diversity	4 – 2 dBi dual-band 2.4/5GHz omni	5 VDC PoE
MSM320-R (US and WW)	2 – a/b/g	outdoor NEMA-rated	1 – 10/100 (RJ-45) waterproof	2 – N-type female, waterproof	2 – 5.5 dBi 2.4 GHz omni	PoE
MSM325 (US and WW)	2 – a/b/g/RF sensor	indoor plenum-rated	2 – 10/100 (RJ-45)	4 – Reverse-polarity male SMA with diversity	4 – 2 dBi dual-band 2.4/5GHz omni	5 VDC PoE
MSM335 (US and WW)	2 – a/b/g 1 – RF sensor	indoor plenum-rated	1 – 10/100/1000 (RJ-45) 1 – Serial (DB-9) female	2 – Reverse-polarity male SMA with diversity	6 – 2.4/5 GHz omni (3 per flap)	48 VDC PoE
MSM410 (US and WW)	1 – a/b/g/n draft	indoor plenum-rated	1 – 10/100/1000 (RJ-45) 1 – Serial (RJ-45)	None	3 – 2.4/5 GHz omni	PoE
MSM415*	1 – RF sensor (a/b/g/n)	indoor plenum-rated	1 – 10/100/1000 (RJ-45) 1 – Serial (RJ-45)	None	3 – 2.4/5 GHz omni	PoE
MSM422 (US and WW)	1 – a/b/g 1 – a/b/g/n draft	indoor plenum-rated	1 – 10/100/1000 (RJ-45) 1 – Serial (DB-9) female	4 – 2.4/5 GHz reverse-polarity male SMA (3 with diversity)	5 – 2.4/5 GHz omni (2 with diversity) 3 – 3x3 MIMO 2 – 2.4/5 GHz	48 VDC PoE

*The MSM415 acts *only* as an RF sensor. It does not provide user access.

HP ProCurve MSM313 and MSM323 Series APs

HP ProCurve MSM313 and MSM323 Series APs support software version 5.2.x and below. Although these APs do not support subsequent software versions, they may still be in use on your network. The MSM313 and MSM323 series include:

- MSM323 (J9337A US, J9341A ROW) Access Point (formerly called MSC-3300)
- MSM323-R (J9342A US, J9345A ROW) Access Point (formerly called MSC-3300R)
- MSM313 (J9346A US, J9350A ROW) Access Point (formerly called MSC-3200 US)
- MSM313-R (J9351A US, J9354A ROW) Access Point (formerly called MSC-3200R)

These APs can control the operation of intelligent APs that are distributed throughout a building or campus. MSM313s and 323s deliver a range of services to wireless client devices and ensure consistent quality and security.

In a single turnkey unit that is ideally suited for small and medium-sized deployments, an MSM313 or 323 integrates a full-featured AP and the same award-winning public/guest Internet access service offered in the MSM7xx series controllers. In this way, you can deploy a single architecture across public and private venues of any size. Customers can easily expand RF coverage in larger venues by daisy-chaining MSM313 and MSM323s, using the convenient downstream Ethernet port.

The MSM313 and MSM323s feature full IP routing and network services that enable them to connect directly to a cable or DSL modem and provide a turnkey remote-site networking solution.

Key features of the MSM313 and MSM323 APs include:

- Creates easy-to-use public/guest Internet access (hotspot) services
- “Zero configuration” service interface adapts to client device configuration settings
- Bandwidth management creates multiple service tiers and ensures fair access to bandwidth for users
- Secure user AAA function enables wide range of free or fee-based service models
- Complete IP routing and networking services enables direct connection to the Internet
- Concurrent Universal Access Method (HTML login) and 802.1X login support facilitates migration to Wi-Fi security
- Interfaces for centralized AAA and captive portal and billing functions enables large multilocation networks
- Integrated MultiService Access Point provides turnkey “hotspot in a box” for small venues
- Downstream Ethernet port connects additional APs for expanded RF coverage
- Compliance with 802.11j supports Japanese rules for RF signals.

Table 1-9. HP ProCurve MSM313 and MSM323 Access Point Specifications

Model	802.11 Radios	Enclosure	Ports	Antenna Connectors	Antennas	Power Inputs
MSM313	1 – a/j/b/g	indoor plenum-rated	2 – 10/100 (RJ-45) with daisy-chain support 1 – Serial (RJ-11)	2 – Reverse-polarity male SMA with diversity	2 – 2 dBi dual band 2.4/5GHz omni	5 VDC PoE
MSM313-R	1 – a/j/b/g	outdoor NEMA-rated	1 – 10/100 (RJ-45) waterproof	2 – N-type female with diversity, waterproof	2 – 5.5 dBi 2.4 GHz omni	PoE
MSM323	1 – a/j/b/g 1 – a/b/g	indoor plenum-rated	2 – 10/100 (RJ-45) with daisy-chain support 1 – Serial (RJ-11)	4 – Reverse-polarity male SMA with diversity	4 – 2 dBi dual band 2.4/5GHz omni	5 VDC PoE
MSM323-R	1 – a/j/b/g 1 – a/b/g	outdoor NEMA-rated	1 – 10/100 (RJ-45) waterproof	2 – N-type female, waterproof	2 – 5.5 dBi 2.4 GHz omni	PoE

M111 Client Bridge. HP ProCurve M111 is a product that enables devices without their own wireless NIC to connect to a wireless network. The M111 connects legacy Ethernet or serial communications stations to a wireless LAN. Electronic cash registers, servers, printers and other devices can be deployed in any location where a WLAN signal is available, eliminating the time and expense of installing Ethernet cable for network access.

The M111 integrates into a MultiService Mobility Solution and it is interoperable with any IEEE 802.11 network infrastructure.

Legacy client devices can be easily integrated into a WLAN using the M111, which bridges Ethernet client devices that run a legacy networking protocol to the WLAN, thereby extending wireless network access to a wide range of DECnet, IPX, Appletalk and other devices. An integrated serial-to-TCP/IP converter enables a TIA-232 device, such as a hotel property management system, to communicate with a network node on the WLAN.

Key features of the M111 include:

- Bridges an Ethernet LAN segment or serial interface to your wireless network
- Capacity to bridge Ethernet segments with up to 20 client stations
- Converts a TIA-232 serial data stream to a wireless TCP/IP stream
- Configurable Ethernet MAC and protocol filters for enhanced security
- Hardware-assisted WPA2, WPA, and WEP security for wireless privacy
- 802.1X PEAP WLAN authentication
- Configurable 802.11 a/b/g radio with external antenna connectors

- 100-mw radio and antenna diversity for excellent distance performance
- Centrally manageable as part of the MultiService Mobility Solution
- Plenum-rated enclosure.

MSM317 Access Device. The MSM317 Access Device revolutionizes the way wireless and wired IP-based services are delivered to hospitality and residential properties. The MSM317 integrates wired and wireless connectivity into a small unit that can be quickly and discretely installed in a standard wall box. The MSM317 provides four Ethernet ports, a 2.4GHz 802.11b/g wireless access point, and a pass-through RJ-45 connection for service and user connectivity. One of the Ethernet ports can be configured as an IEEE 802.3af-compliant PoE (power over Ethernet) port to enable service devices such as IP telephones to be powered directly from the MSM317. The MSM317 requires a single powered cable drop to unlock its utility and, through the reduction in cabling, switch ports, and power-sourcing equipment, the MSM317 represents the best value for the delivery of next generation voice, data, and entertainment services.

Key features of the MSM317 access device include:

- 802.11b/g radio
  - Software-controllable output power from 10mW to 100mW EIRP
  - Operating channels configurable based on country regulations
  - 802.11b at 1, 2, 5.5, 11 Mbps
  - 802.11g at 6, 9, 12, 18, 24, 36, 48, 54 Mbps
  - Two integrated 2.4GHz directional antennas with diversity
- Pass-through port
  - Unmanaged RJ-45 connection for service and user connectivity
- A non-blocking managed Layer 2 switch, featuring:
  - Support for four 10/100 Mbps ports with Auto-MDX support
  - Rate limiting
  - IEEE 802.1Q VLANs
  - Four priority queues mapped to IEEE 802.1p or DiffServ
  - IEEE 802.1X for device authentication
- PoE support:
  - System power through PoE
  - IEEE 802.3af -compliant power forwarding through designated PoE port

Determine if You Need External Antennas

External antennas provide additional gain and shaping of RF signals. (See Table 1-8, "HP ProCurve MSM AP and Sensor Specifications" on page 1-47 for information about the type of external antenna connectors each MSM AP supports.)

Omnidirectional antennas provide a hemisphere of coverage with the antenna at the center. Omnidirectional antennas may form the backbone of a wireless site plan with widespread coverage, whether complete or partial.

Directional antennas provide a beam or cone of coverage with the antenna at the apex. Because they are focused on specific areas, they can provide longer or more extended coverage in the areas to which they are directed. Directional antennas can be used to fill in coverage where needed, particularly where complete coverage is desired.

Identify the Wireless Stations

The component of your wireless network that is perhaps least within your control is the stations that connect to the network. Some organizations provide stations to authorized users and can therefore carefully control which stations (the wireless cards and clients) are allowed to connect.

However, other organizations, such as Internet cafes and hotels, want to provide wireless connectivity for customers who have their own stations, so their network settings must accept a broad range of wireless card and client capabilities.

If your organization controls the wireless stations that will connect to the wireless network, you must ensure that they can support the security settings that you choose. (See "Choose the Security Protocols" on page 1-60 for more information.)

Also consider the following:

- Most workstations and laptops have an 802.1X supplicant (included with Windows XP SP2 or later), but PDAs and smartphones might not. If the station does not have a supplicant, you can usually install one.
- Stations that boast 108 Mbps with 802.11g can attain that speed only with APs from the same vendor.

Plan Coverage and Capacity

The size of the cells should depend on desired data rates and station density. Consider the types of applications that the network must support and whether these applications require high-speed connections. Also consider the number of clients that will be using each cell. For example, if a network should support all of the applications of a contemporary wired network, you should plan smaller cells in which most stations can connect at 54 Mbps. On the other hand, if users will primarily browse the Internet, rates can be much slower and the cell larger.

On a typical wireless client, the receiver sensitivity at 54 Mbps is 20 dBm lower than the sensitivity at 1 Mbps. Because power falls off as a square of distance, and dBms are logarithmic power units, this 20-dBm difference translates to a tenfold decrease in range, when taking nothing but free-space path loss into account. In a closed or cluttered environment, the maximum range is compressed, as is the difference between smaller and larger cells, so a 54 Mbps cell might be only a third the diameter of a 1 Mbps cell in a closed space. See “Calculations for Transmission Range” in Appendix B, “Reference Tables.”

You might plan smaller cell sizes than you would at first expect because coverage is a two-way proposition: a cell is the area in which an AP and stations can communicate, so the size depends on station hardware as well as the AP. Check your equipment documentation for ranges, keeping in mind that those ranges might be for open environments and minimal bandwidth.

A first impulse is to blanket an area with as much signal as possible, but consider where coverage is actually needed. Is it actually important for the signal to reach all hallways, stairwells, and corners? Although you should be careful not to spread coverage to unnecessary areas, you should also consider how much cell overlap might be needed. For example, if you plan to have VoWLAN on your network, you should plan cells that overlap significantly and provide no less than -65 dBm (3.162 x 10^{-7} mW) coverage in any area.

In the end, the best plan is to sketch out preliminary locations for APs, taking into account all of the issues discussed above, and then plan to adjust as your prototype reveals where you need to fill in or shape the signal. Although you should carefully plan your coverage area, many final decisions must wait for the initial deployment, including:

- The transmit power necessary to create adequate coverage areas, considering physical obstacles and sources of RF interference.

  If you plan to use automatic power control (APC), you should consider this when planning the transmit power. When using APC, you should run your APs at least 6 dBm below the maximum level to leave room for them to boost the power when required. See "Redundancy for MSM Controllers" on page 1-111 for more information.
- The best placement for APs, considering obstacles and interference
- The best shape for cells
- External antennas, if required
- The degree of overlap needed between cells

To assist you in this planning (and in the eventual implementation), it is recommended that you use the HP ProCurve RF Planner.

Planning Coverage and Capacity with HP ProCurve RF Planner or HP ProCurve Mobility Manager

HP provides two tools that simply the complex task of planning a wireless networking infrastructure by allowing you to model WLAN coverage. These tools allow you to place APs on your company's unique site map and factor in common variables, such as physical features, building materials, and WLAN equipment characteristics. They also facilitate deployment by enabling the assessment of security risks and generating equipment lists.

HP ProCurve RF Planner. RF Planner is built on a unique, patent-pending RF propagation model. This model provides outstanding accuracy by drawing from a comprehensive knowledge base of RF characteristics for HP ProCurve MSM APs and Controllers, third-party equipment (APs and directional antennas), and building materials. Open-air modeling capabilities facilitate the design of outdoor campus and municipal networks.

RF Planner provides the following key features:

- Advanced prediction model for access point and RF sensor placement.
- Device database with preset options for common wireless equipment from a variety of manufacturers.
- Ability to add new wireless equipment (access points, sensors, antennas) to the database.
- Building material database.
- Cross floor coverage.
- Ability to plan 802.11n coverage as well as 802.11a/b/g coverage.

Once you model the layout of a facility, you can place APs using a simple drag-and-drop operation to generate RF maps and a comprehensive set of deliverables, including:

- Site model for future RF planning
- Bill of Materials (BoM) for APs and antennas, including:
  - Number, location, and configuration of wireless APs
  - Antenna types and location
- RF Maps
  - Security View—coverage inside the perimeter, coverage beyond the perimeter (spillage view), and redundancy
  - APs:—coverage, spillage, channel allocation, interference, and redundancy

RF Planner also allows you to model coverage for sensors, which can be used with HP RF Manager. An Intrusion Detection System/Intrusion Prevention System (IDS/IPS), RF Manager can protect your network against rogue APs and attacks that target wireless networks. (For more information, see “Use RF Manager to detect unauthorized APs” on page 1-97.)

HP ProCurve Mobility Manager. An add-on to HP ProCurve Manager Plus (PCM+), PMM allows you to configure, manage, and monitor MSM Controllers and MSM APs as well as legacy mobility devices such as HP ProCurve AP 530 or HP ProCurve Wireless Edge Services Module. On the MSM Controllers, for example, you can configure VSCs and radio settings as well as more advanced security features such as AP detection.

You can use PMM to configure these settings on a single device. Because PMM integrates tightly with PCM+, however, you can also configure these settings for an entire group of devices, simultaneously.

PMM also includes site-planning and deployment tools to help you design wireless coverage for a new wireless network or to improve coverage for an existing network. To design your wireless network, you can:

- Upload a floor plan
- Customize the environment to include obstacles and the type of space
- Plan the placement of your wireless devices
- View heat maps, which show the predicted wireless coverage given the placement of the devices, surrounding obstacles, and the type of space
- Run a report to determine which devices you must purchase to implement your planned network
- Adjust settings for radios and antennas as needed and deploy those settings to managed devices
- Adjust wireless coverage as needed over time

Once you deploy your wireless devices, PMM enables you to monitor your wireless network with a dashboard that displays data and traffic metrics collected throughout the network. PMM also provides a number of reports, which help you prove regulatory compliance and conduct your own audits.

Advantages of Integration with PCM+

Because PMM is tightly integrated into PCM+, you have the ability to manage and monitor both wired and wireless devices from a single management console. This allows you to apply consistent policies across both your wired and wireless networks and to monitor traffic end-to-end. (For more information about using PCM+ to monitor the wireless network, see “Monitor Network Performance” on page 1-109.)

By adding HP ProCurve Identity Driven Manager (IDM) (another PCM+ snap-in), you can apply security policies to both your wired and wireless networks and simplify the setup for dynamic VLANs, dynamic ACLs, and dynamic QoS settings. Finally, HP ProCurve Network Immunity Manager (another snap-in) helps protect against attacks launched anywhere on your network.

Planning Without a WLAN Modeling Tool

If you do not have a WLAN modeling tool, you will need to plan the implementation manually. You should obtain a clean floor plan and draw directly on it or use drafting or drawing software such as Microsoft Visio. Sketch in or place your coverage cells on the floor plan. To calculate the approximate size of a cell, see "Calculations for Cell Size" in Appendix B, "Reference Tables."

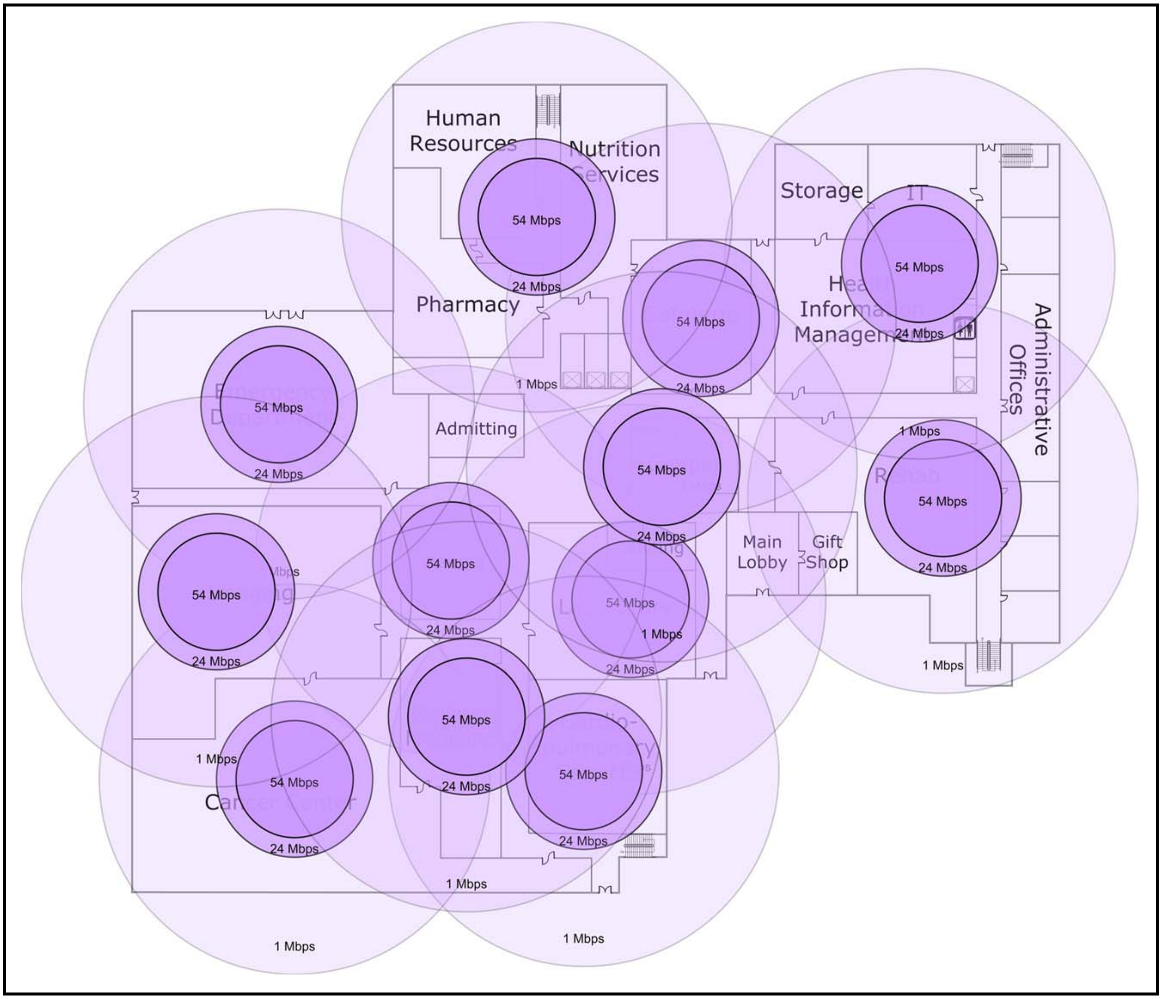


Figure 1-8. 802.11b/g Coverage Cells in Visio

The example above uses a different transparency level for each data rate.

Multi-Level Coverage. If your site has more than one level, you will need to consider the issue of cells and channels in three dimensions. With an RF map or cell plan for each level, consider how each cell relates to the cells directly above or below it.

Keep in mind that the transmission pattern of the AP internal (omnidirectional) antenna appears circular from above, but from the side it is more like a flattened oval. Because you will probably mount your APs near the ceiling, it is likely that an AP transmissions will "leak" up to the next level.

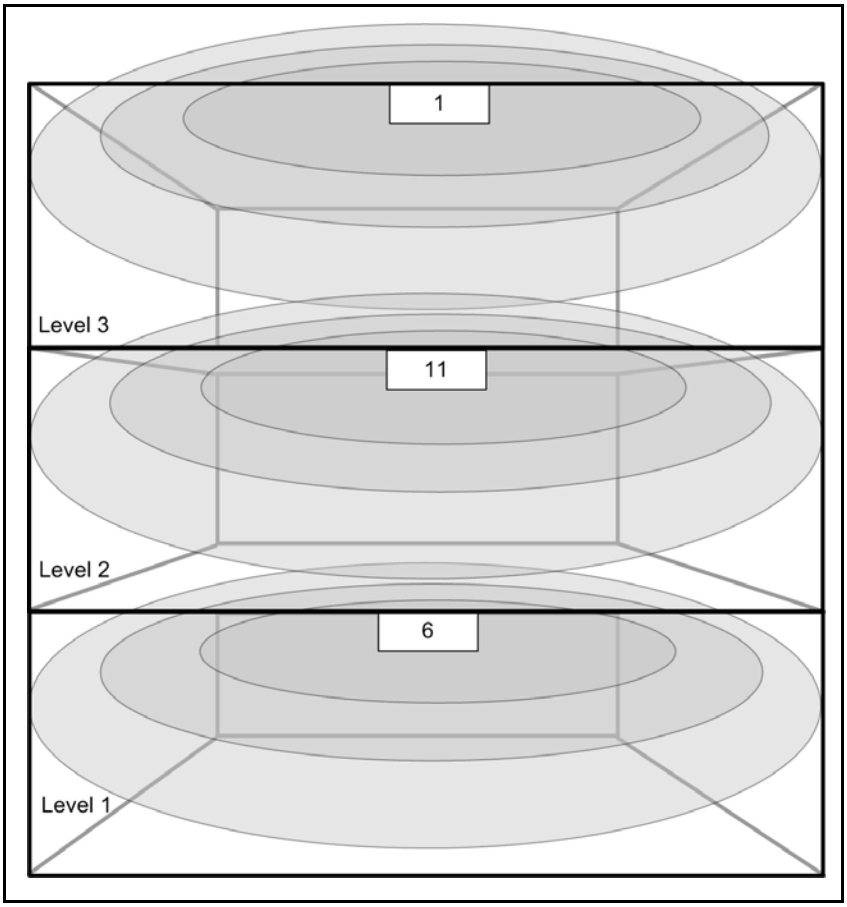


Figure 1-9. Cross-Section of a Three-Level Building

Depending on the construction materials that were used for each floor, the signals from an AP may or may not interfere with the AP above it. On the other hand, sometimes you can take advantage of this inter-floor "leakage" to provide additional coverage if the signal is strong enough from the lower floor. Either way, make sure that you adjust your channel selection to account for multiple-level deployments.

Begin Planning Wireless Security

Wireless networks have opened a new world of convenient, anytime, anywhere access. Unless you carefully configure security for your wireless network, however, this access may extend to anyone—whether or not you want that person to access your network. Initially, you will need to consider the following when designing wireless security:

- Physical security
- Security protocols
- VSC design
  - Levels of trust
  - Relationship to VLANs
- Firewalls
- MAC lockout
- Traffic filters

Plan Physical Security

When you consider security for a wireless network, you should first think of securing the APs. For example, you should try to install APs in a place that can be locked or in at least an inaccessible plenum space. Given the nature of wireless networks, this is not always possible, but you should at least explore the option. Although the MSM335 and MSM422 AP mounting bracket has a Kensington-style lock to keep the AP from being removed, you should take further precaution to prevent anybody from accessing the AP interfaces.

Once you have configured the APs and ensured that you can access them through the Ethernet network, you should disable console access so that unauthorized users cannot establish a serial connection and try to guess the username and password that grants manager access.

To prevent hackers or even employees from attaching an unauthorized (rogue) AP to your network, you should implement 802.1X on your edge switch ports. You would then disable 802.1X only on the ports in which the APs and controllers are connected.

If you have some legacy switches that do not offer 802.1X functionality, you may want to consider replacing them so that you can begin to secure your network from the edge. (See Table 1-16 on page 1-93.)

Choose the Security Protocols

When deciding on security protocols for your VSC, you have several options at your disposal. The first are those that are provided by the 802.11 standard itself:

- Open or closed system beaconing
- Open system or shared-key validation
- Encryption or no encryption

You can further enhance the security of your wireless system with supplemental security measures such as:

- Authentication
- Strong encryption
- Access controls

The security options offered by the 802.11n, 802.11b, 802.11g, and 802.11a standards are very rudimentary and designed to provide easy access more than block intruders. However, even if you choose to use stronger security methods (such as 802.11i with 802.1X authentication), you still need to choose these options properly to integrate them with your additional security methods.

Open or Closed System Beaconing. With “open system beaconing,” APs openly advertise their available SSIDs in 802.11 beacon frames. When users look for available wireless networks, the open system SSIDs will show up in the users’ lists.

A closed-system configuration blocks the advertising of SSIDs in 802.11 beacon frames. It has been suggested that closed systems are more secure because an unauthorized wireless station cannot see the SSIDs available on the AP. This may provide some security from casual intruders; determined intruders, however, can use wireless sniffer tools to monitor 802.11 frames to determine which SSIDs are supported by the APs. Because intruders can readily get the information that the closed system blocks, the use of a closed system provides little actual protection from a determined intrusion attempt.

Open or Shared-Key Validation. In the 802.11 standards literature, the term “authentication” is used to refer to a type of pre-association handshake between the station and the AP. After this kind of “authentication,” the station must then associate with the AP before it can transmit data on the medium. Because of the potential confusion with true authentication (where there is establishment of identity or legitimacy), the term "validation" will be used in this design guide instead of "authentication" to describe the following two processes:

- **Open system**—No key or secret is exchanged between the station and the AP. The station merely sends a request to be validated, and the AP accepts.

Note

Do not confuse 802.11 open system validation with the open system operations for beaconing the SSID, described in the previous section. An AP can operate in closed system and use open system validation. In such a case, the AP does not beacon the SSID, but a station authentication request must include the correct SSID.

Conversely, an AP can advertise the SSID (operate in open system) and use shared-key validation. However, the most typical combination is open system beaconing and open system validation.

Typically, with open system validation, any station can connect to the VSC. But an AP can check the source MAC address in the station request and use that address to decide whether the station can connect. This security option is called MAC authentication (MAC-Auth). Because every wireless client has a MAC address, all wireless devices can be authenticated through MAC-Auth. You can also enable MAC-Auth to identify your network devices to reduce the threat of rogue APs.

MAC-Auth should not be your network sole protection against attack, however. Malicious users can capture wireless frames to or from an approved device and extract a valid MAC address. In a tactic known as *spoofing*, they then replace the invalid MAC address of their device with the valid extracted address to gain network access. MAC-Auth is only one layer in what should be a multi-layered approach to security.

Note

The Web-based management tool refers to MAC-Auth as *MAC-based authentication*. This guide refer to it as *MAC-Auth*.

There are two kinds of MAC-Auth:

- **Local MAC-Auth**—The MAC addresses of allowed and denied wireless stations are configured separately on each AP or controller.
- **RADIUS MAC-Auth**—The list of allowed MAC addresses is maintained on a central RADIUS server. APs can also receive dynamic settings for the station that are stored on the RADIUS server.

- **Shared-key**—This option was designed for use with WEP. Only stations with the correct key can be validated. The AP sends a challenge text to the station, which encrypts the text with the key and sends it back to the AP for validation.

Caution

Shared-key validation contains a design flaw that comprises the secret key. If you choose static WEP for your security method, you should use open system validation. Users must still know the correct key to associate to the VSC.

Note

A VSC that uses shared-key validation cannot use 802.1X authentication after association. For the best possible security, use open system validation in the pre-association stage and authentication after association.

In summary, you should almost always use open system validation, and you may add MAC-Auth to this validation.

If the pre-association validation is successful, the station sends an association request to the AP, which the AP can accept or reject. If the AP accepts and no authentication is in place, the AP allows the station to forward data frames. It also takes responsibility for receiving responses for the wireless station and forwarding them back to it. The association remains active until it is terminated by either party.

Encryption or No Encryption. Encryption transforms data in the wireless frame so that unauthorized users cannot interpret the data. If no encryption is selected, the data packets are transmitted across the medium in plaintext, and anyone with a wireless client can read the data.

An early alternative was to use WEP, a simple encryption method wherein the wireless station and the AP use the same key to encrypt all traffic. The key is determined by the administrator of the AP, who must tell each prospective user what the key is. Because the key does not change automatically, this implementation is called “static WEP.”

Unfortunately, the WEP design includes several flaws, and widely available software can easily exploit these flaws to crack the shared key. It is possible to crack a WEP key after collecting fewer than 100,000 frames of encrypted network traffic. This can be done in minutes on a reasonably busy network.

WEP was the only encryption option specified in the original 802.11 standard. However, wireless devices now support supplemental security options—for both encryption and authentication.

Supplemental Security. The authentication and encryption methods provided by 802.11 may be adequate for home users, but if you need to comply with HIPAA, FERPA, FISMA, or other security standards, you must choose stronger authentication and encryption methods.

Authentication is vital to wireless network security because it ensures that only authorized users access the network. Unlike the pre-association validation options, the supplemental authentication options are true authentication methods. They more rigorously ensure that only legitimate users can connect. One or more of the authentication methods described below should be used in addition to the validation methods provided by 802.11.

- **Web-Auth**—Like MAC-Auth, Web-Auth enables end users to authenticate and connect to the network without special utilities or configurations on their stations. The stations require a Web browser only. However, unlike MAC-Auth, a user must participate in the authentication process, entering credentials—a username and password—on a Web page.

  The network access control decision is based on the validity of the username and password. Because the Web browser has become a standard user application, most workstations, laptops, PDAs, and smartphones support Web-Auth.

Note

The MSM Controller's Web-based management tool refers to Web-Auth as *HTML-based authentication*. This guide refers to it as *Web-Auth*.

- **IEEE 802.1X**—The industry-standard IEEE 802.1X protocol provides the most secure form of network access control. Its standardized framework enables vendor-neutral implementations.

  802.1X binds the state of a user's port (open or closed) to the user's authentication state, thus ensuring that users are properly identified and controlled as soon as they connect to a network.

  With 802.1X, a user's login credentials are submitted to a RADIUS server for verification, a process that can require several seconds. If users are required to re-authenticate, such as when roaming between subnets, the 802.1X exchange will cause a noticeable delay. Every station must have an 802.1X supplicant, and every edge device (switch, AP, or router) must support 802.1X authentication.

  An 802.1X supplicant can be installed on a station as software from a third-party vendor or as part of an OS. In addition, many vendors of wireless clients include an 802.1X supplicant as part of the product. You must also consider which Extensible Authentication Protocol (EAP) the station 802.1X supplicant supports.

802.1X supplicants can be found in the following:

- Infrastructure devices:
  - HP MSM APs (software version 5.4 and above)
  - HP ProCurve managed switches
- Stations:
  - Windows 2000 SP4 and later
  - Mac OS 10.3 and later
  - Linux Red Hat 8.0 and later (WPA supplicant)
  - SUSE Linux Enterprise Server 9 or later (WPA supplicant)
  - OpenX Project Xsupplicant for Linux
  - Juniper Networks Odyssey client

Typically, 802.1X supplicants on stations require some form of user interaction; however, some smartphones and printers automatically submit credentials such as a subscriber identity module (SIM) or digital certificate.

Table 1-10 shows which kinds of stations are compatible with each kind of authentication method.

Table 1-10. Station Compatibility of Authentication Methods

	MAC-Auth	Web-Auth	802.1X
Supported stations	All stations	Most stations with user interfaces	Workstations and laptops with current OSs, some APs, printers, fax machines, some PDAs, and some smart phones
Requirements for support	A standard client	Web browser support	OSs that include an 802.1X supplicant or third-party supplicants

EAP provides a framework for a variety of authentication protocols, which are called EAP methods. You must carefully consider which EAP methods are appropriate for your stations and your environment. Common methods include EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), and Protected EAP (PEAP) protocol. The EAP method on the station must match at least one method supported by the RADIUS server (which might support multiple methods).

The APs provide a variety of options for implementing 802.1X on your network. You can either handle 802.1X authentication with the MSM Controller or an external RADIUS server. If you choose to use an external RADIUS server, you can choose to have the APs forward the authentication traffic directly to the RADIUS.

When deciding which type of authentication method to use for a VSC, you need to consider the types of devices that will connect to the VSC, the degree of control that you will have over those devices, the sensitivity of network data, and the existing network infrastructure.

For example, when you provide public access, you can expect a wide variety of devices to connect to the network—laptops, smartphones, PDAs—and most of them will not be under the control of the network administrators. Your authentication method should therefore require no more than standard software such as a Web browser.

On the other hand, if your organization owns all of the wireless devices, you can require that the devices have specialized software installed.

Table 1-11. Comparison of Authentication Methods

Authentication Method	Advantages	Disadvantages	Security Level
MAC-Auth	• Control over which stations connect to the network • No software on the station • Easy to combine with other security	• Not scalable • High administrative overhead • Susceptible to MAC-address spoofing • Hardware-based rather than user-based authentication	Low • Low-to-medium effort to crack • Prevents casual, unauthorized users
Web-Auth	• Ideal for public access • Control over which users access the network • No configuration required for stations • No 802.1X supplicant required • Centralized user authentication	• No encryption by default • RADIUS server required • Web browser interface required • User interaction required • No authentication of headless devices • No seamless roaming	Medium • Medium-to-high effort to crack • Prevents more diligent attacks than MAC-Auth does
802.1X	• Control over both users and devices that access the network (because devices can have supplicants) • Automated encryption key assignment to protect against data sniffing • Centralized user authentication or distributed user authentication • Flexibility in the EAP option you select	• More network requirements such as an 802.1X-capable switch and a RADIUS server • Must have 802.1X supplicant on the station	High • High effort to crack—attackers must forge authorized user credentials to gain entry • Exact level depends upon the underlying EAP method

The following supplemental encryption methods are listed in order of weakest to strongest.

- **Dynamic WEP**—Dynamic WEP encryption provides authentication for a WLAN station using an 802.1X exchange between the station and a RADIUS server through an AP. During these exchanges, WEP keys are dynamically generated.

  The dynamic WEP approach provides centralized user authentication (at the RADIUS server) as well as mutual authentication of both station and server. It provides better protection than static WEP through the use of dynamic per-user, per-session keys, because each user has a unique key for each association. In addition, the use of per-session keys prevents an attacker from seeing all network traffic when a single key is cracked.

  Dynamic WEP requires an 802.1X-capable RADIUS server and 802.1X supplicant software on each station.

- **WPA**—WPA provides authentication and encryption for stations. WPA supports two modes of operation:

  - **Dynamic**—An 802.1X authentication exchange occurs between the station and the authentication (RADIUS) server. The authenticator (either the AP, in a distributed architecture, or the controller, in a centralized architecture) facilitates the exchange. In addition to authenticating the user, this exchange generates dynamic keys for encryption.
  - **Pre-Shared Key (PSK)**—This option does not offer true authentication. Instead a station proves that it is authorized to connect to the WLAN by encrypting its association request with the correct key. This key is *derived* from a static password that is shared in advance; however, from that password, the station and the AP generate unique (per-session) encryption keys. The authentication takes place between the station and the authenticator and does not involve a RADIUS server.

  Once the authentication (either dynamic or PSK) has been accomplished, WPA uses TKIP to encrypt packet data and ensure data privacy. TKIP changes the encryption key with every frame. WPA also includes an algorithm called “Michael” to verify data integrity in the unlikely event that an encryption key is somehow compromised.

  WPA requires a WPA-capable station, and the dynamic mode requires an 802.1X-capable RADIUS server. Generally, an enterprise would use the 802.1X mode, whereas PSK mode is more suited to home office use.

- **WPA2**—WPA2 is similar to WPA but employs even more secure encryption through CCMP with AES, an algorithm which provides both data privacy and integrity. WPA2 is fully compatible with the 802.11i standard.

Note WPA with TKIP encryption was cracked in 2008. WPA2 with CCMP/AES is now considered the most secure. If your equipment does not support CCMP/AES and you must use TKIP, set the key rotation interval to 300 seconds or fewer and disable QoS if it is not required.

Table 1-12 is a summary of the advantages and disadvantages of each encryption method.

Table 1-12. Comparison of Encryption Methods

Method	Pros	Cons
Static WEP	• Encrypts data • Controls which users send and receive data (because users must have the key)	• Keys maintained manually and rarely changed • Keys maintained separately on each AP • Key can be cracked if enough frames are collected
Dynamic WEP	• Generation and distribution of per-session keys • Secure, centralized distribution of global keys • Key rotation • User-based authentication • Widely supported	• Per-session keys (the default) can be cracked • Frequent rotation of keys adds overhead • A RADIUS server is required • Stations must support 802.1X
WPA-PSK	• No need for RADIUS server • No need for 802.1X supplicant • Per-frame keys • Secure key distribution and rotation with TKIP or CCMP • Optional CCMP/AES	• Weaker authentication • Not supported by older clients • Increased AP workload
WPA/WPA2	• Per-frame keys • Secure key distribution and rotation with TKIP or CCMP • Centralized user authentication • Optional CCMP/AES	• Not supported by older clients • Increased AP workload • RADIUS server is required • Stations must support 802.1X

Table 1-13 shows which encryption options are available for each authentication method.

Table 1-13. Encryption Options Available for Authentication Methods

Authentication Method	Encryption Options	Recommendation
Password (or shared key)	Static WEP	Not recommended
	WPA-PSK	For small organizations
802.1X	Dynamic WEP	Acceptable in some circumstances

Authentication Method	Encryption Options	Recommendation
	Dynamic WPA/WPA2	Preferred
Web-Auth	None on its own	Acceptable for non-secure access; can be combined with WPA-PSK
MAC-Auth	None on its own	Adds some security to methods such as WPA-PSK

For added flexibility, you can enable more than one authentication method at the same time. The following table shows the results for all authentication scenarios.

Design the VSCs (Wireless LAN Profiles)

A wireless LAN profile, or a “service set” (as it is called in the IEEE 802.11 standards literature), specifies all the settings for a wireless network, or WLAN, including the SSID, various security settings, and other advanced settings for QoS and wireless traffic management.

As you learned previously, on the MSM products, each wireless LAN profile is called a VSC. A station can join only one VSC at a time.

To plan your VSCs, divide your users into groups according to the level of security that they will need to access the wireless network. For example, you can create a public-access VSC for guests, who will access only the Internet. Then they can easily access the VSC, but must log in through the Web to access sensitive network resources.

When connecting your VSCs to the wired network, you must take into account two important factors:

- Level of trust
- Relationship to VLANs

Level of Trust. Depending on who will associate to a VSC, you can designate a VSC as "trusted" or "untrusted."

A trusted VSC provides access for users who are well-known to your company. For example, your company knows employees or temporary employees, and because you hired them, you are reasonably confident that they will not attack your network. You may also have some control over these users' stations so that you can ensure that they are not vulnerable to attack. For example, your company may regularly apply patches, or you may have a solution that enforces endpoint integrity before users access the network.

Because you want to allow these users to access confidential information on your company's network, you want them to prove their identity before they access your wireless network. For trusted VSCs, therefore, you will typically impose the tightest security measures possible—802.1X with WPA2.

Untrusted VSCs provide access for users who are less well known. For example, you may provide guest accounts for visitors such as customers or suppliers. Because you have less information about guest users and no control over their equipment, you may want to employ a firewall between your untrusted VSCs and the rest of the network. The controller contains its own firewall. For a standalone AP, you would apply the existing firewall for wired devices. (See "Plan Guest Access" on page 1-88.)

Relationship to VLANs. Both the APs and the controllers allow you to use VLANs to control how wireless traffic is forwarded to the wired network.

If you are using the autonomous architecture, the APs support both static VLANs and dynamic VLANs.

- **Static VLANs**—You can associate each VSC with one static VLAN, which is called the *egress VLAN*. By default, when users associate with a VSC, they are automatically assigned to this VLAN.

  For example, if you already have two VLANs on your wired network—VLAN_EMP for regular employees and VLAN_CON for contractors—you could create VSC_A for employees and VSC_B for contractors. You could then configure the security for VSC_A so that only employees would be allowed to connect to VSC_A. (For example, if the VSCs were using preshared keys to authenticate users, only employees would know the key for VSC.) Then you would create a static association between each VSC and its corresponding VLAN. (See Figure 1-10.) (Instead of creating two VSCs, you could create one and use dynamic VLAN assignments.)

With static VLANs, anyone who joins a VSC automatically gets access to the corresponding VLAN without any further security intervention. For this reason, you have to take care that the VSC security settings are sufficient to prevent anyone from getting into restricted VLANs.

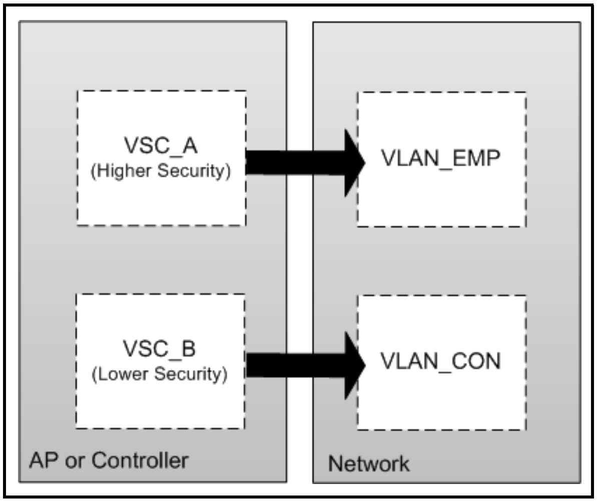


Figure 1-10. Static VLANs

- **Dynamic, or User-Based, VLANs**—The MSM APs and MSM Controllers support dynamic VLANs in both a standalone and an optimized WLAN architecture.

  In a standalone architecture (when AP are operating in autonomous mode), dynamic, or user-based, VLANs override the static, or egress, VLAN associated with the VSC. The AP queries a RADIUS server, which looks up the VLAN assignment for the user's group and passes that assignment back to the autonomous AP. The user's dynamic VLAN assignment overrides the VSC egress VLAN. In this way, many users can connect to the same VSC but receive different levels of access.

  For example, imagine that you have the same two VSCs as in the previous example, but you need to separate your employees into VLANs for executives (EXE) and accounting (ACC), and you want to separate non-employees into contractors (CON) and guests with Internet-only access (INT). (See Figure 1-11.)

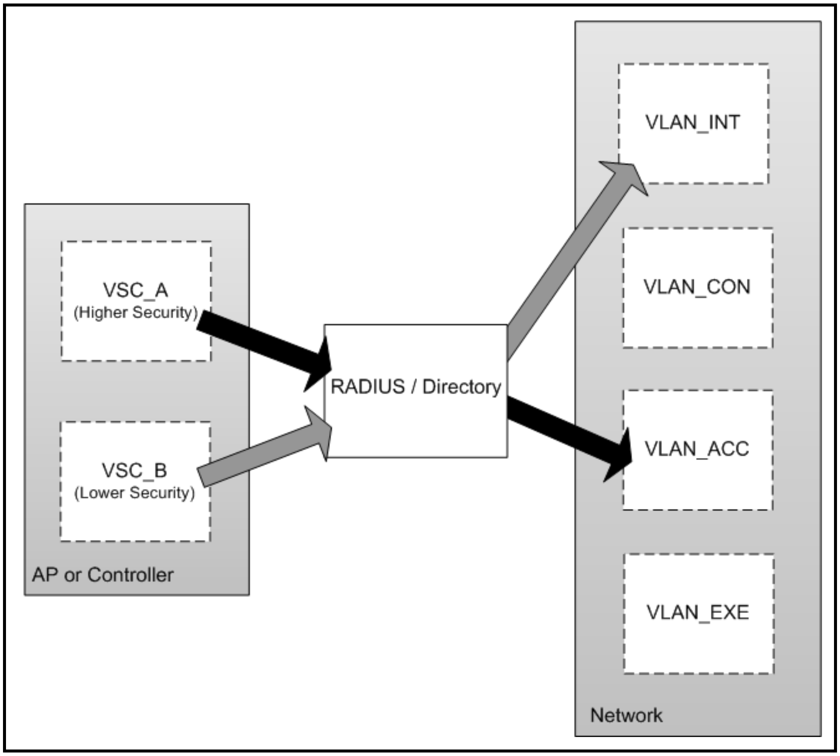


Figure 1-11. Dynamic VLANs

When user "Anna" in accounting joins VSC_A, the RADIUS server gives Anna's VLAN assignment to the AP—VLAN_ACC. The network is set up to give users in VLAN_ACC access to resources that accountants need, so Anna has a consistent experience over the wired and wireless connections. (It would also be possible to give Anna access to different VLANs according to the time and location at which she accesses the VSC, depending on the policies that were set up through an external RADIUS server, a directory, or a network management tool such as IDM.)

On the other hand, when user "Joe," an executive, connects to VSC_A, he is assigned to VLAN_EXE and enjoys the services and resources designated for executives.

Similarly, "David," a guest, joins VSC_B and is assigned to the Internet-only VLAN_INT. However, network administrators may not want to configure a VLAN assignment for guests on the RADIUS server. In this case, the RADIUS server sends no assignment, and the AP places David in the static VLAN assigned to VSC. The network administrators must make *very* sure that the static VLAN is the Internet-only VLAN_INT.

If you use the optimized WLAN architecture, you have several options for configuring VLANs to control traffic.

If you choose to use distributed forwarding (the APs forward user traffic directly on to the network), you have the same VLAN options that you have with the autonomous architecture: you can configure an egress VLAN for each VSC, and you can configure dynamic VLANs for users. You simply set the egress VLAN when you bind the VSC to an AP group (as of the 5.4 software release, the egress VLAN is also referred to as the egress network). Then the AP forwards traffic received on that VSC as tagged for that VLAN. If you want to use dynamic VLANs, you create the VLAN assignment on the RADIUS server that the APs use to authenticate users. The RADIUS VLAN assignment takes precedence over the egress network.

If you choose to use centralized access control, the traffic is controlled at the MSM Controller, and the egress network in the VSC binding has a slightly different function. This setting determines the VLAN on which APs forward user traffic toward the MSM Controller. Any resources in this VLAN will be accessible to unauthenticated users (although you can enable a wireless security filter that limits users' traffic to their router, the MSM Controller, essentially forcing the users to pass all traffic through the controller). Often, the best practice is to leave the egress VLAN without a setting in the VSC binding and to enable the client data tunnel on the VSC, which forces the AP to tunnel all user traffic directly to the MSM Controller. Then you do not need to worry about extending a VLAN from the controller to the APs nor about protecting resources in this VLAN.

When the MSM Controller receives the users' traffic, it matches it to the centralized-access-controlled VSC. When you are using MSM APs, the APs send the SSID, allowing the controller to easily match the traffic to the VSC. If you are using third-party APs, you can use the VSC ingress VLAN to identify the traffic that should be assigned to a particular VSC. You simply create a VLAN on the controller's LAN port (no IP address) and assign that VLAN as the VSC ingress VLAN. Then you configure the third-party APs with this VLAN as the static VLAN for the WLAN in question. You can also use the VSC ingress VLAN to match wired traffic to the VSC. For example, you could make all switch ports untagged members of this VLAN, and allow guests to connect to these ports.

After the MSM Controller matches the traffic to the VSC, it is ready to control it. You have several options for using VLANs to control traffic at the MSM Controller:

- **Static VLANs**—You can set an egress VLAN at the VSC-level. You can assign VSC egress VLANs based on the type of user traffic the controller receives:
  - **Unauthenticated**

    You can specify a VSC egress VLAN for traffic from users who have not attempted to be authenticated. For example, if a guest user associates with a VSC and does not try to enter any login credentials, the controller places the guest's traffic in this VLAN.
  - **Authenticated**

    You can specify a VSC egress VLAN for traffic from users who have been authenticated and have been granted access to the public access interface.
  - **Intercepted**

    You can specify a different VSC egress VLAN if you want to intercept and redirect traffic from specific users. To enable traffic interception for these users, you must specify the appropriate setting in each user's RADIUS account.
- **Dynamic VLANs**—You can also set user-based egress VLANs, which take precedence over the VSC egress VLAN. If the users are being authenticated to an external RADIUS server, this server sends the VLAN assignment using the standard RADIUS attributes. If the users are being authenticated by the MSM Controller, you can set the user-based egress VLAN in the user's account profile.

Note: Using the Mobility Traffic Manager can affect where users' traffic is distributed once it has been assigned to a VLAN. See "Use Mobility Traffic Manager to Control Where Traffic Is Distributed into the Wired Network" on page 1-79 for more information about this feature.

Wireless-Only VLAN. When using the optimized WLAN architecture, you may decide to create a wireless-only VLAN. That is, the wireless VLAN exists only on the MSM Controller; it is not extended onto the wired network. In this case, you will need to enable NAT on the MSM Controller so that stations can access the Internet.

If you are using subnets instead of VLANs to separate collision domains, you might want to create a separate scope of IP addresses on your DHCP server for guests and use ACLs to deny guests access to confidential resources.

Use the Firewall, MAC Lockout, or Traffic Filters

Depending on your company's environment, you may want to apply these security measures to further control access to network resources:

- Firewall
- MAC lockout
- Traffic filters

The HP mobility products help you to implement these measures. Table 1-14 displays which products support each measure.

Table 1-14. Security Capabilities of ProCurve MSM Products

Security Capability	Products that Support the Capability	Enhanced Capabilities with RF Manager + MSM AP Sensors	Guide Section
Firewall	MSM Controller	—	"Invoke the MSM Controller Internal Firewall" on page 1-75
MAC lockout	• Autonomous MSM APs • MSM Controller + controlled MSM APs	Configure MAC lockout on multiple non-controlled APs (such as third-party APs)	"Use MAC Lockout" on page 1-76
Traffic filters	• Autonomous MSM APs • MSM Controller + controlled MSM APs	—	"Configure Filters for a VSC" on page 1-76

Invoke the MSM Controller Internal Firewall. The MSM Controller provides an internal stateful-inspection firewall. This firewall is enabled by default; it affects incoming and outgoing packets on the controller Internet port.

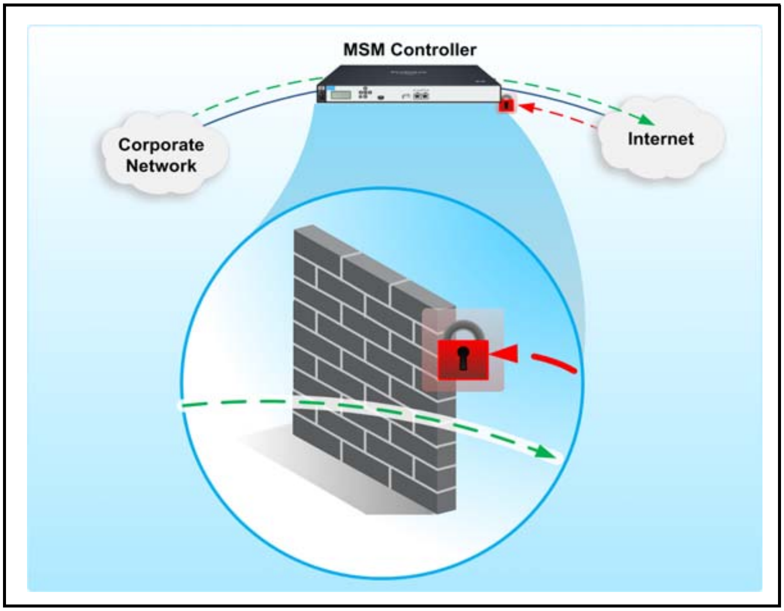


Figure 1-12. Integrated Firewall

The controller firewall has two factory-configured settings:

- **Low**—All outgoing and incoming traffic between your network and the Internet is allowed except NetBIOS traffic.

  Use the Low security setting only when your network has other firewalls or security solutions—or when you do not care about protecting the devices behind the MSM Controller LAN port.

- **High**—All outgoing traffic (traffic sent from your network and the Internet) is allowed except NetBIOS traffic. All incoming traffic is denied.

  This security setting allows your users to initiate sessions, but blocks any sessions initiated from the Internet, protecting your network from attack.

Whenever you want more granular control over your users, you should select the firewall custom setting, which allows you to configure specific firewall rules. For example, you might want to prohibit your users from playing online games, so you configure rules that deny traffic destined to the ports associated with those games.

The firewall rules can be configured according to:

- Source address and mask
- Destination address and mask
- Direction of traffic
- Services (ports)

Use MAC Lockout. Using the MSM Controller, you can configure a list of devices that are not allowed to associate with each VSC, based on the MAC address of the device wireless devices. This list includes clients connected to:

- AP wireless ports
- AP wired ports (including switch ports)
- AP local mesh ports
- Controller's LAN port

MAC lockout does not apply to the controller's Internet port.

MAC lockout is supported in both controlled and autonomous modes. In controlled mode lockout lists are propagated to all APs managed by a controller. (The MSM devices also support MAC filters that are applied to VSCs. See "Wireless MAC Filter" on page 1-78.)

If you are using RF Manager, you can create a list of banned MAC addresses, and sensors will then take active measures to block or disrupt communications from devices with those MAC addresses.

Configure Filters for a VSC. As an additional layer of security available, you can configure several types of filters which restrict wireless traffic or the wireless users allowed on the network. The filters apply to individual VSCs. Both the MSM Controller and autonomous MSM APs support these filters.

- **Wireless Security Filter**

  An AP is responsible for bridging traffic between a wireless and wired network. Wireless security filters force APs to bridge all traffic to a specific upstream device (such as an MSM Controller or a routing switch.) Use a wireless security filter to restrict wireless traffic to the proper device for forwarding that traffic.

  For example, in many environments, particularly public access ones, wireless users are placed on their own subnet. They do not need to access other devices in this subnet but only the Internet and perhaps a limited set of resources in the private network. Thus, all of their traffic should be bridged to their default router at Layer 2. (At Layer 3, the traffic might be destined to a variety of valid IP addresses.)

On the other hand, a hacker often sends traffic to other devices within its subnet in an attempt to disrupt communications or to hack into your network. When you impose a wireless security filter, the AP blocks these communications.

Note Typically, you should not impose wireless security filters when users need to access resources within their own subnet. For example, accounting employees connect to the VSC and are placed in the same subnet used in the wired network by financial databases.

The type of wireless security filter that you can configure depends on whether or not you have implemented centralized access control for the VSC.

- Centralized access control

  When you use the MSM Controller for centralized access control on the VSC, the wireless security filter allows the AP to forward only user traffic that is addressed (at Layer 2) to the controller. It must block all other traffic.

  In this case, you must make sure that the controller is the wireless station default gateway. Otherwise, all user traffic will be blocked by the AP.

- Distributed forwarding

  When you do not use the MSM Controller for centralized access control on the VSC, you have several options for security filters. You can restrict traffic to:

  – The AP default gateway

    If you select this option, make sure that the wireless stations have the same default router as the AP. In other words, the stations and the AP must be on the same subnet (VLAN).

  – A specified MAC address

    Select this option when wireless stations that connect to this VSC are placed on a different subnet from their AP default gateway. Input the MAC address of the station default gateway on their subnet.

  – A custom list

    You can create a custom list of allowed MAC addresses. For example, you might select this option when wireless users’ who connect to this VSC are placed in several different VLANs. They have different default gateways, and you must specify the MAC address for each gateway.

- **Wireless MAC Filter**

  Wireless MAC filters control which wireless devices are allowed to connect to the VSC. On each VSC, you can create one of two types of list:

  - An allow list—Use this type (sometimes called a white list) when you want to create an exclusive pool of devices allowed to connect. For example, you could specify the MAC address for each of your company's wireless devices.
  - A block list—This type (sometimes called a black list) acts much like a MAC lockout feature. All devices are allowed to connect except the ones specified on the list, which are blocked by APs.

Note

On each VSC, you can create either an allow list or a block list. You cannot specify both allowed MAC addresses and blocked MAC addresses on a single VSC.

If the VSC enforces MAC-Auth, the wireless MAC filter takes precedence. That is, the AP checks the VSC MAC list before it checks the local or remote MAC-Auth list, ensuring that a station on a block list is not inadvertently granted access and that a station on an allow list is not inadvertently denied access.

- **Wireless IP filter**

  With wireless IP filters, you can restrict wireless-to-wired traffic to specific destination IP addresses or subnets. For example, in a public access VSC, you could specify the IP address of your public Web server. APs would drop all other traffic before bridging it into the wired network.

Note

A wireless IP filter controls the IP addresses to which wireless stations can send traffic. It offers more granular control of the endpoints (or servers) that wireless users can access.

A wireless security filter controls the MAC addresses to which wireless stations can send traffic. It controls whether wireless users can communicate with any device in its subnet (including other wireless devices) or only its default gateway.

Check the Existing VLANs on the Wired Network

After you outline your security plan, you should check your wired network to determine whether or not the VLANs into which wireless traffic is bridged are extended to network locations where you plan to install the APs. If these VLANs have been created on the switches that connect to the APs, you simply need to make each AP's switch port a member of the appropriate VLANs. For example, the VLAN on which APs will exchange management traffic with the controller is typically an untagged membership. If you are using dynamic VLANs, you will make each AP's switch port a tagged member of these VLANs.

If the VLANs into which wireless traffic is bridged do not extend to the network locations where APs will be installed, you have two choices: extend the VLANs or use the Mobility Traffic Manager feature to control where traffic is distributed into the wired network. (The Mobility Traffic Manager feature was introduced in version 5.4 of the MSM Controller software.)

Use Mobility Traffic Manager to Control Where Traffic Is Distributed into the Wired Network

To understand how you can use Mobility Traffic Manager to control where traffic is distributed, consider the example network in Figure 1-13. This network includes several subnets, each of which is associated with a department. The company is adding a wireless network and wants every AP to support wireless users in every department. The network administrators have configured a VSC that will enforce 802.1X authentication to a network RADIUS server, which assigns users to dynamic VLANs according to their identity.

Mobility Traffic Manager will make the deployment of this solution very simple. The APs can be deployed wherever the company wants without any need to extend different VLANs to those locations. If a user is assigned to a VLAN that is not supported on his or her AP, the AP simply tunnels the user's traffic to the controller at the network core. The controller can then apply the dynamic VLAN assignment and distribute the traffic into the wired network.

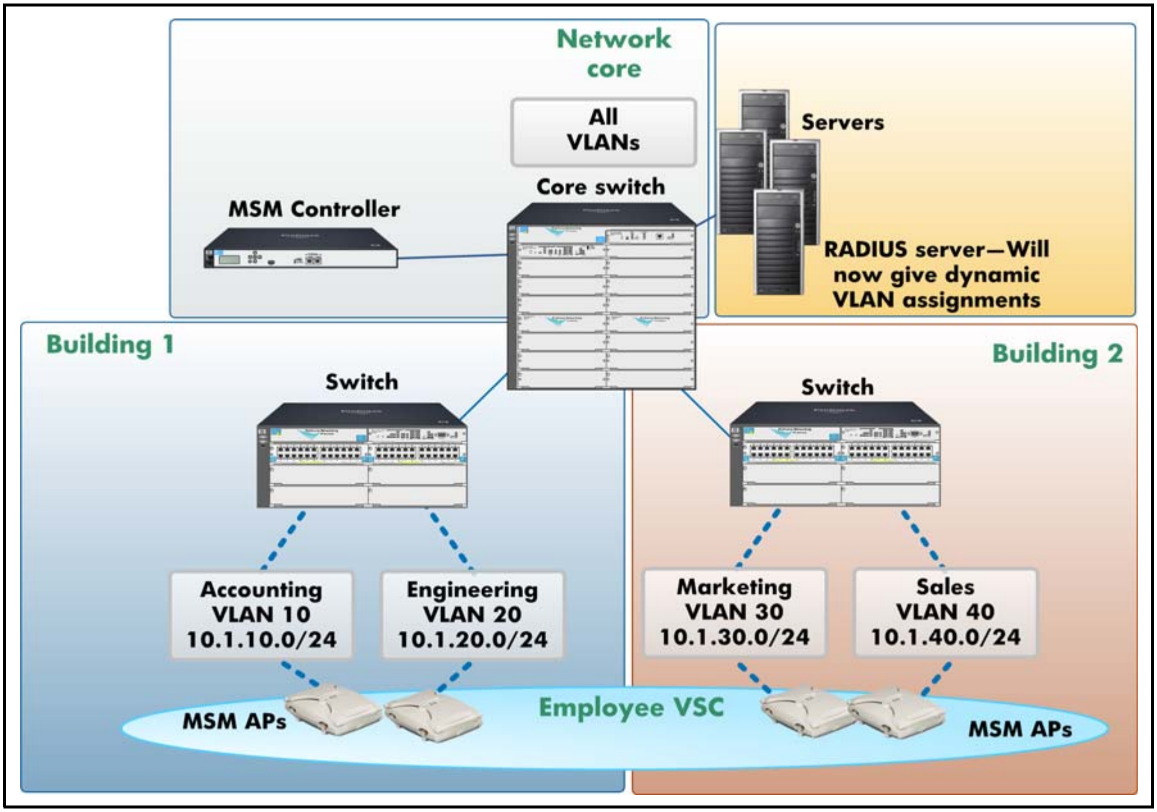

Network core
All VLANs
Core switch
MSM Controller
Servers
RADIUS server—Will now give dynamic VLAN assignments
Building 1
Building 2
Switch
Switch
Accounting VLAN 10 10.1.10.0/24
Engineering VLAN 20 10.1.20.0/24
Marketing VLAN 30 10.1.30.0/24
Sales VLAN 40 10.1.40.0/24
MSM APs
Employee VSC
MSM APs

Figure 1-13. Mobility Traffic Manager

When a user connects to this network, the AP checks its list of local networks, which were configured on the MSM Controller and downloaded to the AP as part of its configuration. If the VLAN is one of the AP's local networks, it forwards the traffic directly into the wired network. If the VLAN is not one of the AP's local networks, the AP tunnels the traffic to its controller and also sends a visitor request, which includes the VLAN assignment sent by the RADIUS server. The controller uses this information to determine where to terminate the tunnel for the user's traffic.

The controller checks the VLAN assignment in the visitor request against its Layer 3 networks table. Among other information, this table includes all VLANs in network profiles that are configured on the controller and all VLANs that have been discovered from other controllers in the Layer 3 Mobility Domain. (You use network profiles to define networks and assign them to controllers.)

In the network shown in Figure 1-13, there is only one controller. If the user's VLAN assignment matches a network profile assigned to the controller, it is the handler for that traffic and terminates it. The controller's Internet port must be a tagged member of that VLAN so that it can distribute the traffic into the wired network.

Figure 1-14 shows a multi-controller environment that is using Mobility Traffic Manager to distribute traffic into the wired network. When a user authenticates to this network, the AP checks the user's VLAN against its list of local networks. Because the user's VLAN is not a local network, the AP tunnels the traffic to its own MSM Controller.

The MSM Controller checks its Layer 3 networks table and determines that the traffic should be terminated at the controller in Network B. Therefore, it sends the traffic over a data tunnel established with this controller.

The controller that is assigned to be the handler is responsible for terminating the traffic. It forwards the traffic on the port on which the user's assigned VLAN is configured, tagging the traffic appropriately.

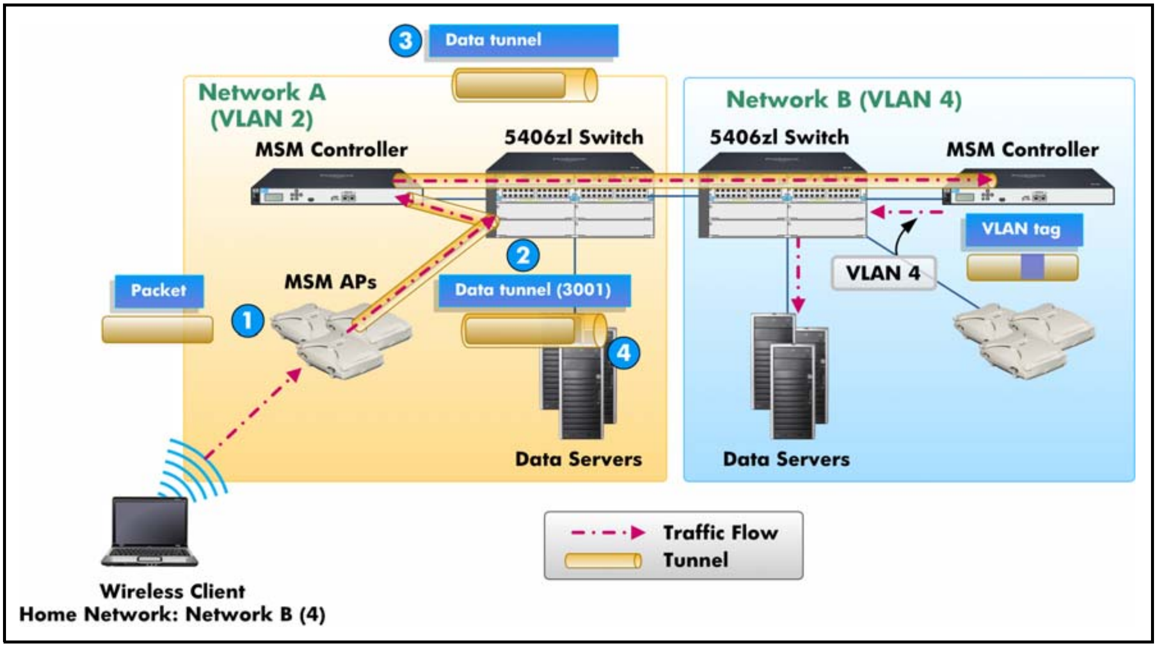


Figure 1-14. Using Mobility Traffic Manager in a Multi-Controller Environment

The two Mobility Traffic Manager examples have focused on using dynamic VLANs to determine the user's local network. However, it is also possible to use the egress VLAN in the VSC binding to determine the local VLAN.

To plan your Mobility Traffic Manager configuration, you should decide:

- If the user's local network will be determined by a dynamic VLAN or the egress VLAN in the VSC binding
- Where the traffic will be terminated

(Traffic must always be terminated at an MSM Controller.)

(For more information about configuring Mobility Traffic Manager, see the *HP ProCurve MSM 7xx Controller Management and Configuration Guide* for the 5.4 software release.)

Plan Roaming

In your initial planning, you asked users where they wanted to roam. Based on your deployment planning, determine whether users need to roam between:

- APs that are on the same subnet (Layer 2 roaming)
- APs that are on different subnets (Layer 3 roaming)

Layer 2 (RF) Roaming. Layer 2 or RF roaming is sometimes called "simple" roaming because most 802.11-compliant APs natively support it, including MSM devices. The APs can hand off the roaming station's session at the Data Link Layer; no additional solution is required to enable a station to move from one AP to another.

If you want users to be able to roam between two APs, you must deploy those APs in such a way that they support Layer 2 roaming between each other. The guidelines for establishing a single-subnet RF coverage area that supports roaming between APs are as follows:

- The APs support the Physical Layer.

  APs can communicate only with stations that support the same wireless standards (802.11b, 802.11g, 802.11a, 802.11n). However, a wireless station can roam between radios that support different standards as long as the station supports different standards.
- All of the APs must support the same SSID.
- All APs and stations must have the same security settings.

- The AP cells should overlap to ensure that there are no gaps in coverage and to ensure that the station will always have a connection available. (This is not an absolute requirement, but it is good practice.)
- The APs must place users in the same VLANs or subnets.

Layer 3 (Network) Roaming. Like Layer 2 roaming, Layer 3 roaming requires that the station roam between two APs that support the same SSID (VSC). However, Layer 3 roaming becomes necessary if a station tries to move between two APs that support the same VSC but bridge user traffic into different VLANs or subnets.

When a station successfully authenticates and associates with a VSC on the first AP, it typically receives a valid IP address through a DHCP server. (Alternatively, the station could be configured to use a static IP address that is on the correct subnet.) The AP also puts the station into the VLAN assigned to that VSC or into the dynamic VLAN assigned to the user.

If this station then tries to move to another AP and that AP bridges its traffic to a different subnet, the station cannot use the IP address that was valid for its association with the first AP. Therefore, the handoff between the two APs must include the Network Layer as well as the Data Link Layer—that is, the station must roam at Layer 3. Because most APs do not have the capability to handle Layer 3 roaming, reassociation fails, and the user loses network connectivity. The user will then have to reinitiate the wireless connection, including any authentication.

Figure 1-15 illustrates a network that requires Layer 3 mobility. The AP on the left places wireless stations in VSC A in VLAN 1 while the AP on the right places stations in VSC A in VLAN 20.

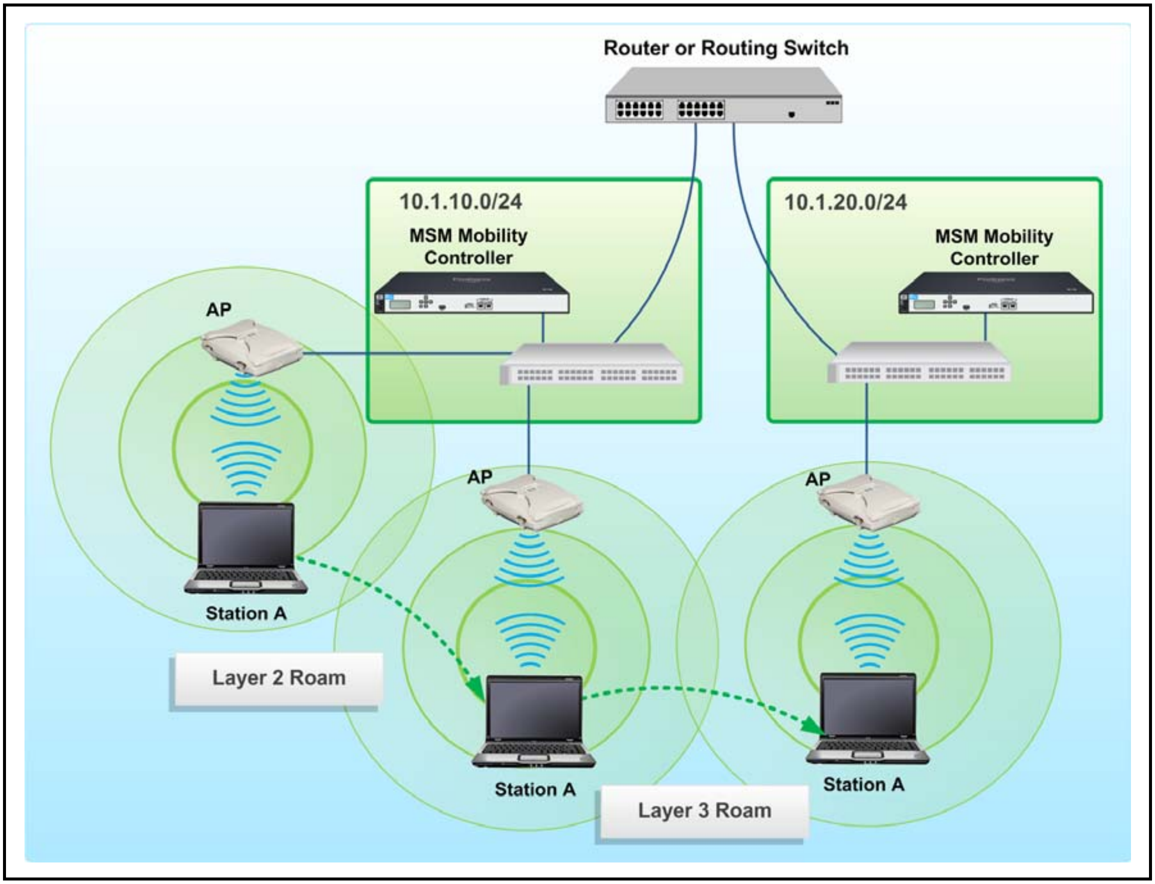


Figure 1-15. Layer 2 and Layer 3 Roaming

When a Layer 3 roaming solution is implemented, the Layer 2 reassociation process proceeds just as it does for Layer 2 roaming. The Layer 3 roaming solution then provides a way for the station to function on the new subnet without having to receive a new IP address.

The MSM Controllers support Layer 3 mobility with a Mobility or Premium license. As mentioned earlier, the MSM765zl includes a Premium license, so it supports Layer 3 roaming as soon as it is activated. With the purchase of an optional Mobility license for the MSM710 and Premium license for the MSM760, you can configure an MSM Controller to support Layer 3 roaming.

Layer 3 mobility is supported across several MSM Mobility Controllers. When a station roams to an AP controlled by a different controller, the controller knows how to handle the traffic so that the station can keep its current IP address.

Now that you understand the difference between Layer 2 and Layer 3 roaming, you can delve deeper into the factors that affect how smoothly a station roams.

Factors on the Station That Affect Roaming. The factors that affect the station response to roaming are the following:

- **Wireless client**—The 802.11 standard assigns to wireless stations the responsibility of deciding when they should roam to another AP, but the standard does not mandate the factors they use to determine whether to roam. These criteria end up as proprietary algorithms on each vendor's wireless client.

  Typically, roaming decisions are based on factors such as the AP signal strength and missed beacons. For example, a station will usually roam to another AP under the following circumstances:

  - As the user moves the station, the station either loses the AP signal (moves out of range) or detects another AP that supports the same SSID (VSC) but has a stronger signal.
  - Interference decreases an AP signal, and the station detects an AP that supports the same SSID and has a stronger signal.
  - An AP becomes unavailable, and the station detects another AP that supports the same SSID.
- **Wireless station's OS**—Some operating systems are more tolerant of handoffs than others. Some provide buffering to maintain the station's session during handoff. Others drop the IP stack during handoff.
- **Application**—Some applications tolerate small interruptions better than others. If users are accessing a TCP connection-oriented application, they should not notice much of a performance change during a roam. However, if users want to use a UDP connectionless application such as VoWLAN, performance during roaming can be an issue. IEEE has developed the 802.11r standard to enable wireless networks to support fast roaming for VoWLAN applications.

- **Authentication method**—Supplemental authentication such as 802.1X will slow down the roaming process, because the station must re-authenticate to the new AP. See “Fast Roaming” on page 1-87 for steps that you can take to mitigate the latency.

If decisions about these factors are within your control, you will have to carefully research the capabilities of each station’s NIC, OS, and application to determine its tolerance levels. Eventually, you will have to test the devices yourself on site.

If you are providing wireless services to customers and devices that are not within your control, you will need to plan for a wide range of capabilities. In some cases, you will not be able to solve the problem of dropped sessions, so you should prepare users for that eventuality.

Roaming Types. When a station roams from one AP to another, there is always a brief interruption in the signal as the station session is handed off from one AP to the next. The handoff between APs is handled by your wireless hardware, but the station’s reaction to the interruption can vary, depending on several factors. In some cases, the IP stack will be dropped during handoff, and the station has to re-associate and/or re-authenticate to the new AP. In other cases, the session will not be interrupted by the handoff.

Roaming can be placed into three categories relative to the user experience:

- **Seamless roaming**—The defining feature of a seamless roam is not speed but preservation of the user’s authentication, IP address, and active sessions. The user does not need to log in again, and a user browsing the Internet probably does not notice a seamless roam, whereas a user accessing a real-time application may detect a slight lag.
- **Fast roaming**—A fast roam takes less than 50 µs. An MSM Mobility Controller (a controller with a Mobility license) implements Opportunistic Key Caching to support fast roaming. When a roam is described as “fast,” it is also assumed to be seamless.

Note

Fast roaming as a standard refers to roaming for 802.1X with WPA. However, other roams can take under 50 µs.

- **Not seamless roaming**—If a roam is not seamless, users must log in again after moving within the range of the new AP so that their stations can re-authenticate or change their IP addresses.

Fast Roaming. You may need to configure some settings to speed up the roaming process if one or more of your VSCs meet both of these conditions:

- Enforces 802.1X (with WPA encryption)
- Supports performance-sensitive wireless devices such as VoWLAN phones, security cameras, and other devices that run interactive or real-time applications

In this case, you must install a Mobility license on the MSM710 or a Premium license on the MSM760. The MSM765zl includes a Premium license. You can then implement Opportunistic Key Caching on a VSC, as described in the next section.

Note

Stations also must support Opportunistic Key Caching for the fast roaming to work. Be sure to consider this requirement when you select wireless client software.

Opportunistic Key Caching. Although WPA with 802.1X strengthens security for wireless communications, it has one drawback: it increases the time required to roam from one AP to another because the station must re-authenticate with the new AP and agree on encryption keys. In fact, 802.1X re-authentication is the most time-intensive part of the roaming process.

To reduce this latency, the MSM Mobility Controller applies Opportunistic Key Caching. APs send encryption keys to the controller when stations first authenticate. The controller sends the keys to all APs in the same mobility domain. When a station roams, the new AP already knows the keys so the station does not have to reauthenticate.

In summary, Opportunistic Key Caching provides the following benefits to clients that support it:

- Eliminates delays associated with reauthentication
- Provides hand-offs in less than 50 µs, as required for time-sensitive services such as voice
- Preserves a user’s RADIUS-assigned parameters such as security, QoS, and VLAN, enabling a smooth transition of all services to which the user has access

Roaming for Public Access Networks (Guests). To implement a public access network (which uses Web-Auth), you must use centralized access control. Because the MSM Access Control handles all authentication and user traffic, stations roam seamlessly between all controlled APs.

However, in a system with multiple controllers providing public access networks, stations cannot roam between APs that are controlled by different controllers.

If you are using 802.1X, you may need to mitigate the delay that 802.1X authentication incurs during the roaming process—particularly, when wireless users run voice, video, or other performance-sensitive applications. In other words, you need fast roaming.

If your wireless network requires Layer 3 roaming or fast roaming, the MSM Controller must have a Mobility or Premium license. With the MSM710 and the MSM760, you must purchase this license separately. The Premium license is included when you purchase the MSM765zl.

Note

When a VSC implements an optimized WLAN architecture with centralized access control, the MSM Controller automatically handles roaming between its APs. You *cannot* configure Opportunistic Key Caching or Layer 3 mobility on this VSC.

Plan Guest Access

MSM Controllers allow you to customize guest access to meet the needs of both your company and its guest users. To start, you must decide what type of guest users you want to support. You have the option of creating the following types of guest users:

- **Free access guests**

  Free access guests receive complimentary access for a limited time. Although they are not required to submit login credentials for authentication, the MSM Controller creates a temporary account for controlling each free access user.

- **Self subscribers**

  Self subscribers must pay for their wireless access. When they set up their payment, self subscribers also create an account that they can use to log in again later.

- **Presubscribers and known guests**

  Presubscribers and known guests authenticate and log in using an account that has been created for them. You can require these guests to pay or not pay for their wireless account.

Free Access Guests

Free access guests require little configuration setup. You simply install an SSL certificate, enable the free access option, and set a time limit for the access. The MSM Controller tracks the sessions of these guests and prevents them from logging in again after they have used up their time.

Self Subscribers

If you want your wireless network to support self subscribers, you must:

- Set up payment services through a third-party such as Authorize.Net
- Create one or more subscription plans, which define the type of network access provided for a fee
- Configure the MSM Controller login pages to support subscription plan purchase and allow users to create their own accounts

The MSM Controller stores billing records for paying guests. Optionally, you can configure the controller to forward billing records to an external server.

Presubscribers and Known Guests

If you want to charge guests for access and control which guests connect to the network, you can set up presubscriber accounts in one of the following ways:

- The presubscribers pay for the subscription offline at the same time that the staff member sets up their account.
- The staff member sets up the presubscriber's account but leaves it deactivated. The presubscriber can then purchase the actual subscription of his or her choice later.

Alternatively, you can simply create accounts for known guests and not charge them for using the wireless network. For example, you might want to allow guest access only to your company's partners who are visiting the main office. Before one of these guests can log in, you or a company staff member must create an account for the guest.

Controlling Guests' Access to the Network

Because guests are less trusted than other wireless users, you will want to carefully control which network resources they can access. The MSM Controller provides a great deal of flexibility to do this. For example, you can authenticate users to an external RADIUS server and configure RADIUS attributes to control users' access through a dynamic VLAN or access control list (ACL). You can also configure attributes locally (on the controller) and apply these attributes to all guest users, to a subset of guest users, or to just one guest user. These attributes are configured and applied in the following ways:

- **Subscription plans**—You can create subscription plans for self subscribers, presubscribers, and known guests, but these plans do not affect free access guests. Through subscription plans, you can control attributes such as:
  - Online time
  - Traffic quotas
  - Bandwidth level
  - Validity period
- **Default account profile**—You can use the default AC profile to configure a variety of attributes that apply to all guest users. For example, you can configure:
  - Access rights using egress VLANs or access control lists (ACLs)
  - Customized settings for QoS such as rate limits (inbound and outbound) or the traffic's priority level (called Bandwidth level in the profile)

  Subscription plans and other account profiles take precedence over the default account profile. For example, if you apply an access list to the default account profile, that access list applies to free access users, self subscribers, known guests, and presubscribers. However, if you then apply a different access list to a known guest's or presubscriber's account profile, the default account profile's ACL no longer applies.
- **Account profiles**—You can use account profiles to apply attributes to a subset of users (such as all presubscribers).
- **Site attributes**—You can configure site attributes that apply to the public access interface globally and affect all users (including unauthenticated ones).
- **Unauthenticated user access list**—You can configure a user access list to allow guests to reach limited resources in the private network before they authenticate. Site attributes apply to all public access users (authenticated or unauthenticated), so you can use unauthenticated user access lists to create a more limited set of resources for unauthenticated guests than for authenticated guests. For example, you could allow access to *.microsoft in the site access list. Then you could deny access to particular microsoft sites in the unauthenticated user list.

Because the MSM Controller provides so many options for controlling guest access, you should consult the *HP ProCurve MSM 7xx Controller Management and Configuration Guide* for the 5.4 software release before you begin configuring attributes.

Determine Which Port or Ports You Will Use to Connect the MSM Controller to the Network

The two ports on the MSM Controller have been designed to perform specific functions, as listed in Table 1-15. For some environments, however, you may want to connect only the Internet port to the wired network. For example, if you do not want the MSM760 Controller to provide dynamic IP addresses to APs and it is not supporting a lot of guest traffic, you may want to connect only its Internet port to the wired network. Keep in mind, however, that for this configuration you will need to perform some additional configuration steps. For example, you will need to enable AP discovery on the Internet port.

Note

If you are using the MSM765zl Controller, the LAN port (also called port 2) should not be disabled because one of the module's processes uses this port to communicate with the switch.

You can use Table 1-15 to help you decide which port or ports to connect to your network as well as which VLANs should be configured on each.

Table 1-15. Roles for MSM Controller Ports

Role	LAN port	Internet port
Discovering and managing APs	Enabled by default	Can be enabled in **Controller** > **Management** > **Device discovery** window
Providing DHCP services for APs and other devices *You can configure separate DHCP ranges in each VSC (the subnet should be reserved for the VSC and does not need to exist as a VLAN on the controller).	Supported for both APs and other devices (enabled in the **Controller** > **Network** > **Address allocation** window): • On the LAN port (untagged), using the global scope • On VSCs with centralized access control and DHCP enabled	• Not supported for APs • DHCP services *are* supported for wireless devices connected to APs on the controller's Internet port *when* the AP sends their traffic to the controller on a client data tunnel – Client data tunnel created in the VSC – DHCP enabled on client data tunnels in **Service Controller > Network > Address allocation > DHCP Server configuration** window (default)

Role	LAN port	Internet port
Receiving traffic from wireless public access users and mapping it to a VSC	Supported by default—SSID maps the traffic to the VSC when either: • Location-aware functionality is enabled (automatic for VSCs that use the server for centralized access control) • A client data tunnel is enabled on the VSC When you set an egress VLAN in the VSC binding, the VLAN must map traffic to the VSC: – Configured as a tagged VLAN on the MSM Controller LAN port – Set as an ingress VLAN in the VSC	Supported (by SSID) when APs send the users' traffic on a client data tunnel
Egressing traffic from public access users	Supported when the VSC (or user) egress VLAN is configured as a tagged VLAN on the LAN port	Supported (and recommended) in two ways: • Over the VSC (or user) egress VLAN (also configured as a tagged VLAN on the Internet port) • Using the routing table—Internet port untagged or tagged VLAN is the forwarding interface in a route to the traffic's destination
Providing access to the MSM Controller Web browser interface (management tool)	Supported (can be disabled in the **Controller** > **Management** > **Management tool** window)	Supported (can be disabled in the **Controller** > **Management** > **Management tool** window)

Verify Your Wired Topology

Often, you will be adding an MSM Solution to an existing wired network. You must check the wired infrastructure and verify that your plan for providing wireless access will work well within it.

Although this guide focuses on implementing an MSM Solution in an HP environment, you can implement this industry-leading, open-standard-compliant solution in any environment, no matter which vendor provides the switches.

You should check:

- **Bandwidth requirements**—Does the wired network have sufficient bandwidth to handle the wireless traffic? This is particularly important to check if you are implementing an 802.11n network.

- **PoE requirements**—If the existing switches do not support PoE, you may want to upgrade the switches to PoE-enabled switches. You can choose from among the following to add to the wired infrastructure:

Table 1-16. PoE-Enabled HP ProCurve Switches

Switch Series	PoE
8200zl	X
5400zl	X
5300xl	X*
3500yl	X
2600	X**

* With PoE module; ** PWR models only

Note

If your existing switches do not have PoE, you can purchase an HP ProCurve 1-Port Power Injector (J9407A).

Apply Additional Layers of Security

Strong access controls are the foundation for a secure network, preventing unauthorized users from accessing your network and eavesdroppers from intercepting your company's wireless communications. However, networks today are the targets for increasingly sophisticated attacks, which cannot be rebuffed through strong access controls alone.

Unfortunately, internal users' stations are frequently the launching pads for these attacks. When users disconnect their laptops from the company network and connect them to insecure, public networks, they can put your company network at risk. Users' stations might become infected with a virus or worm, or an attacker might breach the station security. When these compromised stations are reconnected to the company network, an infection can spread rapidly across the internal network, and security breaches can open a gaping hole into your network. In these instances, users become unwilling participants in the attack.

Other times, users may deliberately abuse their network rights to launch attacks—stealing information or wreaking havoc on the network.

Rogue, or unauthorized, APs represent another threat. Some rogue APs are attached to the network by employees who simply want wireless access and are too impatient to wait for the IT department to provide it. Although these employees have good intentions, they may subject the network to attacks because they do not know how to implement strong WLAN security.

Other rogue APs may be attached to the network by attackers who obtain physical access to your company. These APs are designed to masquerade as legitimate company APs, luring users into entering their login credentials. The attackers collect the credentials and then use them to access the network and steal information or damage IT resources.

To protect against these types of attacks, you can implement:

- Neighbor AP detection

  Neighbor AP detection is also sometimes referred to as rogue AP detection because it allows you to identify rogue APs.
- Intrusion Protection System/Intrusion Detection System (IDS/IPS)

  An IDS/IPS detects and mitigates Denial of Service (DoS) attacks or other threats.
- Endpoint integrity solutions

  Endpoint integrity solutions are sometimes called endpoint integrity solutions because they test endpoint integrity (security settings, security software, and freedom from viruses and malware) before allowing the endpoints to connect to the network.

The HP mobility products help you to implement these measures. Table 1-14 displays which products support each measure.

Table 1-17. Security Capabilities of ProCurve MSM Products

Security Capability	Products that Support the Capability	Enhanced Capabilities with RF Manager + MSM AP Sensors	Guide Section
Neighbor AP detection	• Autonomous MSM APs • MSM Controller + controlled MSM APs	• Configure AP detection on a network-wide scale • Classify detected APs as: – Rogue (unauthorized APs connected to your wired network) – Authorized (your own APs) – Misconfigured (authorized APs that do not enforce the proper security settings) – External (APs not connected to your wired network) – Honeypot/Evil twin (unauthorized APs with the same SSIDs as authorized APs) • Predict the approximate location of the detected APs • Automatically block or disrupt traffic from rogue APs	“Detect Unauthorized or Rogue APs” on page 1-96 “Enforce Additional Security Measures with HP ProCurve RF Manager Controller” on page 1-98
IDS/IPS	HP ProCurve RF Manager Controller	• Detects and automatically defends against – DoS attacks – Configured Intrusion Prevention Policies – Active WEP cracking attacks – Spoofed clients (even if the original client is inactive)	“Enforce Additional Security Measures with HP ProCurve RF Manager Controller” on page 1-98
Endpoint integrity	NPS with IDM		“Enforce Endpoint Integrity” on page 1-103

Detect Unauthorized or Rogue APs

Unauthorized (or rogue) APs can seriously compromise the security of a corporate network—whether they connect to the wired network and open an insecure backdoor or whether they act as honeypot APs, phishing for users' credentials and data.

It is therefore important that these APs be identified as quickly as possible. You can combat unauthorized APs in several ways:

- **Use 802.1X to secure the wired network**

  As mentioned earlier in this guide, 802.1X with WPA2 is the strongest security for controlling access to wireless networks. Likewise, 802.1X is the strongest security for protecting access to the wired network and can help prevent rogue APs from being connected to the wired network. By enabling 802.1X on switch ports, you can require users and devices to authenticate before they can transmit data onto the wired network.

  Of course, your switches and endpoint devices must support 802.1X. The devices connecting to the network must have an 802.1X supplicant, which can submit the user's or the device's login credentials. For example, the MSM AP includes an 802.1X supplicant, which you can configure to submit valid login credentials.

  The switches must be able to function as authenticators, preventing devices from transmitting data until the user or device submits valid login credentials. Finally, your network must have an authentication server, which is typically a RADIUS server, to verify whether or not the login credentials are valid.

- **Authenticate APs to the MSM Controller**

  The MSM Controller can prevent unauthorized APs from becoming one of its controlled APs. The MSM Controller can also collect information about all APs in the area whether or not the APs are controlled.

  Enforcing authentication for controlled APs prevents unauthorized APs from becoming controlled by and receiving settings from the MSM Controller. In this way, you can prevent users from installing APs in locations where you do not want to provide wireless access.

  After you enable authentication, the MAC address for each AP that attempts to discover the controller is checked against one of the controller source lists for authorized APs. If the AP MAC address is listed in one of the controller source lists, the controller flags the AP as authorized and assumes control of it. Otherwise, the AP is listed as discovered but unauthorized. It does not receive any configurations from the MSM controller.

The controller can authenticate APs against any of three sources:

- Local list
- Entries in a RADIUS server database
- File stored on an FTP or HTTP server

You can select multiple sources, in which case the controller considers an AP as authorized as long as its MAC address is listed in at least one of the selected sources.

■ **Use MSM APs to gather information about neighbor APs**

MSM APs can gather information about neighbor APs whether they are functioning as controlled APs or autonomous APs.

- Controlled APs—Once an AP is adopted by the MSM Controller, it constantly scans for beacons from neighboring APs. Each controlled AP passes this information on to the controller, so the controller is aware of APs on both the wired and wireless networks.

  You cannot classify the identified APs as authorized or unauthorized, but you can learn valuable information about the AP, such as the MAC address, the SSID it beacons, and the wireless frequency and channel it is using. You can then attempt to locate and deal with the unauthorized AP.

- Autonomous APs—Autonomous APs can monitor their surroundings for neighboring radios, which helps you to locate possible rogue APs or possible sources of interference. You can configure AP radios to periodically scan their surroundings while also sending and receiving traffic from wireless stations, or you can dedicate one radio to constantly scanning for beacons from neighboring APs.

  To identify unauthorized APs, an autonomous AP compares the MAC address of each discovered AP against a manually defined list of authorized APs (a list in XML that specifies valid MAC addresses and SSIDs). If the discovered AP does not appear in the list, its name is shown in the list of unauthorized APs.

■ **Use RF Manager to detect unauthorized APs**

The RF Manager works with radios of MSM APs that are configured to act as sensors. Each sensor constantly scans for beacons from neighboring APs and reports this information to the RF Manager.Unlike an MSM Controller or autonomous AP, the RF Manager can take active measures against a rogue AP. See “Enforce Additional Security Measures with HP ProCurve RF Manager Controller” on page 1-98.

You can also use RF Planner to incorporate neighbor AP detection into your wireless coverage planning. You can view all your AP radios on a site map and select which ones should act as dedicated sensors. You can then determine whether all areas in your site are being monitored adequately. In additional, because the sensors cannot support wireless users, they are not included in coverage predictions.

In addition, you can export the site map that you created with RF Planner and import it to RF Manager.

Enforce Additional Security Measures with HP ProCurve RF Manager Controller

The RF Manager, an additional security appliance that you can install anywhere in your network, protects your network from wireless intrusions and threats. Providing IDS/IPS capabilities, RF Manager can:

- Detect wireless denial-of-service (DoS) attacks
- Detect attacks that specifically exploit Wired Equivalent Privacy (WEP) vulnerabilities
- Mitigate the detected vulnerabilities and attacks
- Locate harmful devices
- Provide extensive (and highly customizable) notification and reporting

The RF Manager relies on sensors to help it collect information and enforce RF Manager's actions. Table 1-18 lists the four MSM APs that have RF sensors: the MSM320 and MSM320-R APs, which require the purchase of a sensor license, and the MSM325 and MSM335 APs, which can always act as sensors.

In addition, HP offers the MSM415, which functions only as a sensor. The MSM415 enables you to dedicate an 802.11a/b/g/n radio to RF security. When deployed along with an MSM422, the two APs work together to provide constant client access and security scanning for 802.11n.

Table 1-18. HP ProCurve MSM313 and MSM323 Access Point Specifications

Model	Radios	RF Sensor License	Enclosure	Ports	Antenna Connectors
MSM320 (US and WW)	1 – a/b/g 1– a/b/g or a/b/g RF sensor*	Must be purchased separately and manually installed	indoor plenum-rated	2 – 10/100 (RJ-45)	4 – Reverse-polarity male SMA with diversity
MSM320-R (US and WW)	1 – a/b/g 1– a/b/g or a/b/g RF sensor*	Must be purchased separately and manually installed	outdoor NEMA-rated	1 – 10/100 (RJ-45) waterproof	2 – N-type female, waterproof
MSM325 (US and WW)	1 – a/b/g 1– a/b/g or a/b/g RF sensor	Included with AP	indoor plenum-rated	2 – 10/100 (RJ-45)	4 – Reverse-polarity male SMA with diversity
MSM335 (US and WW)	1 – a/b/g 1 – a/b/g RF sensor	Included with AP	indoor plenum-rated	1 – 10/100/1000 (RJ-45) 1 – Serial (DB-9) female	2 – Reverse-polarity male SMA with diversity
MSM415	1 – a/b/g/n RF sensor	Included with AP	indoor plenum-rated	1 – 10/100/1000 (RJ-45) 1 – Serial (RJ-45)	None

*Radio can only act as and RF sensor once the appropriate license is installed

The MSM320 and 320-R (with license), MSM325, and MSM335 can use one radio (or two in the case of the MSM335) to provide client access while using another radio to enforce continuous, real-time RF security without affecting the performance of the other radio or radios. Dedicating separate radios to RF security scans and to client access prevents “timeslicing,” a method used by most vendors that interrupts security to provide client access and suspends client access to perform security scanning-thereby compromising network security and rendering time-sensitive applications such as voice unusable.

Working in conjunction with these sensors, the RF Manager works in two ways to protect your network: it provides security and monitoring.

Security. The RF Manager protects the network as directed by Intrusion Prevention Policies, automatically quarantining offending APs and clients.

Intrusion prevention can be enabled against the following threats:

- **Rogue APs**—an unauthorized AP that is connected to the wired network
- **Misconfigured APs**—authorized APs that do not enforce the proper security settings for your system
- **Client Mis-association**—authorized clients connected to a rogue or external (neighboring) APs

- **Unauthorized Associations**—unauthorized and banned clients that connect to authorized APs.
- **Ad hoc Connections**—peer-to-peer connections between clients.
- **MAC Spoofing**—an AP that spoofs the wireless MAC address of an authorized AP
- **Honeypot/Evil Twin APs**—a neighboring AP that has the same SSID as an authorized AP
- **Denial of Service (DoS) Attacks**—attacks that degrade the performance of an official WLAN, such as the following:
  - Authentication and association flood attacks—An attacker spoofs multiple stations, sending so many authentication or association requests that the AP cannot handle them all. The AP begins to deny new requests, and legitimate stations cannot connect.
  - Disassociation and deauthentication flood attacks—The attacker masquerades as the AP and sends spoofed disassociation or deauthentication frames to other wireless stations, disrupting their associations. Although the stations quickly reassociate with the AP, the attacker continues to send disassociation frames to end the station sessions.
  - Disassociation and deauthentication broadcast flood attack—These attacks are similar to the disassociation and deauthentication flood attacks. However, the attack sends the spoofed frames to the broadcast address for the SSID, disrupting the associations for all stations.
  - EAPOL Start flood attack—An attacker floods the AP with EAP start frames, causing the AP to allocate resources for EAP sessions. Eventually, the attack consumes all of the AP resources.
  - EAPOL Logoff flood attack—An attacker send spoofed EAP Logoff frames to the AP, disrupting the authentication process for other stations.
  - Premature EAPOL Success and Failure flood attacks—An attacker sends spoofed EAP Success or Failure frames to another wireless station, which confuses the client software and prevents the station from authenticating.
- **WEP Attacks**—active that exploit WEP vulnerabilities to access your network. RF Manager can detect and protect against the following:
  - Active WEP cracking attacks—The system can detect attempts to crack your WEP key, locate the attacker, and take automatic defensive measures.
  - Client fingerprinting—The system builds RF signatures of authorized clients. RF Manager uses these fingerprints to detect spoofed clients even if the original client is inactive.

- Weak WEP keys—RF Manager's event details indicate the level of risk of WEP key cracking.
- Publicly Secure Packet Forwarding (PSPF) detection for authorized WEP APs—AP details indicate if it relays packets among wireless clients.
- WEPGuard Report—RF Manager's WEPGuard report summarizes WEP related vulnerabilities in the wireless infrastructure.

The RF Manager provides you with various levels of prevention-blocking mechanisms for detected threats. There is a trade-off between security and efficacy. The stronger the action RF Manager takes, the fewer channels it can act on. So, when selecting the prevention level, you must consider your network's need to detect threats across a larger RF spectrum versus your network's need to prevent unwanted communication.

You can set any of the following prevention levels:

- **Block**—A single sensor can block unwanted communication on any one channel in the 802.11b/g band and any one channel in the 802.11a band.
- **Disrupt**—A single sensor can disrupt unwanted communication on any two channels in the 802.11b/g band and any two channels in the 802.11a band.
- **Interrupt**—A single sensor can interrupt unwanted communication on any three channels in the 802.11b/g band and any three channels in the 802.11a band.
- **Degrade**—A single sensor can degrade the performance of unwanted communication on any four channels in 802.11b/g band and any four channels in the 802.11a band.

Monitoring. The RF Manager enables you to carefully monitor your network and gather information about it. Monitoring events provides information about the following:

- AP
- Client
- Sensor
- Server
- Traffic
- Troubleshooting

Reports. RF Manager allows you to create custom reports and use predefined compliance reports according to your network's needs. RF Manager can automatically check your compliance with your organization's legal obligations, such as Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLBA), and Payment Card Industry (PCI) Standard. Additionally, information about devices and events is also available in the form of ready made reports.

With RF Manager, you have extensive flexibility to customize the look and feel of reports. This includes selecting different foreground and background colors, specifying customized text for headings, and selecting only those parameters that need to appear in the generated report. Collated data can be viewed either as bar or pie charts. Reports are now available in PDF format, in addition to HTML and XML formats, available earlier. You can also archive reports.

Redundancy. Because protecting your network against wireless threats and intrusions is critical to safeguarding your company's confidential data, you have two options for protecting against network failures that affect RF Manager or its sensors:

- High-availability mode for RF Manager
- Offline mode for sensors

To reduce the chances of RF Manager going offline, you can configure RF Manager in high availability (HA) mode with another RF Manager. The two RF Managers connect on their second port, and each is assigned an HA interface IP address. Each RF Manager also has a network IP address. They share a cluster IP address, which is the address that sensors contact.

One device acts as the Active RF Manager and owns the cluster IP address; the other RF Manager is in Standby mode. The Active RF Manager's configuration and status are mirrored to the Standby RF Manager, which takes over as the Active RF Manager if the other device fails. (For more information about this option, see the *Management and Configuration Guide for HP ProCurve RF Manager and Sensors*.)

In the event that a sensor loses connectivity with RF Manager, sensors can actually operate on their own without RF Manager. Functions are limited, but HP ProCurve sensors are unique in providing any intrusion prevention in the event of a network failure that separates the intrusion detection and prevention system (IDS/IPS) and the sensor. The offline functions include:

- Classifying devices and detecting threats

  RF Manager periodically sends lists of APs, clients, and associations to sensors, which the sensors cache. When the sensor begins offline operation, it has these lists. Then the sensors only need to classify new devices, which they can do (although in a more limited way than RF Manager).

  By default, sensors store information for up to 128 APs, 128 clients, and 128 associations. You can increase these limits up to 500 each.
- Mitigating threats
- Storing events and alerts and sending them to RF Manager when the connection is reestablished

You must configure sensors' offline operation settings in the sensors' configuration template. Settings include device classification policies and intrusion prevention policies.

With RF Planner, you can plan where to place sensors. In this way, you can determine which areas of your site are protected by the RF Manager IDS and IPS capabilities.

Enforce Endpoint Integrity

When you enforce endpoint integrity, you require that all stations must meet minimum security standards such as having the latest virus updates and patches. With Windows NPS, which integrates with IDM and can even run on an HP ProCurve ONE platform, you can also test each endpoint for viruses and other malware, missing patches, insecure browser security settings, and the presence of a firewall. Those endpoints that do not comply with your organization's policies can be quarantined until they are compliant.

Perform the Initial Setup

After you have finished the preliminary planning, you should visit the site at least one more time to confirm your observations from the previous survey. Do a site walk-through to make note of any additional obstacles or conditions that would affect your installation.

If you are using PMM or RF Planner to plan your coverage, finalize all of the information, taking care that the transmission power and channel are set for each device that you will install. Use PMM or RF Planner to generate a bill of materials report and then purchase your equipment from an authorized HP vendor.

Configure Initial Settings on the APs and MSM Controllers

You are now ready to configure the initial settings on your devices and ensure that you can manage them before you install them in their final location. Because wireless devices are often installed in hard-to-reach areas, it is particularly important to test your settings before the devices are deployed.

Configure Initial Settings on Autonomous MSM APs. To ready an autonomous MSM AP, you should connect a station directly to the AP on its Ethernet port and access the AP Web-based management tool. Then set the AP to autonomous mode, select the correct country, assign the AP a valid IP address and default gateway on your network, and so forth.

To protect the devices from unauthorized access, you should immediately change the default setting for the management passwords. Otherwise, anyone who knows these default settings can access your devices and view or change configuration settings.

Configure Initial Settings on an MSM Controller. To ready the MSM Controller, connect a station directly to its LAN port and access the controller's Web browser interface. Assign the controller a valid IP address and default gateway in your network and configure its internal DHCP server (if you are using it for your deployment).

You can then install the controller in its final location.

Note

If you have configured your controller to act as a DHCP server on its LAN port, it may begin assigning IP addresses to clients that should be receiving a dynamic IP address from a network DHCP server.

If you have a network DHCP server, you should disable DHCP on the controller *before* connecting it to your network.

Note that you need to configure some additional settings before installing MSM APs:

- Configure VSCs. (See "Configure VSCs" on page 1-106.)
- Provision AP discovery if necessary. (See "Configure Initial Settings on Controlled MSM APs" on page 1-105.)

- If you plan to require APs to authenticate to the controller or to a RADIUS server, configure the appropriate settings. Also complete any necessary configuration on an external RADIUS server.

Refer to the *HP ProCurve MultiService Mobility Implementation Guide* for complete instructions.

Configure Initial Settings on Controlled MSM APs. At factory defaults, an MSM AP is set to controlled mode. If you place the APs and the MSM Controller in the same VLAN, you should be able to install the APs in their final location without any preconfiguration. (The APs must be able to communicate with the MSM Controller, so you should ensure that the uplinks between switches are tagged with the appropriate VLAN.) The APs will automatically discover the MSM Controller, and the MSM Controller will begin to manage them.

However, you should always verify the process before you install an AP in its final location—particularly when you plan to require controlled APs to authenticate to the controller or to a RADIUS server. Connect the AP to an accessible port that is in the same VLAN as the controller and verify that the controller discovers and assumes control of the AP.

You must provision the AP discovery settings before you install the AP in its final location if:

- The AP is in a different VLAN from the MSM Controller.

  The discovery settings can include the MSM Controller's IP address or domain name. (In the latter case, you must also specify the IP address of the DNS server that can resolve the domain.)

- The controlled AP uses a local mesh to connect to the controller.

  In the connection settings, specify that the AP connects through a local mesh. You must also configure the local mesh provisioning profile on the MSM Controller.

You can provision the AP using the MSM AP's Web browser interface or the MSM Controller's Web browser interface. To use the latter method, first configure the appropriate settings on the MSM Controller. Then connect the AP to a port in the same VLAN as the controller, and the AP will automatically receive the settings. You can connect multiple APs and an MSM Controller to a single switch to provision all of the AP discovery or connection settings at the same time.

Rather than provisioning the AP discovery settings, you can use DHCP for Layer 3 AP discovery. In this case, you specify vendor-specific class information that will allow the MSM APs to locate the controller. When the MSM APs send their vendor class identifier in a DHCP request, the DHCP server returns the vendor-specific options defined on the server. These values are returned as DHCP option 43 (vendor-specific information) and can be interpreted only by an MSM device. (The instructions for configuring this option are included in Chapter 5: "Manufacturing Implementation" in the *HP ProCurve MultiService Mobility Implementation Guide*.)

Configure VSCs

It is best practice to configure VSC settings (whether on the MSM Controller or on autonomous APs) before connecting the APs to your network. Otherwise, users might connect to the default wireless network and send insecure traffic into your network.

Configure the VSC settings that you determined using the guidelines in "Begin Planning Wireless Security" on page 1-59.

Install the MSM Devices

You are now ready for a preliminary installation. In addition to the wireless devices, you should take the following to the installation site:

- Laptop with PMM or RF Planner and site views loaded
- Floor plan
- Tape measure to calculate distances
- Pencils to mark the locations of APs
- Duct tape to temporarily mount radios
- Ladders
- Two-way radios
- Laptop running site survey software
- Wireless traffic analyzer
- Wireless device with the NIC that you have chosen as a test station (this can be the laptop with RF Planner)

Install the MSM Controllers and temporarily mount the APs in the location you planned. As you mount the APs, record each device's serial number. Connect the APs to the network and ensure that the controllers detect the APs and can manage them. In the MSM Controller's Web browser interface, APs are listed by their serial number. You can check this number against the list you created.

Verify the Network Is Ready to Authenticate Users

If you are using 802.1X authentication, Web-Auth, or RADIUS MAC-Auth, you should test connectivity between authenticators and their RADIUS servers. See Table 1-19 to find the authenticators in your deployment.

Table 1-19. Authenticators Based on Architecture

Architecture	Authenticators	RADIUS Server
Centralized	MSM Controller	MSM Controller or external RADIUS server
Distributed with centralized authentication	MSM Controller	MSM Controller (or external RADIUS server)
Distributed without centralized authentication	MSM APs	External RADIUS server (or MSM Controller)
Autonomous AP	MSM APs	External RADIUS server
Autonomous AP with centralized Web-Auth	MSM313, 313-R, 323, or 323-R	External RADIUS server

Also make sure that:

- All necessary accounts are configured on RADIUS servers or in your directory

  See “New User Accounts” on page 1-107.
- All necessary policies are in place on the RADIUS servers

  See “RADIUS Policies” on page 1-108.

New User Accounts. If you are planning to grant new users access to the wireless network, you must set up accounts for them. For example, you can add a guest group and guest accounts to your directory server. Then create a policy on your RADIUS server to grant users in the new guest group the appropriate access.

If you are using an MSM Controller as the RADIUS server, you can create user accounts and specific settings for those accounts. See the section below for more details.

RADIUS Policies. RADIUS policies allow users to authenticate to the network and grant them their VLAN assignments and other rights. When you use the MSM Controller's internal RADIUS database, you can configure user's settings with account profiles. For other RADIUS servers, the easiest way to set up dynamic settings is through IDM. (For instructions on using IDM, see the *HP ProCurve Access Control Security Solution Implementation Guide*.)

See Table 1-20 for the settings that you can configure on the MSM Controller RADIUS server or on another RADIUS server using IDM.

Table 1-20. Dynamic User Settings

Setting	Configurable on MSM Controller	Configurable on Other RADIUS Servers with IDM
VLAN Assignment	X	X
Rate limit	X	X
Traffic priority	X	X
ACLs	X	X
Customized attributes	X	

Note that, if your wired network already enforces authentication to a RADIUS server, you can use existing policies as long as two criteria are met:

- Wireless users are the same users who have been accessing the network through wired connections.
- Users should have exactly the same rights regardless of whether they have a wired or wireless connection.

Otherwise, you need to create new policies (or modify existing ones) to accommodate the new users and to specify the wireless-specific rights.

Configure Radio Settings

Refer to the radio settings that you (or a site surveyor) calculated in the planning stages whether with PMM, RF Planner, or another method. Configure these settings either through the MSM Controller or manually on autonomous MSM APs.

Reassess RF Coverage

When all of the APs are up and running, you should reassess your coverage plan.

Reassess Coverage with RF Planner. RF Planner includes a calibration tool that helps to make your coverage plan more realistic. In RF Planner, select the Calibration View. The planner gives you a set of calibration points for which you should take signal strength readings, averaging signal strength over time for greater accuracy. When you click the **Calibrate** button, the planner adjusts the predicted coverage to take into account obstructions and interference.

Survey the Installation. If you are not using RF Planner, you should measure signal strength and integrity using a laptop with site survey software that displays the signal strength and data rate.

Walk through the site slowly, and carefully record signal levels on the floor plan. Your software should tell you about the kinds of interference in any given place, whether it is from another AP on the same channel or another source of RF interference.

Adjust APs Based on Your Assessment. After you reassess coverage, adjust the position, and possibly radio settings, of your APs to improve the signal levels. Continue the iterative process of analyzing the signal and making adjustments until you have found the best location and settings for each radio. If you are using RF Planner, update the locations and settings for your APs in your site plan.

Do not forget to test the signal in areas where you do not want the signal to go. Go outside the building and measure signal levels in the parking lot or on the street. If possible, measure signal levels in nearby businesses.

Monitor Network Performance

Your next step is to test the wireless network itself. When possible, perform this test during business hours so that you can see how the network operates under normal conditions.

Use the test station to see if you can join the VSCs that you have already created. If possible, log in as different users and verify that the correct rights are granted to each type of user and that restrictions are applied properly. Move from place to place and verify that roaming works as you anticipated. If you are using Mobility Traffic Manager, ensure that traffic is tunneled and then terminated at the right MSM Controller.

You can then allow actual users to begin accessing the network. Once the wireless network is in use, you should periodically monitor it. Monitoring usage is particularly important when the wireless network is first deployed.

With the 5.4 software release, the MSM Controllers and APs support sFlow, is a statistical-sampling technology that can be used to gather detailed information about your both wired and wireless networks. This industry standard supports the following components:

- sFlow agent (actually, usually many sFlow agents)
- sFlow proxy (optional)
- sFlow collector

The sFlow agent uses statistical traffic sampling to send the sFlow collector enough information for the collector to create an accurate profile of network traffic within a margin of error.

In addition to agents and collectors, sFlow supports proxies, which operate between the sFlow agent and the sFlow collector. An sFlow proxy collects all of the traffic data from the agent (or agents) and repackages the information so that it appears to be the source. When an sFlow proxy is used, the collector is not aware of the sFlow agents that provide statistical information to the sFlow proxy.

The sFlow collector receives and analyzes the packaged information. From this information, the collector creates a statistical model of network traffic that can be used for network troubleshooting, traffic management, billing, or security auditing by an intrusion detection and prevention system (IDS/IPS).

MSM APs act as sFlow agents, and MSM Controllers act as sFlow proxies, collecting information from MSM APs. (See Figure 1-16.) Note that the controller does not generate any sFlow information of its own: only MSM APs generate sFlow information.

HP PCM+ / HP ProCurve Network Immunity Manager (NIM) acts as an sFlow collector. PCM+ can help you analyze traffic, while NIM can monitor traffic for threats.

Because both HP ProCurve switches and MSM devices support sFlow, PCM+ allows you to monitor your complete network infrastructure—both wired and wireless. You can see which devices are using the most bandwidth and where the network is congested.

For wireless networks, sFlow includes extensions that provide wireless-specific traffic attributes such as the channel used for transmission and reception, the SSID in use, and the encryption algorithm used. Also, if the traffic was encrypted, the sFlow data can contain the unencrypted payload to allow deeper visibility.

Just as PCM+ can monitor the entire network, NIM can protect against threats that target your wired and wireless networks. If a threat is detected, NIM can apply the same actions to both networks or apply different actions to each one.

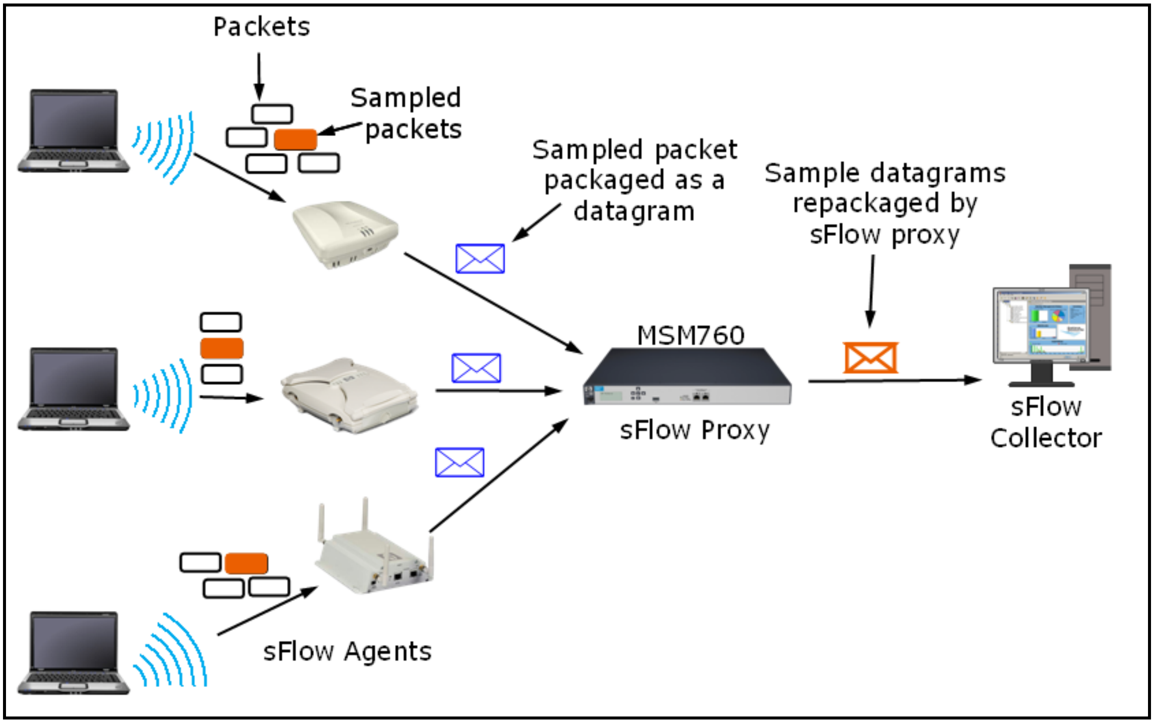

Packets
Sampled packets
Sampled packet packaged as a datagram
Sample datagrams repackaged by sFlow proxy
MSM760
sFlow Proxy
sFlow Collector
sFlow Agents

Figure 1-16. Using sFlow to Monitor Your Wireless Network

Provide Increased Reliability

For many companies, wireless access has become as critical to their business as traditional wired access. Recognizing the importance of wireless access, HP Networking offers products designed with high availability in mind.

Redundancy for MSM Controllers

If you need redundancy in your MSM Controller configuration, you can set up a controller team with up to five MSM Controllers. (A controller team is supported with the 5.4 software release.) Not only does the team allow you to manage these controllers from a single management interface, it also provides failover capabilities if a controller is separated from the other members and becomes unavailable.

When you create a team, you designate one of the MSM Controllers as the team manager. The team manager is then responsible for sending configuration changes to other team members and for updating team members' software. Team members in turn update their controlled MSM APs with both configuration settings and software.

When you set up a team, you assign it a virtual IP address. The IP address is associated with the team manager, and you use this virtual IP address to configure and manage the team.

If the team manager becomes unavailable:

- The team elects an interim team manager
- The team's virtual IP address is associated with the interim team manager

The team manager's controlled APs are handled just as any team member's controlled APs would be handled in a failover situation: the APs migrate to other team members.

Of course, the controlled MSM APs that are migrated to another controller must be able to find that controller. For example, if the MSM APs are provisioned, you must include all the team members in the provisioning configuration.

The team knows the total number of APs it is allowed to manage. That is, it pools the AP licenses on each controller. If a controller fails, its licenses can be used by other controllers to manage its APs. However, each controller can manage a maximum of 200 APs. For redundancy, therefore, a team can manage a maximum of 800 APs.

When failover occurs and controlled MSM APs migrate to another MSM Controller, noncentralized traffic fails over seamlessly. However, access-controlled traffic and Layer 3 Mobility traffic do not fail over. Users on access-controlled VSCs or roaming at Layer 3 must log in again. After this brief interruption, however, these users can resume their work.

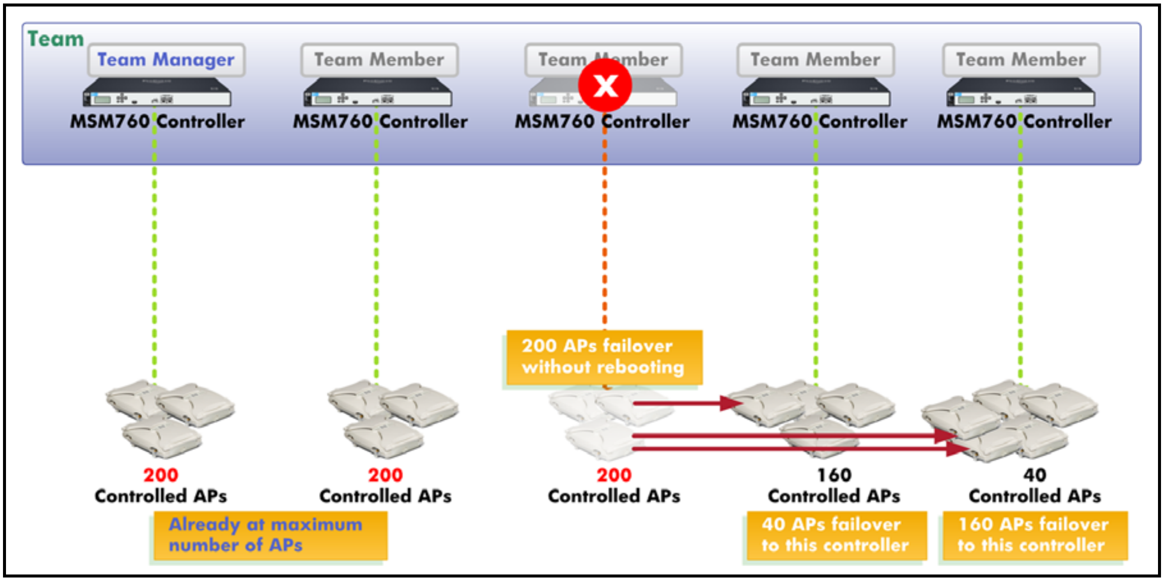


Figure 1-17. Failover in a Controller Team

Redundancy for RF Manager

For deployments that require fail-safe monitoring, you can configure a high-availability (HA) cluster of RF Managers. Two RF Managers form a cluster in which one serves as the primary IPS and the other manager serves as a standby. Then, in the unlikely event that the active manager fails—because of a power failure, for example—the standby manager takes over the role of the active manager.

Highly Available Local Meshes

Controlled MSM APs support dynamic local meshing for increased reliability. For example, if a master AP (the AP that connects to the wired network) fails, the APs that had wireless links to it can connect to another root AP. To create a highly-available local mesh, ensure that each AP that lacks a wired connection can connect wirelessly to at least two master APs.

Upgrading a Wireless Network to 802.11n

The IEEE 802.11n standard increases network speed and reliability as well as extends the operating distance of wireless networks. Current drafts of 802.11n easily provide up to twice the range of 802.11g. In fact, the 802.11n standard will eventually offer many times the speed of 802.11g in maximum configurations. For more technical information about 802.11n, see "802.11n" on page 1-30. This section explains how to plan the upgrade of an existing wireless network to 802.11n.

Reasons to Upgrade to 802.11n

Before you upgrade to 802.11n, you should evaluate your wireless network usage and determine whether your system requires the high speeds that 802.11n offers.

The actual data rate provided by a wireless cell is typically between 30 and 50 percent of the theoretical maximum data rate. For example, the data rate provided by an 802.11g radio might be about 20 Mbps. You should consider 802.11n when your users require greater bandwidth to complete their tasks or to have a quality experience.

Scenarios include:

- Wireless devices run streaming video:
  - Students watch a virtual lecture or participate in a virtual classroom.
  - Security cameras stream video to a central server.
  - Employees watch training videos.
  - Sales representation show videos to customers.
- The area must provide wireless access for a high density of users.

  For example, if 20 users connect to an 802.11g cell, each user only receives about 1 Mbps bandwidth, which may not be adequate for their needs.
- Employees use wireless connections to run high-bandwidth-consuming software such as graphic design software.
- You have noticed that your usage has been rising, and you want to future-proof your network.

Plan the Upgrade

You have decided to upgrade to 802.11n. Now carefully consider your goals and the implications of the upgrade:

1. Plan the scope of the upgrade.
2. Consider the implications on wireless coverage.
3. Plan for backward-compatibility.
4. Consider the affect of high-speed mobility on your wired network.

Plan the Scope of the Upgrade

You can upgrade your entire network at once, or you can choose to upgrade certain areas only. You might want to select one area that seems particularly congested and evaluate the results. If the results are good, you may decide to upgrade other areas as well. All MSM products can interoperate, whether they support 802.11n or not, so you can upgrade at your own pace.

Consider the Implications on Wireless Coverage

When you have selected the areas that you want to upgrade, make a list of all the APs that currently provide wireless coverage in those areas. You will replace these APs with MSM400 series APs, which support 802.11n. The 802.11n cell size will depend on the data rates you want to support. They will likely be larger than 802.11a/b/g cells. Therefore, you might want to install fewer APs and space the APs slightly farther apart. However, if you intend to have the 802.11n MSM APs support much higher data rates, you may prefer to deploy the APs at a one-to-one ratio.

Plan for Backward-Compatibility

When you upgrade only certain areas of your network to 802.11n, you should assume that some 802.11a/b/g stations might enter the MSM400 series AP coverage areas. Therefore, you should plan for backward-compatibility with these standards. In fact, in all but the most controlled environments, you should assume that you must provide some protection for and from the 802.11a/b/g stations.

See “Compatibility and Protection with 802.11n” on page 1-32 for more detailed explanations.

Consider the Affect of High-Speed Mobility on Your Wired Network

Your MSM400 series APs are capable of forwarding more (possibly much more) wireless traffic into the wired network than the APs that they replace—in fact, this is the goal of upgrading the devices. But you must take care to ensure that the wired network can handle the increased traffic.

First, make sure that each new AP connects to a switch port that provides 1 Gbps connectivity. Because the AP switch probably provides connections for other endpoints and other APs, you might want the port uplink to provide 10 Gbps connectivity, but it is not absolutely necessary. The uplink speed you require depends on the types of applications that will be running on your network.

Continue to check uplinks between the new AP switches and the resources that wireless users access. Verify that they can handle the influx of traffic, and, if necessary, implement wired meshes to provide greater bandwidth.

Finally, consider the architecture of your current wireless network. The following architectures can handle the traffic flow for 802.11n:

- Autonomous architecture
- optimized WLAN architecture with distributed forwarding

If you plan to use the 802.11n upgrade to allow an increase in traffic flow, and any of the VSCs that the new APs will support use an optimized WLAN architecture with centralized access control, you might run into problems. All wireless user traffic in the VSCs will be forwarded to the controller, which might cause a bottleneck that prevents you from enjoying the benefits of the upgrade. You should consider changing the architecture for this deployment. Remember that you can still implement centralized authentication with a distributed forwarding architecture.

For more information on architecture options, see “Choose the Architecture” on page 1-33.

Complete the Upgrade

Configure initial settings on your MSM400 series APs as described in the appropriate section:

- "Configure Initial Settings on Autonomous MSM APs" on page 1-104
- "Configure Initial Settings on Controlled MSM APs" on page 1-105

For an autonomous architecture deployment, configure other settings on the new APs, including VSCs and radio settings. Make sure to provide for backward-compatibility as indicated in your plan.

For an optimized WLAN architecture deployment, create a new group for the new MSM400 series APs on the MSM Controller. Configure the 802.11n settings that you planned in the radio settings for this group. Then bind the appropriate VSCs for the areas that you are upgrading to this group.

For detailed instructions on autonomous MSM APs, see the *HP ProCurve MSM3xx / MSM4xx Access Point Management and Configuration Guide*. For detailed instructions on controlled MSM APs, see the *HP ProCurve MSM7xx Controllers Management and Configuration Guide*.

Finally, schedule a network outage. Remove the existing APs and install the MSM422 APs. See "Install the MSM Devices" on page 1-106.

Upgrade Your Wireless Stations

Only stations that also support 802.11n can enjoy the higher speeds that it offers. Make sure to install wireless clients that support 802.11n in your stations. If you do not install such clients in all devices, or if your wireless network supports guests' devices, remember to implement backward-compatibility in the new AP radio settings.

Evaluate the Upgrade

After you install the new APs, you should roam through the site with a laptop running site survey software that displays the signal strength and data rate, looking for areas with inadequate coverage. If necessary, adjust device location and settings. Continue to evaluate the signal on different days and at different times of the day.

You should also evaluate the results of the upgrade. Ask wireless users about their experience. Have they noticed faster speeds? Have they noticed areas of poor coverage? Check the wired network for congestion using tools such as PCM+ Traffic Monitor. Continue to monitor both the wired and wireless network.

Example WLAN Installation

Contents

Overview: PCU Medical Center

This chapter looks at the process of designing a wireless network for a hypothetical organization: ProCurve University Medical Center (PCUMC), a teaching hospital located near ProCurve University (PCU). In this chapter you will consider the most important factors when setting up a wireless network, and examine the decision-making process.

The Site

PCUMC comprises two buildings: a teaching hospital and an office building that holds some doctors' offices and examination rooms. The hospital is three stories and the office building is two. The two buildings are separated by a busy, six-lane road.

Currently, the doctors in the office building cannot access the patient records that are on the hospital LAN. The medical center wants to provide a wireless link between the hospital and the office building across the street.

In addition, PCUMC wants to implement a wireless network in both buildings for user access and for radio frequency identification (RFID) tags that are used for asset control.

As you read through this chapter, assume that you are a part of a team of wireless networking experts who have been hired by the university to help PCUMC develop a wireless solution.

Assess Customer Needs

Your first act is to determine what PCUMC needs and expects from its wireless installation. As described in Chapter 1: “Wireless Network Design Process,” you need to identify:

- The purpose of the wireless installation
- User types
- Usage habits
- User density
- User equipment
- Roaming requirements
- Security needs

Each of these needs will be assessed in the sections that follow, although in some cases the needs will be combined into one section for clarity.

Identify the Purpose of the Wireless Installation

To improve record-keeping accuracy and efficiency, PCUMC has decided to implement an electronic records system (ERS), which medical staff will use at each “point of care,” or location where they interact with patients, such as bedsides, examination rooms, or operating rooms. The software has a client-server architecture with an HTML-based thin client. The amount of traffic between one client and the server averages less than 200 Kbps.

Some of the computers that use this new software will be positioned on rolling carts that can be pushed from room to room. (The ERS client might also be on wired workstations, PC tablets, and smaller handheld devices.)

The hospital also wants to provide Internet access for visitors and patients in the hospital and office building. The hospital wants to provide doctors and other staff members in the office building with wireless access to the appropriate resources in both the office building and the hospital.

PCUMC has chosen an RFID solution that uses “active” RFID tags—battery-powered tags that actively send out locator signals. This RFID solution leverages the Institute of Electrical and Electronics Engineers (IEEE) 802.11b standard instead of requiring proprietary readers. The tags will be used to track patients as well as assets, which means that an RFID tag will be attached to each patient wristband and to each piece of equipment—wheelchairs, IV pumps, monitors, carts, beds, and so on. The broadcast range of the RFID tags is approximately 500 m (1500 ft), and each tag transmits one 512-bit packet every 20 seconds.

The office building is located about 50 m (165 ft) away from the hospital. The traffic that is to be broadcast across this local mesh will consist of client-server communication for the ERS and RFID-tag traffic for the equipment in the doctors' offices.

Identify User Types

You create and distribute a user survey to determine, among other things, who will use the wireless network. (See Appendix C, "Site Survey Forms and Tables" for sample surveys.) From these surveys, you determine that there are several basic types of users:

For the PCUMC hospital, the users are:

- Guests (visitors/patients) (70–150)
- Certified medical personnel (200)
- Uncertified medical personnel (55)
- Administrative personnel (62)

For the PCUMC office building, the users are:

- Guests (visitors/patients) (15–40)
- Certified medical personnel (8)
- Administrative personnel (20)

You also expect to deploy hundreds of RFID tags and dozens of carts using an ERS client.

On the floor plan of the of the hospital, you mark areas where each type of user is most likely to be found.

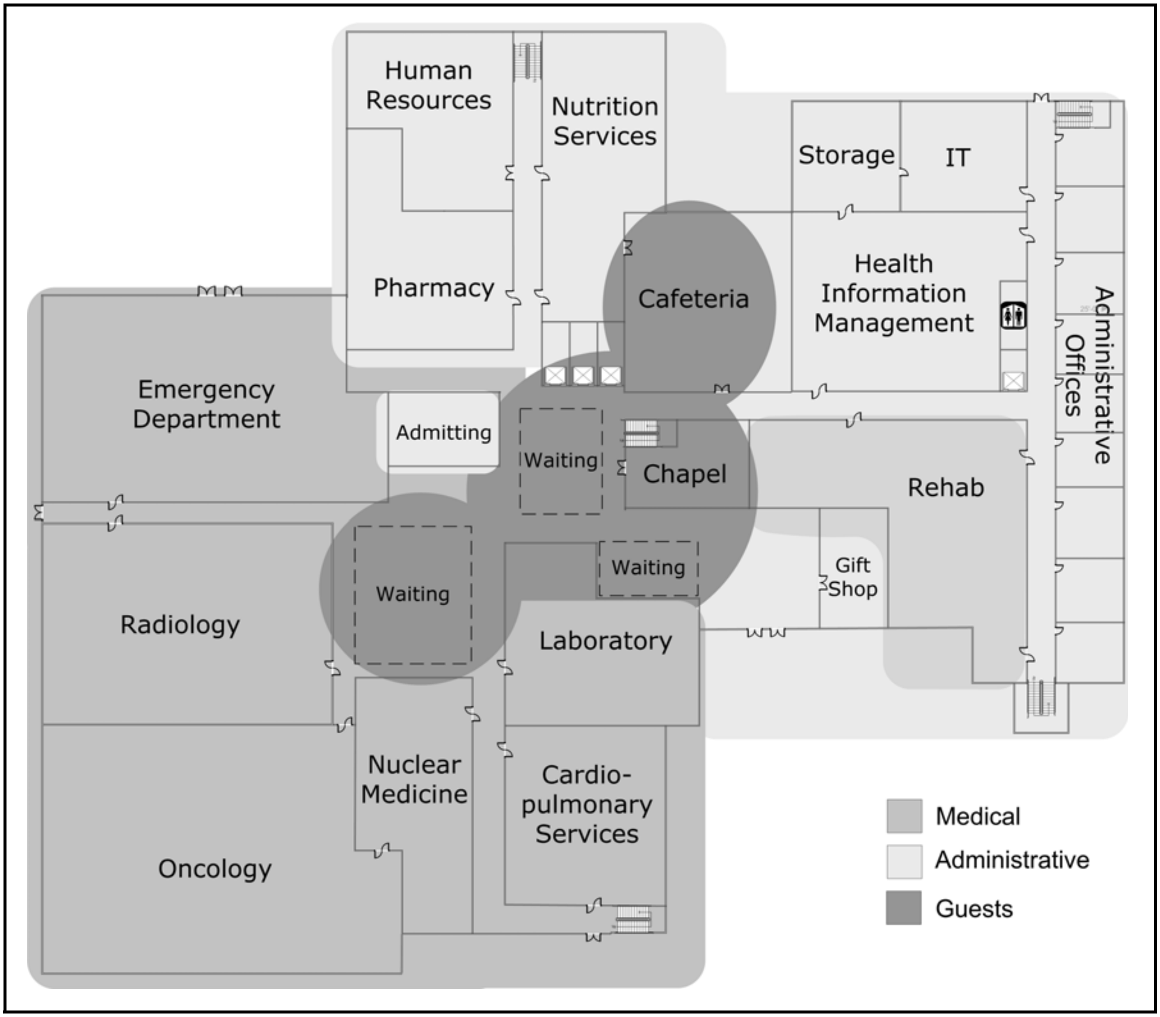


Figure 2-1. Hospital L1—User Types

On level 1 of the hospital, visitors and patients are found mostly in the waiting areas, the chapel, and rehab. Administrative personnel are in Health Information Management, Human Resources, administrative offices, Nutrition Services, Admitting, IT, and the gift shop.

The rest of the first level—Emergency Department, Radiology, Oncology, Nuclear Medicine, Cardiopulmonary, Laboratory, Rehab, and the pharmacy—is primarily used by medical personnel.

In the cafeteria, users from all of the groups can be found.

Because the RFID tags will need to “see” an access device from every point in the hospital, there is no need to mark the areas for RFID tags.

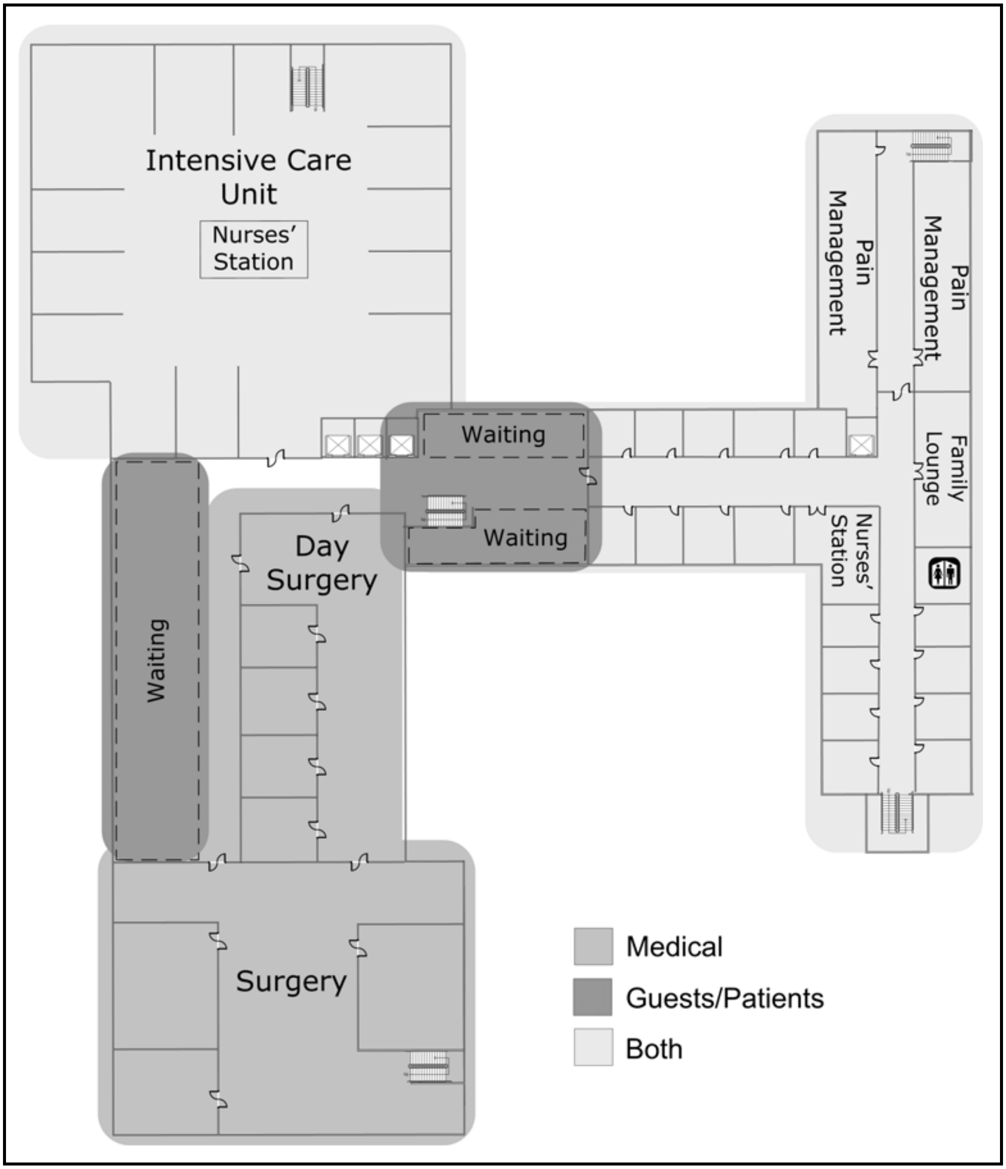


Figure 2-2. Hospital L2—User Types

On the second level, the waiting areas are visitor/patient areas, and in the patient rooms and Pain Management, wireless coverage for this user type will also need to be provided. (Visitor/patient access will not be permitted in Intensive Care.) Medical personnel will be in the surgical areas, Intensive Care, Pain Management, and the patient rooms.

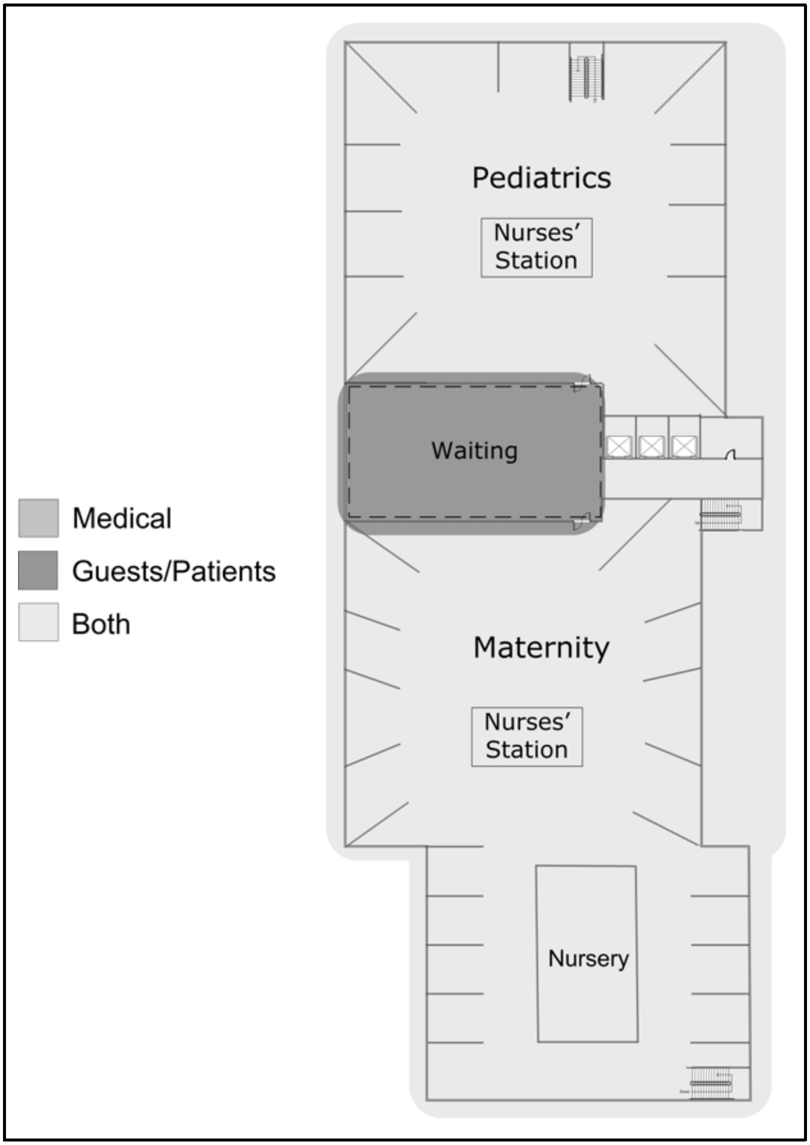


Figure 2-3. Hospital L3—User Types

On level 3, both visitors/patients and medical personnel will need coverage throughout the whole floor, although coverage for medical personnel can be omitted from the waiting areas, if possible.

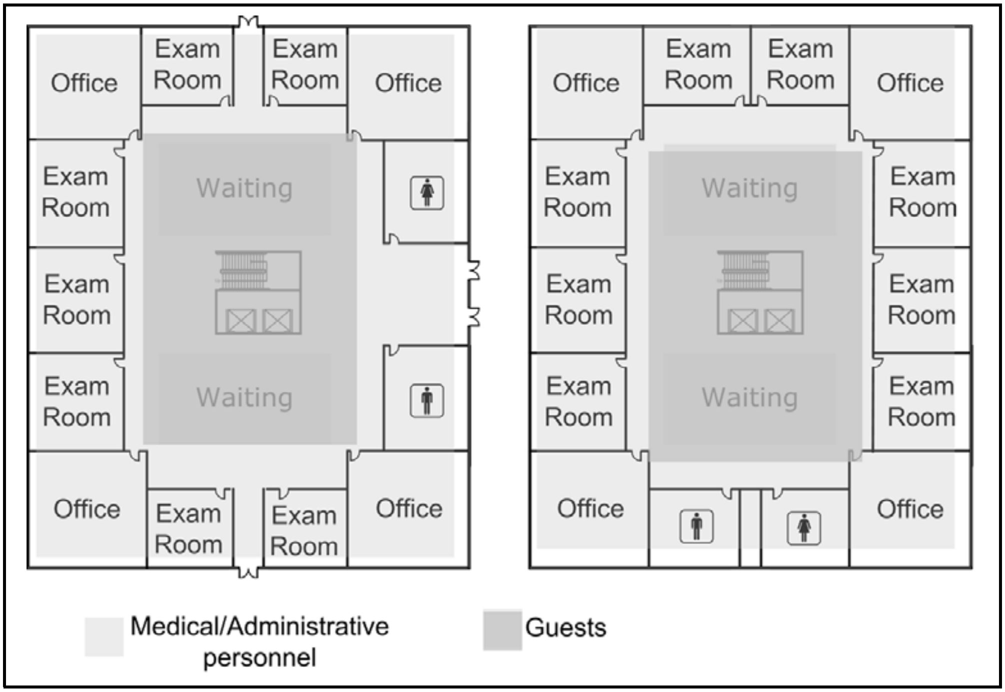


Figure 2-4. Office Building—User Types

In the office building, visitors/patients will need coverage in the waiting areas of both floors. Medical personnel will need coverage in the offices on the perimeter of those same floors. There will also be some RFID tags on both levels.

Identify User Equipment and Usage Habits

The next step is to map the applications and data to user types and their devices, as shown in Table 2-1. You will use this information to plan the PCUMC Virtual Service Communities (VSCs) and estimate bandwidth needs.

Table 2-1. User Devices, Data, and Applications

Device	User Type	Applications	Bandwidth	Sensitive Data
Laptop	Hospital and office administrative	Internet Email Word processing Spreadsheets File transfer	Medium-high	Financial
Laptop	Hospital and office medical (certified and uncertified)	Internet Email Word processing ERS File transfer	Medium-high	Patient records
Laptop	Visitors, patients	Internet	Low	None
PC tablet	Hospital and office medical (certified and uncertified)	ERS	Medium	Patient records
Smartphone	All	Internet	Low	None
RFID tags	None	Locator beacon	Low	None
Personal digital assistant (PDA)	Hospital and office medical (certified and uncertified)	Internet ERS	Low	Patient records
PDA	Hospital and office administrative	Internet Email	Medium	None
PDA	Visitors, patients	Internet	Low	None

(Table C-1 in Appendix C, "Site Survey Forms and Tables" is blank so that you can use it to record information about your organization.)

From this table, you can see that the administrative and medical users plan to use their wireless connections for the same applications they use on the wired network. Their bandwidth demands are therefore the highest.

Those devices that will access HTML applications only—the Internet and the ERS—will require a lower amount of bandwidth, and the RFID tags require the lowest amount of bandwidth of all.

Estimate User Density, Equipment, and Roaming Requirements

From the survey questions about where users intend to connect to the WLAN and how far they plan to move, you create the following maps:

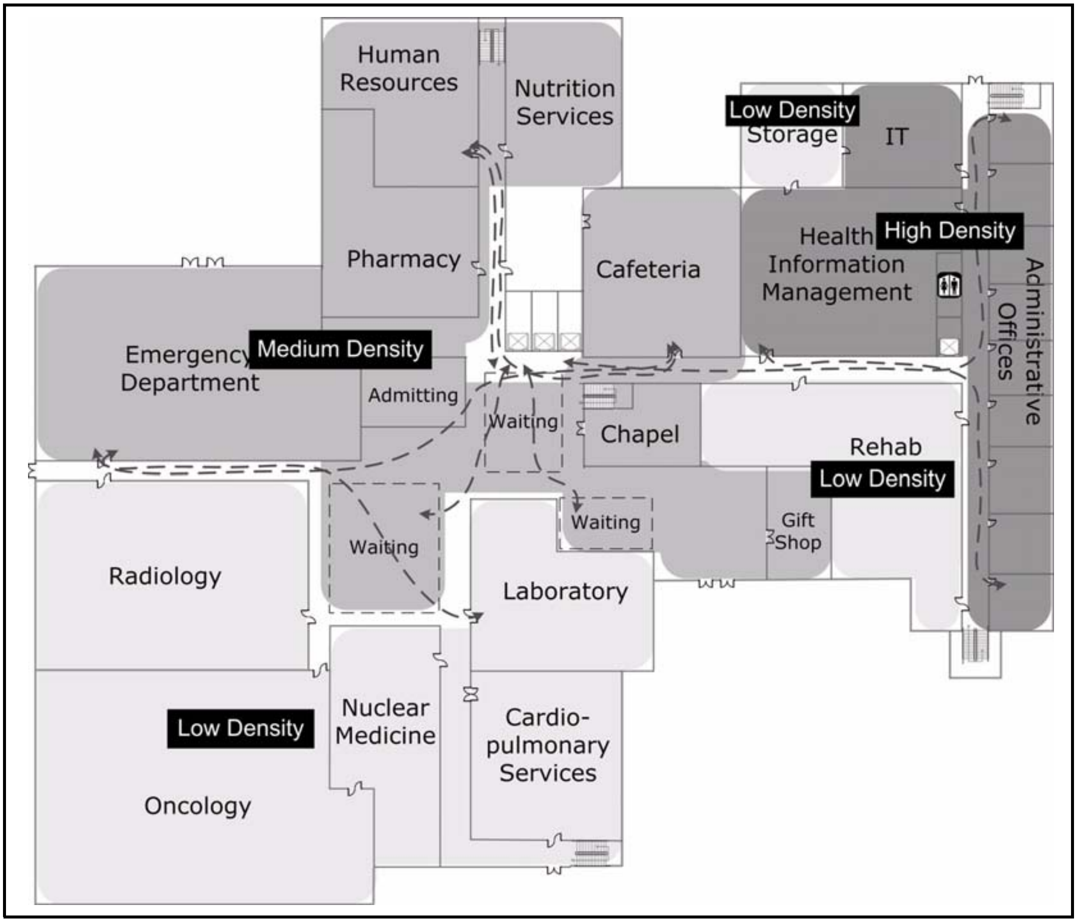


Figure 2-5. Hospital L1—User Density and Mobility

On the first level of the hospital, the density levels are highest in the administrative areas and slightly less so in the public areas. Users expect to connect with laptops and perhaps smart phones.

The most critical types of motion will be from the Emergency Department to the central elevator bank as patients are rushed to Major Surgery on the second floor. Likewise, some patients will be taken from the Emergency

Department to Radiology or other departments when more specialized care is needed. However, it is unlikely that a WLAN connection will need to be maintained in these cases, and it is equally unlikely that a WLAN connection could be maintained inside the moving elevators (unless an access device were installed in each elevator car).

Administrative users expect that they will move among the administrative offices and Health Information Management as well as over to Human Resources. Users are also expected to roam to the cafeteria and to the second and third floors, usually through the central elevator banks.

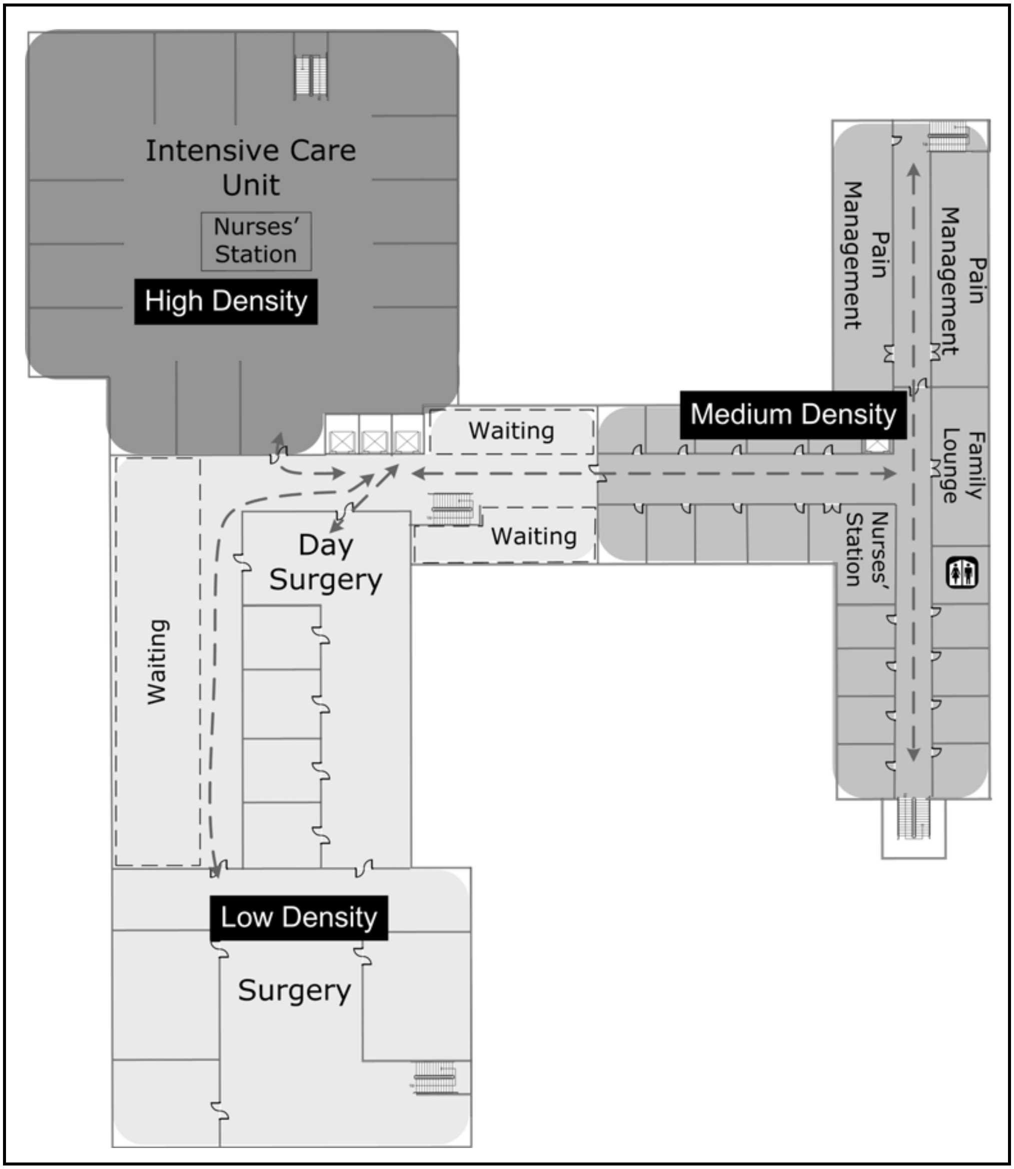


Figure 2-6. Hospital L2—User Density and Mobility

On the second level, the ERS on the mobile carts will be used in the Intensive Care unit, the surgical areas, and the patient rooms. The carts will need a constant connection as they move from room to room or bed to bed.

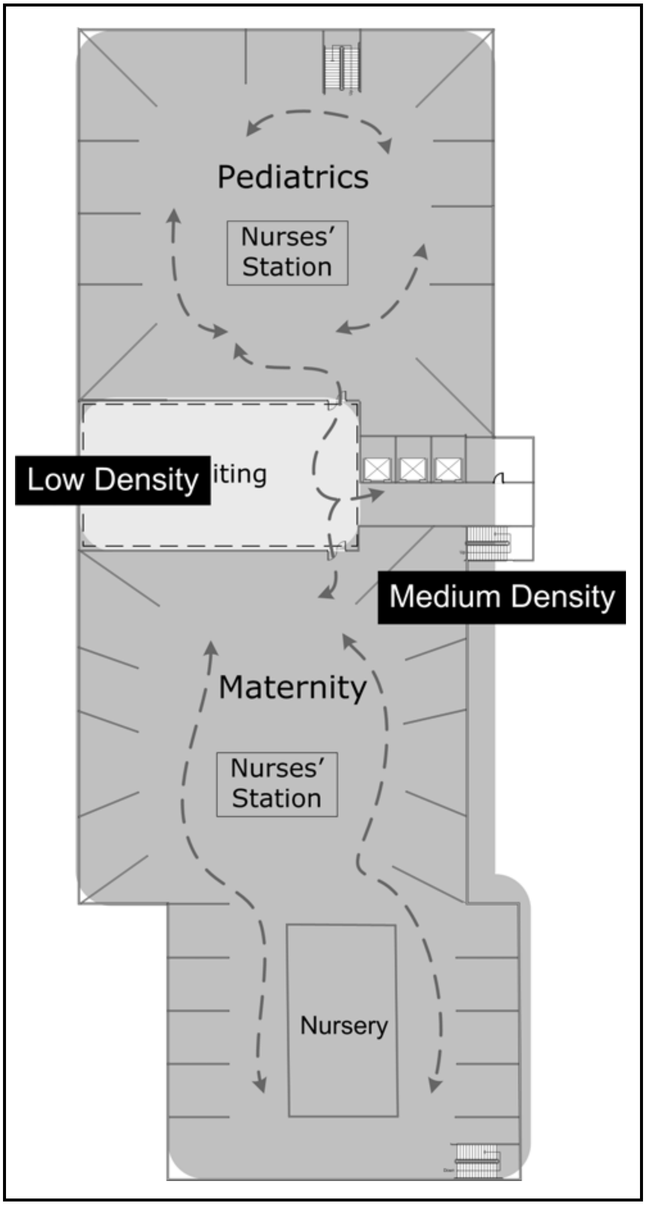


Figure 2-7. Hospital L3—User Density and Mobility

On the third level, the primary users will be those accessing the ERS and sometimes patients (using laptops or smartphones). Connections will need to be reasonably constant throughout the departments.

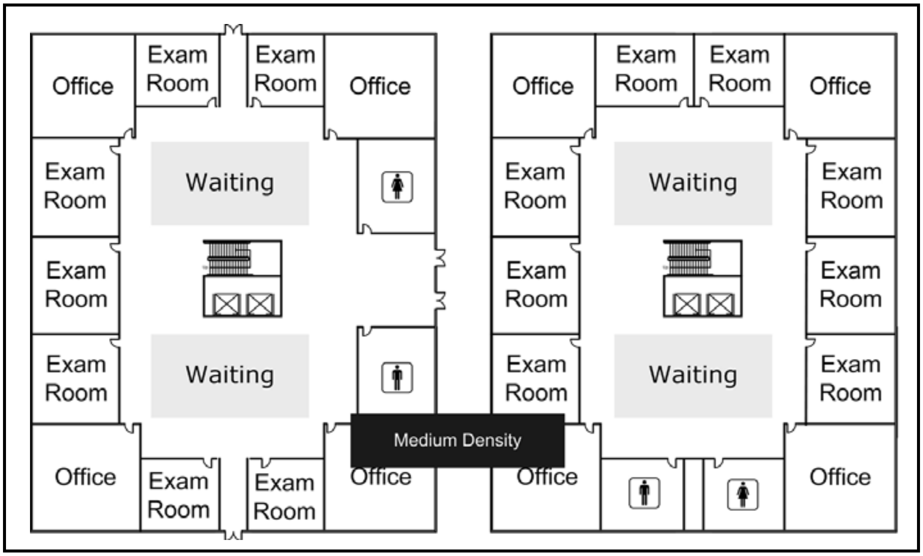


Figure 2-8. Office Building—User Density and Mobility

In the PCUMC office building, user density is lowest in the waiting areas of the first two levels. The rest of the building will have medium user density. Users expect to connect with laptops, primarily. Some guests might try to use smartphones.

The roaming requirements of the office-building users are low: users will not typically need a constant connection as they move.

Assess Security Needs

Consult “Assess Security Needs” on page 1-14 for an explanation of security needs that a site may have. The sections below give an example of assessing these needs for PCUMC.

Determine Risk Tolerance

PCUMC maintains or will maintain the following types of data on its network:

- Scheduling information
- Patient health and insurance data (ERS)
- Hospital financial records
- Employee records
- Equipment inventory (RFID)
- Patient prescriptions
- Drug database

Of these types of data, the most sensitive are the patient health and insurance data, hospital financial records, employee records, and patient prescriptions. Any break-in that compromises this data could result in high recovery costs, damage to PCUMC reputation, lawsuits, or even criminal prosecution.

The wireless network will directly affect the security of the patient health and insurance information stored in the ERS. Other sensitive data may or may not be accessed over a wireless connection; you can determine later whether to place that type of restriction on access. With this information, you create a table, listing network resources and their security level, as shown in Table 2-2.

Table 2-2. Network Resource Security Level

Network Resource	Security Level
Scheduling information	Medium
ERS	High
Hospital financial records	High
Employee records	High
Inventory data	Medium
Patient prescriptions	High
Drug database	Medium
Credit card numbers	High

PCUMC overall risk-tolerance level is therefore extremely low.

(Table C-2 in Appendix C, “Site Survey Forms and Tables” is blank so that you can use it to record information about your organization.)

Observe Applicable Regulations

All U.S. health care providers are subject to the Health Insurance Portability and Accountability Act (HIPAA), which includes provisions regarding patient record confidentiality. As a teaching hospital, PCUMC also has to abide by the Family Educational Rights and Privacy Act of 1974 (FERPA), which includes provisions regarding student record confidentiality. However, because it is a non-profit organization, it does not have to comply with the Sarbanes-Oxley Act of 2002 (SOX), which regulates financial disclosure.

HIPAA Regulations. HIPAA mandates that the Department of Health and Human Services (HHS) should establish national standards of security for electronic protected health information (EPHI). (You should refer to the latest regulations that apply to your company.)

For example, of particular concern to the wireless network are the following issues:

- **Physical access to EPHI storage devices (facility access)**—Entities must "implement policies and procedures to limit physical access to [their] electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."
- **User-based authentication protocols**—Entities must "implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights...."
- **Encryption of EPHI, in storage and during transmission**—Entities must "implement a mechanism to encrypt and decrypt electronic protected health information whenever deemed appropriate."
- **Access to EPHI from unauthorized locations or devices**—Entities must "implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."

FERPA Regulations. FERPA does not mandate standards regarding electronic storage or transmission of sensitive data, only that certain types of information cannot be released to the public without the student's written permission. The regulations mandated by HIPAA are probably sufficient to cover FERPA concerns for the network. The rest of FERPA compliance lies in personnel training.

Because your network must provide the highest security to comply with regulations, you decide to purchase and implement a wireless IDS/IPS solution with HP ProCurve RF Manager Controller and HP ProCurve sensors.

Determine Access Control

Given the above regulations and the network resources you outlined in "Determine Risk Tolerance" on page 2-16, you determine the access needs and list them in a table, as shown in Table 2-3.

Table 2-3. User Access Needs

Network Resource	Users	Access Type	Location	Time
Scheduling information	Hospital and office administrative, hospital uncertified medical	Wired and wireless	Hospital L1, office all levels	Office hours
ERS	Hospital and office certified medical	Wired and wireless	All locations	All days, all times
Hospital financial records	Hospital administrative	Wired only	Hospital L1	Office hours
Employee records	Hospital administrative	Wired only	Hospital L1	Office hours
Inventory data	RFID tags	Wireless only	All locations	All times
Patient prescriptions	Hospital and office certified medical	Wired and wireless	All locations	All times
Drug database	Hospital certified medical	Wired and wireless	All locations	All times

As you recall, the hospital medical personnel have been divided into two groups: certified and uncertified. Certified personnel are doctors, registered nurses, pharmacists, and other employees who are permitted to see patient health records. Uncertified personnel are those employees such as orderlies, nurses aides, volunteers, and others who work in patient care but who are not permitted to see patient health information. (All of the medical staff at the office are certified.)

While consulting with PCUMC administrators and IT personnel, you determine that some sensitive information—such as hospital financial records and employee—should not be accessible in some public locations. You further determine that this information should be accessible only during office hours.

Medical information—ERS, the drug database, patient prescriptions—must be available at all times and in all places to certified personnel, so no time or location restrictions will be applied. The RFID system also will not have time or place restrictions.

(Table C-3 in Appendix C, "Site Survey Forms and Tables" is blank so that you can use it to record information about your organization.)

Conduct the Preliminary Site Survey

For your preliminary site survey, you take with you several copies of the floor plans to mark different types of information on each one. You visit the site during the day to observe usage habits.

Define Space Types

The first level of the hospital is definitely “dense office space” because of the many floor-to-ceiling walls. The second level is part dense office space (such as patient rooms, Pain Management, and surgeries) and part “normal office space” (such as Intensive Care, which has only curtain dividers). When you have more than one type of space in an area, you should plan wireless coverage for the more dense space type, so most of the second level is also “dense office space.” The third level is more open, but it still has dividers, so you call it “normal office space.”

In the office building, all levels qualify as “dense office space.”

Identify Obstacles and RF Interference

While surveying any hospital, you should first note the location of the radiology department and any other room where X-rays or other imaging radiation is generated. The shielding for these areas must by law prevent radiation of any type from penetrating the walls, ceiling, or floor. The RF signals for your wireless LAN will therefore be unable to penetrate this shielding.

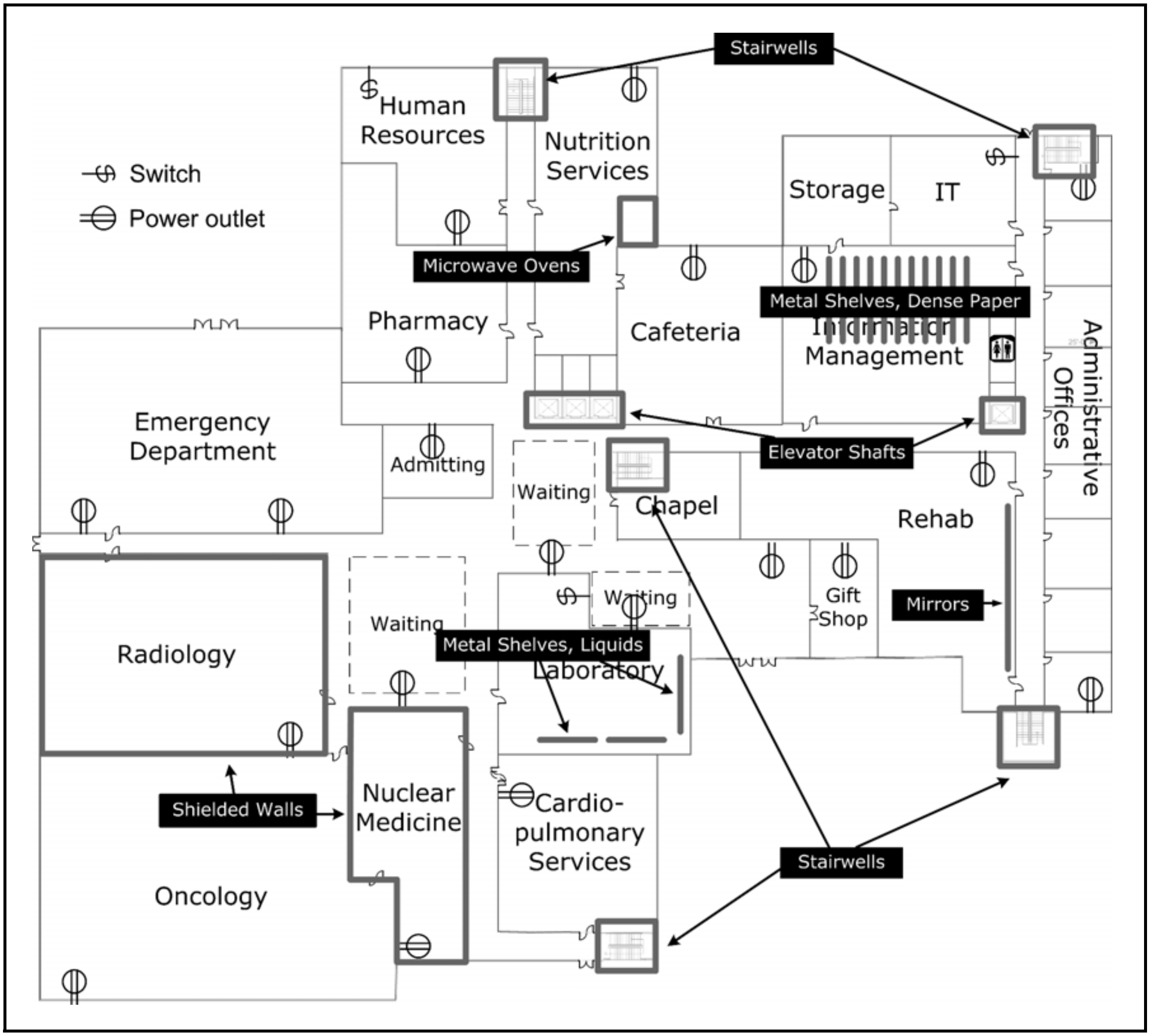


Figure 2-9. Hospital L1—Obstacles and Existing Infrastructure

In the Radiology and Nuclear Medicine departments, you note several shielded rooms.

You then look for tall metal shelving (floor to ceiling) and note what is stored on the shelves. You find the following metal shelves and note their contents and density:

- **Laboratory**—Bottles of liquids, high density
- **Pharmacy**—Bottles of liquids, medium density

- **Nutrition Services**
  - Number 10 cans of foods, bottles of liquids, high density
  - Porcelain dishes, medium density
- **Health Information Management**—Paper patient records, high density
- **IT**—Network equipment rack, high density

Because you will be using RFID tags to track all equipment, you take note of all areas, even those that would ordinarily not need consideration for a wireless LAN. (You would not want to lose track of the equipment because it was moved to a location that does not have wireless coverage.)

Nutrition Services is filled with large metal appliances—a walk-in refrigerator and freezer, ovens stacked two high, and an industrial-sized dishwasher. The ovens generate heat, which can potentially interfere with RF, and the dishwasher has continually moving metal parts that will deflect RF signals differently from moment to moment.

In the neighboring cafeteria, there is a stack of microwave ovens along one wall that will block RF signals. In Rehabilitation, three of the rooms have mirrors covering one wall. These mirrors will reflect all RF waves instead of letting them pass.

As with any structure, you also mark elevator shafts and stairwells, which contain metal and are surrounded by reinforced concrete; and bathrooms, which contain ceramic tile, mirrors, and a high concentration of metal pipes.

In the administrative offices, Human Resources, the pharmacy, and other nonmedical areas, cordless telephones are in use, and you notice a few people, both employees and visitors, wearing wireless headsets for their cellular telephones.

Finally, you mark the location of the network switches (three, including a core switch in IT) and a few convenient power outlets, in case you are unable to provide Power over Ethernet (PoE) for an access point (AP).

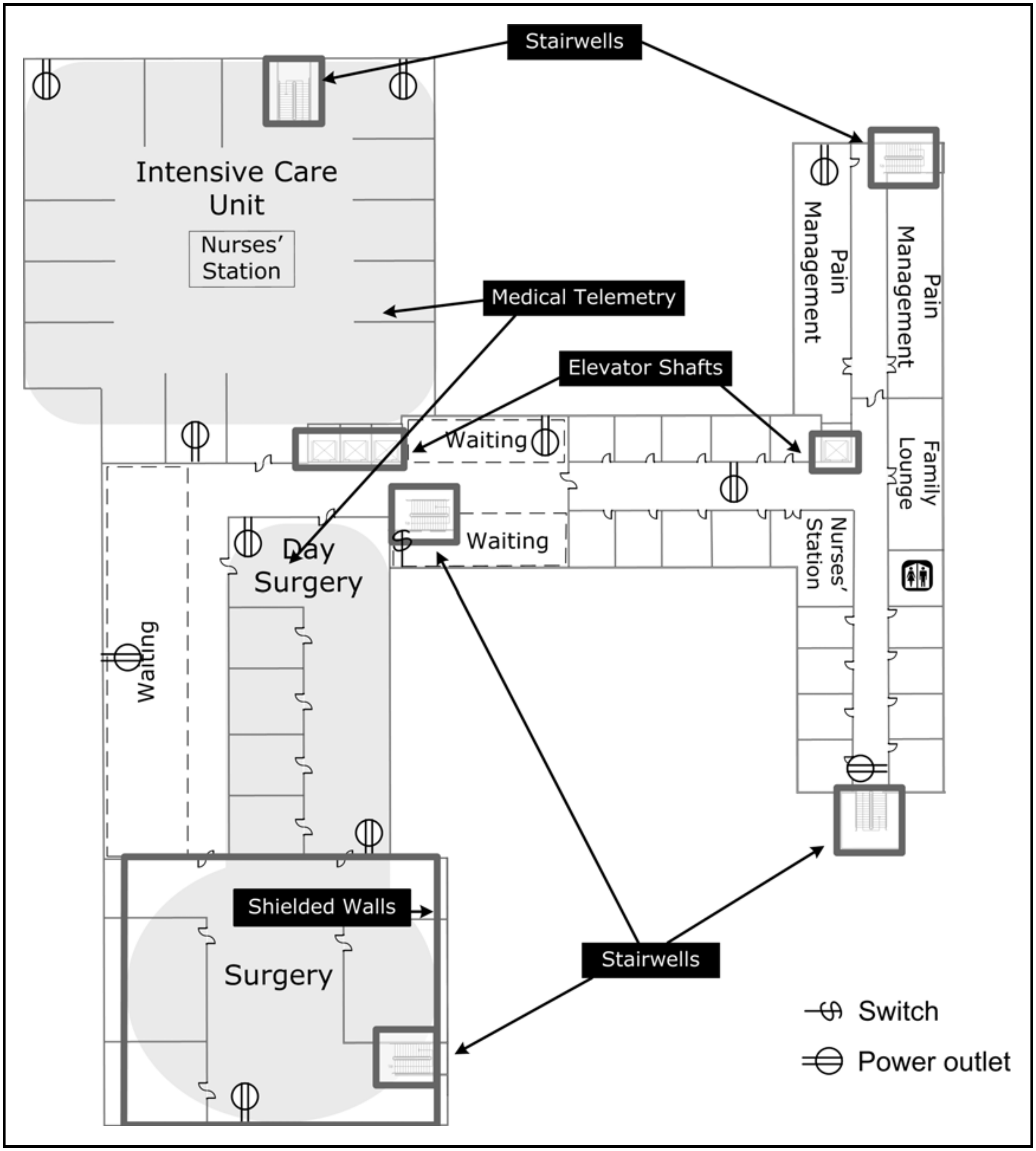


Figure 2-10. Hospital L2—Obstacles and Existing Infrastructure

On the second level, you encounter another shielded area, Surgery, where they sometimes use surgical X-ray machines. (In Day Surgery, they do not.) You also note the storage areas and the bathroom.

You also find that the hospital is already using wireless medical telemetry to monitor patients in the surgical areas and high-risk patients in the Intensive Care Unit. However, they are using Wireless Medical Telemetry Service (WMTS) frequencies, which will not interfere with the WLAN.

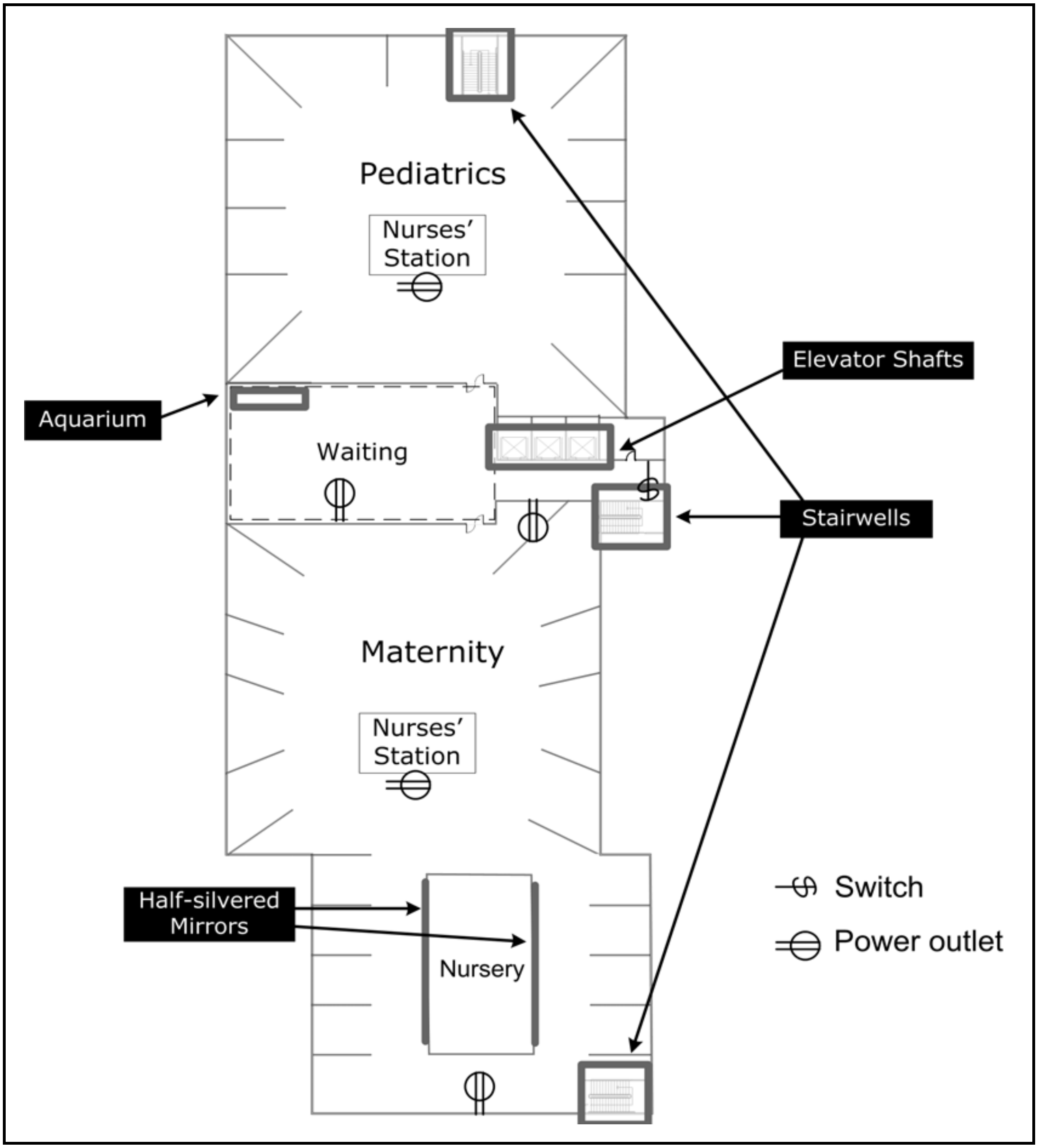


Figure 2-11. Hospital L3—Obstacles and Existing Infrastructure

On the third level you notice a large salt-water aquarium in the waiting area for Pediatrics. You also see that several rooms have one-way mirrors that allow supervisors to observe interns as they examine patients. You also notice the storage areas and bathroom.

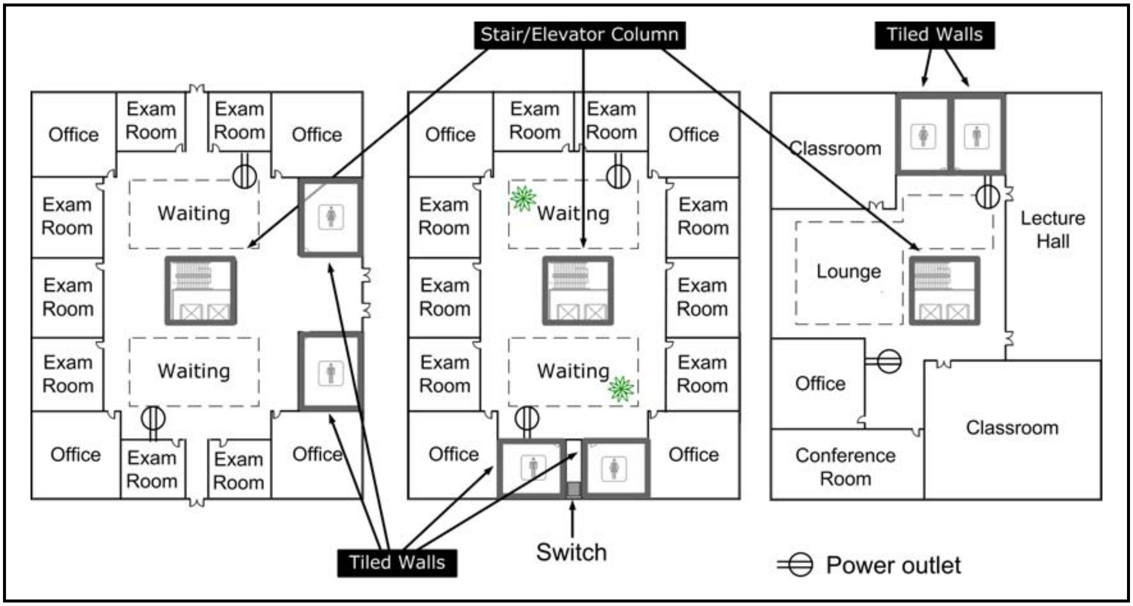


Figure 2-12. Office Building—Obstacles and Existing Infrastructure

In the office building, the primary obstacle is the stair/elevator column in the center of the building. This column of reinforced concrete and metal will block nearly all RF signals.

You also take note of all bathrooms, including the small ones in each doctor's office.

The existing wireless devices and systems are shown in Table 2-4.

Table 2-4. Existing Wireless Systems or Devices

System	Location	Frequency	Range	WLAN Interference
WMTS	Intensive Care Unit Surgical areas	608–614 MHz	10 m	no
Bluetooth headsets	Everywhere	2.45 GHz	10 m	possibly
Cordless telephones	Administration Human Resources Pharmacy	900 MHz	30 m	no

(Table C-4 in Appendix C, "Site Survey Forms and Tables" is blank so that you can use it to record information about your organization.)

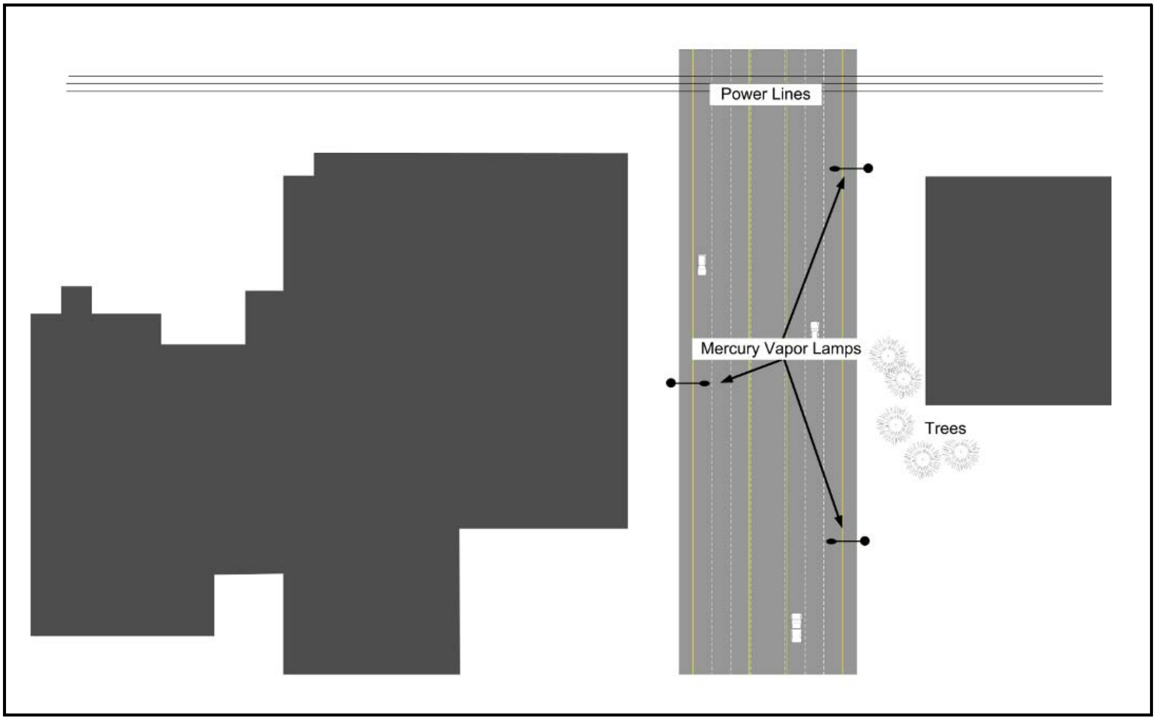


Figure 2-13. Exterior of Hospital and Office Building

While surveying the area between Level 2 of the hospital and the office building, you see pine trees growing near one corner of the office building. These trees could cause interference with the local mesh if the AP is located at that corner of the building.

Another route across the buildings puts the local mesh close to a mercury-vapor streetlight and some high-voltage power lines. High-voltage lines operate at extremely low frequencies (60 Hz in the United States, 50 Hz in the United Kingdom and Europe), but flaws in the transmission lines and equipment can create harmonics in multiples of 50 Hz or 60 Hz that are of a high-enough frequency to interfere with your 2.4 GHz or 5 GHz signals. The mercury vapor lights might also prove to be a problem, but you will need to evaluate how much of a problem through testing.

Evaluate Existing Infrastructure

Because PCUMC (like many organizations) does not have a current network diagram, you must create one that shows the existing network infrastructure. Note all of the switches that you intend to use for APs, any routers or Layer 3 switches, any of the servers that will be part of the installation (such as a RADIUS server for 802.1X authentication), and the network resources to which users will need access. Write down IP addresses and any other information that you consider relevant.

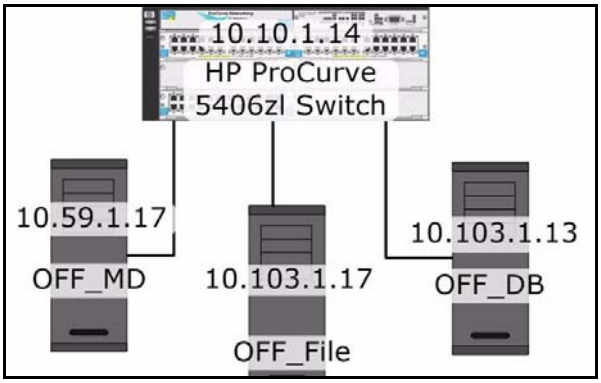


Figure 2-14. Office Building—Existing Network Infrastructure

The network infrastructure in the office building consists of one HP ProCurve 5406zl switch. Two servers, OFF_DB and OFF_File, are the scheduling database and file servers for the office staff, and OFF_MD is a file server for the doctors in that office.

The office building currently does not support Internet or email access, nor is the office-building LAN connected to the PCMCU LAN.

The only security measure requires users to authenticate to the network with a simple username/password combination.

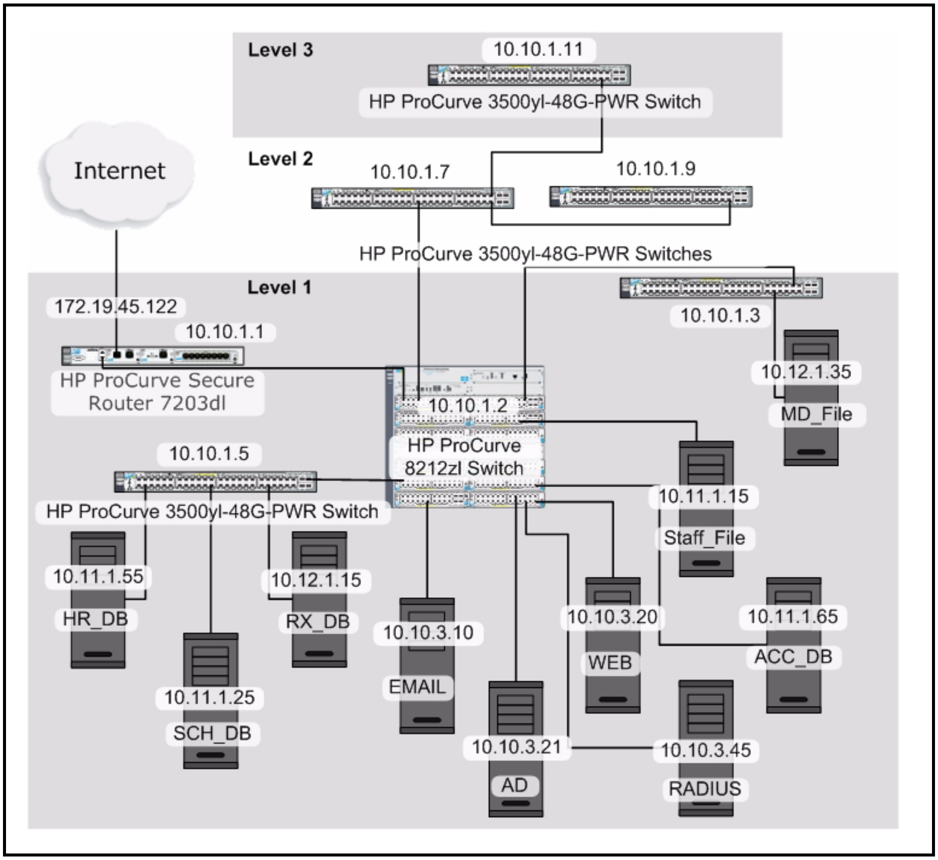


Figure 2-15. Hospital—Existing Network Infrastructure

In the hospital, the core switch is an HP ProCurve 8212zl switch, and five HP ProCurve 3500yl-48G-PWR edge switches connect to it.

There are also Web, email, Active Directory, and RADIUS servers, four databases that contain potentially sensitive information—accounting (ACC_DB), human resources (HR_DB), general drug (RX_DB), and scheduling (SCH_DB).

You record information about the switches, as shown in Table 2-5.

Table 2-5. Existing Network Infrastructure—Switches

Vendor/Model Number	Layer 3	PoE	Free Ports	802.1X	Port Speeds	Uplink Speeds	Location	IP Address
HP 8212zl	Yes	Yes	24	Yes	10/100/1000	10/100/1000	L1, IT room	10.10.1.2
HP 3500yl-48G-PWR	Yes	Yes	7	Yes	10/100/1000	10/100/1000	L1, HR	10.10.1.3
HP 3500yl-48G-PWR	Yes	Yes	9	Yes	10/100/1000	10/100/1000	L1, lab	10.10.1.5
HP 3500yl-48G-PWR	Yes	Yes	11	Yes	10/100/1000	10/100/1000	L2, day surg.	10.10.1.7
HP 3500yl-48G-PWR	Yes	Yes	8	Yes	10/100/1000	10/100/1000	L2, closet	10.10.1.9
HP 3500yl-48G-PWR	Yes	Yes	12	Yes	10/100/1000	10/100/1000	L3, closet	10.10.1.11
HP 5304xl	Yes	No	9	Yes	10/100	10/100	Off L2, closet	10.10.1.14

(Table C-5 in Appendix C, “Site Survey Forms and Tables” is blank so that you can use it to record information about your organization.)

If you plan to implement 802.11n, it is vital that you consider the link speeds of each switch port and the uplink speeds between switches. IEEE 802.11n requires a minimum 1000 bps for the switch port to which the AP is attached; and depending on how much 802.11n traffic you anticipate, you will also need to consider the capacity of the links between switches and the edge router.

Furthermore, many of the 802.11n-capable APs require IEEE 802.3af for Gigabit Ethernet (1000BASE-T) instead of 10/100 Ethernet (10BASE-T and 100BASE-TX), so you will need to ensure that you have the proper type of PoE module or injector for the AP ports.

Because PCUMC plans to implement 802.1X authentication, you must also record information about the RADIUS server(s) and any directory service that you might be using, as shown in Table 2-6.

Table 2-6. 802.1X Infrastructure Devices

802.1X Infrastructure Device			
RADIUS servers	Type: Windows NPS		
	IP address: 10.10.1.45		
Directory services	Type: Windows Active Directory		
	IP address: 10.10.1.21		
	Integrated with RADIUS? yes	yes	no

(Table C-6 in Appendix C, “Site Survey Forms and Tables” is blank so that you can use it to record information about your organization.)

Note

Even if some of your switches are not 802.1X capable, you can still implement the protocol for wireless connections as long as the APs support it.

Servers

Likewise, you must record information about the PCUMC servers, as shown in Table 2-7.

Table 2-7. Existing Servers

Server Name	Function or Contents	IP Address	Security Level
WEB	Web server	10.10.3.20	Low
EMAIL	Email server	10.10.3.10	Medium
RADIUS	RADIUS server	10.10.3.45	High
AD	Active Directory server	10.10.3.21	High
RX_DB	Drug information database	10.12.1.15	Medium
ACC_DB	Hospital finances	10.11.1.65	High
SCH_DB	Scheduling for hospital	10.11.1.25	Medium
HR_DB	Employee records	10.11.1.55	High
OFF_DB	Scheduling for office staff	10.103.1.13	Medium
OFF_File	File server for office staff	10.103.1.17	Medium
OFF_MD	File server for office doctors	10.59.1.17	High

(Table C-7 in Appendix C, “Site Survey Forms and Tables” is blank so that you can use it to record information about your organization.)

Subnets and VLANs

Besides the physical infrastructure, you need to know the logical organization of the network. In PCUMC, the network administrators have already set up VLANs for security purposes. The VLANs that pertain to the office building are shown in the table below; they are assigned to switch ports statically.

Table 2-8. Existing VLANs—Office Building

VLAN ID	Static or Dynamic	IP Address	Switch	Users and Servers
VLAN_59	Static	10.59.1.0/24	10.10.1.14	Office certified medical, OFF_MD
VLAN_103	Static	10.103.1.0/24	10.10.1.14	Office administrative, OFF_DB, OFF_File

(Table C-8 in Appendix C, “Site Survey Forms and Tables” is blank so that you can use it to record information about your organization.)

Most of the VLANs in the hospital, however, are assigned dynamically through a RADIUS server. VLAN_11 is reserved for those employees who work in administrative tasks such as records and admitting. VLAN_12 is for certified medical personnel, and VLAN_13 is for uncertified medical personnel.

Table 2-9. Existing VLANs—Hospital

VLAN ID	Static or Dynamic	IP Address	Switches	Users and Servers
VLAN_10	Static	10.10.0.0/16	10.10.1.2 10.10.1.3 10.10.1.5 10.10.1.7 10.10.1.9	Servers such as RADIUS, WEB, AD, EMAIL
VLAN_11	Dynamic (RADIUS)	10.11.0.0/16	10.10.1.2 10.10.1.5	Hospital administrative, ACC_DB, SCH_DB, HR_DB
VLAN_12	Dynamic (RADIUS)	10.12.0.0/16	10.10.1.2 10.10.1.3 10.10.1.5 10.10.1.7 10.10.1.9	Hospital certified medical personnel, RX_DB
VLAN_13	Dynamic (RADIUS)	10.13.0.0/16	10.10.1.2 10.10.1.3 10.10.1.5 10.10.1.7 10.10.1.9	Hospital uncertified medical personnel

You will use this information later when you plan your VSCs.

Plan the Equipment Layout

At this point, you know enough to decide which devices and solutions suit your needs.

Select a Physical Layer

The hospital has several types of devices with different bandwidth requirements and with different capabilities. For example, the RFID tags only support 802.11b. On the other hand, you would like to use pure 802.11n for connections to the private WLAN. And, although your budget does not permit you to upgrade all of your 802.11b/g clients to 802.11n, you do want to begin upgrading some. Finally, while you cannot be sure of which 802.11 standards guests' devices will support, you do know that most laptops now support 802.11a/b/g.

Because all of these devices will be connecting in the same areas, you must carefully plan the Physical Layer settings for your radios to accommodate all of the devices.

One approach is to configure all AP radios to support every VSC to which your devices connect. In this case, the radios should support 802.11n with backward compatibility for 802.11b/g.

In another approach, you could carefully plan the deployment so that AP radios support different VSCs and different Physical Layer standards. For example, you could deploy several APs that support the private VSC and provide 802.11n, several APs that support the private VSC and provide 802.11b/g, and several APs that support the RFID VSC and provide 802.11b. You could set the pure-802.11n radios to use the 5 GHz frequency. However, you would need to make sure that the 802.11g and 802.11b radios are set to non-overlapping channels.

For the hospital, you decide to take a hybrid approach. You will set some radios to 802.11b/g. These radios will support all types of users. You will set other radios to support pure-802.11n in the 5 GHz frequency. These radios will support private users and ERS devices.

For the local mesh, you decide to use both 802.11n and 802.11a because of the amount of data that the links need to support. You decide to bond channels 52 and 56 on radio 1 and use channel 152 on radio 2. These channels are approved for outdoor use in the United States, as long as the AP supports

Dynamic Frequency Selection (DFS), which the HP ProCurve MultiService Mobility (MSM)422 AP does. Government and military radar may also use these channels, so DFS forces the AP radio to change channels if it detects interference. Changing channels can briefly interfere with the local mesh, but MSM422s have the capability to recover.

In summary, PCUMC will be using the channels listed in Table 2-10.

Table 2-10. Physical Layer Decisions

System	Physical Layer	Frequency (GHz)	Channels	VSCs
Hospital	802.11n	5	36	private
	802.11b/g	2.4	1,6,11	RFID, private, public
Office Building	802.11n	5	36	private
	802.11b/g	2.4	1,6,11	RFID, private, public
Radios that support the local mesh	802.11n	5	52 & 56	—
	802.11a turbo	5	152	

(Table C-9 in Appendix C, “Site Survey Forms and Tables” is blank so that you can use it to record this information for your organization.)

Choose the Type of AP Architecture

You decide that the best option for the hospital is the optimized WLAN architecture with a combination of distributed and centralized intelligence. The sheer number of radios that will be needed to provide coverage makes it practical to have a centralized configuration for all of them, so you will plan to deploy at least one MSM Controller.

The RFID tags and ERS carts will be roaming throughout the entire hospital, so you want to maintain consistency throughout the site for the AP settings, and you want to allow the APs to forward all traffic directly onto the network. However, you want to use the controller built-in Web login page for guests (the public VSC), so on this VSC you will use a centralized intelligence approach.

In the office building, you also decide on a similar approach. On the first and second floors the network is open to patients and visitors, so APs in this area will support the public VSC, which will use an optimized WLAN architecture with centralized intelligence. However, both the RFID and private VSCs will use an optimized WLAN architecture with distributed intelligence.

For the local meshes, you will use four APs in controlled mode to create a dynamic mesh. Two of the APs will serve as masters to which the other two APs can connect. This builds redundancy into the local mesh. In the event that one of the masters fails, the other APs can connect to the second master.

Again, you record these settings, as shown in Table 2-11.

Table 2-11. Architecture Decisions for PCUMC

Location	Architecture
PCUMC Hospital	Optimized WLAN with both centralized and distributed intelligence
PCUMC Office Building	Optimized WLAN with both centralized and distributed intelligence
Local Mesh	Dynamic mesh in controlled mode

(Table C-10 in Appendix C, "Site Survey Forms and Tables" is blank so that you can use it to record information about your organization.)

Select the Equipment

Although you could manage both the PCUMC hospital and office building networks with a single MSM controller (if you were controlling less than 200 APs), because you are connecting the two networks with a local mesh, to provide network independence you should choose to an MSM Mobility Controller in each building. You will join your controllers in a team. Therefore, in the event that one controller fails, its APs will fail over to another controller in the team. If the local mesh goes down, and a controller loses contact with the team manager, each controller will continue to function independently until the team can be reformed. This builds both controller and AP redundancy into the solution.

You select the MSM765zl Mobility Controller for your controllers because it can control the largest number of users and APs and is installed in the existing 8212zl and new 5406zl switches.

To work alongside the MSM765s, you will deploy MSM422 APs, which will provide the 802.11n coverage and 802.11b/g for your wireless network. You will also deploy several MSM320 APs to provide more (non-802.11n) coverage in public areas in particular. You will also deploy MSM415 Sensors, which can monitor 802.11a/b/g/n transmissions, to collaborate with RF Manager in protecting the network.

For each local mesh, you will use four MSM422s. You will configure a dynamic mesh with two masters and two slaves, providing failover protection should any one AP fail. This dynamic mesh configuration will also significantly increase the mesh throughput when all APs are functioning at full capacity. You will use the APs as dedicated radio bridges, using both of each AP's radios for the mesh. And you will enable Spanning Tree Protocol (STP) to prevent network loops.

PCUMC hardware is recorded in Table 2-12.

Table 2-12. Initial WLAN Hardware Decisions

Location	Hardware
Hospital	MSM765zl Mobility Controller
	MSM422 APs
	MSM320 APs
	MSM415 Sensors
Office Building	MSM765zl Mobility Controller
	MSM422 APs
	MSM320 APs
	MSM415 Sensors
Local Mesh	MSM422s

(Table C-11 in Appendix C, "Site Survey Forms and Tables" is blank so that you can use it to record information about your organization.)

For the ERS carts, you decide on network interface cards (NICs) that support 802.11b/g and have a sensitivity of –71 to –94 dBm. The operating system of the laptops that are positioned on the carts already includes an 802.1X supplicant.

For new employee laptops, you will choose NICs that support 802.11b/g/n or 802.11a/n and have a receiver sensitivity of –71 to –94 dBm. Almost all OSs currently installed on laptops have a built-in wireless client and 802.1X supplicant.

For the local mesh, you will choose antennas according to HP ProCurve RF Planner predictions.

Choose a Management Solution

The university already uses HP ProCurve Manager Plus (PCM+) with HP ProCurve Identity Driven Manager (IDM) to control wired and wireless user access in the office building. In the hospital, the RADIUS solution has been sufficient thus far, and it would *technically* be possible to configure the existing Network Policy Server (NPS) to place time and location restrictions on user access; but because IDM provides unified wired/wireless network management plus easy user-access configuration, switching to PCM+ is a logical decision. The hospital therefore configures IDM to manage configuring dynamic settings on NPS.

You will use the MSM765zl Mobility Controllers to manage the APs.

As mentioned earlier, you have also chosen to purchase an HP ProCurve RF Manager Controller to help manage network security on your wireless network.

Plan Coverage and Capacity with RF Planner

You now have enough information to begin to plan your wireless implementation. The first step will be to create a diagram of your site and place your MSM APs.

This section provides an example of using HP ProCurve RF Planner to plan coverage. Detailed instructions on how to use RF Planner are outside the scope of this design document. See the *HP ProCurve RF Planner Admin Guide* and the *HP ProCurve Multiservice Mobility Implementation Guide*.

You can also use HP ProCurve Mobility Manager (PMM) to plan RF coverage. See the *HP ProCurve Manager Network Administrator's Guide Version 3.10 (includes PMM 3.01)*.

Indoor Locations

First, you create location nodes, upload floor plans for your site, specify other properties and dimensions of the space, add objects that might affect RF propagation, and enable the RF maps. RF Planner provides map types or views to aid you in planning your wireless implementation. The most effective way to use the RF maps is usually as follows:

1. Place APs using the WLAN planning wizard.
2. If you have chosen to use the RF Manager Controller as part of your security solution, manually place your sensors.
3. Start with **Coverage View** evaluation, and then view the coverage with spillage. You should evaluate the **Coverage View** for each 802.11 standard in each frequency band. Adjust the transmit power levels for each radio, move the APs, and add external antennas until you have the desired amount of coverage in each operating mode.

4. Switch to **Redundancy View** and add more APs, if necessary, until you have the desired level of redundancy.
5. In **Link Speed View**, ensure that you can provide the desired link speeds, adding more APs as necessary.
6. In **Interference View**, select channels and adjust the transmit power levels for each radio, move the APs, or reassign channels until you have minimized the amount of interference. For multifloor buildings, be sure to assess cross-floor interference.
7. Check each RF map again to ensure that the final adjustments you have made did not adversely affect the link speeds, coverage, or redundancy.
8. For the **Calibration Points View**, the planner creates points at which you should physically check the RF signal once you have deployed your devices.

If you have multiple levels in the building plan, add each level to the building plan and follow the same procedure.

Example Plan

When beginning to plan the layout of your APs, you should start using the WLAN planning wizard. Using the wizard, you can place devices according to one of two planning objectives.

- **Coverage Planning** ensures that your entire space is covered by the wireless network with a specified minimum data rate. This is the best option if you are not necessarily concerned about whether the network can support certain applications.
- **Capacity Planning** ensures that your entire space is covered by the wireless network *and* that your network meets specified user application requirements.

In this example, you want to ensure that all areas receive coverage at a basic minimum data rate, but are not concerned that user application requirements are met. Therefore, you will use coverage planning to place your APs.

Note

Because this chapter is meant to provide a broad overview of designing a wireless network, this guide will only show the full decision-making process for a single level of the office building. However, the same process should be followed for each level of each site.

Coverage View

Once you place your devices using the WLAN planning wizard, the coverage view is displayed. By default, this view shows the coverage for all 802.11 standards in all frequency bands.

The coverage appears as shown in Figure 2-16.

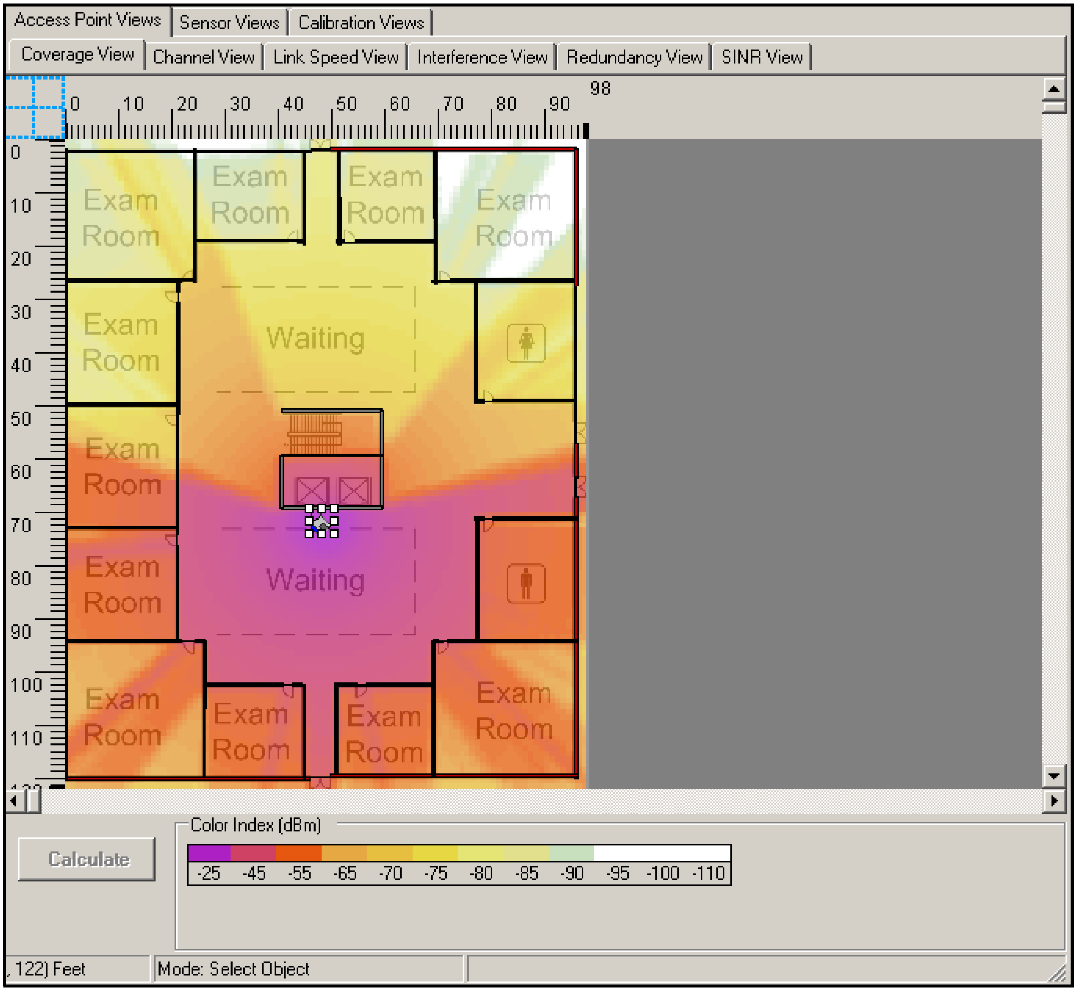


Figure 2-16. RF Planner—Initial Coverage View

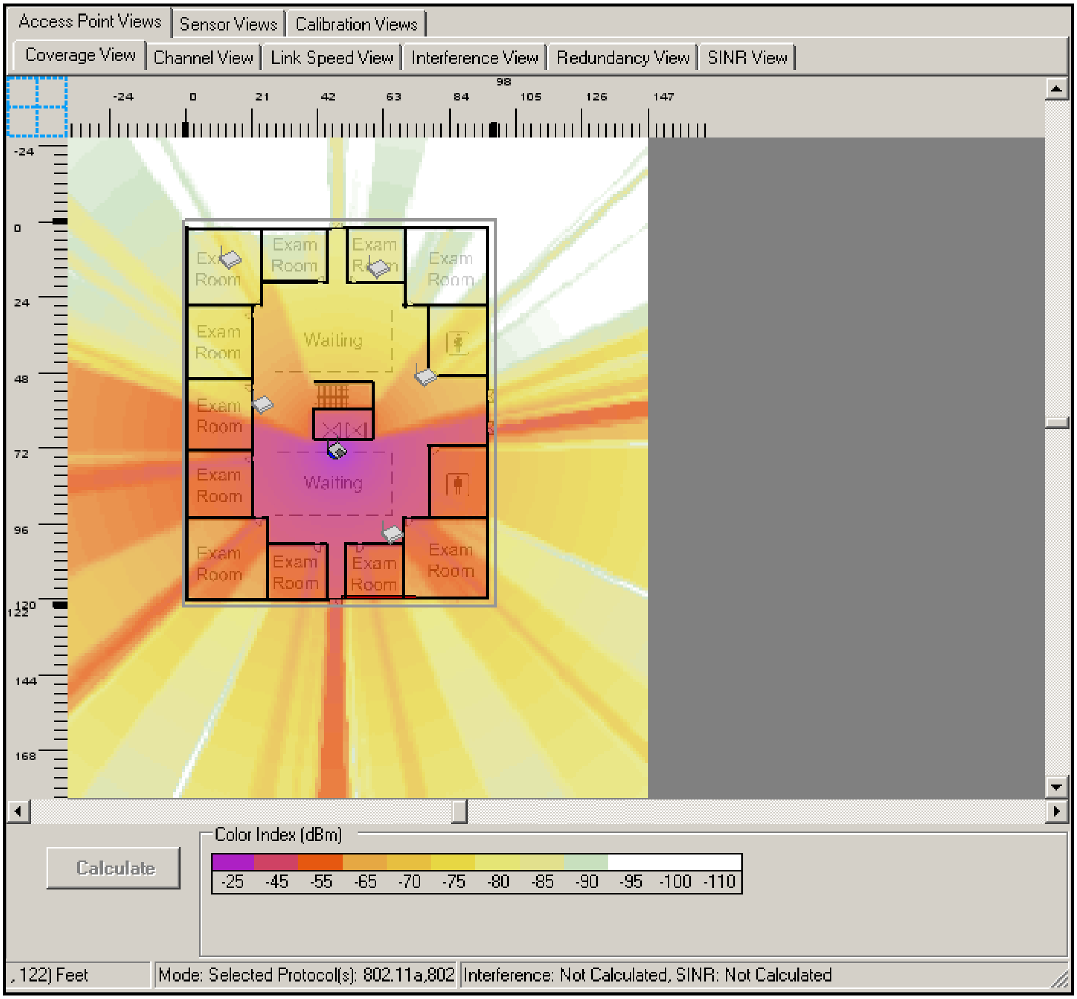
Figure 2-16 shows the RF coverage for the example site with Medium Signal Certainty Level and an accuracy level of 1, predicting the most likely range of APs. Each color corresponds to a range of signal levels.

If you used a .gif file for your location map, the RF signal level is displayed as shades of grey. If you used a .jpg file (as in this example), the RF signal level is displayed according to the color index at the bottom of the window. It is much easier to read the RF signal levels when using a .jpg file, so ProCurve Networking strongly recommends using this file format for your location map.

The strongest signal—the signal that you want—is indicated by the purple color that surrounds the AP in Figure 2-16. The weakest signal is indicated by the white color in the upper-right-corner exam room.

802.11n (5 GHz) Coverage View. In the example network, you are using 802.11n in the 5 GHz band and 802.11b/g on your network, so you should evaluate coverage for each of these operating modes.

The Coverage View for 802.11 in the 5 GHz band is shown in Figure 2-17.

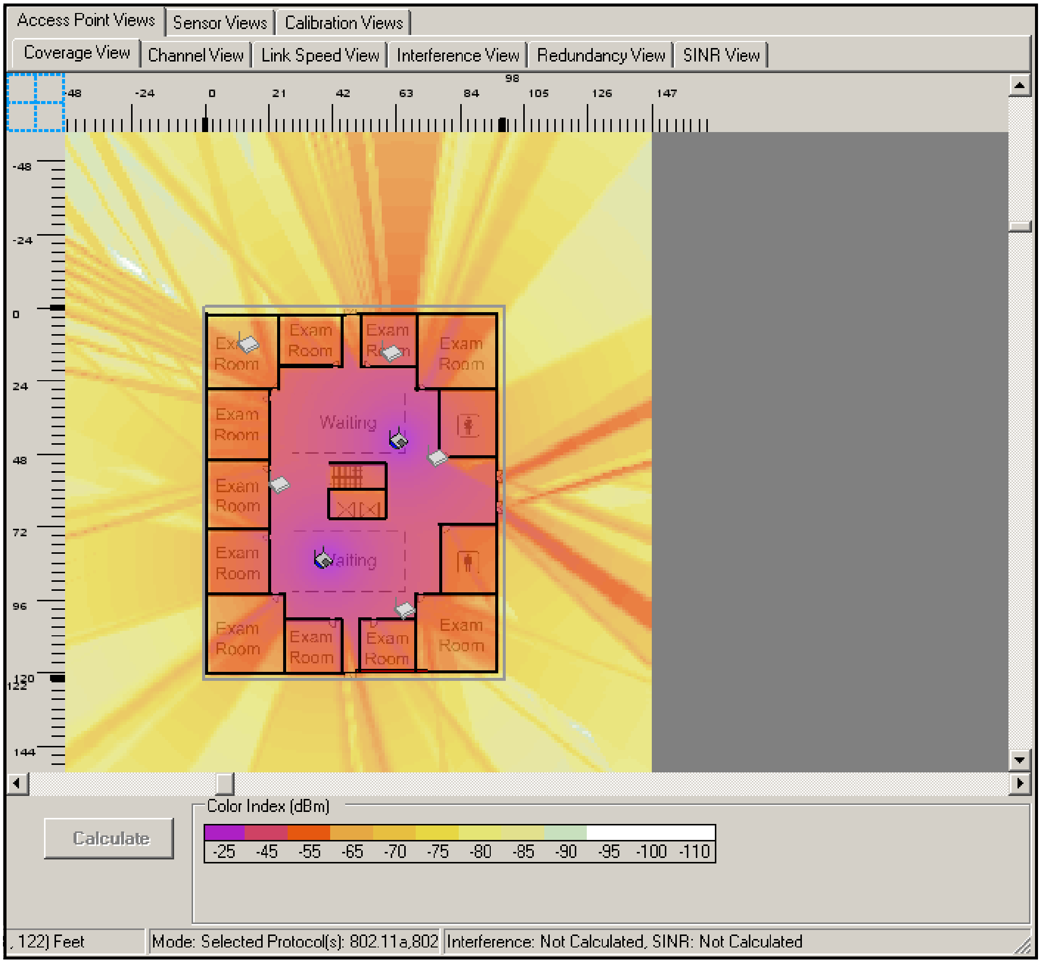


, 122) Feet | Mode: Selected Protocol(s): 802.11a,802 | Interference: Not Calculated, SINR: Not Calculated

Figure 2-17. RF Planner—Initial Coverage View (802.11n 5 GHz with Spillage)

You can see that the coverage is good in the lower sections of the building, but the signal is weak in the upper sections, especially in the upper-right-corner exam room.

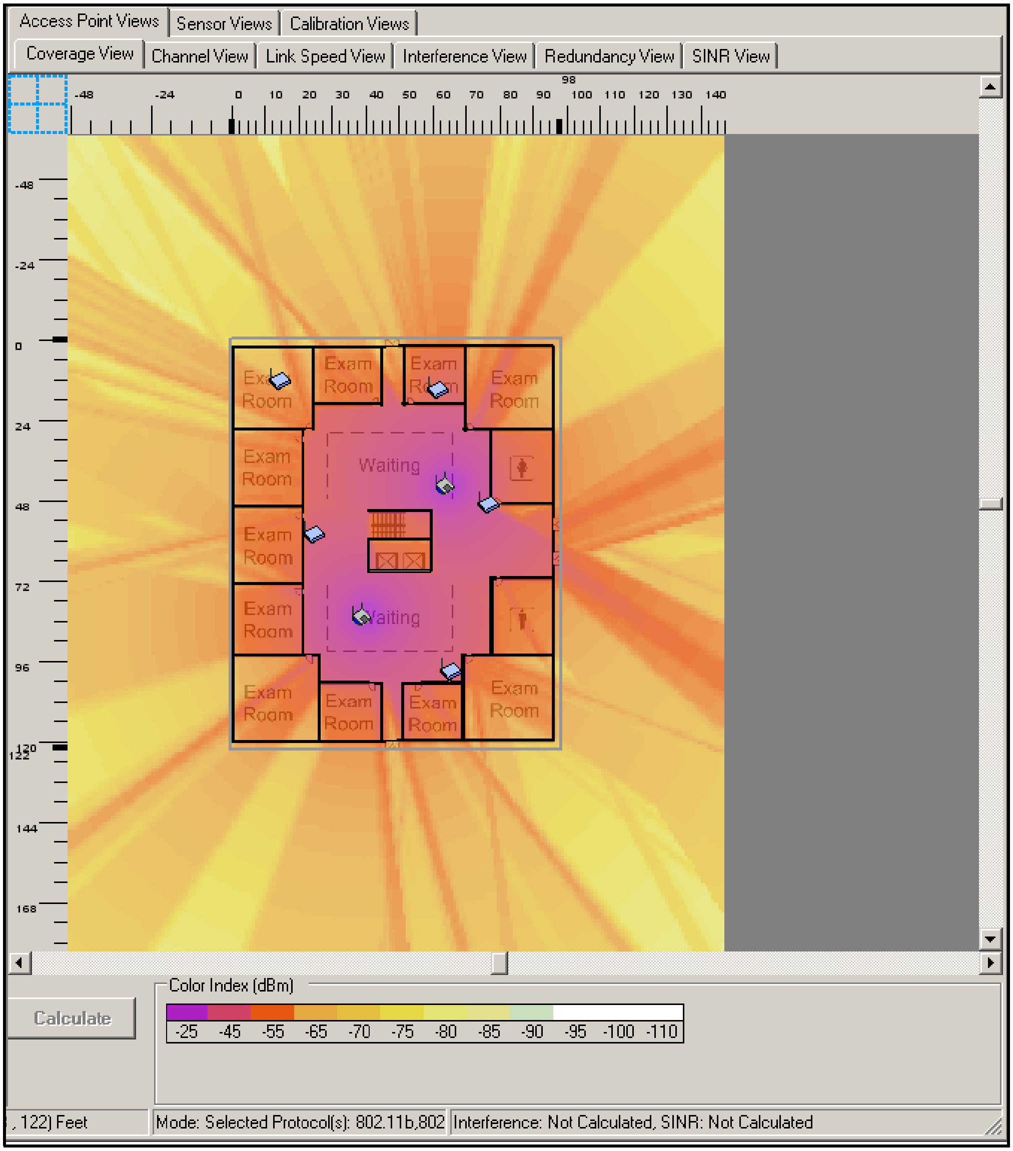
Figure 2-18 shows the layout after a new AP and five new sensors have been added and the transmit power on each AP has been decreased. After evaluating coverage with external antennas, administrators decide not to purchase any external antennas. They are satisfied with the coverage in Figure 2-18. Although there is still significant signal leakage outside of the building, the signal is not strong enough to be of concern.



, 122) Feet | Mode: Selected Protocol(s): 802.11a,802 | Interference: Not Calculated, SINR: Not Calculated

Figure 2-18. RF Planner—Access Point Coverage View (Adjusted 802.11n Coverage with Spillage)

802.11b/g Coverage View. The Coverage View for 802.11b/g after all adjustments have been made is shown in Figure 2-19. The network administrators have reduced the transmit power on both of the APs.

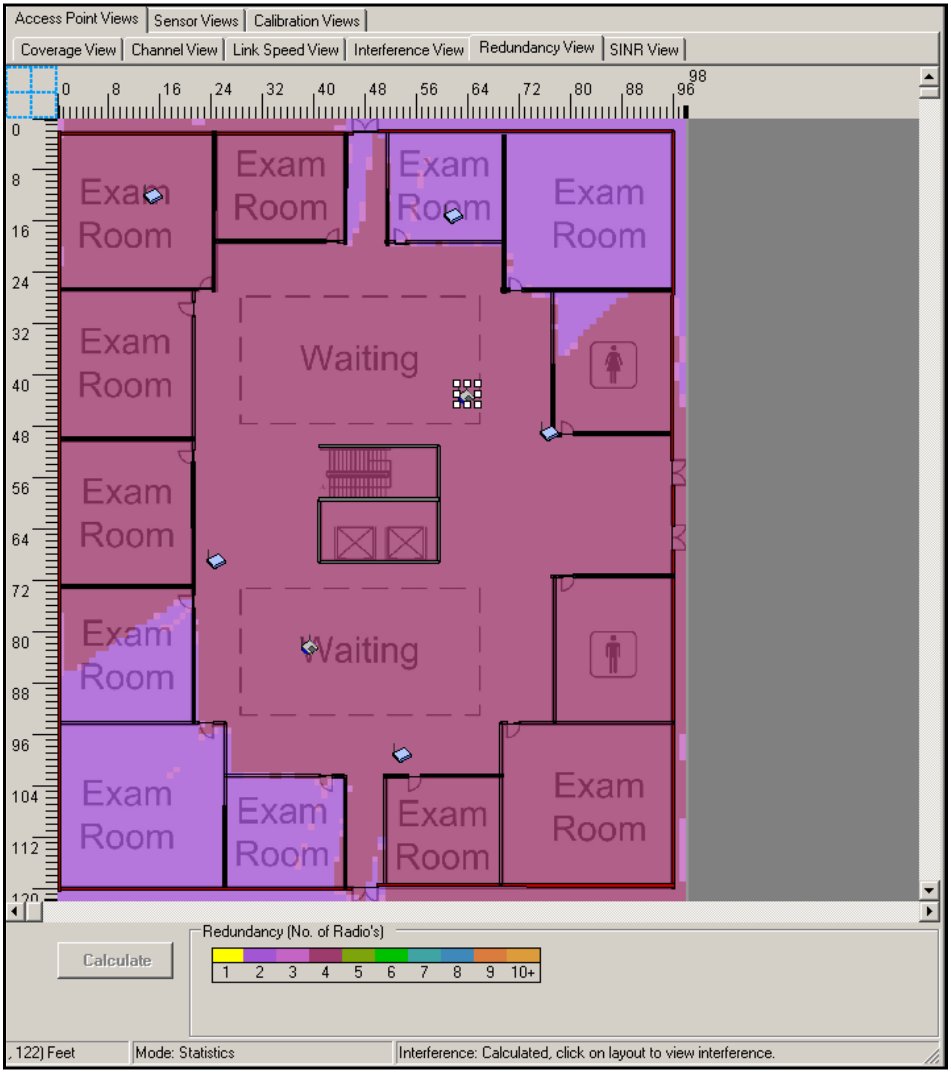


, 122) Feet | Mode: Selected Protocol(s): 802.11b,802 | Interference: Not Calculated, SINR: Not Calculated

Figure 2-19. RF Planner—Access Point Coverage View (Adjusted 802.11b/g Coverage)

Redundancy View

To ensure that your network will provide access in the unlikely event that one of your APs fails, you should check your network redundancy. Every point of your layout should be covered by at least two APs (or more if your site requires).



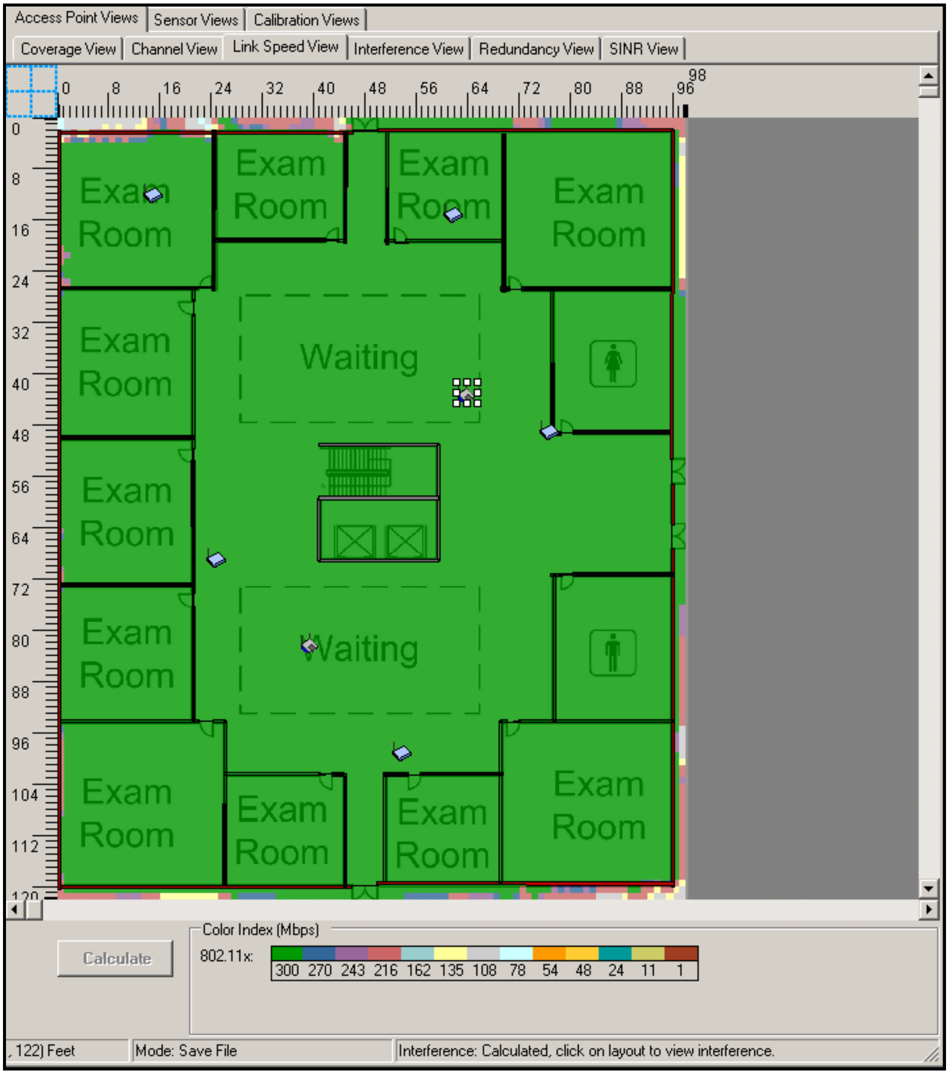
, 122) Feet | Mode: Statistics | Interference: Calculated, click on layout to view interference.

Figure 2-20. RF Planner—Access Point Redundancy View

Figure 2-20 verifies that every point of the example layout is covered by at least two APs.

Link Speed View

The **Access Point Link Speed** view shows the maximum 802.11 downlink connection speed available at each point on the layout. You will use this layout to ensure that you have planned for the appropriate link speed for your environment.



Color Index (Mbps)

802.11x:	300	270	243	216	162	135	108	78	54	48	24	11	1

, 122) Feet | Mode: Save File | Interference: Calculated, click on layout to view interference.

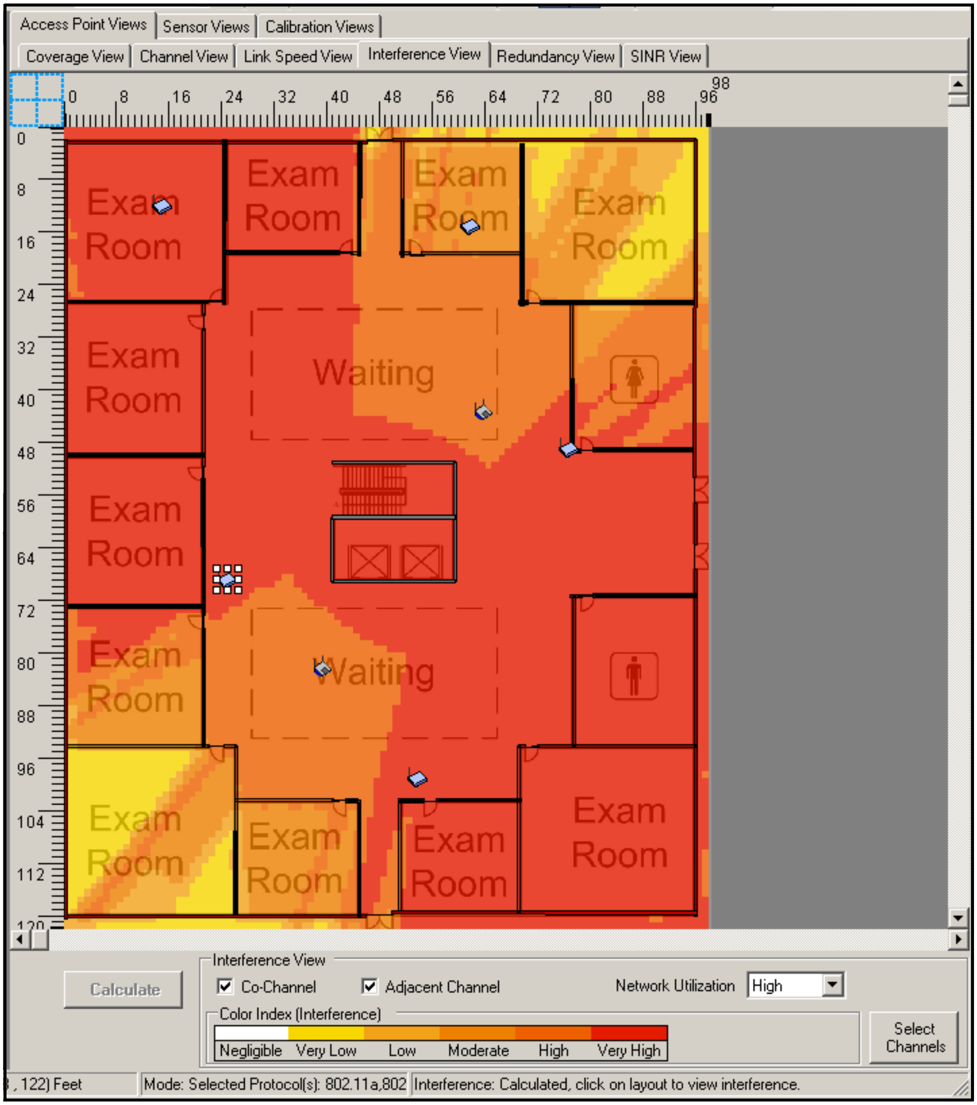
Figure 2-21. RF Planner—Access Point Link Speed View

The link speed is displayed according to the color index at the bottom of the window. The dark green color represents areas with the highest link speed, whereas the brown color represents areas with the lowest link speed. If any section of your layout does not have the link speed you want, you should adjust your radio power settings.

In Figure 2-21, the entire layout is supported by a link speed of 300 Mbps—the best link speed available—so you do not need to adjust any of the radio transmit powers.

Interference View

Based on the signal strength of different access points operating on the same channel at your site, the Interference View displays where and how strong interference is, helping you minimize it to provide better network connectivity and throughput. You can choose to view co-channel, adjacent channel, or total interference. The different colors represent the amount of interference, which ranges from negligible to very high.



☑ Co-Channel ☑ Adjacent Channel

Network Utilization: High

, 122) Feet

Mode: Selected Protocol(s): 802.11a,802

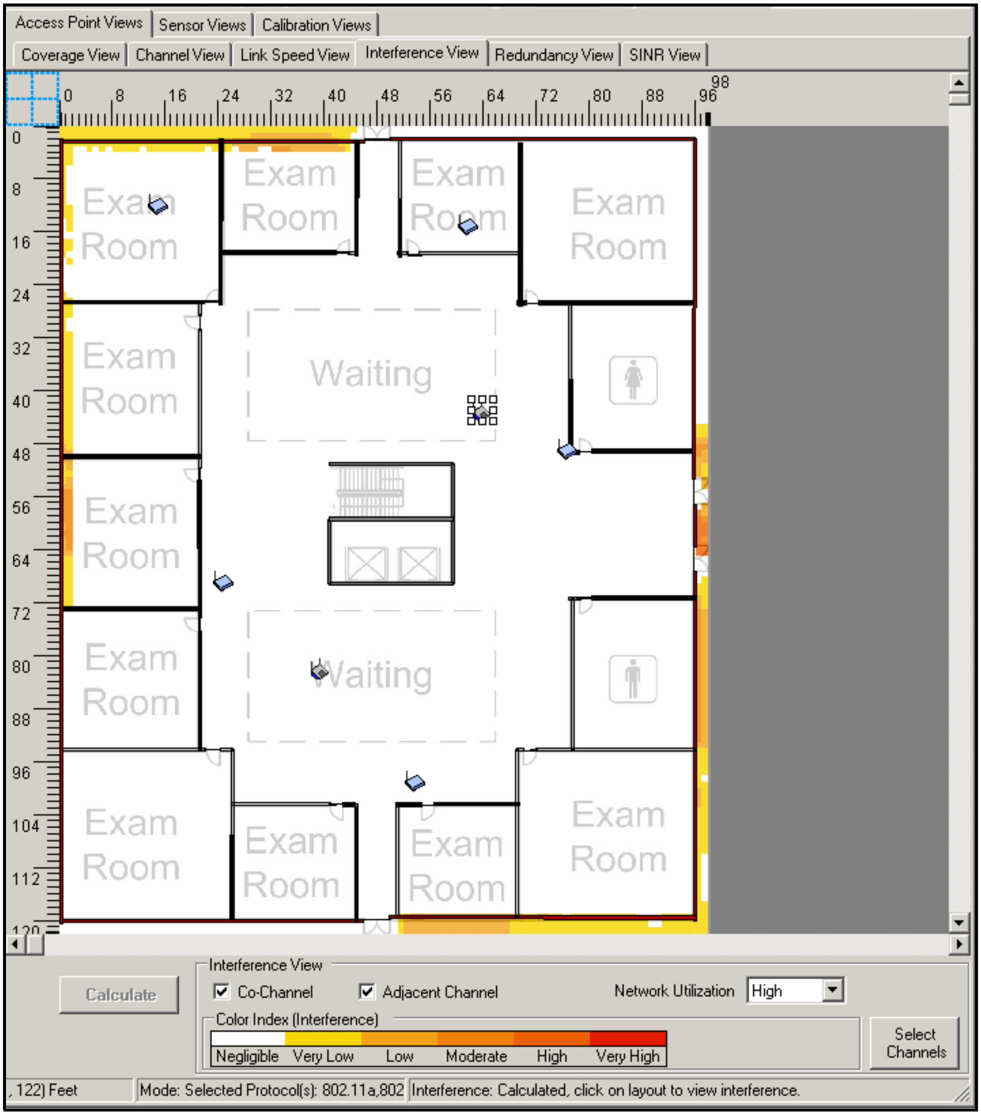
Interference: Calculated, click on layout to view interference.

Figure 2-22. RF Planner—Interference View

The Interference View in Figure 2-22 shows that the signals interfere with each other almost everywhere. You have not yet assigned the AP channels, so significant interference is to be expected.

Auto Channel Assignment. To solve the problem, you should assign channels using the **Auto Channel** tool, and then view one channel at a time and adjust the transmit power levels until interference is minimized.

Figure 2-23 shows the layout once the channels have been adjusted.



Interference View

☑ Co-Channel ☑ Adjacent Channel

Network Utilization: High

Color Index (Interference): Negligible, Very Low, Low, Moderate, High, Very High

,122) Feet | Mode: Selected Protocol(s): 802.11a,802 | Interference: Calculated, click on layout to view interference.

Figure 2-23. RF Planner—Access Point Interference View

Cross-Floor Interference. After adjusting the radio settings for the floor to minimize interference, you should check the cross-floor interference by adjusting RF Planner filters.

In this example, only the first floor has been configured in RF Planner, so there is no cross-floor interference. If your layout does have cross-floor interference, you should adjust the signal strength, placement, and channels of the APs on each floor.

Calibration Points

Switch to **Calibration View** to see the points at which you should check your *actual* AP signal strength. After you deploy your APs, you should measure the signal at each of these points. Then return to the Calibration View and input the results. This will allow RF Planner to more accurately predict your coverage. Once you add your measurements, you should recheck each view to ensure that the newly predicted coverage is still sufficient.

Outdoor Locations

When planning outdoor locations, you follow steps similar to those for an indoor location. However, because you are often very limited in the available positions for AP placement, you will probably need to manually place your AP.

1. Place APs manually or using the WLAN planning wizard.
2. If you have chosen to use the RF Manager Controller as part of your security solution, manually place your sensors.
3. Start with **Coverage View** evaluation, and then view the coverage with spillage. You should evaluate the **Coverage View** for each 802.11 standard in each frequency band. Adjust the transmit power levels for each radio, move the APs, and add external antennas until you have the desired amount of coverage in each operating mode.
4. Switch to **Redundancy View** and add more APs, if necessary, until you have the desired level of redundancy.
5. In **Link Speed View**, ensure that you can provide the desired link speeds, adding more APs as necessary.
6. In **Interference View**, select channels and adjust the transmit power levels for each radio, move the APs, or reassign channels until you have minimized the amount of interference.
7. Check each RF map again to ensure that the final adjustments you have made did not adversely affect the link speeds, coverage, or redundancy.

8. For the **Calibration Points View**, the planner creates points at which you should physically check the RF signal once you have deployed your devices.

If you have multiple levels in the building plan, add each level to the plan and follow the same procedure.

Example Plan

In this example, PCUMC is planning a local mesh to link the office building with the hospital. You can use RF Planner to plan this link and ensure that the APs will have the signal strength to support the necessary bandwidth.

To plan the local mesh, you can use the formulas in “Calculations for Transmission Range” in Appendix B, “Reference Tables” or you can use the RF Planner and create an outdoor layout. In this example, you will add an outdoor location node to the PCUMC project.

Figure 2-24 shows the speed link view for PCUMC local mesh between the office building and the hospital after the APs have been manually placed in their initial positions.

Note Although the signal for the local mesh is directed outdoors, the MSM422 APs *themselves* are designed for outdoor implementations.

Note If your outdoor layout is meant for users, you should follow the same method you used for the indoor layout.

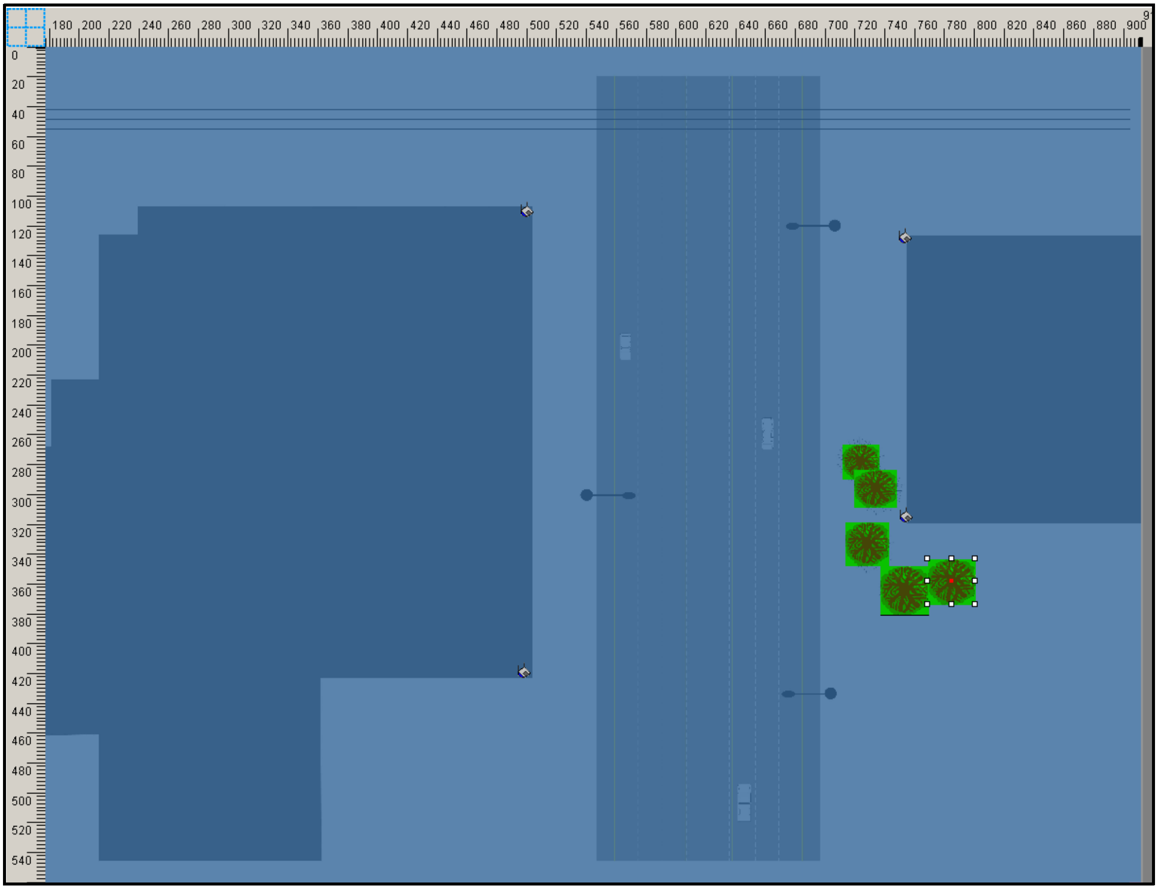


Figure 2-24. RF Planner—Access Point Link Speed View

Figure 2-24 shows that the outdoor APs provide a link speed of approximately 270 Mbps. The signal, however, is not directed across the local mesh: it is uniform throughout the layout. Therefore, administrators decide to add 18-dBi Yagi antennas to each AP 802.11n external antenna connectors.

External Antennas

PCUMC administrators have decided to add external antennas to the local mesh APs in order to direct the signal. The MSM422 includes four external antenna connectors—three for the 802.11a/b/g/n radio, which supports Multiple-Input, Multiple Output (MIMO), and one for the 802.11a/b/g radio.

Figure 2-26 shows the Access Point Link Speed View after the external antennas have been added to all four APs.

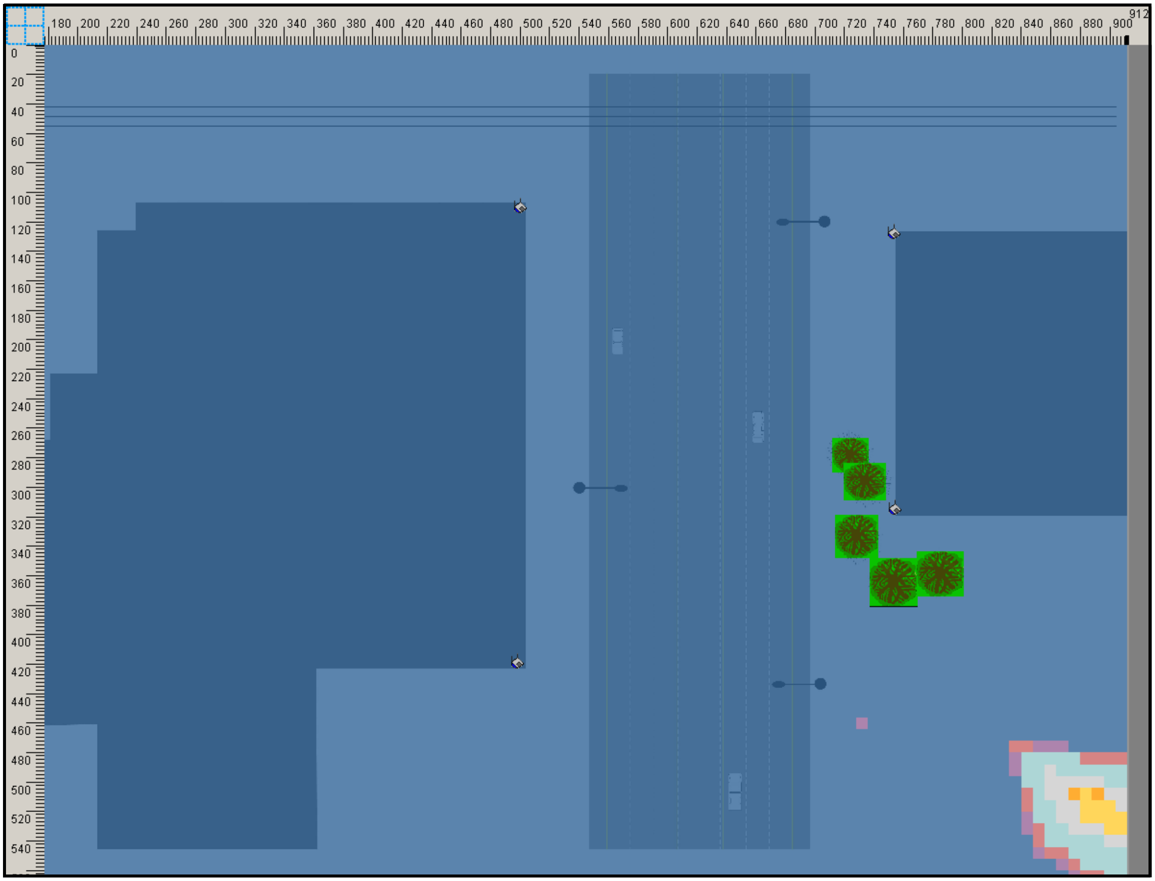


Figure 2-25. RF Planner—Access Point Link Speed View (with External Antennas)

You can see that the link speed across most of the layout is still approximately 270 Mbps, although the RF Planner now predicts a slightly lower link speed in the lower right corner of the layout.

To get a better idea of what the overall coverage and concentration of the signal looks like, you should check the **Access Point Coverage View**, as shown in Figure 2-26.

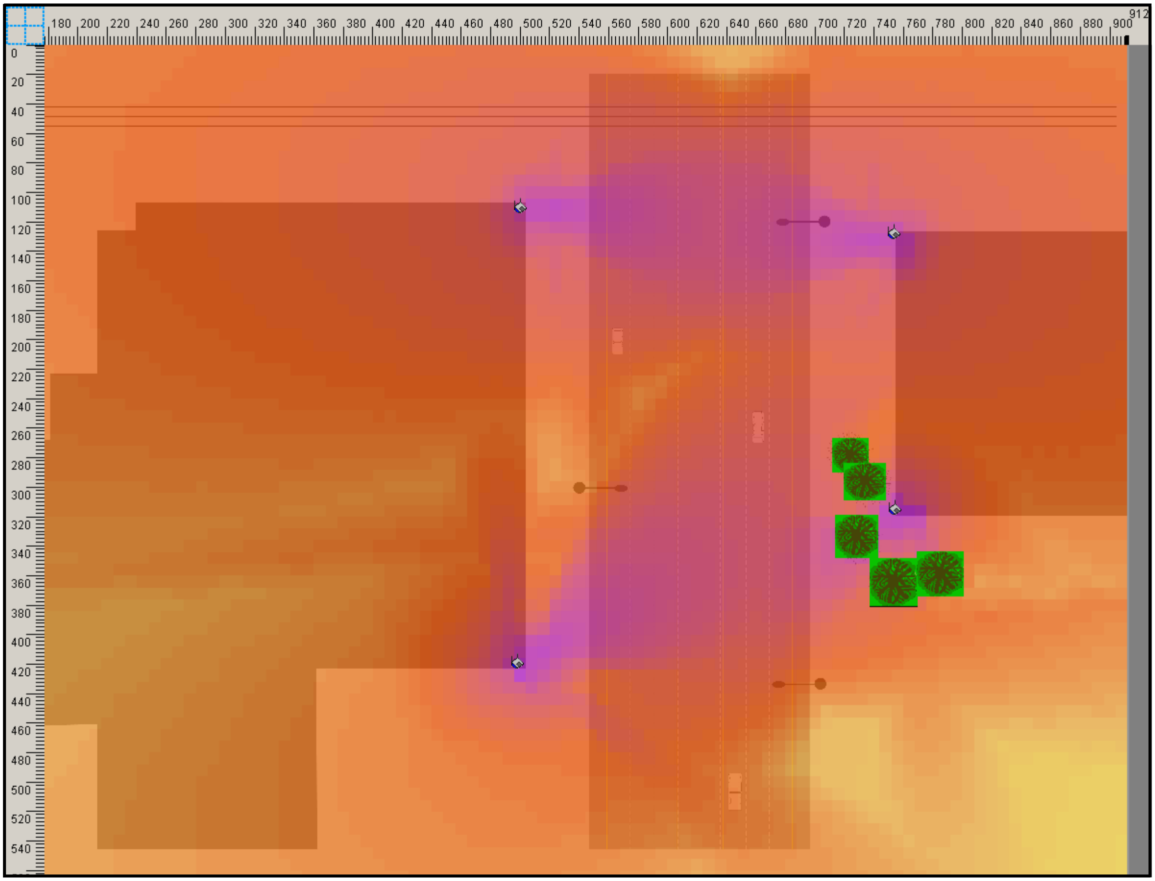


Figure 2-26. RF Planner—Access Point Coverage View (with External Antennas)

You can see that the signal is concentrated across the local mesh, sending the strongest signal between the master and participant APs.

Create a Security Plan

As you design PCUMC VSCs, you also need to take the following into account:

- You must comply with the HIPAA and FERPA standards as described in "Observe Applicable Regulations" on page 2-17.
- The RFID tags cannot authenticate to the network except with MAC-Auth, nor can they use encryption. Someone with a packet sniffer could find out the MAC address of an RFID tag, spoof its MAC address, and enter the network that way.
- The ERS carts will probably be left unattended while the user cares for a patient or attends to an emergency. It is important that unauthorized users not be able to access the ERS from these carts or other devices.
- You do not want even authorized users to access patient records, financial data, or employee records in public areas such as the cafeteria or waiting areas, thereby exposing private information to curious onlookers.
- You do not want attackers or regular users to set up rogue APs.

Table 2-13 lists the security requirements for PCUMC.

Table 2-13. Security Compliance

Security Requirement	Compliance Measure	Adequate?
Compliance with HIPAA and FERPA.	TBD	
Physical access to electronic information systems is limited while properly authorized access is allowed.	TBD	
Technical policies and procedures grant access to EPHI only to those persons or software programs that should be allowed such access rights.	TBD	
A mechanism encrypts and decrypts EPHI during transmission.	TBD	
The network can verify that a person or entity seeking access to EPHI is the one claimed.	TBD	
RFID tags cannot become a back door for unauthorized access.	TBD	
The ERS carts require a 30-second timeout before the user is logged out of the local OS.	TBD	

Security Requirement	Compliance Measure	Adequate?
ERS, prescription, financial, and human resources databases are not accessible in general public access areas.	TBD	
Rogue APs are eliminated.	TBD	

(Table C-12 in Appendix C, "Site Survey Forms and Tables" is blank so that you can use it to record your specialized security requirements and proposed compliance measures.)

Plan Physical Security

Because the HIPAA Security Rule mandates adequate physical security on a facility level, you will implement the following measures:

- All APs will be accessible only to IT administrators. They will be mounted out of sight above the acoustic tiles in the false ceiling space (not a plenum ceiling) or in locked rooms or enclosures to prevent someone from stealing them. Where possible, the CAT5 cords will be locked onto the MSM APs. Management access will be permitted only through the controllers.
- The MSM422s that will be used for the local meshes will be installed on the second floor of each building in a locked room or enclosure, and the external antennas will be installed on the roof. Each MSM422 will be connected to its antenna with a low-loss cable.
- The ERS carts will require biometric (thumbprint) authentication, and access will time out after 30 seconds of inactivity.
- Access to the ERS, prescription, financial, and human resources databases will not be permitted in the cafeteria, waiting areas, or any other areas of general public access.

Choose Security Options

You have identified several types of users and devices that require wireless access. These users are listed in the rows of Table 2-14.

Table 2-14. Security Options

	SSID broadcast	Encryption	Authentication
Certified medical staff	Closed	WPA2	802.1X (EAP-TLS)
Uncertified medical staff	Closed	WPA2	802.1X (EAP-TLS)
Administrative staff	Closed	WPA2	802.1X (EAP-TLS)
RFID tags	Open	None	MAC-Auth
Guests	Open	None	Web-Auth (HTML authentication)

For the guests, you want the service set identifier (SSID) to be broadcast in the beacon frames so that guests' wireless clients can see the VSC and associate with it. You also want to broadcast the SSID for all RFID tags and ERS carts. All of the other users will need to know the SSID ahead of time.

You do not want to provide encryption for guest or RFID traffic because the traffic will not contain sensitive or private data, nor will guests or RFID tags be allowed on private segments of the network (because of additional security measures described later). Furthermore, the RFID tags do not support encryption, and you do not know which encryption method the patients and visitors support.

For guest authentication, you choose to enforce Web-Auth. However, you will offer free guest access, enabling guests to access the Internet without authenticating. (In some countries, this might not be an option, so you should plan to install a solution such as Guest Management Software for creating guest accounts.)

For the RFID tags, your only authentication option is MAC-Auth because the tags do not have 802.1X supplicants. To prevent the RFID VSC from becoming a back door into the network through MAC spoofing, you set up your network security so that intruders cannot use the RFID MAC addresses to gain access to anything but the RFID server, which contains low-security data. For example, you could put all RFID traffic on a separate VLAN.

All employees, whether medical or administrative staff, require the highest degree of security. Their traffic must be encrypted with WPA2 AES-CCMP. For the greatest security, users will authenticate to the network RADIUS server via 802.1X. Their credentials will consist of digital certificates installed on their laptops and on ERS carts (it will be up to the domain to control which users are allowed to log on to the OS of specific domain devices such as ERS carts).

Design the VSCs

Once you know your security requirements, you can begin to plan VSCs to meet those requirements. When users and devices have the same requirements, you can usually place them in the same VSC.

Table 2-15 lists PCUMC's VSCs and the information required to begin planning VSC settings. As you see, all employees will connect to the PCUMC VSC. RFID tags will connect to a different VSC so that they can be authenticated with MAC-Auth. Both of these VSCs feature distributed traffic forwarding by APs.

Visitors and patients will be assigned to the Guests VSC, which will implement HTML authentication and centralized access control.

Table 2-15. Initial VSC Assignments—Hospital and Office Building

VSC (SSID)	SSID broadcast	Encryption	Authentication	Use Controller for Authentication and Access control	Users
PCUMC	Closed	WPA2	802.1X (EAP-TLS)	Do not use controller—distributed forwarding	Certified and uncertified medical personnel, and administrative personnel
RFID	Open	None	MAC-Auth	Do not use controller—distributed forwarding	RFID tags
Guests	Open	None	Web-Auth (HTML authentication)	Use controller—centralized	Visitors and patients

(Table C-13 in Appendix C, "Site Survey Forms and Tables" is blank so that you can use it to record information about your organization's VSCs.)

Now, you will need to decide how to associate the VLANs with the VSCs.

For a VSC that features distributed traffic forwarding such as the PCUCM and RFID VSCs, you can assign VLANs in these ways:

- Egress network in the VSC binding (static)

  You can associate each VSC with one static VLAN, which is called the *egress network* in the VSC binding. By default, when users associate with a VSC, they are automatically assigned to this VLAN. This is the VLAN on which the *AP* forwards traffic.

- Dynamic, or User-Based, VLANs

  When the RADIUS server grants the user access, it also assigns the user to a VLAN. The user's dynamic VLAN assignment overrides the VSC egress VLAN.

For a VSC that features centralized access control, such as the Guests VSC, you can assign VLANs in these ways:

- VSC-based egress VLANs (static)

  The VSC egress VLANs determine the VLAN that the *controller* uses to forward the guests' traffic onto the wired network. You can assign different VSC-based VLANs to different types of traffic, such as authenticated and unauthenticated.

- Dynamic, or User-Based, VLANs

  When a guest authenticates, the RADIUS server (whether an external RADIUS server or the MSM Controller's local server) assigns the guest to a VLAN. This VLAN must be configured on the controller's port (typically, the Internet port).

You will use a static VLAN in the VSC binding for the RFID VSC. For the PCUMC VSC, the network RADIUS server will assign users to dynamic VLANs as configured in IDM. The users in the hospital already receive dynamic VLAN assignments on their wired connections, so the correct policies are in place in IDM (and the IDM agent on NPS). For new users, you might need to create new policies. For example, at PCUMC, office medical and administrative staff require different levels of access than hospital medical and administrative staff, so you need to add the new groups to IDM and set up the new policies.

"Check the Existing VLANs on the Wired Infrastructure" on page 2-59 will explain how you ensure that users' traffic can always be forwarded in the VLANs to which they are assigned.

For the Guests VSC, you will create a VLAN just for wireless guests on the controller's Internet port and set the VSC egress VLAN for authenticated users to this VLAN. "Check the Existing VLANs on the Wired Infrastructure" on page 2-59 will explain how you set up this new VLAN in the wired infrastructure. (Alternatively, you could not specify any VSC egress VLAN or user-based VLAN and have the MSM Controllers simply route guest traffic out their Internet port, implementing ACLs as they do).

Note that guest users need to receive a DHCP address before they authenticate. The controller's DHCP server, however, is not available when you have configured a controller team, so you must configure DHCP relay on the VSC. You will specify the subnet on which users will request addresses, and then you must add a scope for that subnet on the network DHCP server, as described in "Check the Existing VLANs on the Wired Infrastructure" on page 2-59.

Table 2-16. VSC-to-VLAN Assignments

VSC	Trusted	Egress network in VSC Binding	Egress VLAN in VSC	Dynamic VLANs (assigned by RADIUS server and IDM agent)	VLAN IP
Guests	No	N/A	VLAN_16	None	10.16.1.0/28
RFID	No	VLAN_5	N/A	None	10.5.0.0/16
PCUMC	Yes	N/A	N/A	VLAN_11	10.11.0.0/16
				VLAN_12	10.12.0.0/16
				VLAN_13	10.13.0.0/16
				VLAN_59	10.59.1.0/24
				VLAN_103	10.103.1.0/24

(Table C-14 in Appendix C, “Site Survey Forms and Tables” is blank so that you can use it to record the VSC-to-VLAN assignments that you make.)

Plan RADIUS Policies

When you have VSCs, such as PCUMC’s, which authenticate users to an external RADIUS server, you (or another administrator) must plan the RADIUS policies that permit user’s the correct level of access. For example, as mentioned above, you might need to configure dynamic VLAN assignments or other dynamic settings. You can also customize policies to allow or restrict access at different times and from different locations.

Because the hospital decided to install PCM+ with IDM, you can use IDM as an easy way to customize the RADIUS policies. You will need to synchronize IDM with the PCUMC Active Directory database. You can then import Active Directory groups and define policies for those groups to determine the precise user access rights that are associated with each type of user.

To learn how to create user access groups and assign them rights, see the *HP ProCurve Identity Driven Manager User’s Guide* available at www.procurve.com/manuals.

The user access groups shown below pertain to wireless access only: the IT administrators will decide how to restrict user access over the wired network. In addition, guests are not listed because PCUMC guests are given free access (and authenticated transparently against the local MSM Controller). As you see, these policies include VLAN assignments. To make sure that these VLAN assignments control the actual *resources* that users can access, you would need to ensure that appropriate ACLs are configured on routing switches.

Table 2-17. Wireless User Groups and Access Needs

User Access Group	VLAN	Days	Times	Locations	WLAN
Admins (hospital administrative staff)	VLAN_11	All days, holidays	7am – 7pm	Hospital L1, L2, L3	PCUMC
RFID (RFID tags)	None	All days, holidays	All times	All	RFID
Cert Med (hospital certified medical personnel)	VLAN_12	All days, holidays	All times	Hospital L1, L2, L3 Office L1, L2	PCUMC
Uncert Med (hospital uncertified medical personnel)	VLAN_13	All days, holidays	All times	Hospital L1, L2, L3	PCUMC
Off Staff (office administrative staff)	VLAN_59	Weekdays, no holidays	7am – 7pm	Office L1, L2	PCUMC
Off MDs (office certified medical personnel)	VLAN_103	All days, holidays	All times	Hospital L1, L2, L3 Office L1, L2	PCUMC

Use the Firewall, MAC Lockout, or Filters

By default, the guest VSC, which uses the controller for access control, implements wireless security filters (restricting the wireless traffic to the controller, which is the default router and should handle all guest traffic). This is a good security measure, which you will leave it place.

You will also use the default firewall settings to filter guest traffic.

Check the Existing VLANs on the Wired Infrastructure

When evaluating the existing VLANs at PCUMC, you realize that you have planned a new VLAN specifically for the wireless RFID tags and their server. You will need to add this VLAN at the network core.

You also realize that users, who are assigned to their VLANs by the network RADIUS server, might now connect in areas where these VLANs are not available.

All of these VLANs are used by wireless users connecting to VSCs that feature distributed traffic forwarding. In other words, the APs traditionally would need to support the VLAN (that is, it is configured on the switch port that connects to the AP).

However, extending these VLANs through the wired infrastructure from all APs to the network core can be time consuming. You decide to have the MSM Controller implement Mobility Traffic Manager. Then you only need to ensure that all of these VLANs are configured on an MSM Mobility Controller port (and from there connected to the network core). If a wireless user or device is assigned to a VLAN that is not local to its AP, the AP simply tunnels the traffic to its controller for distribution.

You also decided to create a guest VLAN (VLAN_16) on which to egress authenticated guest traffic. You will need to add this as a tagged VLAN the switch port that corresponds to the MSM765zl Mobility Controller's Internet port. Then you could create a guest-only Internet connection (such as a connection to a cable modem) to a switch port that is untagged for the same VLAN. If you wanted to make other resources available to guests, you could connect them to this VLAN as well.

As mentioned earlier, you will also need to plan a subnet from which to assign guests (patients and visitors) DHCP addresses. You will add a scope for this subnet to your network DHCP server; create a route to this subnet on the server's default router, pointing back to the team manager IP address; and have the teaming MSM Controllers controllers implement DHCP relay for this subnet on the public VSC.

Plan Roaming

As you determined earlier, users need to roam throughout the site. However, you probably do not require fast roaming (WPA opportunistic key caching). (You could, however, go ahead and activate this feature in the private VSC, as it is easy to do.) You already plan to use Mobility Traffic Manager, which ensures that users' traffic is always distributed in the correct VLAN; therefore, you do not need to worry about planning Layer 3 (subnet-based) roaming.

Plan Guest Access

You need to decide how your guests will be authenticated. PCUMC wants to allow all visitors and patients free guest access. Therefore, you simply need to enable that option on your MSM Controllers. For guidelines on implementing guest access for paying subscribers or for guests who have accounts configured for them, refer to the *HP ProCurve MSM7xx Series Controller Management and Configuration Guide*.

You already planned how to control the guests' access (in this example, with an egress VLAN) and how to ensure that guests receive DHCP addresses.

Determine Which Port or Ports You Will Use to Connect the MSM Controller to the Network

Because PCUMC's MSM765zl Mobility Controllers are implementing teaming, it is best practice to use both ports.

You will create a VLAN that is just for the MSM Controller LAN ports (port <slot>2 on the switch) and assign the LAN ports IP addresses in a subnet reserved for them.

You will implement teaming discovery on the Internet ports (port <slot>1 on the switch), which will be placed in the VLAN and subnet used by the MSM APs and other infrastructure devices. Note that the network DHCP server needs to assign the APs their IP address because the team does not support DHCP services. You will manage the team on an virtual IP address on the Internet port subnet.

Verify the Wired Topology

You need to verify that your solution is ready to integrate seamlessly into the existing solution.

Because you are implementing Mobility Traffic Manager on PCUMC and RFID VSCs, you do not need to worry about extending the users' dynamic VLANs, nor the RFID tag's static VLAN, throughout the infrastructure. Simply ensure that these VLANs are configured on a port on each MSM Controller, and extend the VLANs from there to the core.

Because many of your wireless users are existing users, you believe that your infrastructure can continue to handle the bandwidth requirements without undue congestion. You will use the Traffic Monitor feature on PCM+ to continue to monitor traffic patterns and look for congestion.

Finally, you see that your HP ProCurve 5400zl switches will support PoE for the MSM APs.

Apply Additional Layers of Security

Because PCUMC has a low risk tolerance, you will now plan additional security features.

Detect Unauthorized or Rogue APs

On its own, PCUMC's MSM solution will provide some detection of rogue APs. However, you will rely on the more sophisticated capabilities of the RF Manager Controller to detect rogue APs and other wireless threats.

Enforcing port authentication on all switch ports is another way to minimize rogue APs. You decide to implement this security. Because APs connect to switch ports, they must authenticate using 802.1X to the network's RADIUS server. You must configure user accounts on the RADIUS server for the APs. And you must configure the 802.1X supplicant on the APs to support the correct EAP method and submit the correct credentials. You can configure a single account in AD for all of the APs to use, or you can configure a separate account for each AP. Best practice is to create a different account for each AP. Creating a different AD user account for each AP is more secure and also gives you better visibility into when a particular AP connects or disconnects.

The MSM Controllers do not have an 802.1X supplicant, however, so you must disable port authentication on the ports to which they connect (the internal switch ports, <slot>1 and <slot>2, for MSM765zls).

Enforce Additional Security Measures with HP ProCurve RF Manager Controller

Detailed instructions on how to configure RF Manager are outside the scope of this design document. See the *HP ProCurve RF Manager Admin Guide* and the *HP ProCurve Multiservice Mobility Implementation Guide*.

HP ProCurve recommends that you plan your IDS/IPS implementation before you install and start configuring RF Manager.

Before installing RF Manager, you should:

- **Organize the locations**

  You should organize your wireless LAN installation by physical location. RF Manager permits you to create *locations* and, within each location you create, *location nodes*.

- **Plan sensor configuration templates**

  Configure which channels you want you sensors to monitor and defend.

  - **Channels to Monitor**—Sensors are enabled to monitor wireless LAN traffic on these channels.
  - **Channels to Defend**—Sensors are enabled to transmit wireless LAN traffic on these channels to protect your network against various wireless LAN threats.

- **List the Sensors' MAC addresses and locations**

  It is best practice to document your sensors. (However, RF Manager can discover your sensors on its own and help you document them.) In this example, you have used RF Planner to plan sensor locations, so you only need to document where you will place each of the sensors you purchased.

- **Obtain organization images (.gif or .jpg) and floor maps of your locations**

- **Plan the placement of MSM APS and sensors**

  In this example, you used RF Planner to decide where each of you APs and sensors will be installed.

- **Plan SSID security settings**

  You already planned your VSC security settings in “Choose Security Options” on page 2-54 and “Design the VSCs” on page 2-56. You will match each SSID’s security settings in RF Manager with those you configure on each VSC.

- **SSIDs by location**

  To further strengthen security, you can determine into which networks users in particular SSIDs can forward traffic. You should also specify which SSIDs, if any, provide guest access. “Configure the VSCs” on page 2-73 shows this information for the example network.

- **Allowed MSM AP vendors**
- **Document no Wi-Fi networks**

  Your network might include subnets on which APs are not allowed to forward users traffic directly. For example, you might not want an AP to forward user traffic directly on to the server subnet because the traffic should be routed and controlled before reaching servers. These are called no wi-fi networks in RF Manager. Specifying these networks helps prevent malicious users from setting up rogue MSM APs on your network.

- **Plan automatic classification**

  A stable, functioning RF Manager implementation requires that you classify all MSM APs and all clients that RF Manager detects. The exact meaning of each classification is defined by policies that you set up.

  Table 2-18 shows all possible MSM AP classifications.

Table 2-18. AP Classifications

Classification	Definition
Uncategorized	Newly discovered APs that have not been classified
Authorized APs	APs that you have explicitly authorized
Potentially Authorized APs	Newly discovered APs that might be authorized
Rogue APs	APs that have been identified as rogue
Potentially Rogue APs	Newly discovered APs that might qualify as rogue
External APs	APs that have been identified as belonging to another network.
Potentially External APs	Newly discovered APs that might belong to another network
Indeterminate APs	Newly discovered APs whose classification cannot be determined
Misconfigured APs	Authorized APs whose settings do not conform to security settings for location

In Table 2-19, you can see which settings you can enable for automatic station classification. The first column in the table displays a Client classification, the second displays an AP classification, and the third displays the options for the client's classification after this type of client connects to this type of AP. The client can be reclassified or it can maintain its existing classification.

If a client and AP combination is not displayed in the table, then an association between this client and AP cannot automatically reclassify the client. For example, Authorized clients are never automatically reclassified.

Table 2-19. Automatic Client Classification Settings

Client Classification	AP State	Desired classification
All newly detected clients	n/a	Uncategorized Authorized Unauthorized
Uncategorized	Authorized	Authorized Uncategorized
Uncategorized	Authorized—Guest SSID	Authorized Uncategorized
Uncategorized	Authorized but Misconfigured	Authorized Uncategorized
Uncategorized—Connected but not sending traffic	Authorized	Authorized Uncategorized
Uncategorized	External	Unauthorized Uncategorized
Uncategorized	Rogue	Unauthorized Uncategorized
Uncategorized	Potentially External	Unauthorized Uncategorized
Uncategorized	Potentially Rogue	Unauthorized Uncategorized
Unauthorized	Authorized	Authorized Unauthorized
Unauthorized	Authorized—Guest SSID	Authorized Unauthorized
Unauthorized	Authorized but Misconfigured	Authorized Unauthorized
Unauthorized—Connected but not sending traffic	Authorized	Authorized Unauthorized

- **Optionally, create authorized AP and client lists**

  To authorize MSM APs and/or clients without having to manually sort them in the Web browser interface, you can import an authorized MSM AP list, authorized client list, and/or an unauthorized client list.

- **Plan the Intrusion Prevention Policy**

  You configure the intrusion prevention policy by defining what constitutes a threat in categories such as rogue APs, misconfigured APs, and client misassociation. When an MSM AP or a client matches this policy, it will be automatically moved into quarantine. When an AP is quarantined, sensors send disassociation frames to disconnect all clients that attempt to connect to the AP. When a client is quarantined, sensors send disassociation frames to disconnect the client from the AP that is banned from connecting to.

Table 2-20. Intrusion Prevention Policy

Rogue APs
APs that are categorized as rogue
Uncategorized APs that are connected to the network
Uncategorized APs that are potentially rogue
Uncategorized APs that are potentially authorized
Uncategorized, indeterminate APs
Banned APs
Misconfigured APs
Authorized APs whose configuration is not compliant with security policy
Client Misassociation
Authorized client is connected to an authorized AP with guest SSIDs
Authorized client is connected to an external AP
Authorized client is connected to an uncategorized AP that is not connected to the network
Authorized client is connected to an uncategorized AP that is potentially external
Authorized client is connected to an uncategorized AP that is indeterminate
Unauthorized Associations
Unauthorized client is connected to an authorized AP (excluding guest APs)
Uncategorized client is connected to an authorized AP (excluding guest APs)
Banned client is connected to an authorized or rogue AP or an uncategorized AP that is indeterminate or connected to the network
Banned client is connected to an authorized AP

Ad Hoc Connections
Authorized client is participating in any ad hoc network
MAC Spoofing
APs that spoof the MAC address of any authorized AP
Honeypot/Evil Twin APs
Authorized client is connected to a honeypot/evil twin AP
Denial-of-Service (DoS) Attacks
Any device that is launching a DoS attack on the network

- **Plan the Intrusion Prevention Level**

  The intrusion prevention level determines the number of channels on which a sensor can simultaneously quarantine devices. The fewer the number of channels that a sensor is switching between, the better the sensor can block unwanted communications.

  Your options are as follows:

  - **Block**—A single sensor can block unwanted communication on any one channel in the 802.11b/g band and any one channel in the 802.11a band.
  - **Disrupt**—A single sensor can disrupt unwanted communication on any two channels in the 802.11b/g band and any two channels in the 802.11a band.
  - **Interrupt**—A single sensor can interrupt unwanted communication on any three channels in the 802.11b/g band and any three channels in the 802.11a band.
  - **Degrade**—A single sensor can degrade the performance of unwanted communication on any four channels in the 802.11b/g band and any four channels in the 802.11a band.

- **Plan email notification for events**

  You can set up certain security events to trigger an email.

- **Plan reports**

  RF Manager is preloaded with several reports that conform to common compliance standards such as the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act, and the Payment Card Industry Data Security Standards (PCI DSS). You can also create customized reports.

  You can also generate other types of reports, such as incident, infrastructure, and client reports.

Enforce Endpoint Integrity

Due to the complexity of enforcing endpoint integrity and the risks of excessive support calls from users locked out of the network, PCUMC has decided not to implement endpoint integrity at the initial rollout of wireless services. Because the solution includes NPS and IDM, you can always decide to enforce endpoint integrity later. NPS and other Windows components will test endpoints' integrity, and IDM will help you configure the correct settings to be applied to non-compliant endpoints.

Provide Increased Reliability

Controller teaming enables you to provide seamless failover for non-centralized traffic. APs are adopted by the other controllers in the team, and they continue to forward traffic directly onto the network with no visible change to end users.

You are already planning to implement teaming for this solution.

However, you should understand that seamless failover is not provided for centralized traffic. When designing VSCs, you should consider if and how you want the traffic to failover. For example, the guest traffic will not failover seamlessly. The guests users would need to reauthenticate to the other controller when their controller fails.

The PCUMC and RFID traffic will only fail over seamlessly if the traffic is being forwarded locally instead of tunneled to the MSM Controller using Mobility Traffic Manager. Therefore, you will plan your solution to forward traffic locally when possible. For example, the user VLANs in the hospital are available throughout the infrastructure. Therefore, you could configure these VLANs and local networks on hospital APs, allowing these APs to forward hospital users' traffic locally.

Perform the Initial Setup and Survey

It is important to set up and test your network methodically. If you set up all aspects of the network first and then test afterward, it will be more difficult to troubleshoot. As with any other kind of experiment, it is always best to change only one variable at a time.

You should take the following to the installation site:

- Ideally, a laptop that shows your RF plan (for example, runs RF Planner) so that you can update the plan on the spot
- Floor plan
- Tape measure or other device to calculate distances
- Pencils to mark access-device locations
- Duct tape or hooks to temporarily mount radios
- Ladders
- Two-way radios
- Spectrum analyzer
- Wireless traffic analyzer
- Wireless client that you have chosen as a test station (this can be the laptop with the RF plan)

Note

A discussion of how to implement the RF Manager Controller solution, including deploying APs, is beyond the scope of this guide. Refer to the *MultiService Mobility Implementation Guide* or to the appropriate manual for your RF Manager Controller.

Configure the Initial Settings and Set Up the Infrastructure

Set up the new servers and VLANs and then configure the initial settings (such as IP, Simple Network Management Protocol [SNMP], and AP authentication settings) on the APs and the controllers. Connect the APs to the network but do not mount them in their final locations. Make sure that the APs receive IP addresses and are discovered by their controller.

The new network devices for the first level are shown in Figure 2-27.

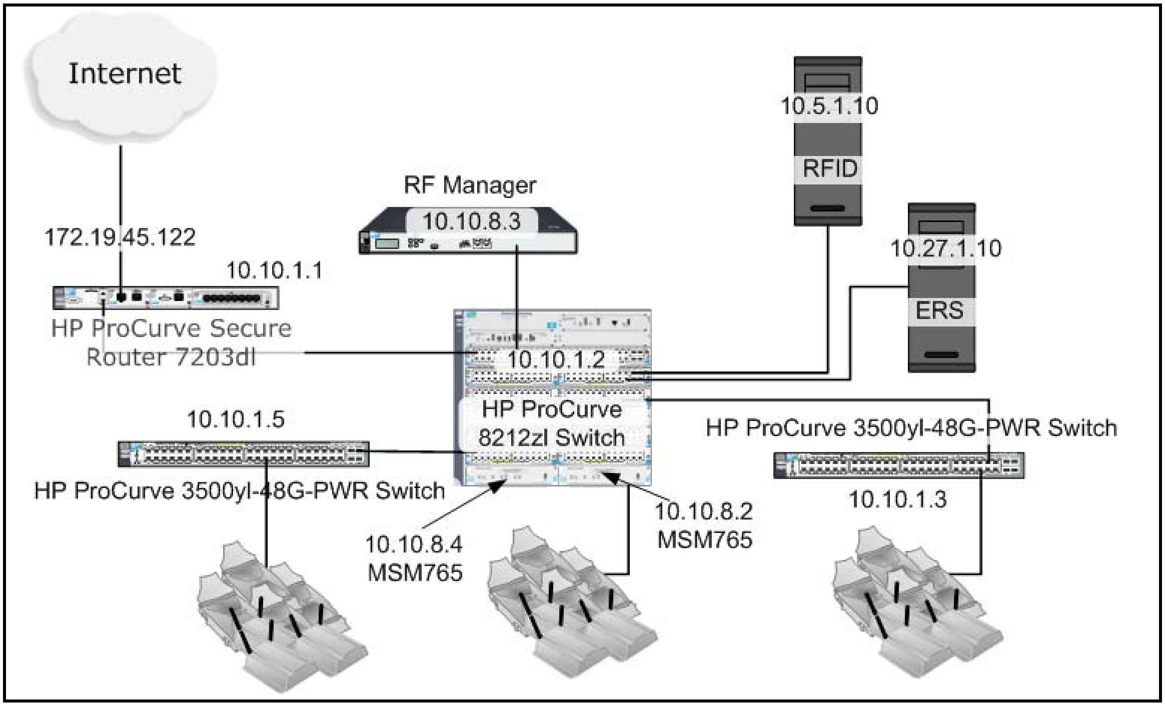


Figure 2-27. Hospital L1—New Network Devices

The 8212zl switch will provide PoE for all of the APs that are connected to it. The APs that are connected to the 3500yl-48G-PWR switches will also get their power from those switches. And the switches will power the sensors as well.

The new network elements for the second and third levels are shown in Figure 2-28.

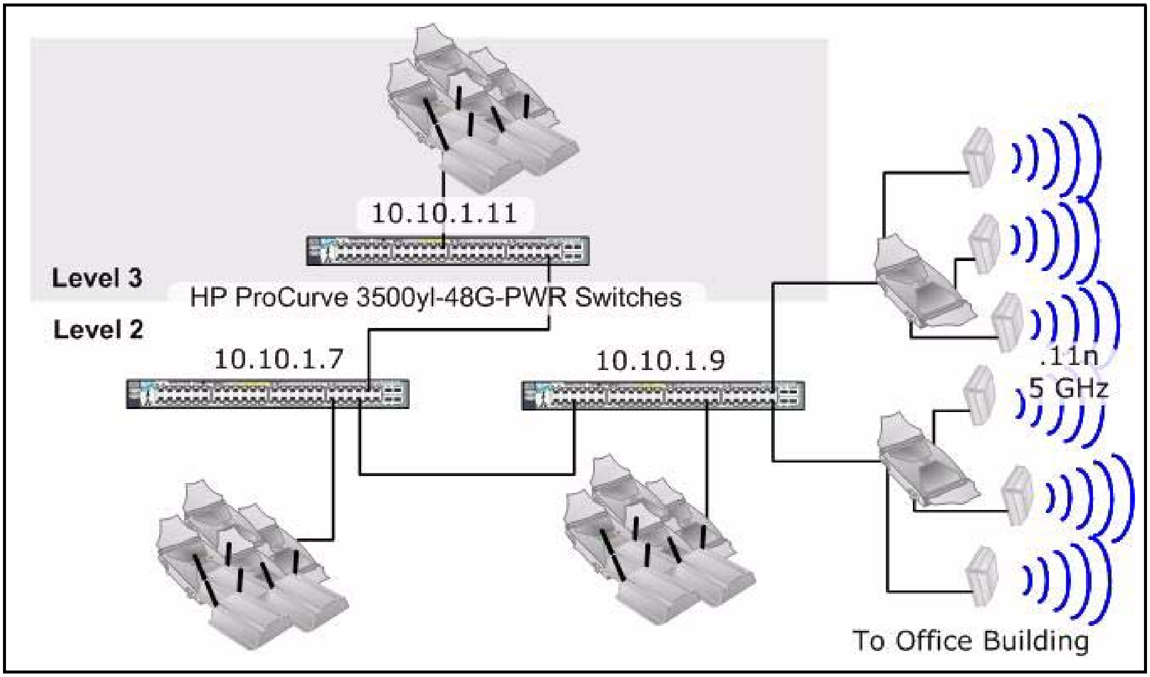


Figure 2-28. Hospital L2 and L3—New Network Devices

On the hospital second floor is the local mesh to the office building. These APs and the other APs on the floor will be powered by the 3500yl-48G-PWR switches.

In the office building, the new network infrastructure is as follows:

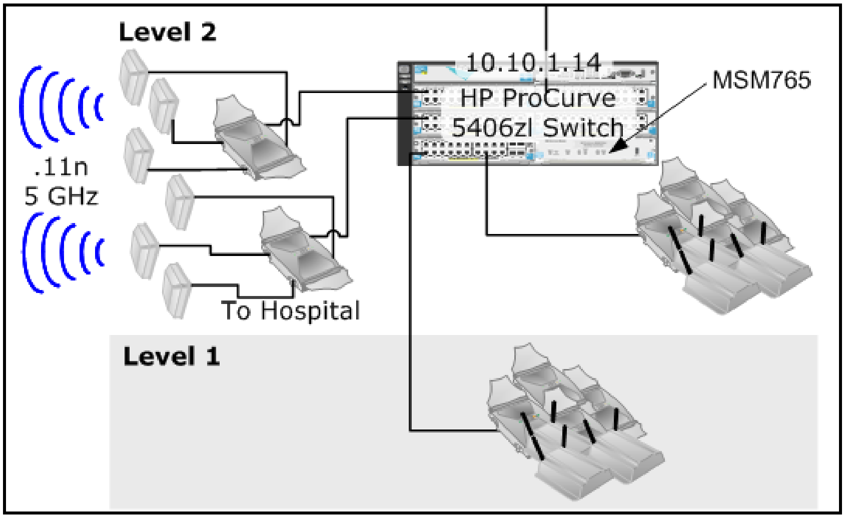


Figure 2-29. Office Building—New Network Devices

PCUMC administrators decide to replace the 5304xl switch with an HP ProCurve 5406zl switch. (The other option was to install a PoE-enabled xl module along with a separate power injector, but administrators decided that the larger capacity of the 5406zl switch plus the greater selection of zl modules would help to future proof the network). Both the MSM422s that are the masters of the local meshes and the MSM422s and MSM320s that serve the office building users will get their power via PoE.

Set Up User Accounts and Policies

Set up the user access groups in IDM first by binding Active Directory to IDM and importing any new users and user groups. Set up the access controls as shown in Table 2-17 on page 2-59. If necessary, create new user accounts in Active Directory.

Establish the Local Mesh

Follow the instructions in your MSM APs and MSM Controllers management and configuration guide to configure the local mesh. After you have configured the correct settings on all APs in the mesh, test that the mesh has been established.

Configure the VSCs

Now you need to return to the controller and configure the VSCs and bind them to AP groups. Either make all of the VSCs open system right now for testing purposes or configure the closed system SSID into your wireless client.

You will support all VSCs on each MSM422's a/b/g radio. You will preserve the MSM422 a/b/g/n radio for the PCUMC VSC. You will configure all VSCs on the MSM325 APs. Configuring all VSCs on all APs will ensure that hospital staff can maintain their connections as they move. The security features already in place (closed SSIDs, access policies on IDM, and so forth) will ensure that the correct users connect to the correct VSCs at the correct times and locations.

Mount the MSM APs

The next step is to mount the MSM APs provisionally, making sure to place the APs in the location indicated on the RF Planner Report. Make sure that each access device has power.

When positioning the antennas, remember the following rules:

- The antenna must be at least 2 m (6 ft) from other radios.
- No one should come within 25 cm (10 in) of the antenna during normal operation.
- If possible, mount the antenna clear of building supports, reflective objects, and other objects that might cause dead spots and multipath (but remember that multipath is not a problem for 802.11n).
- Outdoor installations require a lightning arrestor. Some countries require this device to be installed professionally.
- For the MSM422s, you should position the flaps to attain optimal reception.
  - Wall mount—closed or open fully
  - Ceiling mount—closed or open to 90°

Monitor Network Performance

You should walk through the building with a test client to verify which VSCs you can "see" in each location. Check the signal level at calibration points and input the actual level in RF Planner to calibrate the plan. Adjust the plan, move APs, and alter AP settings as necessary.

Note

If you have decided to implement different VSCs in different areas, you should also check the areas where you see each VSC. If you see one in an area where you do not want it, adjust the Tx level on the appropriate AP—unless that causes an unacceptable loss of coverage somewhere else.

Use a test client to authenticate to the VSCs on each radio and see if you can access the VLANs. For VSCs that support 802.1X authentication and dynamic VLANs, create a test user in each user group. Then log in as various users and make sure that you can access only the network resources that are assigned to that user group. Use the traffic analyzer again to check for throughput quality.

Use the wireless traffic analyzer to check for dropped packets and other signs of throughput problems. Again, if there are any problems, check your most recent configuration changes to see if you made any mistakes.

Finally, try to access services in the other building to ensure that the local mesh is working correctly.

Assess Your Security

Once you have set up and tested the network that you planned, you can start to assess whether you have met your security goals. Of course, you and other administrators will continue to assess the security solution on an ongoing basis.

Table 2-21. Security Compliance

Security Requirement	Compliance Measure	Adequate?
Physical access to electronic information systems is limited while properly authorized access is allowed.	APs are mounted inside ceilings or locked rooms, and cages are installed with locks; console access is disabled; MSM APs are required to authenticate with 802.1X.	Yes
Technical policies and procedures grant access to EPHI only to those persons or software programs that should be allowed such access rights.	802.1X authentication and IDM user access policies (which include dynamic VLANs and access control lists [ACLs]) prevent unauthorized access of the ERS.	Yes
A mechanism encrypts and decrypts EPHI during transmission.	WPA/WPA2 is used for all ERS transmissions.	Yes
The network can verify that a person or entity seeking access to EPHI is the one claimed.	802.1X provides mutual authentication.	Yes
RFID tags cannot become a back door for unauthorized access.	IDM policies place all traffic from the RFID VSC in the RFID VLAN and restrict routing out of that VLAN.	Yes

Security Requirement	Compliance Measure	Adequate?
The ERS carts require a 30-second timeout before the user is logged out of the local OS	Settings on this group of domain computers are changed to time out and lock station after 30 seconds of inactivity (beyond the scope of the mobility solution).	Yes
ERS, prescription, financial, and human resources databases are not accessible in general public access areas.	VSCs that provide access to sensitive information are not available in public access areas OR employees are trained not to access those databases in public OR the databases are not available over wireless connections.	Yes
Rogue APs are eliminated.	802.1X device authentication is supported, and RF Manager and sensors are in place on the network.	Yes

Finalize the Wireless Network

With all of the settings complete, make a final check of the network—VSC security, VLAN access, wireless coverage, and the local mesh. Secure the MSM APs in their final locations with the appropriate hardware.

Set up some test cases to see if you can break into the network. If you find a hole, patch it with the appropriate measures.

Finally, return to the site during peak business hours, after the users have had time to acquaint themselves with the wireless network. Use the spectrum analyzer to check coverage levels and compare them to the levels you last measured. Check throughput quality. You can also survey users to find out what they have experienced.

HP ProCurve Networking Resources for Wireless Networks

Services and Support

This design guide has taken you through the process of designing a wireless network solution. However, no design guide, no matter how comprehensive, can predict your environment exactly. ProCurve Networking provides several personalized services to further help you design a solution.

HP Networking Elite Partners

HP Networking recommends that customers use Elite Partners to assess, deploy, and maintain their wireless network solution. ProCurve has certified Elite Partners to ensure they can expertly deliver the following services:

- **Assessment services**—solution design, configuration, and on-site survey
- **Deployment services**—installation of the solution and configuration
- **Support services**—maintenance and support

HP Networking Elite Partners have the highest level of training available from HP, based on the number of HP Accredited System Engineers (ASE) on staff. These ASEs are certified by HP to have the skills and expertise to implement the product features and technologies required in an enterprise wireless network environment.

For larger, specialized engagements, customers can also use HP Services for their networking services needs. Please contact your local HP Sales Office if you are interested in discussing your networking service needs with an HP Services professional.

Implementation Guide

The *HP ProCurve MultiService Mobility Implementation Guide* (available at www.procurve.com/manuals) provides step-by-step instructions for creating a wireless network solution that meets the needs of a particular environment. It also covers ongoing maintenance of a site, including adjusting the radio frequency (RF) signal.

The implementation guide includes switch configurations and step-by-step processes for the components of wireless network solutions:

- HP ProCurve MultiService Mobility (MSM) Controllers
- HP ProCurve MultiService Mobility (MSM) Access Points (APs)
- HP ProCurve RF Manager Controller
- HP ProCurve RF Planner
- HP wireless management products

In addition, the implementation guide includes step-by-step instructions for setting up Microsoft Windows services used in the solutions.

Additional Resources

ProCurve also provides other resources to help you plan your wireless network and select the best products, based on your environment and your organization's unique requirements:

- Demos of wireless products
- Mobility solution briefs
- Mobility case studies
- White papers

To access these resources, visit
www.procurve.com/solutions/mobility/resources.htm.

All HP ProCurve documentation and other resources are available at:
www.procurve.com/manuals

A

Glossary

Numeric

802.1Q A **VLAN** tagging standard for LANs.

802.1X A port-based **authentication** standard for LANs. 802.1X forces **endpoints** to authenticate, establishing a point-to-point connection if authentication succeeds, or blocking the connection if authentication fails. By basing authentication on secure **EAP** methods, 802.1X authentication can prevent eavesdroppers from reading intercepted messages. The 802.1X standard requires three components: the **supplicant**, which runs on the endpoint device; the authenticator, which is typically a switch or an **AP**; and the authentication server, which is usually a **RADIUS** server. For more information, see IEEE 802.1X at *http://www.ieee802.org/1/pages/802.1x.html.*

802.3af A **PoE** standard for IEEE 802.3 (wired Ethernet).

802.11 The IEEE standard for wireless LANs. For more information, see IEEE 802.11 at *http://standards.ieee.org/getieee802/802.11.html.*

802.11a A version of **802.11** that broadcasts at 5 GHz and provides a maximum speed of 54 Mbps.

802.11b A version of **802.11** that broadcasts at 2.4 GHz and provides a maximum speed of 11 Mbps. It is not compatible with 802.11a.

802.11e A standard that defines quality of service (QoS) for wireless networks.

802.11g A version of **802.11** that broadcasts at 2.4 GHz and provides a maximum speed of 54 Mbps. It is compatible with 802.11b but not with 802.11a.

802.11h A standard that specifies dynamic channel and power control for radar avoidance in the 802.11a spectrum.

802.11i The enhanced security standard for **802.11**, which supersedes **WEP** security. For more information, see the standard at *http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.*

802.11j A version of **802.11a** that complies with Japanese frequency allocations.

802.11n An emerging **802.11** standard that is intended to increase network speed and reliability as well as to extend the operating distance of wireless networks. After its expected ratification in early 2009, 802.11n will provide transmission speeds of up to 248 Mbps or 500 Mbps with channel bonding. 802.11n will also operate in either the 2.4 GHz or 5 GHz frequency bands—enabling it to provide backward compatibility for 802.11a/b/g devices. For more information about this standard and others that are being developed, see *http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm.*

802.11r An amendment to **802.11** to specify fast **handoffs** from one **access device** to another. For more information about this standard and others that are being developed, see *http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm.*

802.11y An emerging **802.11** standard that will allow use of the 3560-3700 MHz band in the United States. For more information about this standard and others that are being developed, see *http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm.*

802.15 The **PAN** standard that is used by **Bluetooth**.

802.15.4 The **PAN** standard that forms the base for **ZigBee** and **Wibree**.

802.16 Also called **WiMAX**, a standard for broadband wireless access that transmits in the 2–66 GHz range and covers several kilometers for point-to-point transmissions.

A

access control The ability to determine which endpoints can access the network and the level of access they receive. Access can be controlled based on an endpoint compliance with network standards, for example, or on other configurable settings. See also NAC.

access control zone A physical area of an organization that is defined by the way that users (public or private) will access the network (wired or wireless). For example, a foyer where non-employees access the network wirelessly is a public wireless zone, whereas the internal offices where employees use wired workstations is a private wired zone.

access device Any device that permits access to a wireless network, such as an **AP**.

access point *See* **AP**.

ACL *Access Control List.* A set of rules that network devices such as routers, switches, and **access devices** use to control access to network resources and to identify packets that require special handling due to technologies such as **QoS** or NAT. An ACL can be configured to select packets according to values in their headers, such as IP protocol, source and destination IP address, and source and destination TCP or UDP ports.

AES *Advanced Encryption Standard.* A block cipher that was adopted as an encryption standard. It is often used in symmetric key cryptology. For more information, see FIPS PUB 197 at *http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf.*

AM band The set of frequencies between 520 kHz and 1610 kHz that is used for monaural commercial radio broadcasts.

antenna A passive device that is used to send and receive **RF** signals. The more **gain** an antenna has, the more it focuses the RF signal being transmitted in a specific direction or plane and the more sensitive it is to incoming RF signals from that same direction or plane.

AP *Access Point.* A network component that receives and sends wireless LAN signals to wireless **NIC**s through its **antenna**. An AP is functionally equivalent to a bridge and may serve as an interface to a wired network via an Ethernet cable.

AP detection A capability of APs that permits them to detect any neighboring APs. It can be used to detect rogue APs or neighboring APs in the same physical area.

architecture In the context of wireless networks, “architecture” describes the point of control for the MSM APs. In “optimized WLAN” architecture, multiple APs are controlled centrally by a Multiservice Access Controller. In “autonomous” architecture, one or multiple APs operate independently of one another, and each AP must be configured separately.

association An initial linking between a wireless **station** and an **access device** that occurs after **validation** and before **authentication**. Upon association, an access device registers the station with the network and allocates resources to permit the station to transmit data over the wireless medium.

APC Adaptive Power Control. A feature of APs that permits them to change their transmit power when they detect neighboring APs that are transmitting on the same channel. The AP will either reduce its transmit power to avoid interference or increase power to compensate for a failed neighboring AP.

attenuation The diminution of an **RF** signal. Attenuation can result from interference from other RF signals, blocking from an obstacle, or dissipation over long distances.

authentication The process of confirming the identity of an **endpoint** or an end user before granting a network connection. Authentication can be implemented through the use of passwords, **keys**, or digital **certificates**.

authorization The process of controlling the network resources and services that an end user can access, usually based on the end user's identity. Authorization is sometimes called "access control," although **access control** is properly broader than authorization alone.

B

beacon frame A periodic frame sent out by **access devices** on an **802.11** network to announce their availability and services.

bill of materials A list of parts that is needed to create a unit. In the context of RF Planner, it is the list of wireless components that are needed to create the wireless LAN that you planned with RF Planner.

biometrics The use of the unique attributes of a human body that can be used to absolutely differentiate one person from another, such as fingerprints, voice prints, or retinal patterns.

Bluetooth An industrial standard for **PAN**s based on **802.15**. Bluetooth is designed to operate at short distances, for example, between a cellular telephone and its wireless headset.

BSSID *Basic Service Set IDentifier*. The MAC address of the AP radio for a specific Extended Service Set (**ESS**). Some APs can enable more ESSs than they have BSSIDs, in which case more than one ESS will be linked to the same BSSID. However, only one of the ESSs will be included in that BSS beacon frame.

C

C band The group of frequencies between 4 GHz and 8 GHz.

CBC *Cipher Block Chaining*. A block cipher mode of operation wherein the previous encrypted block is used to transform the next block prior to its encryption. For more information, see NIST Special Publication 800-38A at *http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf*.

CCMP *Counter Mode with* ***CBC*** *Message Authentication Mode Protocol.* An **802.11i** encryption protocol that uses **AES**. For more information, see the IEEE 802.11i-2004 standard at *http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.*

CDMA *Code Division Multiple Access.* A wireless access method employed by **cellular telephones** that distinguishes signals by their encoding (as opposed to **TDMA**, which distinguishes them by time slot and **FDMA**, which distinguishes them by frequency).

cell The area in which an **RF** signal is broadcast. A cell size is determined by the transmitter power level and **antenna gain,** while its shape is determined by the type of antenna the transmitter uses and obstacles within and around the cell. The term *cell* usually describes the coverage area of an access point or a **cellular telephone** base station.

cellular telephone A telephone that connects to the telephone system via radio transmission. Unlike a **cordless telephone**, a cellular phone has its own number and can be used anywhere it is in range of its service provider transmission towers. Cellular telephones broadcast at frequencies of 900 MHz, 1800 MHz, or 1900 MHz.

certificate An electronic document that contains a public **key** and is digitally signed by a third-party issuer such as a certificate authority. Digital certificates are used for network **authentication**. They contain the certificate holder's name or other identifying information, a serial number, the expiration date, and a copy of the certificate holder's public key, which validates data signed by the corresponding private key.

channel A narrow band of contiguous wireless frequencies that has been designated by a standards body as a single unit for transmission.

CHAP *Challenge Handshake Authentication Protocol.* An **authentication** protocol that is incorporated in **RADIUS**. With CHAP, the authenticator sends the client a "challenge" text. The client creates a **hash** value from its pre-shared password and the text. The authenticator also creates a hash value from the same text. The authenticator compares the hash values. If they match, authentication succeeds and the link is established. For more information, see RFC 2759 at *http://www.ietf.org/rfc/rfc2759.txt.*

closed system A **WLAN** in which the **SSID** is *not* broadcast in the **beacon frame**s and **stations** cannot **associate** and **authenticate** with the **access device** unless they already know the SSID. Also see **open system**.

coordinated architecture *See* **architecture**.

cordless telephone A telephone that uses wireless technology to connect the speaker and receiver to a base unit that is connected to telephone land-lines. Unlike a **cellular telephone**, a cordless telephone is part of a conventional land-line installation and can be used only within a short distance of the base unit. Cordless telephones are licensed to transmit at 800 MHz, 900 MHz, and 2.4 GHz.

coverage A term to describe the area over which an **RF** signal propagates.

credentials A username and its corresponding password.

crosstalk The "contamination" of one signal by another; for example, when you can hear conversations on telephone lines other than the one you are using.

D

data store The location where an **endpoint** or user **credentials** are stored. Possible data stores are a local database of users, a Windows domain controller that runs Active Directory, an LDAP server such as OpenLDAP or Novell eDirectory, or a **RADIUS** server.

DES *Data Encryption Standard*. A published encryption algorithm that uses a 56-bit symmetric key to encrypt data in 64-bit blocks. For more information, see FIPS PUB 46-3 at *http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf*.

DFS *Dynamic Frequency Selection*. A provision of **802.11h** that permits a radio in a wireless LAN to change its frequency when it detects **interference** from an outside source or another wireless LAN within range that uses the same **channel**.

digital certificate *See* **certificate**.

directional antenna A type of **antenna** that broadcasts signals mostly in one direction. *See also* **omnidirectional antenna**.

DSRC *Dedicated Short-Range Communications*. A subset of **RFID** technology that is used primarily in automotive applications such as electronic toll collection. It transmits in the 5.9 GHz band in the U.S. and the 5.8 GHz band in Europe and Japan. For more information, see *http://www.standards.its.dot.gov/Documents/advisories/dsrc_advisory.htm*.

DSSS *Direct Sequence Spread Spectrum*. A method of transmitting **RF** signals to prevent eavesdropping wherein the signal is encoded and spread across multiple frequencies at low power. It is the most-used **PHY layer** of the **802.11b** standard and is also used by **802.11g** for the lower data rates. *Also see* **FHSS**.

dynamic VLAN A **VLAN** whose members are assigned based on user information in a **RADIUS** server. Also see **static VLAN**.

dynamic WEP A version of **WEP** that employs a **RADIUS** server to generate a new encryption **key** for each session. Dynamic WEP requires **802.1X**-compliant software on both ends of the **authentication** session.

E

EAP *Extensible Authentication Protocol*. A protocol that allows PPP to use authentication protocols that are not part of the PPP suite. For more information, see RFC 3748 at *http://www.ietf.org/rfc/rfc3748.txt*.

EAP-GTC ***EAP*** *with Generic Token Card*. An implementation of EAP that uses a token card for **authentication**. For more information, see RFC 3748 at *http://tools.ietf.org/html/rfc3748*.

EAP-TLS ***EAP*** *with* ***TLS***. An implementation of **EAP** that provides mutual **certificate authentication** between client and server. For more information, see RFC 2716 at *http://tools.ietf.org/html/rfc2716*.

EAP-TTLS ***EAP*** *with Tunneled* ***TLS***. An implementation of **EAP** in which the server authenticates with a **certificate**, but the client authenticates (usually with a password) using a different protocol that is sent over a secure tunnel. For more information, see the Internet Draft at *http://www3.ietf.org/proceedings/02jul/I-D/draft-ietf-pppext-eap-ttls-01.txt*.

endpoint Any device that connects to a network, such as a desktop computer, a laptop computer, or a server.

endpoint integrity The functionality that examines all **endpoint**s that attempt to connect to the network and prohibits unsafe or non-compliant endpoints from gaining network access. Endpoint integrity ensures that an endpoint that attaches to the network meets configured criteria (for example, an antivirus program is present and running with current signatures) before allowing it to access network resources.

EPHI *Electronic Protected Health Information*. A term used in **HIPAA** literature to describe private information about a patient’s health that is stored on electronic media.

ERS *Electronic Records System*. Any computerized system that stores health information about patients, from prescriptions to insurance data to medical history.

ESS Extended Service Set. In wireless technology, an ESS is a set of one or more interconnected BSSs and WLANs that appear as a single BSS. Each ESS has a unique, 48-bit identifier called the ESSID, which functions as the network name. Although ESSID is more precise, the industry commonly uses the general term SSID to signify the network name.

Extensible Authentication Protocol *See* **EAP**.

F

fast roaming **Roaming** with a **handoff** of less than 50 µs.

FDMA *Frequency-Division Multiple Access*. A wireless access method employed by **cellular telephones** that distinguishes signals by their frequency (as opposed to **TDMA**, which distinguishes them by time slot and **CDMA**, which distinguishes them by encoding).

FERPA *Family Educational Rights and Privacy Act* of 1974. A U.S. law to protect private student data such as grades and other scholastic information. For more information, see the full text at *http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html*.

FHSS *Frequency-Hopping Spread Spectrum*. A method of transmitting **RF** signals to prevent eavesdropping that involves rapidly “hopping” from one narrow band to another in a sequence that is known only to the sender and receiver. It is a rarely used **PHY layer** for **802.11b** and is also used by **Bluetooth** and other short-range technologies. *Also see* **DSSS**.

FISMA *Federal Information Security Management Act* of 2002. A U.S. law that governs information security for federal agencies. The full text of FISMA is at *http://csrc.nist.gov/drivers/documents/FISMA-final.pdf*.

FM band The set of frequencies from 87.8 MHz to 108.0 MHz that is used to transmit commercial stereophonic radio signals.

frame retransmission Wireless LAN devices that use the **802.11** MAC layer send acknowledgment (ACK) packets after receiving every data packet. If an ACK packet is not received, the **station** resends the last frame until an ACK packet is received or the retransmission limit is reached.

G

gain *See* **antenna**.

GLBA *Graham-Leach-Bliley Act*. A U.S. law that regulates how financial companies may collect, distribute, and store personal data. The section of the law that concerns the protection of personal information is found at *http://www.ftc.gov/privacy/glbact/glbsub1.htm*.

GPS *Global Positioning System*. A wireless system that consists of 24 satellites in medium earth orbit that transmit microwave signals to earthbound receivers. The signals permit a receiver to determine its exact location, speed, direction, and time. Civilian GPS transmits at 1227.60 MHz and 1575.42 MHz. For more information, see the GPS Web site at *http://www.gps.gov.*

GRE *Generic Routing Encapsulation.* A stateless tunneling protocol that is used to transmit layer-3 packets in an IP network. For more information, see RFCs 1701, 1702, 2784, and 2890 at the IETF Web site at *http://tools.ietf.org/html.*

GSM *Global System for Mobile Communications*. A cellular telephone standard that originated in Europe and is now widespread. GSM operates in four frequency ranges, depending on the country: 850 MHz, 900 MHz, 1.8 GHz, and 1.9 GHz.

GTC *See* **EAP-GTC**.

H

handoff The transfer of a **station** network session from one **access device** to a neighboring access device during **roaming**.

hash A number generated by running a string of text through an algorithm. The hash is substantially smaller than the text itself and is unique because algorithms transform data in such a way that it is extremely unlikely that some other text will produce the same hash value. The hash is also irreversible: the encryption cannot be reversed to obtain the original text.

heat map A diagram that is produced by **RF Planner** to show how **RF** signals propagate in a given space. The “hotter” (darker colored) the area, the stronger the signal, meaning that more bandwidth is available in that area.

HIPAA *Health Insurance Portability and Accountability Act.* A U.S. law to address abuses in the health care industry. Its relevance to computer networking concerns the privacy of **EPHI**.

HiperLAN A European Telecommunications Standards Institute (ETSI) competitor to IEEE 802.11 that transmits in the 5 GHz range. The standard comes in two versions, HiperLAN/1 and HiperLAN/2, both of which are considered defunct.

I

IAS *Internet Authentication Services*. The Microsoft implementation of **RADIUS**.

IDM *Identity Driven Manager.* A ProCurve networking solution that provides management of user-based profiles (including **ACL**s, **QoS** settings, and rate limits). IDM assigns various profiles to end users based on their identity (community), access time, and access location.

IKE *Internet Key Exchange.* A protocol that is used to set up a security association in the IPsec protocol suite.

IMSI *International Mobile Subscriber Identity.* A unique number that is stored in a **SIM** and is used by **GSM** and **UMTS** mobile telephones. The number helps providers locate the phone and acquire other information.

induction A phenomenon wherein an electrical current is generated in a conductor (such as a copper wire) by placing it in a moving magnetic field. In **RFID** technology, the RFID reader generates an electrical current in the tag with radio frequencies, and the current is just strong enough to send a faint “backscatter” signal to the reader.

infrared The band of frequencies from 60,000–430,000 GHz, which is just outside the red edge of the visible spectrum. Infrared is commonly used with remote control devices, and unlike **RF**, cannot penetrate walls or other solid objects.

interference The collision of an **RF** signal with another RF signal such that the signal is distorted, diminished, or cancelled out.

ISM bands *Industrial, Scientific, and Medical bands*. A set of frequencies that was set aside internationally for unlicensed, non-communication transmissions by entities in the industrial, scientific, and medical fields. The most common ISM frequencies are 13.553–13.567 MHz, 26.957–27.283 MHz, 40.66–40.70 MHz, 902–928 MHz, 2.400–2.500 GHz, 5.725–5.875 GHz, 24–24.25 GHz, and 61–61.5 GHz.

K

key In cryptography, a key is a unique value or string of text that is used to encrypt data when that data is run through an encryption or **hash** algorithm. To decrypt or dehash the data, a device must apply the correct key to the encrypted data. The length of a key generally determines how difficult it will be to decrypt the data.

Ki An authentication **key** that is stored on a **SIM** and is used to encrypt the **ISMI** along with a random value.

L

layer 2 roaming Movement of a **station** from one **access device** to another access device on the *same* subnet.

layer 3 roaming Movement of a **station** from an **access device** on one subnet to an access device on *another* subnet.

LEAP *Lightweight* ***EAP***. A wireless LAN **authentication** protocol developed by Cisco systems.

LMDS *Local Multipoint Distribution Service.* A wireless telephony technology that is used for long-distance, point-to-point transmissions, often for the "last mile," the connection between the user and the nearest switching station.

local mesh This feature replaces the need for Ethernet cabling between **AP**s, enabling expanded wireless coverage through the use of wireless bridges to transport network traffic in hard-to-wire or outdoor areas.

M

MAC-Auth *MAC Authentication.* **Authentication** that is based on the **endpoint** MAC address rather than on the user's **credentials**. MAC-Auth does not require device configuration or end-user interaction; instead, the authenticator handles sending the MAC address to the authentication server to be checked against permit and deny lists.

MD5 *Message-Digest algorithm 5*. A **hash** algorithm used to create digital signatures. MD5 is a one-way hash function that transforms and condenses data into a fixed string of digits called a message digest. A variety of protocols use MD5 to check a message data integrity as well as authenticate the sender. Some protocols, such as **EAP-MD5**, require passwords to be transmitted as hashes rather than in plaintext. For more information, see RFC 1321 at *http://tools.ietf.org/html/rfc1321*.

medical telemetry Wireless technology that transmits a patient's vital signs over **RF** frequencies. Most medical telemetry uses the **WMTS** frequencies, but some systems use wireless LAN frequencies.

MIC (Michael) *Message Integrity Code*. A packet integrity check algorithm used by **WPA**. It is often referred to as "Michael."

mobility domain A grouping of MSM Mobility Controllers that permits **layer 3 roaming**. A controller in a mobility domain can transfer session information about a **roaming station** to other controllers in the same domain.

MS-CHAP *Microsoft* ***CHAP***. The Microsoft implementation of CHAP. For more information, see RFC 2759 at *http://tools.ietf.org/html/rfc2759*.

N

NAC *Network Access Control*. A security implementation that attempts to control access to a network by enforcing security policies, restricting prohibited traffic types, identifying and containing end users that break rules or are noncompliant with policies, and stopping and mitigating security threats.

neighbor recovery A self-healing feature of the **AP** that permits one AP to take over the workload of a failed neighboring AP.

network access control *See* **NAC**.

NFC *Near-Field Communication*. A short-range wireless technology that transmits at 13.56 MHz and uses magnetic **induction** for data transmission. NFC is primarily for use in **cellular telephones** and permits the user to "read" special messages encoded in posters and other printed material. For more information, see the NFC forum at *http://www.nfc-forum.org/home*.

NIC *Network Interface Card*. A printed circuit board that includes a cable jack or **antenna** that gives a computing device access to a network. Every NIC has a MAC address that is unique to that card.

O

OFDM *Orthogonal Frequency-Division Multiplexing*. A type of **RF** modulation that uses a large number of sub-carriers that are orthogonal (at right-angles) to each other to suppress **crosstalk** between each carrier frequency. OFDM is the modulation scheme for **802.11a** and the higher data rates of **802.11g**.

omnidirectional antenna An **antenna** that broadcast signals equally in all directions. *See also* **directional antenna**.

open system A **WLAN** in which the **SSID** is broadcast in the **beacon frames**. *See also* **closed system**.

Opportunistic Key Caching The process of caching, or saving, the encryption **key**s used by **WPA** to authenticate users on every **AP** in a mobility domain, allowing wireless users to roam to a new AP without having to reauthenticate.

P

PAN *Personal Area Network*. A short-range wireless network that usually replaces cables for computer peripherals such as a mouse, keyboard, speakers, or headsets. IEEE **802.15** is the standard for **Bluetooth** and other PANs.

PCI DSS *Payment Card Industry Data Security Standard*. An industry security standard for companies that process credit card information. For more information, download the standard from *https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm*.

PDA *Personal Digital Assistant*. A handheld computing device that can run applications or store data. Some PDAs have **RF** or **infrared** transmission capabilities.

PEAP *Protected* ***EAP***. A transport mechanism developed to provide much of the security of **EAP-TLS** without forcing **endpoints** to use digital **certificates**, thereby drastically cutting the work required to implement the protocol. PEAP requires only a server-side **PKI** certificate to create a secure **TLS** tunnel to protect end-user **authentication**.

PHY layer The *phy*sical layer of a network transmission, which can be copper wire, radio frequencies, or fiber optics.

PIPEDA *Personal Information Protection and Electronic Documents Act*. A Canadian law to protect data privacy, especially with regard to personal information. It is similar to **GLBA** in the U.S.

PKI *Public Key Infrastructure.* A system of digital **certificates**, certificate authorities, and other registration authorities that verify each party in an Internet transaction. A PKI enables devices to privately exchange data using a public infrastructure such as the Internet by managing **keys** and certificates.

plenum ceiling A type of ceiling that consists of a gap between the true ceiling and a hanging grid with acoustic tiles placed in it. The gap is a plenum only if the gap is engineered as part of the building ventilation system. Only plenum-rated equipment should be placed inside a plenum ceiling.

PMK caching A **fast-roaming** technique that permits a wireless **station** to reauthenticate to an **AP** after it has disassociated from it by using the same **key** as in its previous session.

PoE *Power over Ethernet.* Technology that permits the transmission of electrical energy over Ethernet cabling to provide power to a component on the end of the cable, typically an **AP**.

pre-association A term to describe activity that takes place prior to a **station**'s **association** with an **AP**.

pre-authentication A **fast-roaming** technique that permits a wireless station to quickly find and authenticate to a new **AP** before disassociating with the previous AP.

PSK *Pre-Shared Key.* An alphanumeric character string agreed upon by two parties in advance. In **IKE** negotiations, peers can exchange a pre-shared key that is between 8 and 255 characters long to authenticate each other before opening the IKE security association.

public key infrastructure *See* **PKI**.

Q

QoS *Quality of Service.* A service provided by some network protocols such that the network prioritizes traffic or guarantees a particular level of performance to a type of data flow.

R

radio port *See* **RP**.

RADIUS *Remote Authentication Dial-In User Service.* A protocol that allows a server to store all of the security information for a network in a single, central database. The server stores and manages end-user information so that it can authenticate the end users. The server also maps end users to the services that they are allowed to access. For more information, see RFC 2865 at *http://www.ietf.org/rfc/rfc2865.txt*.

receiver sensitivity A value expressed in negative dBm (decibels relative to one milliwatt) that describes how much power a signal must have to be detected by the receiver. The higher the absolute value of the number, the more sensitive the receiver. Therefore, a receiver sensitivity of –90 dBm is better than –80 dBm.

RF *Radio Frequency.* A generic term to refer to anything related to radio frequencies.

RFID *Radio Frequency IDentification.* A set of technologies that employ radio frequencies, usually on tags, for locating and/or identifying objects, animals, or people. RFID tags can be active, passive, or semi-passive. The active tags are battery powered and send out beacon signals. Semi-passive tags use battery power to store data that they have collected but not to send a signal. Passive and semi-passive tags send out signals only when they come near a magnetic **induction** field from an RFID tag reader. RFID tags operate on a variety of frequencies: 125–134.2 kHz, 140–148.5 kHz, 13.56 MHz, 433 MHz, 865–928 MHz, 902–928 MHz, and 2.4 GHz.

roaming The act of moving a wireless **station** out of the range of one **access device** into the range of another while maintaining connectivity. Roaming can occur at layer 2 or layer 3 and can be seamless (no interruption for the application) or not seamless.

rogue AP An **AP** that is not authorized to connect to the network or to transmit in the area. A rogue AP can be installed by an attacker who wishes to intercept legitimate traffic or by a user who merely wants to have wireless access to the network.

Rx *Receive*. As opposed to **Tx**, which is *transmit*.

S

S band The set of radio frequencies from 2 GHz to 4 GHz. Common usage includes weather radar, satellite radio, communications satellites, Mobile Satellite Services networks, and the 802.11a/g and 802.16e standards.

seamless *See* **roaming**.

sFlow A statistical sampling technology that allows organizations to gather information about their wireless and wired networks. It requires two main components: the sFlow agent or agents and the sFlow collector. The sFlow agent uses statistical traffic sampling to send the sFlow receiver enough information for the receiver to create an accurate profile of network traffic within a margin of error. The sFlow agent inspects traffic from its data sources.

An sFlow proxy operates between the sFlow agent and the sFlow receiver. The sFlow proxy collects all of the traffic data from the agent (or agents) and repackages the information so that it appears to be the source. When an sFlow proxy is used, the receiver is not aware of the sFlow agents that provide statistical information to the sFlow proxy.

shared secret Any **authentication** information such as a password that is "known" by two or more network devices. The shared secret is identical on both devices.

SIM *Subscriber Identity Module*. A removable **smart card** that is used in mobile phones to store **authentication credentials** and other information for the subscriber network.

smart phone A **cellular telephone** that has Internet access capabilities.

SNR *Signal-to-Noise Ratio*. A value that describes the relationship between signal power and corrupting interference. The higher the ratio, the stronger the desired signal and the less obtrusive the noise.

SOX *Sarbanes-Oxley Act of 2002*. A U.S. federal law that was enacted to improve the accuracy and reliability of corporate disclosure. Though primarily concerned with audits and transparency, SOX also includes provisions for the security of sensitive data.

SSID *Service Set IDentifier*. A user-defined name for a **WLAN** subnet. All of the devices on the same wireless subnet use the same SSID. When a wireless network card searches for a WLAN, the SSID for each detected network is usually displayed.

standalone architecture *See* **architecture**.

static VLAN A **VLAN** that is populated by predetermined users or devices through a one-to-one assignment. *See also* **dynamic VLAN**.

static WEP A deployment of **WEP** wherein the **key** is manually assigned and changed. It is the default type of WEP and is highly vulnerable to break-ins.

station The term used by IEEE **802.11** standards literature for a device on a wireless LAN, usually a device that associates with an **AP**, but also a device in a peer-to-peer wireless network.

STP *Spanning Tree Protocol.* A protocol that eliminates network loops by de-activating redundant connections. For more information, see IEEE 802.1D at *http://www.ieee802.org/1/pages/802.1D-2003.html.*

supplicant The component of **802.1X** that requests access to a network. It communicates with the **RADIUS** server to submit an end user's **credentials** (and also to authenticate the RADIUS server to the **endpoint**). Supplicants include native supplicants on Windows Vista, XP SP2, and 2000 SP4; MAC OS 10.3; as well as third-party supplicants such as Juniper Odyssey 4.2 and Open1X Xsupplicant 1.2.8.

T

TDMA *Time Division Multiple Access.* A wireless access method employed by **cellular telephones** that distinguishes signals by their time slot (as opposed to **FDMA**, which distinguishes them by frequency and **CDMA**, which distinguishes them by encoding). TDMA is used in **GSM** and other cellular systems. Dynamic TDMA, a variant, is used in **HiperLAN**/2, **WiMAX**, and **Bluetooth**.

telemetry *See* **medical telemetry**.

TKIP *Temporal Key Integrity Protocol.* A link-layer security protocol that is used in **WPA** to correct deficiencies in **WEP**. For more information, see *http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.*

TLS *Transport Layer Security.* The successor to SSL. It prevents eavesdropping on communications between Internet client and server. For more information, see RFC 2240 at *http://www.ietf.org/rfc/rfc2246.txt.*

TPC *Transmit Power Control.* A feature of **802.11h** that permits the lowering of power output when other networks are in range.

transceiver A radio that can both transmit and receive signals.

TTLS *Tunneled **TLS**.* An extension to TLS that does not require the client to be authenticated by a certificate authority–signed **PKI** certificate. For more information, see the Internet Draft at *http://tools.ietf.org/html/draft-funk-eap-ttls-v1-01.*

Tx *Transmit.* As opposed to **Rx**, which is *receive.*

U

UHF band *Ultra High Frequency band*. The set of frequencies from 300 MHz to 3 GHz. Applications include television broadcast, cellular telephones, cordless telephones, WLANs, satellite radio, and amateur radio.

UMTS *Universal Mobile Telecommunications System*. A third-generation **cellular telephone** technology successor to **GSM**. Also called 3GSM. For more information, see the specification at *http://www.3gpp.org/ftp/Specs/html-info/21101.htm*.

V

validation An alternate term for "**authentication**" as it is used in the IEEE **802.11** standards literature. The standard uses the term "authentication" to refer to a type of **pre-association** handshake rather than the process of verifying user or device identity.

VHF band *Very High Frequency band*. The set of frequencies from 30 MHz to 300 MHz. Applications include **FM band** radio, television broadcast, terrestrial navigation systems and marine and aircraft communications.

VLAN *Virtual Local Area Network*. A standard that enables network administrators to group end users by logical function rather than by physical location. VLANs are created on switches to segment networks into smaller broadcast domains, enhance network security, and simplify network management. For more information, see IEEE 802.1Q at *http://www.ieee802.org/1/pages/802.1Q.html*.

VoIP *Voice over Internet Protocol*. Also called "IP telephony," the routing of voice conversations via packets over an IP network such as the Internet.

VoWLAN *Voice over **WLAN***. **VoIP** over a Wi-Fi network.

VSC *Virtual Service Community*. A collection of configuration settings that define key operating characteristics of the wireless network, or WLAN, including the SSID, various security settings, and other advanced settings for QoS and wireless traffic management. Also, an access group to which users must authenticate before they can send data over the wireless medium.

W

war driver Someone who uses a directional **antenna** to pick up signals from a company's **WLAN**. War drivers are so called because they often drive along the road to see which signals they can pick up. They often analyze wireless packets to obtain information on the network's structure and security protocols, and they can sometimes connect to a WLAN if the security settings are not strong enough.

WDS *Wireless Distribution System*. See **local mesh**.

Web-Auth *Web Authentication*. A method for authenticating end users that does not require a client utility on the **endpoints**. The network access server redirects end users to a Web page in which the end users submit their **credentials**. The server retrieves the credentials and submits them to an **authentication** server.

WEP *Wired Equivalent Privacy.* An encryption protocol that is part of the IEEE **802.11** suite for wireless LANs. Its purpose is to provide security that is equivalent to an unsecured wired LAN. It has been superseded by **WPA** and **IEEE 802.11i**. For more information, see IEEE 802.11 at *http://standards.ieee.org/getieee802/802.11.html.*

Wibree A low-power, short-range standard that is similar to **Bluetooth**. It operates at 2.4 GHz at 1 Mbps over 10 m. Applications include wrist watches, toys, keyboards, and sports sensors. For more information, see the Wibree Web site at *http://www.wibree.com*.

WiMAX *Worldwide Interoperability for Microwave ACCess*. Based on IEEE **802.16**, it is sometimes called wireless MAN. It is designed for long-distance, point-to-point links and can be used as a **wireless bridge** between Wi-Fi hotspots or as a link between an ISP to an end user. It operates at 2–11 GHz and 10–66 GHz and uses scalable **OFDM** access (SOFDMA) as the modulation scheme. For more information, see the WiMAX Forum at *http://www.wimaxforum.org/home*.

wireless bridge See **local mesh**.

wireless USB A wireless version of USB. It operates at frequencies from 3.1 GHz to 10.6 GHz with a maximum data rate of 480 Mbps at 3 m. It uses the Multiband-**OFDM** (MB-OFDM) modulation scheme. Applications include wireless game controllers, MP3 players, flash drives, hard disks, digital cameras, printers, and scanners. For more information, see the Universal Serial Bus Web site at *http://www.usb.org/developers/wusb*.

WLAN *Wireless LAN*. The generic term for any LAN that has radio frequencies as its **PHY layer**.

WMM *Wi-Fi MultiMedia*. Also known as WME (Wireless Multimedia Extensions), a Wi-Fi Alliance certification that is based on **IEEE 802.11e** to provide **QoS** features to **802.11** networks.

WMTS *Wireless* ***Medical Telemetry*** *Services*. A set of frequencies that have been set aside for the remote monitoring of a patient's vital signs over radio frequencies. The frequencies are 608–614 MHz, 1395–1400 MHz, and 1427–1432 MHz. For more information, see the FCC Web site at *http://wireless.fcc.gov/services/index.htm?job=service_home&id=wireless_medical_telemetry.*

WPA *Wi-Fi Protected Access*. A standard created by IEEE and the Wi-Fi Alliance to address the security weaknesses in **WEP**. It includes **TKIP** for key assignment and the **Michael** algorithm for packet integrity checking.

WPA2 An implementation of **WPA** that includes the mandatory elements of **802.11i**. In addition to **TKIP** and **Michael**, it has the **CCMP** encryption algorithm.For more information, see the Wi-Fi Alliance at *http://www.wi-fi.org/knowledge_center/wpa2*.

WPA-PSK ***WPA*** *using a Preshared Key.* **PSK** refers to a **key** that is shared between two stations before it needs to be used, such as over a secured channel or non-electronically (the end user is told the correct key).

X

Xsupplicant An **802.1X supplicant** developed by the Open1X project to run on Linux platforms. It permits authentication to a **RADUIS** server and use of the **EAP** protocols. For more information, see *http://open1x.sourceforge.net.*

Y

Yagi antenna Also known as a Yagi-Uda **antenna**, a common type of **directional antenna** that consists of one driven dipole, a reflector, and one or more directors. *See also* **omnidirectional antenna**.

Z

ZigBee A specification that is based on the IEEE **802.15.4** standard for low-power, low-data-rate digital radios that require long battery life. Applications include wireless headphones, embedded sensing, home automation, warning systems, and medical data collection. For more information, see the ZigBee Alliance at *http://www.zigbee.org/en/index.asp*.

Reference Tables

IEEE Family of Wireless Standards

The table below shows the current state of the 802.11x and other standards for wireless transmission. Fields marked "unknown" show where the standard has not yet been defined.

Table B-1. IEEE 802.x Standards

Standard	Frequency Range	Maximum Rate (Mbps)	Indoor Range* (m)	Use
802.11a	5 GHz	54	35	WLAN
802.11b	2.4 GHz	11	45	WLAN
802.11g	2.4 GHz	54	40	WLAN
802.11n	2.4 and 5 GHz	248; 600 with channel bonding	70	WLAN
802.11y	3.65–3.70 GHz	54	50	Fixed P2P, point-to-mobile
802.15	2.4 GHz	1	10	PAN
802.15.4	868 MHz 902–928 MHz 2.4 GHz	0.1	10	Low-rate PAN
802.16	2–66 GHz	40	10,000	LAN/MAN broadband wireless (WiMAX)
802.20	< 3.5 GHz	> 1	n/a	Mobile broadband wireless access (MBWA) (vehicular mobility)
802.22	54–862 MHz	unknown	n/a	Wireless regional area network (WRAN) point-to-multipoint

*Ranges are for comparison purposes only. Actual range will vary depending on many factors.

Table B-2. Modulation Coding Scheme (MSC) Rates for 802.11n

						GI= 800ns		GI = 400ns	
				CBPS		Data Rate (Mbps)		Data Rate (Mbps)	
MCS Index	Spatial Streams	Modulation	Coding Rate	20 MHz	40 MHz	20 MHz	40 MHz	20 MHz	40 MHz
0	1	BPSK	1/2	52	108	6.5	13.5	7.2	15
1	1	QPSK	1/2	104	216	13	27	14.4	30
2	1	QPSK	3/4	104	216	19.5	40.5	21.7	45
3	1	16-QAM	1/2	208	432	26	54	28.9	60
4	1	16-QAM	3/4	208	432	39	81	43.3	90
5	1	64-QAM	2/3	312	648	52	108	57.8	120
6	1	64-QAM	3/4	312	648	58.5	121.5	65	135
7	1	64-QAM	5/6	312	648	65	135	72.2	157.5
8	2	BPSK	1/2	104	216	13	27	14.4	30
9	2	QPSK	1/2	208	432	26	54	28.9	60
10	2	QPSK	3/4	208	432	39	81	43.3	90
11	2	16-QAM	1/2	416	864	52	108	57.8	120
12	2	16-QAM	3/4	416	864	78	162	86.7	180
13	2	64-QAM	2/3	624	1296	104	216	115.6	240
14	2	64-QAM	3/4	624	1296	117	243	130	270
15	2	64-QAM	5/6	624	1296	130	270	144.4	300
16	3	BPSK	1/2	156	324	19.50	40.50	21.67	45.00
17	3	QPSK	1/2	312	648	39	81	43.33	90
18	3	QPSK	3/4	312	648	58.5	121.5	65	135
19	3	16-QAM	1/2	624	1296	78	162	86.67	180
20	3	16-QAM	3/4	624	1296	117	243	130	270
21	3	64-QAM	2/3	936	1944	156	324	173.33	360
22	3	64-QAM	3/4	936	1944	175.5	364.5	195	405
23	3	64-QAM	5/6	936	1944	195	405	216.67	450
24	4	BPSK	1/2	208	432	26	54	28.89	60
25	4	QPSK	1/2	416	864	52	108	57.78	120
26	4	QPSK	3/4	416	864	78	162	86.67	180
27	4	16-QAM	1/2	832	1728	104	216	115.56	240
28	4	16-QAM	3/4	832	1728	156	324	173.33	360
29	4	64-QAM	2/3	1248	2592	208	432	231.11	480

CBPS = Coded Bits per Symbol; GI = Guard Interval

						GI= 800ns		GI = 400ns	
				CBPS		Data Rate (Mbps)		Data Rate (Mbps)	
MCS Index	**Spatial Streams**	**Modulation**	**Coding Rate**	**20 MHz**	**40 MHz**	**20 MHz**	**40 MHz**	**20 MHz**	**40 MHz**
30	4	64-QAM	3/4	1248	2592	234	486	260	540
31	4	64-QAM	5/6	1248	2592	260	540	288.89	600
32	1	BPSK	1/2		48		6		6.67

CBPS = Coded Bits per Symbol; GI = Guard Interval

Table B-3. Protection Mechanism Overhead

Protection Mechanism	Channel Bandwidth (MHz)	Aggregated Frame Size (Bytes)	PHY Data Rate (Mbps)	Link-Layer Throughput (Mbps)	Protection Overhead (Percent)
RTS-CTS	40	1500	300	36.84	88
	40	66535	300	258	14
	20	1500	144	32.5	77
	20	66535	144	133.9	7
CTS-to-Self	40	1500	300	44.6	85
	40	1500	600	48.22	92
	40	66535	600	475.47	21
L-SIG TXOP					< 0.1

Table B-4. Wireless Modes; Shaded Cells = MSM422 Only

	Frequency (GHz)	Bit Rates (Mbps)	Channel Widths (MHz)
802.11b	2.4	11	20
802.11g	2.4	54	20
802.11 b/g	2.4	11, 54	20
802.11a	5	54	20
802.11a Turbo	5		40
802.11n	5	300	40
802.11n	2.4	300	40
802.11n/a	5	270, 54	40, 20
802.11n/g	2.4	270, 54	40, 20
802.11n/b/g	2.4	270, 11, 54	40, 20

Calculations for Transmission Range

RSL Formula

To calculate received signal level (RSL) between site A and site B, use the following formula:

RSL = (EIRP of site A (dBi)) – (path loss between sites (dBm)) + (receiver sensitivity of site B (dBi))

If the RSL is higher than the receiver's sensitivity level, the signal is probably strong enough (but always verify through real-world testing).

EIRP Formula

Effective isotopic radiated power (EIRP) is the measurement of signal strength generated by a radio system and output through the antenna. EIRP is measured in units of decibels over isotropic (dBm).

To calculate EIRP:

EIRP = (transmit power (dBm)) – (cables and connectors (dB)) + (antenna gain (dBi))

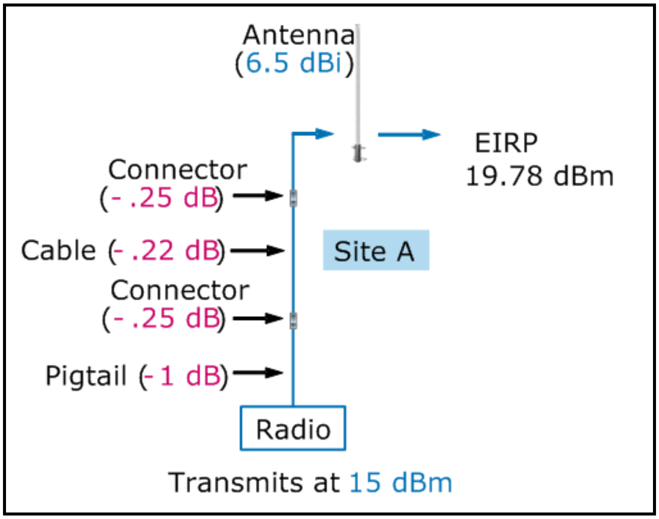


Figure B-1. Example EIRP Calculation

The figure shows the calculation for EIRP for a radio operating at 15 dBm and connected to a 6.5 dBi gain antenna:

15 dBm – (1 dB + .25 dB + .22 dB + .25 dB) + 6.5 dBi = 19.78 dBm

Path-Loss Formula

The path-loss equation uses these variables:

- Lp = free-space path loss in dBi
- F = frequency in GHz
- D = distance in meters

$Lp = 32.4 + 20 \log_{10} F + 20 \log_{10} D$

Wireless networks use one of two frequencies, so you can use these simplified equations:

- 2.4 GHz

  $Lp = 40.0 + 20 \log_{10} D$
- 5 GHz

  $Lp = 46.4 + 20 \log_{10} D$

The free-space equation assumes only that power falls off as a square of the distance. This assumption emerges as the 20 coefficient in the equation:

$10 * \log D^2 = 20 * \log D$

The following are scattering exponents (D^x) for some typical environments.

Table B-5. Scattering Exponents

Type of Space	Scattering Exponent
Open outdoors spaces	2 for short distances; add .5 for each 200 m
Outdoors with trees or buildings	3 or 4
Indoors with open spaces	2.5
Indoors with cubicles or other partitions	3.5
Indoors with walls	4 or 5

Thus, if your company has a building with fully divided offices, you might use this equation to calculate path loss:

$32.4 + 20 \log_{10} F + 20 \log_{10} D$

Table B-6 lists the attenuation values for common materials.

Table B-6. Approximate RF Attenuation Values for Common Materials

Material	Thickness in Inches	Thickness in Centimeters (Approximation)	Attenuation, dB 2.4 GHz	Attenuation, dB 5 GHz
Red brick	3.5	9	7–8	13
	7	18	13	32
	10.5	27	20	33
Concrete[1]	4	10	15–22	18–25
	8	20	36–44	45–55
	12	30	50–65	74–85
Reinforced concrete	8	20	42–46	53–57
Masonry block	8	20	15	17
	16	40	22	27
	24	60	32	39
Cinder block	7.5	19	6–7	9–10
Stucco[2]	1	2.5	14–15	12–13
Brick-faced concrete	4 (concrete)	10	29	41
(Brick veneer 3.5 in./90 mm.)	8 (concrete)	20	48	67
Glass	0.25-0.75	0.6-1.9	0.5–1	1–2
Ceiling tile (suspended)	0.6	1.5	0.1	0.2
Drywall	0.25–0.625	0.6–1.6	0.5–1	0.5–1
Plywood	0.25–1.25	0.6–3.2	1.5–2	1.5–2
Solid wood[3]	1.5–2	4–5	3–4	4–6
(Spruce, pine, and fir)	3	8	6	8
	4.5	12	11	13
	6	16	15	20

[1] Concrete values vary, depending on mix ratios and age. Attenuation typically increases as curing times increase.

[2] Stucco is concrete poured over steel diamond mesh.

[3] The attenuation for wood can vary from the typical values listed in this table, depending on the moisture content. The higher the moisture content, the higher the attenuation, especially in the 2.4 GHz band.

Sources: *National Institute of Standards and Technology Report*, NISTIR 6055, Oct. 1997; Magis Network, “Propagation Losses Through Common Building Materials,” Aug. 2002; and Daniel M. Dobkin, *RF Engineering for Wireless Networks: Hardware, Antennas, and Propagation* (Newnes, 2005).

Conversion between Milliwatts and Decibels

To convert between dBm and mW, use these formulas.

Convert dBm to mW:

$$YmW = 10^{\frac{XdBm}{10}}$$

For example:

$$63mW \approx 10^{\frac{18dBm}{10}}$$

Convert mW to dBm:

$$XdBm = 10\log_{10}(YmW)$$

For example:

$$18dBm \approx 10\log_{10}(63mW)$$

Calculations for Cell Size

These tables list approximations for the maximum cell size that you should expect in various environments. Sizes are calculated theoretically from the following assumptions and then rounded to approximate values:

- Radios operate at 15 dBm
- A station's wireless NIC has a receiver sensitivity of:
  - –90 dBm at 1 Mbps
  - –80 dBm at 24 Mbps
  - –70 dBm at 54 Mbps

Environment Definitions

These are the definitions for the environment types:

Open

Open environments are those containing relatively unobstructed space such as in warehouses, large retail spaces, arenas, and outdoor locations. Of course, such environments are rarely entirely empty; for instance, large metal shelves such as those found in many warehouses are significant sources of obstruction for radio signals. Outdoors, trees can also cause attenuation.

Semi-Open

Semi-open spaces are office environments with many partitions such as cubicles or movable walls. Such environments may 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 the environment.

Closed

Closed environments are typical for homes or corporate offices that have floor-to-ceiling walls and permanent doors. You will need to pay close attention to the construction materials in the walls as you create your preliminary plan; the type of material affects signal attenuation between offices.

Path Loss

Table B-7. Path Loss at 2.4 GHz

Environment	High-End Loss	Low-End Loss
Entirely open, no interference or obstructions	40 + 25 log D	40 + 20 log D
Open indoors	40 + 25 log D	42 + 25 log D
Outdoor, urban environment	40 + 40 log D	40 + 30 log D
Indoor, semi-open	40 + 40 log D	40 + 25 log D
Indoor, closed	40 + 40 log D	40 + 40 log D

Table B-8. Path Loss at 5 GHz

Environment	High-End Loss	Low-End Loss
Entirely open, no interference or obstructions	46 + 25 log D	46 + 20 log D
Open indoors	46 + 25 log D	48 + 25 log D
Outdoor, urban environment	46 + 40 log D	46 + 30 log D
Indoor, semi-open	46 + 40 log D	46 + 30 log D
Indoor, closed	46 + 40 log D	46 + 40 log D

Calculations for Wavelength

Some obstacles such as pine-tree needles or wire mesh interfere with RF signals only when their length (needles) or the gap between the wires (mesh) approaches multiples or fractions of the wavelength. Use the following formula to calculate the wavelength of a signal at a given frequency:

[wavelength (cm)] = [speed of light (cm/sec)] / [frequency (hertz)]

$$\lambda = \frac{c}{f}$$

$$\lambda = \frac{3 \times 10^{10}}{2.4 \times 10^{9}}$$

$$\lambda = 12.5$$

Table B-9. Wavelengths of WLAN Frequencies

Frequency	Wavelength		1/2 Wavelength	
	in	cm	Inches	Centimeters
2.4 GHz	4.92	12.5	2.46	6.25
5 GHz	2.36	6.0	1.18	3.0

New Colubris Product Names

The products mentioned in this design guide were originally offered by Colubris Networks before it was acquired by HP ProCurve. Table B-10 shows the Colubris product names and the new, HP ProCurve names.

Table B-10. Colubris-to-HP ProCurve Product Name Converter

Colubris Product Name	HP ProCurve Product Name	HP ProCurve Product Number
MSC-5100 Enterprise Mobility (US/CA, UK, EUR, AUS/NZ, ARG)	MSM710 Mobility Controller	J9325A
MSC-5200 (US/CA, UK, EUR, AUS/NZ, ARG)	MSM730 Mobility Controller	J9326A
MSC-5500 (US/CA, UK, EUR, AUS/NZ, ARG)	MSM750 Mobility Controller	J9327A
MSC-5100 Access Service (US/CA, UK, EUR, AUS/NZ, ARG)	MSM710 Access Controller	J9328A
MSC-5200 Access Service (US/CA, UK, EUR, AUS/NZ, ARG)	MSM730 Access Controller	J9329A
MSC-5500 Access Service (US/CA, UK, EUR, AUS/NZ, ARG)	MSM750 Access Controller	J3930A
MSC-3300 US	MSM323 US Access Point	J3937A
MSC-3300 (JAPAN, KOREA, ROW)	MSM323 WW Access Point	J9341A
MSC-3300R US	MSM323-R US Access Point	J9342A
MSC-3300R (JAPAN, KOREA, ROW)	MSM323-R WW Access Point	J9345A
MSC-3200 US	MSM313 US Access Point	J9346A
MSC-3200 (JAPAN, KOREA, ROW)	MSM313 WW Access Point	J9350A
MSC-3200R US	MSM313-R US Access Point	J9351A
MSC-3200R (JAPAN, KOREA, ROW)	MSM313-R WW Access Point	J9354A
Visitor Management Software	Guest Management software	J9355A
MAP-630 US	MSM335 US Access Point	J9356A
MAP-630 ROW	MSM335 WW Access Point	J9357A

Colubris Product Name	**HP ProCurve Product Name**	**HP ProCurve Product Number**
MAP-625 US	MSM422 US Access Point	J9358A
MAP-625 ROW	MSM422 WW Access Point	J9359A
MAP-330 US	MSM320 US Access Point	J9360A
MAP-330 (JAPAN, KOREA, ROW)	MSM320 WW Access Point	J9364A
MAP-330R US	MSM320-R US Access Point	J9365A
MAP-330R (JAPAN, KOREA, ROW)	MSM320-R WW Access Point	J9368A
MAP-330R AP+Sensor US	MSM325 Access Point	J9369A
MAP-330 AP+Sensor (JAPAN, KOREA, ROW)	MSM325 WW Access Point	J9373A
MAP-320 US	MSM310 US Access Point	J9374A
MAP-320 (JAPAN, KOREA, TAIWAN, ROW)	MSM310 WW Access Point	J9379A
MAP-320R US	MSM310-R US Access Point	J9380A
MAP-320R (JAPAN, KOREA, ROW)	MSM310-R WW Access Point	J9383A
WAP-200 US	M110 US Access Point	J9385A
WAP-200 (KOREA, TAIWAN, ROW)	M110 WW Access Point	J9388A
WCB-200 (US/CA, UK, EUR, KOREA, TAIWAN)	M111 Client Bridge	J9389A
RF Manager 1500 Enterprise	RF Manager 100 IDS/IPS system	J9397A
RF Manager 1300 Basic	RF Manager 50 IDS/IPS system	J9398A
RF Planner	RF Planner	J9400A
CNMS-200 Software for RHEL and CentOS	CNMS 200 Software	J9428A
CNMS-500 Software for RHEL and CentOS	CNMS 500 Software	J9429A

Site Survey Forms and Tables

Use these forms and tables as models for your own site survey forms.

Network Administrator Survey

The following sample worksheet is designed to help you interview IT managers and other manager in charge of network service at a potential wireless site.

Site name:	
Contact:	

1. What type of wireless implementation are you planning?
   a. A new wireless network
   b. An expansion of an existing wireless network
2. If the network is an expansion of an existing network, what equipment do you currently own?

   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____

____

____

____

3. Which wireless clients are supported on the network (Circle all that apply)
   i. 802.11a
   ii. 802.11b
   iii. 802.11g
   iv. 802.11n (2.4 GHz)
   v. 802.11n (5 GHz)

4. List the channels used by currently operating 802.11 devices.

   ____

5. Does your organization use 802.1X authentication?
   a. yes
   b. no
   c. no, but we intend to

6. In which locations is wireless network access indispensable?
   a. Building 1, Floor 1
   b. Building 1, Floor 2
   c. Building 2, Floor 1
   d. Building 2, Floor 2
   e. Building 3, East Wing
   f. Building 3, West Wing
   g. Cafeteria
   h. Courtyard

7. Where would access be nice, but is not required?
   a. Building 1, Floor 1
   b. Building 1, Floor 2
   c. Building 2, Floor 1
   d. Building 2, Floor 2
   e. Building 3, East Wing
   f. Building 3, West Wing
   g. Cafeteria
   h. Courtyard

8. Will users roam between APs in different subnets?

   a. Yes

   b. No

9. Which activities should the wireless network accommodate? Circle as many as apply.

   a. Browsing the Internet or using an HTTP client

   b. Checking email

   c. Video conferencing or using other streaming video applications

   d. Downloading or uploading files to an FTP site

   e. Editing documents or spreadsheets stored on a server

   f. Running graphical editing software stored on a server

   g. Voice over WLAN

10. Approximately how many users do you anticipate will use the wireless network at launch?

    a. 1 to 10

    b. 10 to 30

    c. 30 to 50

    d. 50 to 100

    e. 100 to 300

    f. 300 to 1000

    g. More than 1000

11. Approximately how many users do you anticipate will use the wireless network 6 months from now?

    a. 1 to 10

    b. 10 to 30

    c. 30 to 50

    d. 50 to 100

    e. 100 to 300

    f. 300 to 1000

    g. More than 1000

12. Approximately how many users do you anticipate will use the wireless network 12 months from now?

    a. 1 to 10

    b. 10 to 30

    c. 30 to 50

    d. 50 to 100

    e. 100 to 300

    f. 300 to 1000

    g. More than 1000

13. Which types of users must the wireless network accommodate? Circle all that apply.

    a. Employees with equal levels of access to network resources

    b. Employees with different levels of access to network resources

    c. Contractors

    d. Temporary employees

    e. Customers or other guests

    f. General public

14. Which wireless technologies does your site currently include? Circle all that apply.

    a. Cordless telephones

    b. Bluetooth and other short-range wireless

    c. Wireless telemetry (medical, industrial)

    d. RFID

    e. WiMAX

    f. Other

15. Which areas are included within a 150 m radius of your intended location for the AP? Circle all that apply.

    a. Areas controlled by your organization, closed to public access

    b. Areas controlled by your organization, open to public access

    c. Areas controlled by other companies

    d. Private residences

    e. Public areas

16. Consult nearby organizations. Do any of these organizations currently operate, or plan to soon implement, a wireless network?

    a. Yes

    b. No

17. Does your organization have any requirements for where APs must be installed?
    a. APs must be hidden
    b. APs must be readily accessible
    c. APs must be installed in a locked room
    d. APs must be in a plenum ceiling
    e. APs must be outdoors

18. What changes to buildings may occur in the next year?
    a. On-site construction
    b. Installation of cubicles
    c. Addition of, or movement of, building contents (such as furniture or file cabinets)

19. With which security regulations must your organization comply? Circle all that apply.
    a. SOX
    b. FISMA
    c. FERPA
    d. HIPAA
    e. GLBA
    f. PCI DSS

User Survey

The following worksheet provides an example of a user survey for employees who will want to access the wireless site once it is implemented.

Name:	
Telephone/email:	
Department/position:	

1. Where do you require wireless service? Circle as many as apply.
   a. Building 1, Floor 1
   b. Building 1, Floor 2
   c. Building 2, Floor 1
   d. Building 2, Floor 2
   e. Building 3, East Wing
   f. Building 3, West Wing
   g. Cafeteria
   h. Courtyard

2. Where would you like, but not require, wireless service? Circle as many as apply.
   a. Building 1, Floor 1
   b. Building 1, Floor 2
   c. Building 2, Floor 1
   d. Building 2, Floor 2
   e. Building 3, East Wing
   f. Building 3, West Wing
   g. Cafeteria
   h. Courtyard

3. When do you intend to be connected to the wireless network? Circle as many as apply.
   a. Before normal work hours (9:00 am)
   b. 9:00 am–11:00 am
   c. 11:00 am –1:00 pm
   d. 1:00 pm–3:00 pm
   e. 3:00 pm–5:00 pm
   f. After normal work hours (5:00 pm)
4. How long do you typically expect to remain connected?
   a. For less than 15 minutes
   b. 15–30 minutes
   c. 30 minutes–1 hour
   d. 1–3 hours
   e. 3–6 hours
   f. 8 hours
   g. All day
5. For which activities do you intend to use your wireless network connection? Circle as many as apply.
   a. Browsing the Internet
   b. Checking your email
   c. Video conferencing or using other streaming video applications
   d. Downloading or uploading files to an FTP site
   e. Editing documents or spreadsheets stored on a server
   f. Running graphical editing software stored on a server
   g. Voice over IP
6. What kind of data do you intend to access over the wireless connection? Circle as many as apply.
   a. Proprietary information (company confidential)
   b. Financial records (banking, credit card)
   c. Medical records
   d. Student records
   e. Classified material (government, military)
   f. Personal information (phone numbers, Social Security Numbers)
   g. Other sensitive or confidential information

7. While connected to the wireless network, do you intend:
   a. To stay in the same location
   b. To move from place to place

8. If you answered yes to the previous question, how far do you anticipate that you will move? Circle as many as apply.
   a. Less than 20 m (65 ft)
   b. 20–50 m (65–165 ft)
   c. 50–150 m (165–490 ft)
   d. 150–500 m (490–1640 ft)
   e. Between floors in the same building
   f. Between buildings

9. Which device or devices will you use to access the network? Circle as many as apply.
   a. Company-issued laptop or PC tablet
   b. Personal laptop or PC tablet
   c. Company-issued handheld device (PDA, smart phone)
   d. Personal handheld device

Wireless Network Documentation

You can use the tables in this section to document the steps you take to plan the wireless network.

User Devices, Data, and Applications

Use this table to map user types to applications, devices, and data. See

Table C-1. User Devices, Data, and Applications

Device	User Type	Applications	Bandwidth	Sensitive Data

Network Resource Security Level

Use this table to list data types and the security level that they require.

Table C-2. Network Resource Security Level

Network Resource	Security Level

User Access Needs

Use this table to record network resources, who will access them, and how and when they will be accessed.

Table C-3. User Access Needs

Network Resource	Users	Access Type	Location	Time

Existing Wireless Systems or Devices

Use this table to record existing wireless systems or devices on the site.

Table C-4. Existing Wireless Systems or Devices

System	Location	Frequency	Range	WLAN Interference

Network Infrastructure Devices

Use these tables to record your existing network infrastructure devices.

Table C-5. Network Infrastructure Devices—Switches

Vendor/Model Number	Layer 3 Switching	PoE	Gig PoE	Free Ports	802.1X	Port Speeds	Uplink Speeds	Location	IP Address

Use this table to record your existing 802.1X infrastructure devices.

Table C-6. 802.1X Infrastructure Devices

802.1X Infrastructure Device		
RADIUS servers	Type: IP address:	 IP address:
Directory services	Type: IP address: Integrated with RADIUS?	 IP address: yes no

Use this table to record existing servers.

Table C-7. Existing Servers

Server Name	Function or Contents	IP Address	Switch	Security Level

Existing VLANs

Use this table to record existing VLANs.

Table C-8. Existing VLANs

VLAN ID	Static or Dynamic	IP Address	Switches	Users and Servers

Physical Layer Decisions

Use this table to record your decisions about the VSC's Physical Layer.

Table C-9. Physical Layer Decisions

System	Physical Layer	Frequency (GHz)	Channels

Architecture Decisions

Use this table to record your decisions about WLAN architecture.

Table C-10. Architecture Decisions

Location	Architecture

Hardware Decisions

Use this table to record your hardware decisions.

Table C-11. WLAN Hardware Decisions

Location	Hardware

Security Compliance

Use this table to record your specialized security requirements and the measures you have or will take to meet them.

Table C-12. Security Compliance

Security Requirement	Compliance Measure	Adequate?

VSCs

Use these tables to record your initial VSC settings.

Table C-13. Initial VSC Settings

VSC (SSID)	SSID broadcast	Encryption	Authentication	Use Controller for Authentication and Access control	Users

VSC-to-VLAN Assignments

Use this table to record your VSC to VLAN assignments.

Table C-14. VSC-to-VLAN Assignments

VSC	Trusted	VLAN	VLAN IP	Linkage	Datastore

VSC Security Assignments

Use this table to record your VSC security assignments.

Table C-15. VSC Security Assignments

VSC (SSID)	SSID Broadcast	Validation	Encryption	Authentication

Wireless User Groups and Access Needs

Use this table to record the settings for HP ProCurve Identity Driven Manager.

Table C-16. Wireless User Groups and Access Needs

User Access Group	Network Resources	Days	Times	Locations	VSCs

Radio Settings

Use this table to record the 802.11 standard, channel, transmit power, and VSC settings for each radio.

Table C-17. Radio Settings

Radio	IEEE 802.11	Channel	Tx Power	VSCs
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				

Index

Technology for better business outcomes

To learn more, visit www.hp.com/go/procurve/

hp® ProCurve Networking

April 2010
Manual Part Number

5998-0589