**Applicable ProCurve Products**

- HP ProCurve Manager Plus (J9056A)
- HP ProCurve Identity Driven Manager (J9012A)
- HP ProCurve 8212zl Switch (J8715A)
- HP ProCurve 540zl Switch (J8697A)
- HP ProCurve 5406zl-48G Switch (J8699A)
- HP ProCurve 5412zl Switch (J8698A)
- HP ProCurve 5412zl-96G Switch (J8700A)
- HP ProCurve 5304zl Switch (J4850A)
- HP ProCurve 5304zl-32G Switch (J8166A)
- HP ProCurve 5308xl Switch (J4819A)
- HP ProCurve 5308xl-48G Switch (J8167A)
- HP ProCurve 5348xl Switch (J4849A)
- HP ProCurve 5372xl Switch (J4848B)
- HP ProCurve RF Manager 100 IDS/IPS system (J9397A)
- HP ProCurve RF Manager 50 IDS/IPS system (J9398A)
- HP ProCurve CNMS 200 software (J9428A)
- HP ProCurve CNMS 500 software (J9429A)
- HP ProCurve Guest Management software (J9355A)
- HP ProCurve RF Planner (J9400A)
- HP ProCurve RF sensor license (J9384A)
- HP ProCurve MSM710 Mobility Controller (J925A)
- HP ProCurve MSM730 Mobility Controller (J926A)
- HP ProCurve MSM750 Mobility Controller (J927A)
- HP ProCurve MSM710 Access Controller (J928A)
- HP ProCurve MSM730 Access Controller (J929A)
- HP ProCurve MSM750 Access Controller (J930A)
- HP ProCurve MSM323 US Access Point (J3937A)
- HP ProCurve MSM323 WW Access Point (J3941A)
- HP ProCurve MSM323-R US Access Point (J3942A)
- HP ProCurve MSM323-R WW Access Point (J3945A)
- HP ProCurve MSM313 US Access Point (J9351A)
- HP ProCurve MSM313-R US Access Point (J9350A)
- HP ProCurve MSM313-R WW Access Point (J9354A)
- HP ProCurve MSM422 US Access Point (J9358A)
- HP ProCurve MSM422 WW Access Point (J9359A)
- HP ProCurve MSM410 US Access Point (J9426A)
- HP ProCurve MSM410 WW Access Point (J9427A)
- HP ProCurve MSM335 US Access Point (J9357A)
- HP ProCurve MSM335 US Access Point (J9369A)

**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.
1 Wireless Network Design Process

Contents

Introduction ................................................. 1-4
Terminology .................................................. 1-4
Designing a New Wireless Network ...................... 1-5
Assess Customer Needs .................................... 1-5
Identify the Purpose of the Wireless Installation .... 1-6
Conduct a User Survey .................................... 1-8
Identify User Types ........................................ 1-8
Determine Usage Habits ................................... 1-9
Estimate User Density ...................................... 1-10
Identify User Equipment .................................. 1-11
Determine Roaming Requirements ....................... 1-12
Assess Security Needs .................................... 1-13
Conduct the Preliminary Site Survey ..................... 1-18
Identify Obstacles ......................................... 1-19
Identify RF Interference ................................... 1-20
Evaluate the Existing Infrastructure ..................... 1-26
Locate Power Outlets and Switches ..................... 1-27
Plan the Equipment Layout ................................ 1-27
Select a Physical Layer .................................... 1-27
Choose the Architecture ................................... 1-32
Select the Equipment ....................................... 1-41
MultiService Mobility Access Controllers and Mobility Controllers .................. 1-41
Client Bridge ................................................ 1-43
MultiService Mobility Access Points .................... 1-44
External Antennas .......................................... 1-48
Switches ...................................................... 1-48
Wireless Clients ............................................. 1-49
Choose a Management Solution ......................... 1-50
Plan Coverage and Capacity ............................................. 1-51
Planning with the RF Planner ........................................ 1-52
Planning Without the RF Planner ..................................... 1-53
Create a Security Plan .................................................... 1-56
Plan Physical Security .................................................. 1-56
Designate Access Zones ................................................. 1-57
Design the VLANs ......................................................... 1-58
Design the Wireless LAN Profiles (VSCs) ......................... 1-58
Choose the Security Protocols ....................................... 1-63
Determine User Restrictions .......................................... 1-72
Apply Additional Layers of Security .................................. 1-73
Invoke the MSM Controller’s Internal Firewall ................. 1-76
Use MAC Lockout ......................................................... 1-77
Configure Filters for a VSC ............................................. 1-77
Control Unauthorized or Rogue APs ................................. 1-80
Implement the RF Manager’s Wireless IDS/IPS ................ 1-82
Enforce Endpoint Integrity .............................................. 1-84
Perform the Initial Setup ............................................... 1-84
Configure Initial Settings on the APs and MSM Controllers .... 1-84
Configure VSCs .......................................................... 1-87
Install the MSM Devices ................................................ 1-87
Verify the Network is Ready to Authenticate Users .......... 1-87
Configure Radio Settings ............................................... 1-89
Implement Roaming ....................................................... 1-89
Layer 3 (Network) Roaming .......................................... 1-93
Reassess Coverage ....................................................... 1-95
Monitor Network Performance ....................................... 1-96
Provide Increased Reliability .......................................... 1-96
Provide Radio Failover with Automatic Power Control on the APs ......................................................... 1-97
Highly Available Local Meshes ...................................... 1-97
Upgrading a Wireless Network to 802.11n .......................... 1-98
  Reasons to Upgrade to 802.11n .......................... 1-98
  Plan the Upgrade ........................................ 1-99
  Plan the Scope of the Upgrade ...................... 1-99
  Consider the Implications on Wireless Coverage 1-99
  Plan for Backward-Compatibility .................. 1-99
  Consider the Affect of High-Speed Mobility on Your Wired Network .......................... 1-100
  Complete the Upgrade ................................ 1-101
  Upgrade Your Wireless Stations .................. 1-101
  Evaluate the Upgrade ................................ 1-101

2 Example WLAN Installation

Contents ................................................... 2-1

Overview: PCU Medical Center .......................... 2-3
  The Site ................................................. 2-3

Assess Customer Needs ................................. 2-4
  Identify the Purpose of the Wireless Installation 2-4
  Identify User Types .................................. 2-5
  Identify User Equipment and Usage Habits .......... 2-10
  Estimate User Density and Determine Roaming Requirements 2-11
  Assess Security Needs .............................. 2-15
    Determine Risk Tolerance ......................... 2-16
    Observe Relevant Regulations .................. 2-17
  Determine Access Control .......................... 2-18

Conduct the Preliminary Site Survey ................. 2-19
  Define Space Types .................................. 2-19
  Identify Obstacles and RF Interference ............ 2-19
  Evaluate Existing Infrastructure .................. 2-19
    Servers ............................................ 2-27
    Subnets and VLANs .............................. 2-30
Plan the Equipment Layout ........................................ 2-32
  Select a Physical Layer ........................................ 2-32
  Choose the Type of AP Architecture .......................... 2-33
  Select the Equipment ......................................... 2-34
  Choose a Management Solution ................................ 2-35

Plan Coverage and Capacity with RF Planner ................. 2-36
  Indoor Locations ............................................. 2-36
  Example Plan .................................................. 2-37
    Coverage View ............................................. 2-37
    Redundancy View ......................................... 2-42
    Link Speed View .......................................... 2-43
    Interference View ........................................ 2-44
    Calibration Points ........................................ 2-47
  Outdoor Locations ........................................... 2-47
  Example Plan .................................................. 2-48
    External Antennas ......................................... 2-49

Create a Security Plan .......................................... 2-52
  Account for Physical Security ............................... 2-53
  Designate Access Zones ..................................... 2-53
  Design the VLANs ............................................ 2-57
  Design the VSCs ............................................. 2-58
  Choose the Security Protocols ............................... 2-60
    Security Settings for the Local Mesh Links .............. 2-63
    Determine User Restrictions .............................. 2-64

Perform the Initial Setup and Survey ......................... 2-66
  Configure the Initial Settings and Set Up the Infrastructure ........................................ 2-66
    Set Up User Accounts and Policies ........................ 2-70
  Configure the VSCs ........................................ 2-70
  Mount the Access Devices ................................... 2-74
  Monitor Network Performance ............................... 2-75

Apply Additional Layers of Security .......................... 2-76

Finalize the Wireless Network .................................. 2-77
3 HP ProCurve Networking Resources for Wireless Networks

Services and Support ................................................. 3-1
HP ProCurve Networking Elite Partners ....................... 3-1
Implementation Guide ............................................. 3-2
Additional Resources ............................................. 3-2

A Glossary

B Reference Tables

IEEE Family of Wireless Standards .............................. B-1
WLAN Frequencies ................................................. B-5
Calculations for Transmission Range ......................... B-6
  RSL Formula ......................................................... B-6
  EIRP Formula ....................................................... B-6
  Path-Loss Formula ............................................... B-7
Receiver Sensitivities and Transmit Powers of HP ProCurve
  Products ............................................................. B-9
  Conversion between Milliwatts and Decibels .............. B-11
Calculations for Cell Size ........................................ B-12
  Environment Definitions ....................................... B-12
    Open .............................................................. B-12
    Semi-Open ...................................................... B-12
    Closed .......................................................... B-12
  Path Loss ........................................................ B-13
Calculations for Wavelength .................................... B-14
New Colubris Product Names ..................................... B-15
C  Site Survey Forms and Tables

Network Administrator Survey ........................................... C-1

Wireless Network Documentation ....................................... C-9
  User Devices, Data, and Applications ................................. C-9
  Network Resource Security Level ..................................... C-10
  User Access Needs ......................................................... C-11
  Existing Wireless Systems or Devices ................................. C-12
  Network Infrastructure Devices ....................................... C-13
  Existing VLANs ............................................................. C-15
  Physical Layer Decisions ................................................. C-16
  Architecture Decisions .................................................. C-16
  Hardware Decisions ....................................................... C-17
  Security Compliance ..................................................... C-18
  VSCs ............................................................................ C-19
  VSC-to-VLAN Assignments ............................................... C-20
  VSC Security Assignments ............................................... C-21
  Wireless User Groups and Access Needs .............................. C-22
  Radio Settings ............................................................... C-23

D  Supplementary Information

EAP Methods ................................................................. D-1
  EAP-Message Digest 5 (MD5) ............................................. D-2
  EAP-TLS (Transport Level Security) .................................... D-3
  EAP-Tunneled TLS (TTLS) ............................................... D-3
  Protected EAP (PEAP) ..................................................... D-4
  Lightweight EAP (LEAP) .................................................. D-4
  EAP-Subscriber Identity Module (SIM) ............................... D-4
  EAP-Generic Token Card (GTC) ......................................... D-4

Super G ................................................................. D-5
HIPAA Security Standards .................................................. D-6
  Physical Safeguards ..................................................... D-6
    Facility Access Controls ............................................. D-6
    Workstation Use ..................................................... D-7
    Workstation Security ............................................... D-7
    Device and Media Controls ......................................... D-8
  Technical Safeguards .................................................. D-9
    Access Control ...................................................... D-10
    Integrity ............................................................. D-11
    Security Guide for Offsite Users of EPHI ......................... D-12
Wireless Network Design Process

Contents

Introduction ................................................. 1-4
Terminology .................................................. 1-4
Designing a New Wireless Network ...................... 1-5
  Assess Customer Needs ................................. 1-5
  Identify the Purpose of the Wireless Installation .... 1-6
  Conduct a User Survey ................................. 1-8
  Identify User Types ...................................... 1-8
  Determine Usage Habits .................................. 1-9
  Estimate User Density .................................. 1-10
  Identify User Equipment .............................. 1-11
  Determine Roaming Requirements .................. 1-12
  Assess Security Needs ............................... 1-13
  Conduct the Preliminary Site Survey ............. 1-18
  Identify Obstacles ..................................... 1-19
  Identify RF Interference ........................... 1-20
  Evaluate the Existing Infrastructure ............ 1-26
  Locate Power Outlets and Switches .............. 1-27
Plan the Equipment Layout ............................ 1-27
  Select a Physical Layer .............................. 1-27
  Choose the Architecture ............................ 1-32
  Select the Equipment ................................. 1-41
MultiService Mobility Access Controllers and Mobility Controllers .............................. 1-41
  Client Bridge ............................................ 1-43
  MultiService Mobility Access Points ............ 1-44
External Antennas .................................................. 1-48
Switches .......................................................... 1-48
Wireless Clients ..................................................... 1-49
Choose a Management Solution ............................. 1-50
Plan Coverage and Capacity ................................... 1-51
  Planning with the RF Planner ............................... 1-52
  Planning Without the RF Planner ......................... 1-53
Create a Security Plan ............................................ 1-56
  Plan Physical Security ....................................... 1-56
  Designate Access Zones ..................................... 1-57
  Design the VLANs ............................................. 1-58
  Design the Wireless LAN Profiles (VSCs) ............... 1-58
  Choose the Security Protocols ............................. 1-63
  Determine User Restrictions ............................... 1-72
Apply Additional Layers of Security ....................... 1-73
  Invoke the MSM Controller’s Internal Firewall ........ 1-76
  Use MAC Lockout ............................................. 1-77
  Configure Filters for a VSC ................................. 1-77
  Control Unauthorized or Rogue APs ....................... 1-80
  Implement the RF Manager’s Wireless IDS/IPS .......... 1-82
  Enforce Endpoint Integrity .................................. 1-84
Perform the Initial Setup ........................................ 1-84
  Configure Initial Settings on the APs and MSM Controllers 1-84
  Configure VSCs ............................................... 1-87
  Install the MSM Devices ..................................... 1-87
  Verify the Network is Ready to Authenticate Users .... 1-87
  Configure Radio Settings .................................... 1-89
  Implement Roaming ............................................ 1-89
  Layer 3 (Network) Roaming ................................. 1-93
  Reassess Coverage ............................................ 1-95
  Monitor Network Performance .............................. 1-96
Provide Increased Reliability ................................. 1-96
  Provide Radio Failover with Automatic Power Control on the APs ........................................ 1-97
  Highly Available Local Meshes .............................. 1-97
Upgrading a Wireless Network to 802.11n .......................... 1-98
  Reasons to Upgrade to 802.11n ................................. 1-98
  Plan the Upgrade .................................................. 1-99
    Plan the Scope of the Upgrade .............................. 1-99
    Consider the Implications on Wireless Coverage .......... 1-99
    Plan for Backward-Compatibility ........................... 1-99
    Consider the Affect of High-Speed Mobility on Your
    Wired Network ................................................. 1-100
  Complete the Upgrade ............................................ 1-101
  Upgrade Your Wireless Stations ............................... 1-101
  Evaluate the Upgrade ............................................. 1-101
Introduction

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

■ Design a new wireless network
■ Upgrade the network to 802.11 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 1-98

Terminology

In this design guide, *access point (AP)* will be used as a generic term to describe HP ProCurve MultiService Mobility (MSM) APs. 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.
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.

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

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 Customer 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 1-51
■ “Create a Security Plan” on page 1-56
■ “Apply Additional Layers of Security” on page 1-73
■ “Perform the Initial Setup” on page 1-84
■ “Provide Increased Reliability” on page 1-96

Assess Customer Needs

As an IT professional charged with establishing a wireless network, your first step should be to define the intended purposes of the wireless network and the needs of those who will use it. You should know whether the wireless network is intended to extend the network into new areas, to provide network access to new or temporary users, or simply to enable mobility. Define the purposes and needs in as much detail as possible. 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: some questions you can answer immediately, perhaps even before visiting the installation site; other questions might need to wait for the site survey for a final answer.

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

**Identify the Purpose of the Wireless Installation**

There are two basic purposes for a wireless installation:
- **User access**
- **Local mesh**

These two functions can be used independently or together. In fact, on the ProCurve APs, a single radio can support both functions simultaneously.

---

**Note**

A local mesh is also sometimes called a wireless bridge or a wireless distribution system (WDS). This design guide uses the term *local mesh*.

**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. (See “IEEE Family of Wireless Standards” in Appendix B, “Reference Tables.”)

**Local Mesh.** A local mesh can be used to connect areas if a wired connection is not available or feasible. For example, a company may want to connect the networks in two buildings or areas within a large warehouse. Depending on the AP, 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. However, each AP can support six static local meshes, which you can use to create point-to-multipoint configurations.
Wireless Network Design Process
Designing a New Wireless Network

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 fails, 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 APs 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.

Figure 1-1. Static Local Mesh

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 bridge 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 points

**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. Remember to ask multiple-choice questions rather than open-ended questions so that you can more easily compile and analyze the results.

**Identify User Types**

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 library, for example), all 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 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 basic print services. Their bandwidth needs are therefore lower than for the other groups, and their mobility can vary, depending on the nature of their visit.

Determine Usage Habits

You should also determine usage habits, or 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.
**Wireless Network Design Process**

**Designing a New Wireless Network**

**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 data 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 ahead of time 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. 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 mobile users who will access the wireless network in each area, keeping in mind that the number could fluctuate during the day.
Identify User Equipment

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

Typically, wireless devices fall into one of these groups:

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

- **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. These phones use relatively little bandwidth, are highly likely to roam, and do not tolerate interruptions in the data stream.

- **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 companies 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 1-27.)

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 the devices’ capabilities. You should know if the devices support:

■ 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

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 freely from place to place. As a user moves from one place to another, his or her wireless device may need to disassociate from one AP and reassociate with another to maintain connectivity.

As the network administrator, you cannot explicitly control the mechanism by which a wireless client determines it should roam to a new AP: the roaming algorithm for each wireless client is proprietary, and the manufacturers typically do not release that information. Instead, you can plan for roaming by plotting likely roaming paths throughout the site and ensuring that places such as corridors are adequately covered.
Keep in mind that 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. A roaming wireless client can then receive a strong enough SNR from a new AP to support the required data rates before the wireless client moves out of range of its current AP.

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 the client 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 application may hang, forcing the user to restart the application.

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. Where do users want to roam? Do they expect to maintain uninterrupted access to applications as they roam? Will they notice if the wireless client temporarily drops the connection? Or do they just want to be able to access the wireless network from any location?

Assess Security Needs

You must determine the security needs for the wireless network. If you are establishing a public access network, 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 implementing a wireless network for a company, however, you are responsible for ensuring that your company’s data is protected. With few exceptions, most companies 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 proprietary organization information. However, some customer information—such as credit card numbers—is particularly valuable.

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

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

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

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

Once you know the importance of your organization’s network assets, you can determine its risk tolerance. If your organization stores customers’ credit card numbers, it has a low risk tolerance. That is, if a hacker stole those 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 additional 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.)
Wireless Network Design Process
Designing a New Wireless Network

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

- **Federal Information Security Management Act of 2002 (FISMA)**—FISMA is the primary legislation governing U.S. federal information security. 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). The solutions put into practice corporate security policies that address 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. Further-
Wireless Network Design Process
Designing a New Wireless Network

more, mobile users might inadvertently call up sensitive information in public areas. For example, a banker could call up customer account numbers on her laptop while she sits in the lobby, exposing the information to anyone who cares to look over her shoulder.

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

For more information about setting up access 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’s floor plan and make note of anything that can potentially interfere with your installation.

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

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

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

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

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

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

- Specialty glass—tinted, bullet-proof, energy-efficient, wire mesh, silvered (conventional mirror), or half silvered (two-way mirror) 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’s ventilation system. Building codes forbid placing anything inside a plenum ceiling that is not plenum rated, because toxic fumes from smoldering equipment could be spread quickly through the plenum into other areas of the building.

  If the building has a plenum ceiling, you must select 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 ensure that plenum-rated cables and attachment hardware are used.)

**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.
Wireless Network Design Process
Designing a New Wireless Network

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

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

- **802.15 Variants**

  ZigBee, based on IEEE 802.15.4, is designed for low-data-output, low-power applications such as medical data collection, industrial control, embedded sensors, and home and building automation. ZigBee builds on the 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 systems’ installation.

- **RFID Tags**

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

  There are three kinds of RFID tags:

  - **Passive**—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’s 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.
Wireless Network Design Process
Designing a New Wireless Network

■ 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

<table>
<thead>
<tr>
<th>System Type</th>
<th>Frequencies</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global System for Mobile Communications (GSM)</td>
<td>900 MHz, 1800 MHz, 1900 MHz</td>
<td>Mobile telephony</td>
</tr>
<tr>
<td>and relatives (Code Division Multiple Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[CDMA], Time Division Multiple Access (TDMA),</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Universal Mobile Telecommunications System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[UMTS])</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global Positioning System (GPS)</td>
<td>1227.60 MHz, 1575.42 MHz</td>
<td>Global positioning</td>
</tr>
<tr>
<td>Wireless Medical Telemetry Service (WMTS)</td>
<td>608–614 MHz, 1395–1400 MHz,</td>
<td>Medical monitoring devices</td>
</tr>
<tr>
<td></td>
<td>1427–1432 MHz</td>
<td></td>
</tr>
<tr>
<td>RFID</td>
<td>125–134.2 kHz, 140 –148.5 kHz</td>
<td>Tracking, inventory, payment systems,</td>
</tr>
<tr>
<td></td>
<td>13.56 MHz, 865–928 MHz, 902–</td>
<td>animal identification, electronic</td>
</tr>
<tr>
<td></td>
<td>928 MHz</td>
<td>locks</td>
</tr>
<tr>
<td>AM band</td>
<td>520–1610 kHz</td>
<td>Commercial radio</td>
</tr>
<tr>
<td>FM band</td>
<td>87.8–108.0 MHz</td>
<td>Commercial radio</td>
</tr>
<tr>
<td>UHF band*</td>
<td>300 MHz–3 GHz</td>
<td>Broadcast television</td>
</tr>
<tr>
<td>VHF band</td>
<td>30 –300 MHz</td>
<td>Broadcast television</td>
</tr>
<tr>
<td>Infrared</td>
<td>60,000–430,000 GHz</td>
<td>Remote controls</td>
</tr>
<tr>
<td>Near Field Communication (NFC)</td>
<td>13.56 MHz</td>
<td>Interactive advertising, mobile ticketing</td>
</tr>
<tr>
<td>Local Multipoint Distribution Service (LMDS)</td>
<td>26 GHz, 29 GHz, 31.0–31.3 GHz</td>
<td>Point-to-point, “last mile” telephony</td>
</tr>
</tbody>
</table>

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

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. For example, a 10/100Base-T (Cat5e) or a 10/100/1000 Base-T cable's 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 1-29.) 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 Gigabit PoE (which 802.11n requires), you should consider using a PoE injector.

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
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 will determine the frequency in which the AP will operate. 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 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—such as voice over WLAN (VoWLAN) phones or barcode scanners—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 best choice. 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’s wireless clients need. For example, if your network supports only 802.11b/g only devices (phones and bar code scanners, for example), you must select the 2.4 GHz band.

---

Table 1-3. Wireless Networking Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Frequency (GHz)</th>
<th>Theoretical Data Rates (Mbps)</th>
<th>Probable Maximum Throughput (Mbps)</th>
<th>Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>5</td>
<td>6–54</td>
<td>22</td>
<td>16 non-overlapping</td>
</tr>
<tr>
<td>802.11b</td>
<td>2.4</td>
<td>1–11</td>
<td>5</td>
<td>14 overlapping</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3 non-overlapping</td>
</tr>
<tr>
<td>802.11g</td>
<td>2.4</td>
<td>1–54</td>
<td>22</td>
<td>14 overlapping</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3 non-overlapping</td>
</tr>
<tr>
<td>802.11n</td>
<td>2.4</td>
<td>1–600</td>
<td>144</td>
<td>14 overlapping*</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3 non-overlapping*</td>
</tr>
<tr>
<td>802.11n</td>
<td>5</td>
<td>1–600</td>
<td>144</td>
<td>16 non-overlapping</td>
</tr>
</tbody>
</table>

*If you are not employing channel bonding
Channel overlap in the 2.4 GHz band limits the number of channels that you can use simultaneously. To avoid cross-channel interference, limit your channel use to the non-overlapping channels, listed in Table 1-4. This limited number of non-overlapping channels also affects 802.11n deployments that use channel bonding. Bonding two 20 MHz channels uses two-thirds of the total frequency capacity, so you should use the 5 GHz band when deploying 802.11n with channel bonding.

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

<table>
<thead>
<tr>
<th>Country</th>
<th>Number of Non-Overlapping Channels</th>
<th>Non-Overlapping Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>3</td>
<td>1, 6, 11</td>
</tr>
<tr>
<td>Europe and Australia</td>
<td>3</td>
<td>1, 7, 13</td>
</tr>
<tr>
<td>France and Spain</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>Japan</td>
<td>3</td>
<td>1, 7, 13</td>
</tr>
<tr>
<td>(14 for 802.11b)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rest of world</td>
<td>3</td>
<td>1, 6, 11</td>
</tr>
</tbody>
</table>

The channels that you may use for a wireless network depend on the country where your organization is located. Depending on your country, all or some 2.4 GHz channels may be restricted to indoor use. To see the specific channels by region, see “WLAN Frequencies” in Appendix B, “Reference Tables.”

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.

**802.11n.** As next-generation wireless applications emerge, improved WLAN data throughput capabilities are becoming essential. Even now, enterprise-class, bandwidth-intensive applications such as 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. Video conferencing is an uncertain proposition with 802.11g. Although 802.11g offers a maximum signal rate of 54 Mbps, it enables real-world throughput of half that or less.

In response, the IEEE Task Group N (TGn) and the Wi-Fi Alliance (WFA) have 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 to extend the operating distance of wireless networks.
Current drafts of 802.11n easily provide up to twice the range of 802.11g. Although the TGn’s goal is 600 Mbps maximum signal rate, the final proposal (scheduled for ratification in November 2009) will offer a throughput of approximately 300 Mbps in maximum configurations.

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, draft 2.0 of 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 uses two-thirds of the total frequency capacity.

**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's 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.
Wireless Network Design Process
Designing a New Wireless Network

- **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 MultiService Mobility products, you can choose between two types of architecture:

- **Autonomous**—Includes one or more HP ProCurve MultiService Mobility APs (MSM APs)

- **Optimized WLAN**—Includes at least one HP ProCurve MultiService Mobility Controller series device managing multiple MSM APs

In this architecture, the MSM APs are referred to as controlled APs.

**Note**

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

Whichever architecture you choose, you can establish multiple Virtual Service Communities (VSC) within the system. 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. 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 fast Layer 2 roaming.
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 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’s 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.
Wireless Network Design Process
Designing a New Wireless Network

Autonomous Architecture for a Public Access Network (Centralized Access Control). When you want to establish a public access VSC within an autonomous architecture, you must implement centralized access control on that VSC.

In this architecture, each AP is configured and managed separately. However, they forward all authentication and user traffic in the public access VSC to one of the APs, which is configured as the access controller.

The 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.

Several MSM APs are capable of acting as an access controller:

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

At least one AP in your system must be one of the models. Other APs can be other models.

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.
Figure 1-4. Optimized WLAN Architecture

The optimized WLAN architecture enables you to manage many APs centrally 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 time needed to manage) your wireless network.

In addition to giving you the advantages of centralized management, the optimized WLAN architecture allows you to control how wireless traffic flows into your wired network.

For example, you might have APs handle all user traffic on their own; in this case, the APs simply receive configurations from the controller. Alternatively, you can have the APs forward all user traffic to the controller for handling.
In other words, you select whether intelligence will be centralized at the controller or distributed to the APs at the edge. You can select the type of intelligence individually for each VSC:

- **Centralized Intelligence**

  Centralized intelligence enables the controller to act as the gatekeeper to the wired network, enforcing access controls on all wireless user traffic in this VSC.

  With centralized intelligence, you can also choose to use the controller as a gatekeeper between two distinct segments of the wired network: the public network and the protected network. Access to the public network and its resources is available to all users as soon as they successfully associate with the wireless network. However, to access the private network, users must authenticate (either to the controller or an external RADIUS server).

  One of the main reasons to implement centralized intelligence on a VSC is to create a public access VSC, in which users must authenticate through a login Web page before they can access the protected network.

  Centralizing intelligence 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 this approach is that the controller processes 100 percent of the wireless user traffic. The wireless network thus has a single point of failure, and the traffic detour to the controller adds latency and unnecessary traffic on the LAN backbone. Additionally, a single controller with its single uplink can handle the throughput associated with 802.11a/b/g standards but cannot easily adapt to the increased performance requirements of 802.11n.
### Distributed Intelligence

The distributed intelligence approach allows you to easily scale performance by combining the benefits of centralized management with the benefits of intelligent APs at the edge.

Unlike the centralized intelligence approach, in which all wireless user traffic is forwarded to controller, with the distributed intelligence approach, intelligent APs forward wireless traffic directly into the wired network. They can apply dynamic settings and security measures as they do so.

![Figure 1-6. Distributed Intelligence](image-url)
However, you can choose to send authentication traffic only to the controller for handling. This approach is called distributed intelligence with centralized authentication. You might select this approach when you want to use the controller's internal RADIUS database to authenticate users.

Figure 1-7. Distributed Intelligence with Centralized Authentication
The distributed intelligence 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 strain, and your users experience the full benefit of 802.11n.

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

| Table 1-5. Advantages and Disadvantages to Centralized and Distributed Intelligence |
|------------------------|------------------------|
| **Approach**           | **Advantages**                                      | **Disadvantages**                                      |
| Centralized Intelligence | • Effective coverage of large areas | • Controller must process 100 percent of the network traffic, creating single point of failure |
|                        | • Centralized management of APs with a controller | • Designed to handle the throughput associated with 802.11a/g standards, so it can not easily address the increased performance that comes with 802.11n |
|                        | • An integrated firewall, DHCP server, and RADIUS server for wireless traffic (ideal for networks that have a limited infrastructure) | • No failover mechanism if controller fails |
|                        | • Automatic seamless and fast roaming between all APs controlled by one controller | • Separate management for the wireless network |
|                        | • Authentication and access control for the wireless network independent of the wired network | |
|                        | • Dynamic meshing across a work space | |
|                        | • Handling for client stations configured with invalid static IP addresses | |
| Distributed Intelligence | • Effective coverage of large areas | • Separate management for the wireless network |
|                        | • Centralized management of APs with a controller | • No public access network (Web-Auth) |
|                        | • Fast Layer 2 roaming (< 50 µs) between APs in the same subnet that are connected to the same MSM Mobility Controller | • No integrated DHCP server for wireless users |
|                        | • Layer 3 roaming between APs that are in different subnets | • No integrated firewall for wireless traffic |
|                        | • 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’s internal RADIUS server (the centralized authentication option) | |
Combining Architectures. You might have 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 intelligence for employee VSCs and centralized intelligence for guest VSCs. The same main office may connect through WAN links to small branch offices that have autonomous architectures for mobility.

Select the Equipment

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

MultiService Mobility Access Controllers and Mobility Controllers

The HP ProCurve MSM700 Series includes both Access Controllers and Mobility Controllers.

HP ProCurve MSM700 Series Access Controller. The 802.11n-ready MSM700 Series Access Controllers centrally control the operation of the wireless infrastructure network, provisioning a broad range of identity-based services to ensure consistent QoS and security to stations that use and roam across the network. An integral component of HP ProCurve MultiService Mobility Solutions, the MSM700 Series pushes QoS and security policies to MultiService Mobility (MSM) APs at the network edge, where traffic is forwarded directly from source to destination.

MultiService Mobility features:

- 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:

- Controls a network of MSM APs per controller, ensuring consistent security, QoS, and roaming services from AP to AP (The controller's model number dictates the number of APs that it can control.)
- Central management of wireless access point 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 L2/L3 infrastructure resources, for example, QoS, VLANs, NAC, Active Directory and RADIUS AAA

Security features:

- 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 AAA services
- Built-in stateful firewall for secure connection to Internet
- Secure management interfaces, including SSH/SSL access to command-line and Web browser interfaces, 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
HP ProCurve MSM700 Series Mobility Controllers. The HP ProCurve MSM700 Series Mobility Controllers are ProCurve MSM700 Series Access Controller with a Mobility license installed. This license can be factory installed, or you can install it manually. The Mobility Controllers provide all the benefits of the Access Controllers, as well as two features for improving roaming:

- **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 special client software.

For more information on the mobility features, see “Implement Roaming” on page 1-89.

### Table 1-6. MSM700 Series Features

<table>
<thead>
<tr>
<th>Service pack</th>
<th>MSM710</th>
<th>MSM730</th>
<th>MSM750</th>
</tr>
</thead>
<tbody>
<tr>
<td>Included services</td>
<td>VSC management</td>
<td>VSC management</td>
<td>VSC management</td>
</tr>
<tr>
<td></td>
<td>guest access</td>
<td>guest access</td>
<td>guest access</td>
</tr>
<tr>
<td></td>
<td>ultra-speed roaming</td>
<td>ultra-speed roaming</td>
<td>ultra-speed roaming</td>
</tr>
<tr>
<td>MSM AP scalability</td>
<td>802.11 a/b/g: 10</td>
<td>802.11 a/b/g: 40</td>
<td>802.11 a/b/g: 200</td>
</tr>
<tr>
<td></td>
<td>802.11n: 10</td>
<td>802.11n: 40</td>
<td>802.11n: 200</td>
</tr>
<tr>
<td>Max. simultaneous users</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Max. simultaneous guest access users</td>
<td>100</td>
<td>500</td>
<td>2000</td>
</tr>
<tr>
<td>Network interfaces</td>
<td>10/100/1000 Ethernet</td>
<td>10/100 Ethernet</td>
<td>10/100/1000 Ethernet</td>
</tr>
</tbody>
</table>

**Client Bridge**

HP ProCurve provides a product that enables devices without their own wireless NIC to connect to a wireless network.

**HP ProCurve M111.** The HP ProCurve 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 Solutions 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 Wireless Client Bridge**

- 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

**MultiService Mobility Access Points**

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

**HP ProCurve MSM313 and 323 Series Access Points.** HP ProCurve MSM313 and 323 Series Access Points control the operation of intelligent APs that are distributed throughout a wireless zone, 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 MSM700 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 323s, using the convenient downstream Ethernet port.
The MSM313 and 323s 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 HP ProCurve MSM313 and 323 Access Points**

- 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 1-7. HP ProCurve MSM313 and 323 Access Point Specifications

<table>
<thead>
<tr>
<th>Model</th>
<th>802.11 Radios</th>
<th>Enclosure</th>
<th>Ports</th>
<th>Antenna Connectors</th>
<th>Antennas</th>
<th>Power Inputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSM313</td>
<td>1 – a/j/b/g</td>
<td>indoor plenum-rated</td>
<td>2 – 10/100 (RJ-45) with daisy-chain support 1 – Serial (RJ-11)</td>
<td>2 – Reverse-polarity male SMA with diversity</td>
<td>2 – 2 dBi dual band 2.4/5GHz omni</td>
<td>5 VDC PoE</td>
</tr>
<tr>
<td>MSM313-R</td>
<td>1 – a/j/b/g</td>
<td>outdoor NEMA-rated</td>
<td>1 – 10/100 (RJ-45) waterproof</td>
<td>2 – N-type female with diversity, waterproof 2 – 5.5 dBi 2.4 GHz omni</td>
<td>PoE</td>
<td></td>
</tr>
<tr>
<td>MSM323</td>
<td>1 – a/j/b/g</td>
<td>indoor plenum-rated</td>
<td>2 – 10/100 (RJ-45) with daisy-chain support 1 – Serial (RJ-11)</td>
<td>4 – Reverse-polarity male SMA with diversity</td>
<td>4 – 2 dBi dual band 2.4/5GHz omni</td>
<td>5 VDC PoE</td>
</tr>
<tr>
<td>MSM323-R</td>
<td>1 – a/j/b/g</td>
<td>outdoor NEMA-rated</td>
<td>1 – 10/100 (RJ-45) waterproof</td>
<td>2 – N-type female, waterproof</td>
<td>2 – 5.5 dBi 2.4 GHz omni</td>
<td>PoE</td>
</tr>
</tbody>
</table>
HP ProCurve MultiService Mobility Access Points. The HP ProCurve MSM APs bring intelligence to the network edge, providing scalable, seamless wireless access anywhere, anytime. They dispense multiple network services, enforce robust security and deliver high performance client access, unlike “thin” or “lite” access points. An integral component of HP ProCurve Multi-Service 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.

Coverage features:
- 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:
- 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:
- 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 and MSM335.
- 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 Series Access Point Specifications

<table>
<thead>
<tr>
<th>Model</th>
<th>802.11 Radios</th>
<th>Enclosure</th>
<th>Ports</th>
<th>Antenna Connectors</th>
<th>Antennas</th>
<th>Power Inputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSM310 (US and WW)</td>
<td>1 – a/b/g indoor plenum-rated</td>
<td>2 – 10/100 (RJ-45)</td>
<td>2 – Reverse-polarity male SMA with diversity</td>
<td>2 – 2 dBi dual-band 2.4/5GHz omni</td>
<td>5 VDC PoE</td>
<td></td>
</tr>
<tr>
<td>MSM310-R (US and WW)</td>
<td>1 – a/b/g outdoor NEMA-rated waterproof</td>
<td>1 – 10/100 (RJ-45)</td>
<td>2 – N-type female with diversity, waterproof</td>
<td>2 – 5.5 dBi 2.4 GHz omni</td>
<td>PoE</td>
<td></td>
</tr>
<tr>
<td>MSM320 (US and WW)</td>
<td>2 – a/b/g indoor plenum-rated</td>
<td>2 – 10/100 (RJ-45)</td>
<td>4 – Reverse-polarity male SMA with diversity</td>
<td>4 – 2 dBi dual-band 2.4/5GHz omni</td>
<td>5 VDC PoE</td>
<td></td>
</tr>
<tr>
<td>MSM320-R (US and WW)</td>
<td>2 – a/b/g outdoor NEMA-rated waterproof</td>
<td>1 – 10/100 (RJ-45)</td>
<td>2 – N-type female, waterproof</td>
<td>2 – 5.5 dBi 2.4 GHz omni</td>
<td>PoE</td>
<td></td>
</tr>
<tr>
<td>MSM325 (US and WW)</td>
<td>2 – a/b/g/RF security</td>
<td>indoor plenum-rated</td>
<td>2 – 10/100 (RJ-45)</td>
<td>4 – Reverse-polarity male SMA with diversity</td>
<td>4 – 2 dBi dual-band 2.4/5GHz omni</td>
<td>5 VDC PoE</td>
</tr>
<tr>
<td>MSM335 (US and WW)</td>
<td>2 – a/b/g 1 – RF security</td>
<td>indoor plenum-rated</td>
<td>1 – 10/100/1000 (RJ-45) 1 – Serial (DB-9) female</td>
<td>2 – Reverse-polarity male SMA with diversity</td>
<td>6 – 2.4/5 GHz omni (3 per flap)</td>
<td>48 VDC PoE</td>
</tr>
<tr>
<td>MSM410 (US and WW)</td>
<td>1 – a/b/g/n draft</td>
<td>indoor plenum-rated</td>
<td>1 – 10/100/1000 (RJ-45) 1 – Serial (RJ-45)</td>
<td>None</td>
<td>3 – 2.4/5 GHz omni</td>
<td>PoE</td>
</tr>
<tr>
<td>MSM422 (US and WW)</td>
<td>1 – a/b/g 1 – a/b/g/n draft</td>
<td>indoor plenum-rated</td>
<td>1 – 10/100/1000 (RJ-45) 1 – Serial (DB-9) female</td>
<td>4 – 2.4/5 GHz reverse-polarity male SMA (3 with diversity)</td>
<td>5 – 2.4/5 GHz omni (2 with diversity) 3 – 3x3 MIMO 2 – 2.4/5 GHz</td>
<td>48 VDC PoE</td>
</tr>
</tbody>
</table>
External Antennas

External antennas provide additional gain and shaping of RF signals. (See Table 1-8, “HP ProCurve MSM Series Access Point 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.

The MSM422 and MSM335 have reverse polarity (RP) SMA antenna connectors to connect external antennas in addition to the internal antennas that are included with the APs. Because these two devices are rated for indoor use only, the extra antennas would be used to increase coverage within an existing coverage area; otherwise, you must run cabling between the outdoor antenna and the indoor AP.

Switches

If the existing switches are not adequate to your planned implementation, choose from among the following to add to the wired infrastructure:

Table 1-9. PoE-Enabled HP ProCurve Switches

<table>
<thead>
<tr>
<th>Switch Series</th>
<th>PoE</th>
</tr>
</thead>
<tbody>
<tr>
<td>8212zl</td>
<td>X</td>
</tr>
<tr>
<td>5400zl</td>
<td>X</td>
</tr>
<tr>
<td>5300xl</td>
<td>X*</td>
</tr>
<tr>
<td>3500yl</td>
<td>X</td>
</tr>
<tr>
<td>2600</td>
<td>X**</td>
</tr>
</tbody>
</table>

* 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).
Wireless Clients

The component of your wireless network that is perhaps least within your control is the wireless client of the devices that attach to the network. Some organizations provide wireless devices to authorized users and can therefore carefully control the properties of clients that are allowed to connect.

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

If your organization controls the clients 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 1-63 for more information.) Table 1-10 shows some of the features that are available on wireless clients. (Products were chosen from Internet shopping sites.)

If you cannot control the clients, you should choose network settings that will allow the largest number of users to connect without compromising security. For example, clients whose radios support 802.11b wireless networking are inexpensive and very common, even though the 802.11a standard allows for faster network speeds. 802.11g devices provide comparable speed to 802.11a devices, but fewer clients will be compatible with 802.11g than with 802.11b. Furthermore, some stations do not have an 802.1X supplicant, so you will need to make provisions for other types of authentication.

Currently, there are four primary form factors: a standard PCI card with an external antenna (attached or on a cord), CardBus (PCMCIA), ExpressCard, and USB (flash drive or antenna with USB cable).

Table 1-10. Example Wireless Client Features

<table>
<thead>
<tr>
<th>Form Factor</th>
<th>802.11 Standards</th>
<th>Tx Power (dBm)</th>
<th>Rx Sensitivity (dBm)</th>
<th>WPA</th>
<th>802.11i</th>
<th>802.1X</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI</td>
<td>a, b, g</td>
<td>10 to 20</td>
<td>-71 to -94</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>b, g, n</td>
<td>9 to 13</td>
<td>-70</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b, g, n</td>
<td>14 to 18</td>
<td>-85 to -86</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b, g, n</td>
<td>20</td>
<td>-60 to -90</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>CardBus</td>
<td>a, b, g</td>
<td>13 to 17</td>
<td>-73 to -94</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>a, b, g</td>
<td>10 to 20</td>
<td>-71 to -94</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>b, g, n</td>
<td>14 to 18</td>
<td>-79 to -84</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b, g, n</td>
<td>13 to 17</td>
<td>-65 to -85</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Wireless Network Design Process
Designing a New Wireless Network

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 client does not have a supplicant, you can usually install one. (See the list of supplicants on page 1-67.)

- Clients that boast 108 Mbps with 802.11g can attain that speed only with APs from the same vendor. (See “Super G” in Appendix D, “Supplementary Information” for more information.)

Choose a Management Solution

HP ProCurve Networking has designed its secure mobility solution as an extension of your existing network. If a company’s security policies allow users to access the same resources for both wired and wireless access, the users receive these rights—no matter how they connect. If the company wants to limit a user’s access when the user accesses the network through a wireless connection, the network enforces this policy as well.

HP ProCurve’s CNMS software provides a single, centralized system for managing your autonomous devices. The MSM Controllers can manage up to 200 controlled APs, depending on the model of the controller.

With IDM, you can centrally define and apply policy-based network access rights to enforce network security while providing appropriate access to network users and devices.
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’s hardware as well as the AP’s. Check your equipment’s 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 “Provide Radio Failover with Automatic Power Control on the APs” on page 1-97 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 with the RF Planner

RF Planner simplifies the complex task of planning a wireless networking infrastructure by enabling network managers to accurately model WLAN coverage by factoring in common variables, such as physical features, building materials, and WLAN equipment characteristics. RF Planner also facilitates deployment by enabling the assessment of security risks and generating equipment lists.

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 MultiService Mobility Access Points and Controllers, third-party equipment (access points 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.
Wireless Network Design Process
Designing a New Wireless Network

- 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 wireless access points using a simple drag and drop operation to generate RF maps and a comprehensive set of deliverables, including:
- Site model for future RF planning.
- BoM (Bill of Material) for RF sensors.
- BoM for access points and antennas, including:
  - Number and location of RF sensors
  - Number, location, and configuration of wireless access points.
  - Antenna types and location.
- RF Maps
  - Security View: Coverage inside the perimeter, coverage beyond the perimeter (spillage view), and redundancy.
  - Access Points: Coverage, Spillage, channel allocation, interference, and redundancy.

Planning Without the RF Planner

If you do not have the RF Planner, you can still implement ProCurve Wireless LAN solutions. You can use an RF Manager to create a rudimentary plan, or you can plan the implementation manually. To plan the implementation manually, 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.”.
Wireless Network Design Process
Designing a New Wireless Network

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

The example above, created with Microsoft Visio, 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’s 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’s 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.
Create a Security Plan

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. You will need to consider the following when designing wireless security:

- Physical security
- Access zones
- SSID broadcast
- Validation
- Authentication
- Encryption
- Access control

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 APs’ 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 APs’ 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 1-9 on page 1-48.)
Designate Access Zones

Generally, you can divide the security needs of your users into two categories: public and private. You can then divide your site into zones (on both a physical and network level) to help you see how and where to implement security measures.

**Public Access Zone.** The “public access” security level grants access to only the most basic services such as the Internet or VoWLAN. With a public wireless network, the goal is usually to provide convenient access for guests rather than to provide strong security. Because you have set up network security so that guests cannot access sensitive materials or confidential information, you do not need to worry too much about protecting the data that they access.

**Private Access Zone.** The “private access” security level is reserved for employees or temporary workers who need to access more sensitive areas of the network such as databases and applications and who need connections from a variety of locations. These users may also need to maintain their network connection while they roam. For private access zones, you should typically impose the tightest access control and encryption methods possible.

---

**Note**

The guidelines above were formulated under the assumption that you have control over the equipment that accesses your private wireless zone. If your organization allows employees to bring their own equipment, you must do some extra work to ensure that this equipment meets the standards for your wireless zone.

These zones are classifications for convenience; they provide a way to talk about the different needs that a network design must serve, but they do not have hard boundaries.

Network access zones often overlap: in a conference room, you might have both regular employees and guests working together. In other words, the area is acting as both a private and a public wireless zone.

For purposes of network design, it can be useful to look at overlapping network access zones separately because the best network design may use different technologies to provide an optimal access control solution for the different access needs.
Design the VLANs

As you evaluate the users that need wireless access and compare them to existing VLANs on the wired LAN, you might see the need to create a few more VLANs. For example, if guests were previously not able to access the wired LAN at all, there would not be a VLAN for them. You would therefore create a wireless-only VLAN that is for guests who need wireless access to the Internet (or whichever services you have decided to provide).

**Note**

When creating wireless-only VLANs using the optimized WLAN architecture, you will need to enable NAT 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 make sensitive resources off-limits.

Design the Wireless LAN Profiles (VSCs)

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.

Also think in terms of access zones (see page 1-57). Are there any access zones for which you need to create a separate VSC?

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 use an access-control server such as the ProCurve Network Access Controller (NAC) 800 to enforce endpoint integrity.

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 these 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.

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. 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.)

  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.
- **Dynamic, or User-Based, VLANs**—In autonomous mode, the APs also support dynamic, or user-based, VLANs, which 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’s 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.)
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 intelligence (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 dynamic VLANs for users. You simply set the egress VLAN when you bind the VSC to an AP’s group. If you want to use dynamic VLANs, you create the VLAN assignment on the RADIUS server that the APs use to authenticate users.

If you choose to use centralized intelligence with centralized access control, however, you have two additional options for using VLANs to control traffic. In addition to setting an egress (or static) VLAN and dynamic VLANs, you can configure:

- **VSC ingress VLAN**
  
  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. The third-party APs are configured to send the traffic on this VLAN to the service controller, and then based on this VLAN, the controller applies the appropriate VSC settings to the traffic. (With ProCurve MSM APs, the service controller uses the SSID to identify the traffic that should be assigned to a VSC.) Note that the VSC ingress VLAN should not be assigned an IP address on the controller.

  Also be aware that the VSC ingress VLAN is applied to all traffic tagged with that VLAN. So, any traffic on the wired network that is tagged with the ingress VLAN and routed to the controller will be processed according to the VSC to which the ingress VLAN is mapped.

- **VSC egress VLANs**
  
  APs use the egress VLAN that you specify when you bind the VSC to the APs’ group to forward users’ traffic to the controller. The VSC egress VLANs, on the other hand, determine the VLAN that the controller uses to forward users’ traffic onto the wired network.
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.

**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 beacons
- 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’s 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’s 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's 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.

The Web browser interface refers to MAC-Auth as MAC-based authentication. This guide will refer to it only 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.

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.

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’s 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.

  The Web browser interface refers to Web-Auth as *HTML-based authentication*. This guide will refer to it only as *Web-Auth*. 

---

Note

The Web browser interface refers to Web-Auth as *HTML-based authentication*. This guide will refer to it only 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.

**Note**

The APs do not have an 802.1X supplicant, so you would disable 802.1X authentication on the port to which the APs are connected.

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’s 802.1X supplicant supports.

802.1X supplicants can be found in the following:

- **Infrastructure devices:**
  - ProCurve switches, 2600 series and higher
- **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 requires some form of user interaction; however, some smartphones and printers automatically submit credentials such as a subscriber identity module (SIM) or digital certificate.

Table 1-11 shows which kinds of stations are compatible with each kind of authentication method.
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. See “EAP Methods” in Appendix D, “Supplementary Information” for a complete description of each method plus a decision flowchart for choosing an EAP method. 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 service 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, in a public access zone, 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 1-12. Comparison of Authentication Methods

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

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 1-13 is a summary of the advantages and disadvantages of each encryption method.
Table 1-13. Comparison of Encryption Methods

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

Table 1-14 shows which encryption options are available for each authentication method.

Table 1-14. Encryption Options Available for Authentication Methods

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Encryption Options</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password (or shared key)</td>
<td>Static WEP</td>
<td>Not recommended</td>
</tr>
<tr>
<td></td>
<td>WPA-PSK</td>
<td>For small organizations</td>
</tr>
<tr>
<td>802.1X</td>
<td>Dynamic WEP</td>
<td>Acceptable in some circumstances</td>
</tr>
<tr>
<td></td>
<td>Dynamic WPA/WPA2</td>
<td>Preferred</td>
</tr>
<tr>
<td>Web-Auth</td>
<td>None on its own</td>
<td>Acceptable for non-secure access; can be combined with WPA-PSK</td>
</tr>
<tr>
<td>MAC-Auth</td>
<td>None on its own</td>
<td>Adds some security to methods such as WPA-PSK</td>
</tr>
</tbody>
</table>

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.
Determine User Restrictions

With the data that you obtained about user types (“Identify User Types” on page 1-8), determine which kinds of restrictions you should impose on each user type. Restrictions dictate the resources and services that users can access. For example, you might decide that contractors can access the Internet, email, and selected file servers and databases but not the purchase order system.

In addition to basing restrictions on users’ identities, you can factor in the user's location, access time, VSC, and device. For example, you might decide that no one can access the financial database over a VSC available in public areas or that only executives can access the network on weekends.

Access Controls. Access controls can be implemented at various points in a network, such as the AP, the switch, an appliance, or server software. Many of the controls build on each other and they include:

- **None**—A wireless deployment or a certain VSC can specifically choose not to provide access control. Once a user has been authenticated (if authentication is being used), then all traffic from the user is allowed to continue to its destination.

- **ACLs**—An ACL is an ordered list of rules that selects packets according to header information and dictates whether the infrastructure device should permit (forward) or deny (drop) those packets. ACLs can be configured manually, in which case, they are usually applied to routing switches. For more security and granularity, ACLs can also be configured dynamically at the edge with a RADIUS server and a solution such as IDM. (See “Configure Filters for a VSC” on page 1-77.)

- **Static VLAN**—The AP assigns one VLAN to each SSID that the AP advertises. When a station associates with an SSID, the AP tags all traffic from that station with the corresponding VLAN ID. ACLs (whether static or dynamic) control which traffic can be routed out of the VLAN. In other words, an ACL could permit traffic from the Accounting VLAN to the Financial_Database VLAN.

- **Dynamic VLAN**—The AP assigns the VLAN based on user information that is stored in a RADIUS server. The AP queries the RADIUS server, which passes a VLAN ID for that station to the AP. The AP then tags all station traffic with the corresponding VLAN. Again, static or dynamic ACLs further control the user’s traffic.

- **IDM access policy**—IDM access policies help you to easily set up dynamic VLAN assignments and ACLs for user groups in your network. Through IDM you can also control access based on location, time of day, access type, or device.
Wireless Network Design Process  
Designing a New Wireless Network

- **NAC 800 access policy**—The ProCurve Network Access Controller 800 (NAC 800) is an appliance that can enforce “endpoint integrity,” which is the state of the station with regard to its security settings, installed applications, patches, and other criteria. The NAC 800 can quarantine a station that fails to comply with any of various tests by assigning it to a quarantine VLAN. If, on the other hand, the station passes the test, it is assigned to the user’s typical VLAN. The NAC 800 includes a RADIUS server and can be managed by IDM.

The APs should implement the access control methods you select as long as they are capable of doing so. In some cases, the switch port to which the AP connects might enforce the access control instead; however, this strategy is less desirable for several reasons:

- When the AP implements 802.1X authentication, the EAP exchange further the negotiation of secure per-session keys.
- If the switch port acts as the authenticator, it can authenticate a limited number of users. The number of users varies, depending on the switch. For example, the 3500yl, 5400zl, and 6200yl switches support up to 32 authenticated clients when the port is configured to support 802.1X in user-based mode. Other switches may support fewer authenticated clients per port. Wireless devices do not have the same type of limitation.

**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, today’s networks 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’s 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.

Depending on your company’s environment, you may want to apply additional layers of security to shore up your network defenses against such attacks and to further control access to network resources.

Such additional security measures include:

- **Firewalls**
- **MAC lockout**
- **Additional traffic filters**
- **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 (IPS)**

   An IPS detects and mitigates Denial of Service (DoS) attacks or other threats.

- **Network Access Control (NAC) solutions**

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

The ProCurve mobility products help you to implement these measures. Table 1-15 displays which products support each measure.

The HP ProCurve RF Manager 100 IDS/IPS system, an additional security appliance that you can install anywhere in your network, enhances several of the security features in ProCurve MSM products, as well as provides an IDS/IPS. The third column of Table 1-15 describes these enhancements. Note that, to function correctly, the ProCurve RF Manager must interoperate with MSM APs that are licensed and configured as sensors. It is the MSM AP's sensor that monitors the wireless traffic and reports information back to the RF Manager.
The final column of Table 1-15 indicates the section in this guide where you can learn more about each security capability.

**Table 1-15. Security Capabilities of ProCurve MultiService Mobility Products**

<table>
<thead>
<tr>
<th>Security Capability</th>
<th>Products that Support the Capability</th>
<th>Enhanced Capabilities with RF Manager + MSM AP Sensors</th>
<th>Guide Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>MSM Controller</td>
<td>—</td>
<td>“Invoke the MSM Controller’s Internal Firewall” on page 1-76</td>
</tr>
<tr>
<td>MAC lockout</td>
<td>• Autonomous MSM APs</td>
<td>Configure MAC lockout on multiple non-controlled APs (such as third-party APs)</td>
<td>“Use MAC Lockout” on page 1-77</td>
</tr>
<tr>
<td></td>
<td>• MSM Controller + controlled MSM APs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional traffic filters</td>
<td>• Autonomous MSM APs</td>
<td>—</td>
<td>“Configure Filters for a VSC” on page 1-77</td>
</tr>
<tr>
<td></td>
<td>• MSM Controller + controlled MSM APs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Neighbor AP detection</td>
<td>• Autonomous MSM APs</td>
<td>• Configure AP detection on a network-wide scale</td>
<td>“Control Unauthorized or Rogue APs” on page 1-80</td>
</tr>
<tr>
<td></td>
<td>• MSM Controller + controlled MSM APs</td>
<td>• Classify detected APs as:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Rogue (unauthorized APs connected to your wired network)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Friendly (your own APs)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• External (APs not connected to your wired network)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Predict the approximate location of the detected APs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Automatically block or disrupt traffic from rogue APs</td>
<td></td>
</tr>
<tr>
<td>IPS</td>
<td>RF Manager + MSM APs sensors</td>
<td></td>
<td>“Implement the RF Manager’s Wireless IDS/IPS” on page 1-82</td>
</tr>
<tr>
<td>NAC (endpoint integrity)</td>
<td>NAC 800</td>
<td>—</td>
<td>“Enforce Endpoint Integrity” on page 1-84</td>
</tr>
</tbody>
</table>
Invite the MSM Controller’s 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's Internet port.

![Integrated Firewall Diagram](image)

**Figure 1-12. Integrated Firewall**

The controller’s 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’s 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’s 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 devices’ wireless clients. (See “Wireless MAC Filter” on page 1-79.)

You can also configure MAC lockout through the RF Manager. You create a list of banned MAC addresses, and sensors 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.
Wireless Network Design Process
Designing a New Wireless Network

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 the architecture, whether centralized or distributed.

---

**Note**

As you recall, a centralized architecture is possible when you use an MSM Controller, but it is not required. Controlled APs can participate in a distributed architecture.

---

**Centralized Intelligence Architecture.** When you use the MSM Controller for 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 stations’ default gateway. Otherwise, all user traffic will be blocked by the AP.

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

- The AP’s 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).
Wireless Network Design Process
Designing a New Wireless Network

- A specified MAC address
  Select this option when wireless stations that connect to this VSC are placed on a different subnet from their AP's default gateway. Input the MAC address of the stations' 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 each gateway's MAC address.

**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's 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.
**Wireless Network Design Process**

**Designing a New Wireless 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.

---

**Control 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 using several devices:

- An MSM Controller
- An autonomous AP
- The RF Manager

**MSM Controller.** The MSM Controller can prevent unauthorized APs from becoming controlled by it. It can also collect information about all APs in the area whether controlled or not.

- **Prevent Unauthorized APs from Becoming 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 controllers’ source lists for authorized APs. If the AP’s MAC address is listed in one of the controllers’ 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 authenticates 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.

**Collect Information about All APs**

Once an AP is adopted by the 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 AP.** 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.

**RF Manager.** 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. The RF Manager then categorizes the discovered APs as:

- Authorized—a legitimate AP for your system
- Rogue—an unauthorized AP that is connected to the wired network
- External—an AP that is not connected to the wired network. These APs are often, but not always, neighboring businesses’ APs.

The RF Manager may also classify the APs as “uncategorized.”
An advantage of the RP Manager is that it can locate neighboring APs using the information collected by its sensors. It can then display those APs on a site map. For the best results, you should have at least three sensors so that they can triangulate the neighbors’ positions.

Unlike an MSM Controller or autonomous AP, the RF Manager can take active measures against a rogue AP.

**RF Planner.** You can 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 addition, 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.

**Implement the RF Manager’s Wireless IDS/IPS**

The RF Manager provides a wireless IDS/IPS, which, together with AP radios that are licensed and configured as sensors, protects your network from hackers and vulnerabilities. When you enable this feature, sensors collect wireless traffic samples for the IDS/IPS, with which they maintain constant contact.

The RF Manager analyzes the samples and monitors for unwanted communications and attacks, which include:

- Traffic from rogue APs, including both rogue APs detected by sensors and APs that you manually ban from your system
- Traffic from misconfigured APs (that is, authorized APs that do not enforce the proper security settings for your system)
- Traffic from authorized stations that have connected to the wrong APs (APs that are not part of your system)
- Traffic from unauthorized sessions (for example, from stations that you have banned from your system)
- Traffic from authorized stations participating in ad hoc networks (that is, providing connections for other wireless stations)
- Traffic from APs that are spoofing the MAC addresses of your APs
Traffic from honeypot or evil twin APs

A honeypot (or evil twin) AP is an AP that a hacker configures to support the same SSID as your APs. The honeypot AP outputs an excessively strong signal to lure authorized stations to connect to it.

Traffic associated with DoS attacks 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 stations’ 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’s resources.
- **EAPOL Logoff flood attack**—An attacker sends 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.

When the RF manager detects one of these threats, it has the closest sensor block it. The sensor can quarantine unwanted APs and stations. It can also quarantine honeypot APs and prevent authorized stations from connecting to them. Finally, a sensor can block ad hoc network connections and DoS attacks.

**Integrate with RF Planner.** 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’s 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 the ProCurve NAC 800, you can also test each endpoint for rogue or unauthorized applications (such as file sharing), viruses and other malware, and browser security settings. Those endpoints that do not comply with your organization's policies can be quarantined until they are compliant.

For more information on endpoint integrity and the NAC 800, see the ProCurve Network Access Controller 800 Configuration Guide.

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

Note

The MSM APs do not include 802.1X clients. If your switches enforce 802.1X port authentication, you must take one of these steps:

1. Disable 802.1X on the switch ports to which the APs connect.
   You might select this option when the APs’ switch ports are physically secure.

2. Enable MAC-Auth as an alternative authentication method to 802.1X. Add your APs’ MAC addresses to the database on your RADIUS server.
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's Web browser interface. 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.

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

Note that, if you want an MSM AP to act as a sensor for RF Manager, you must set one of its radios to sensor mode. The AP radio will discover RF Manager on its own.

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 DHCP settings.

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 unintended clients.

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

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

- Configure VSCs.
- If MSM APs require provisioning from the MSM Controller, make sure to enable provisioning and to establish the correct settings. (See “Provision Discovery or Connection Settings” on page 1-86.)
- If you plan to require controlled AP authentication, configure this feature. Also complete any necessary configuration on an external RADIUS or FTP 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. Typically, you can simply install the AP in its final location without any preconfiguration. The AP will automatically discover the MSM Controller, and the controller will begin to manage it.

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

In addition, sometimes you must provision the MSM AP’s discovery or connection settings before you install it in its final location. The section below explains.

Provision Discovery or Connection Settings

You should pre-provision the MSM AP’s discovery settings when, in its final location, the AP will be on a different subnet 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.)

You must pre-provision the MSM AP’s connection settings when, in its final location, the controlled AP uses a local mesh (WDS) 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.

You can pre-provision either type of settings in two ways: with the MSM AP’s Web browser interface or with the MSM Controller. However, you must configure the local mesh provisioning profile on the controller.

To use the latter method, first configure the appropriate settings on the MSM Controller. Then connect the AP to a port on the same subnet 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 APs’ discovery or connection settings at the same time.

After you provision the settings, you can install the AP to its final location.
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 “Create a Security Plan” on page 1-56.

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 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 controllers and provisionally mount the APs where you planned. As you provisionally mount the APs, record each device’s serial number. Ensure that the controllers have detected the APs and can manage them. On the 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 1-16 to find the authenticators in your deployment.
Table 1-16. Authenticators Based on Architecture

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Authenticators</th>
<th>RADIUS Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized</td>
<td>MSM Controller</td>
<td>MSM Controller or external RADIUS server</td>
</tr>
<tr>
<td>Distributed with centralized</td>
<td>MSM Controller</td>
<td>MSM Controller (or external RADIUS server)</td>
</tr>
<tr>
<td>authentication</td>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>Distributed without centralized</td>
<td>MSM APs</td>
<td>External RADIUS server (or MSM Controller)</td>
</tr>
<tr>
<td>authentication</td>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>Autonomous AP</td>
<td>MSM APs</td>
<td>External RADIUS server</td>
</tr>
<tr>
<td>Autonomous AP with centralized Web-</td>
<td>MSM313, 313-R, 323, or 323-R</td>
<td>External RADIUS server</td>
</tr>
<tr>
<td>Auth</td>
<td>Authentication</td>
<td></td>
</tr>
</tbody>
</table>

Also make sure that:

- All necessary accounts are configured on RADIUS servers or in your directory
  
  See “New User Accounts” on page 1-88.

- All necessary policies are in place on the RADIUS servers
  
  See “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.” on page 1-88.

**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 ProCurve Access Control Security Solution Implementation Guide.)

See Table 1-17 for the settings that you can configure on the MSM Controller’s RADIUS server or on another RADIUS server using IDM.
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 RF Planner or another method. Configure these settings either through the MSM Controller or manually on autonomous MSM APs.

### Implement Roaming

After you have set up the wireless network, determine whether users need to roam between:

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

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 you find that your wireless network requires Layer 3 roaming or fast roaming, a valid Mobility license must be installed on your MSM Controller. This license can be factory installed, or you can manually install it after you have purchased the controller.

**Note**

When a VSC implements an optimized WLAN architecture with centralized intelligence (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.

**Roaming Types.** When a station roams from one AP to another, there is always a brief interruption in the signal as the station’s 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.

We can classify roaming 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 would not need to log in again, and a user browsing the Internet probably would 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 also is 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 entering the range of the new AP so that their stations can re-authenticate or change their IP addresses.

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

- **The 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’s 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’s signal (moves out of range) or detects another AP that supports the same SSID (VSC) but has a stronger signal.
- Interference decreases an AP’s 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.

**The OS**—Some operating systems are more tolerant of handoffs than others. Some provide buffering to maintain the station session during handoff. Others drop the IP stack during handoff.

**The 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 is developing the 802.11r standard to enable wireless networks to support fast roaming for VoWLAN applications.)

**The 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 “Opportunistic Key Caching—Fast Layer 2 Roaming for 802.1X” on page 1-92 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 NIC, OS, and application to find out what their tolerance levels are. Eventually, you will have to test the devices yourself on the 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 the users for that eventuality.

**Layer 2 (RF) Roaming.** Layer 2 or RF roaming is sometimes called “simple” roaming because most 802.11-compliant APs natively support it, including ProCurve MSM devices. The APs can hand off the roaming station’s session state 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 APs’ 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.

**Roaming for Public Access Networks.** To implement a public access network (which uses Web-Auth), you must use the centralized intelligence option. 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.

**Opportunistic Key Caching—Fast Layer 2 Roaming for 802.1X.** You must determine when 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 your MSM Controller. You can then implement Opportunistic Key Caching on a VSC. The section below describes the feature in more detail.

**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 Description. 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

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 AP 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 1-13 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.

![Layer 2 and Layer 3 Roaming](image_url)

**Figure 1-13. 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.
**Layer 3 Roaming with the MSM Mobility Controller.** With the purchase of an optional Mobility license, you can configure an MSM Controller to support Layer 3 roaming.

To implement Layer 3 mobility, a controller tracks the home AP of every station that connects to one of its controlled APs. When the station roams to another AP (a foreign AP), the controller handles the forwarding of traffic so that the station can retain its IP address.

A Layer 3 mobility domain can extend 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.

To implement this scenario successfully, you must:
- Purchase a Mobility license for each of the MSM Controllers.
- Ensure that each of the MSM Mobility Controllers can reach the primary controller on their LAN ports.

**Reassess Coverage**

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

**Reassess Coverage with RF Planner.** The RF Planner includes a calibration tool that helps to make your coverage plan more realistic. In the 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.
**Wireless Network Design Process**

**Designing a New Wireless Network**

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 rights are correct for each type of user and that restrictions are applied properly. Move from place to place and verify that roaming proceeds seamlessly. You should not have to log in again as you roam if you configured roaming on your network.

You should then use a wireless packet analyzer to ensure that the wireless LAN is operating within expectations. Test each media type—data, voice, video—to verify that throughput is adequate. For voice and video applications, verify that roaming occurs quickly enough. If possible, ask other users in the building to access the network at the same time to simulate normal use.

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 ProCurve Networking offers products designed with high availability in mind.

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.
Provide Radio Failover with Automatic Power Control on the APs

Even when you carefully design cell coverage and assign neighbor APs non-overlapping channels, AP radios may be able to “hear” other AP radios that are using the same channel. This interference means that multiple AP radios and their associated stations are sharing the same transmission medium, decreasing overall throughput.

If you enable the Automatic Power Control (APC) feature on an AP, a radio can reduce its transmit power to minimize interference while simultaneously maximizing channel coverage. When the radio detects interference, it changes its power level based on your settings.

An APC-enabled radio can also provide self-healing: if a neighboring AP is using the same channel and fails, the APC-enabled radio can boost its power to compensate. Of course, you must physically design your wireless network so that the APs are placed in close-enough proximity to provide failover for each other. You must also configure APC appropriately so that the radio adjusts its power for that neighboring AP.

When planning redundancy for APs, you should keep in mind that an APC-enabled radio will not boost its transmit power to exceed its configured transmission level.

If co-channel interference is discovered, all neighboring APs will shrink their cell size to minimize the interference. They will first adjust their transmit power. If that does not eliminate interference, APs will then increase transmit power to maximum, if possible, and change the minimum data rate to a higher value.

This feature works best when the entire network uses only ProCurve Networking APs, because third party products might not adjust output power. In addition, 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.

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 1-29. 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.
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 APs’ 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 1-31 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's switch probably provides connections for other endpoints and other APs, you might want the port's 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's 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 intelligence

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 intelligence (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 intelligence architecture.

For more information on architecture options, see “Choose the Architecture” on page 1-32.
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 1-85
- “Configure Initial Settings on Controlled MSM APs” on page 1-86

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 these steps, see the HP ProCurve MultiService Mobility Implementation Guide.

Finally, schedule a network outage. Remove the existing APs and install the MSM422 APs. See “Install the MSM Devices” on page 1-87.

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 APs’ 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 devices’ 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+’s Traffic Monitor. Continue to monitor both the wired and wireless network.
Wireless Network Design Process
Upgrading a Wireless Network to 802.11n
Example WLAN Installation

Contents

Overview: PCU Medical Center ......................................... 2-3
   The Site ............................................................... 2-3
Assess Customer Needs .................................................. 2-4
   Identify the Purpose of the Wireless Installation ............ 2-4
   Identify User Types ................................................. 2-5
   Identify User Equipment and Usage Habits .................. 2-10
   Estimate User Density and Determine Roaming Requirements . 2-11
Assess Security Needs .................................................. 2-15
   Determine Risk Tolerance ....................................... 2-16
   Observe Relevant Regulations ................................ 2-17
   Determine Access Control ...................................... 2-18
Conduct the Preliminary Site Survey ................................. 2-19
   Define Space Types .............................................. 2-19
   Identify Obstacles and RF Interference ...................... 2-19
   Evaluate Existing Infrastructure ............................. 2-27
      Servers .......................................................... 2-30
      Subnets and VLANs .......................................... 2-30
Plan the Equipment Layout ........................................... 2-32
   Select a Physical Layer ....................................... 2-32
   Choose the Type of AP Architecture ........................ 2-33
   Select the Equipment ......................................... 2-34
   Choose a Management Solution ............................. 2-35
Example WLAN Installation

Contents

Plan Coverage and Capacity with RF Planner ............................. 2-36
  Indoor Locations ....................................................... 2-36
  Example Plan .......................................................... 2-37
    Coverage View ......................................................... 2-37
    Redundancy View ...................................................... 2-42
    Link Speed View ...................................................... 2-43
    Interference View ..................................................... 2-44
    Calibration Points ................................................... 2-47
  Outdoor Locations ....................................................... 2-47
  Example Plan .......................................................... 2-48
  External Antennas ....................................................... 2-49

Create a Security Plan ....................................................... 2-52
  Account for Physical Security ......................................... 2-53
  Designate Access Zones ................................................ 2-53
  Design the VLANs ....................................................... 2-57
  Design the VSCs ....................................................... 2-58
  Choose the Security Protocols ........................................ 2-60
    Security Settings for the Local Mesh Links ....................... 2-63
  Determine User Restrictions .......................................... 2-64

Perform the Initial Setup and Survey ..................................... 2-66
  Configure the Initial Settings and Set Up the Infrastructure ........ 2-66
    Set Up User Accounts and Policies .................................. 2-70
  Configure the VSCs ..................................................... 2-70
  Mount the Access Devices .............................................. 2-74
  Monitor Network Performance .......................................... 2-75

Apply Additional Layers of Security ..................................... 2-75

Finalize the Wireless Network ............................................. 2-77
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, examination rooms, and classroom facilities. Each building has three stories. The two buildings are separated by a busy, six-lane road.

The medical center wants to provide a wireless link between the hospital and the office building across the street. Currently, the doctors in the office building cannot access the patient records that are on the hospital's LAN, and students and faculty who meet in the top level do not have wireless access to the PCU network.

In addition, PCUMC wants to implement a wireless network 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 will 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 as well as wireless access to the university network for students and instructors in the office building. The hospital wants to provide doctors who have offices in the office building with wireless access to the ERS.

To complement the existing voice-over-IP (VoIP) system, PCU would like to offer wireless VoIP (VoWLAN) service campus-wide, including the office building and 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 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. Students, faculty, and office staff will not be able to access the hospital’s LAN over the wireless link.

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 four basic types of users in the hospital and five types in the office building.

For the PCUMC hospital, the users are:
- Visitors/patients (70–150)
- Medical personnel (255)
- Administrative personnel (62)
- RFID tags (~500)

For the PCUMC office building, the users are:
- Visitors/patients (15–40)
- Doctors (8)
- Office staff (20)
- Medical school faculty and students (20–400)
- RFID tags (~50)

On the floor plan of the hospital, you mark areas where each type of user is most likely to be found.
On level 1 of the hospital, visitors and patients are found mostly in the waiting areas and the chapel, and some are in 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.
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.

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

On the third floor, however, all of the users will be students and faculty of the PCU medical school.
Example WLAN Installation
Assess Customer Needs

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

<table>
<thead>
<tr>
<th>Device</th>
<th>User Type</th>
<th>Applications</th>
<th>Bandwidth</th>
<th>Sensitive Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop</td>
<td>Administrative</td>
<td>Internet, Email, Word processing, Spreadsheets, File transfer</td>
<td>High</td>
<td>Financial</td>
</tr>
<tr>
<td>Laptop</td>
<td>Medical</td>
<td>Internet, Email, Word processing, ERS, File transfer</td>
<td>High</td>
<td>Patient records</td>
</tr>
<tr>
<td>Laptop</td>
<td>Visitors, patients</td>
<td>Internet</td>
<td>Low</td>
<td>None</td>
</tr>
<tr>
<td>Laptop</td>
<td>Students, faculty</td>
<td>Internet, Email, Word processing, File transfer</td>
<td>High</td>
<td>Student records</td>
</tr>
<tr>
<td>PC tablet</td>
<td>Medical</td>
<td>ERS</td>
<td>Low</td>
<td>Patient records</td>
</tr>
<tr>
<td>Wireless VoIP phone</td>
<td>Medical, administrative</td>
<td>VoWLAN</td>
<td>High</td>
<td>None</td>
</tr>
<tr>
<td>Smartphone</td>
<td>All</td>
<td>Internet</td>
<td>Low</td>
<td>None</td>
</tr>
<tr>
<td>RFID tags</td>
<td>None</td>
<td>Internet, Locator beacon</td>
<td>Low</td>
<td>None</td>
</tr>
<tr>
<td>Personal digital assistant (PDA)</td>
<td>Medical</td>
<td>Internet, ERS</td>
<td>Low</td>
<td>Patient records</td>
</tr>
<tr>
<td>PDA</td>
<td>Administrative</td>
<td>Internet, Email</td>
<td>Medium</td>
<td>None</td>
</tr>
<tr>
<td>PDA</td>
<td>Visitors, patients</td>
<td>Internet</td>
<td>Low</td>
<td>None</td>
</tr>
</tbody>
</table>

(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, medical, student, and faculty laptop users plan to use their wireless connections for the same applications they use on the wired network. Their bandwidth demands are therefore the highest.
The wireless VoIP phones in the office building will need the most constant connections because they will often be used while the user is moving, and the application is extremely intolerant of interruptions in the signal.

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 and Determine 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](image)
On the first level of the hospital, the density levels are highest in the administrative areas and slightly less so in the public areas.

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.
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.
On the third level, the primary users will be those accessing the ERS and sometimes patients. Connections will need to be reasonably constant throughout the departments.
In the PCUMC office building, user density is lowest in the waiting areas of the first two levels and in the lounge of the third level. It is extremely high in the classrooms, lecture hall, and conference room, even though the conference room will not be filled most of the time. The rest of the building will have medium user density.

The roaming requirements of the office-building users are negligible: the students will not expect to connect to the network until they are in their seats, and the wireless devices in the offices and exam rooms will not typically be in motion.

Assess Security Needs

Consult “Assess Security Needs” on page 1-13 for an explanation of security needs the site may have.
Determine Risk Tolerance

The 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
- Credit card numbers

Of these types of data, the most sensitive are the patient health and insurance data, hospital financial records, employee records, credit card numbers, and patient prescriptions. Any break-in that compromises this data could result in high recovery costs, damage to PCUMC’s 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>
<thead>
<tr>
<th>Network Resource</th>
<th>Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling information</td>
<td>Low</td>
</tr>
<tr>
<td>ERS</td>
<td>High</td>
</tr>
<tr>
<td>Hospital financial records</td>
<td>High</td>
</tr>
<tr>
<td>Employee records</td>
<td>Medium</td>
</tr>
<tr>
<td>Inventory data</td>
<td>Low</td>
</tr>
<tr>
<td>Patient prescriptions</td>
<td>High</td>
</tr>
<tr>
<td>Drug database</td>
<td>Medium</td>
</tr>
<tr>
<td>Credit card numbers</td>
<td>High</td>
</tr>
<tr>
<td>Student records</td>
<td>High</td>
</tr>
</tbody>
</table>

PCUMC’s 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 Relevant 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 an educational institution, 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). The parts of the standard that concern network security are in “HIPAA Security Standards” on page D-6 of Appendix D, “Supplementary Information.”

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.
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

<table>
<thead>
<tr>
<th>Network Resource</th>
<th>Users</th>
<th>Access Type</th>
<th>Location</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling information</td>
<td>Administrative, uncertified medical, office</td>
<td>Wired and wireless</td>
<td>Hospital L1, office L1 and L2</td>
<td>Office hours</td>
</tr>
<tr>
<td>ERS</td>
<td>Certified medical, office doctors</td>
<td>Wired and wireless</td>
<td>Hospital all levels, office L1 and L2</td>
<td>All days, all times</td>
</tr>
<tr>
<td>Hospital financial records</td>
<td>Administrative</td>
<td>Wired only</td>
<td>Hospital L1</td>
<td>Office hours</td>
</tr>
<tr>
<td>Employee records</td>
<td>Administrative</td>
<td>Wired only</td>
<td>Hospital L1</td>
<td>Office hours</td>
</tr>
<tr>
<td>Inventory data</td>
<td>RFID tags</td>
<td>Wireless only</td>
<td>All locations</td>
<td>All times</td>
</tr>
<tr>
<td>Patient prescriptions</td>
<td>Certified medical</td>
<td>Wired and wireless</td>
<td>Hospital all levels, office L1 and L2</td>
<td>All times</td>
</tr>
<tr>
<td>Drug database</td>
<td>Certified medical</td>
<td>Wired and wireless</td>
<td>Hospital all levels, office L1 and L2</td>
<td>All times</td>
</tr>
<tr>
<td>Credit card numbers</td>
<td>Administrative</td>
<td>Wired only</td>
<td>Hospital L1</td>
<td>Office hours</td>
</tr>
<tr>
<td>Student records</td>
<td>Faculty and students</td>
<td>Wired and wireless</td>
<td>Office L3</td>
<td>All hours</td>
</tr>
</tbody>
</table>

In this table, the 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.

While consulting with PCUMC administrators and IT personnel, you determine that some sensitive information—hospital financial records, employee records, and credit card numbers—should not be accessible through a wireless connection. 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.
You decide not to place time restrictions on wireless access to the PCU network in the office building, leaving any such restrictions to the discretion of the PCU IT staff.

(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 partly dense office space (such as patient rooms, Pain Management, surgeries) and partly “normal office space” (such as Intensive Care, which has only curtain dividers). When you have more than one type of space on a floor, you should plan for wireless coverage for the more dense space type, so 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.
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
Example WLAN Installation
Conduct the Preliminary Site Survey

- **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

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. However, you do not need to provide RF service in the kitchen area.

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.

Because you will be using RFID tags to track all equipment, you take note of equipment storage areas: these areas would ordinarily not need consideration for a wireless LAN, but in this case, they need 802.11b coverage.

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 non-medical 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).
Conduct the Preliminary Site Survey

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.
Example WLAN Installation
Conduct the Preliminary Site Survey

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.

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.
Example WLAN Installation
Conduct the Preliminary Site Survey

Table 2-4. Existing Wireless Systems or Devices

<table>
<thead>
<tr>
<th>System</th>
<th>Location</th>
<th>Frequency</th>
<th>Range</th>
<th>WLAN Interference</th>
</tr>
</thead>
<tbody>
<tr>
<td>WMTS</td>
<td>Intensive Care Unit</td>
<td>608–614 MHz</td>
<td>10 m</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>Surgical areas</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bluetooth headsets</td>
<td>Everywhere</td>
<td>2.45 GHz</td>
<td>10 m</td>
<td>possibly</td>
</tr>
<tr>
<td>Cordless telephones</td>
<td>Administration</td>
<td>900 MHz</td>
<td>30 m</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>Human Resources</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pharmacy</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(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](image)

The network infrastructure in the office building consists of one HP ProCurve 5304xl 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, and there is no network access of any kind on the third floor. The office-building LAN is also not connected to the PCMCU LAN or the PCU 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.
Example WLAN Installation
Conduct the Preliminary Site Survey

Table 2-5. Existing Network Infrastructure—Switches

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

(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 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

<table>
<thead>
<tr>
<th>802.1X Infrastructure Device</th>
<th>Type: IAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS servers</td>
<td>IP address: 10.10.1.45</td>
</tr>
<tr>
<td>Directory services</td>
<td>Type: Active Directory</td>
</tr>
</tbody>
</table>

(Integrated with RADIUS? yes no X)

(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 as long as the access devices support it.

Servers

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

Table 2-7. Existing Servers

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

(Sub 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: whether it has been organized by subnet or by virtual LAN (VLAN). In the case of PCU and 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.

Table 2-8. Existing VLANs—Office Building

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Static or Dynamic</th>
<th>IP Address</th>
<th>Switch</th>
<th>Users and Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_59</td>
<td>Static</td>
<td>10.59.1.0/24</td>
<td>10.10.1.14</td>
<td>Doctors group, OFF_MD</td>
</tr>
<tr>
<td>VLAN_103</td>
<td>Static</td>
<td>10.103.1.0/24</td>
<td>10.10.1.14</td>
<td>Office staff group, OFF_DB, OFF_File</td>
</tr>
</tbody>
</table>
Example WLAN Installation
Conduct the Preliminary Site Survey

(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

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Static or Dynamic</th>
<th>IP Address</th>
<th>Switches</th>
<th>Users and Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN_10</td>
<td>Dynamic (RADIUS)</td>
<td>10.10.0.0/16</td>
<td>10.10.1.2, 10.10.1.3, 10.10.1.5, 10.10.1.7, 10.10.1.9</td>
<td>IT admins, RADIUS, WEB, AD, EMAIL</td>
</tr>
<tr>
<td>VLAN_11</td>
<td>Dynamic (RADIUS)</td>
<td>10.11.0.0/16</td>
<td>10.10.1.2, 10.10.1.5</td>
<td>Administrative, ACC_DB, SCH_DB, HR_DB</td>
</tr>
<tr>
<td>VLAN_12</td>
<td>Dynamic (RADIUS)</td>
<td>10.12.0.0/16</td>
<td>10.10.1.2, 10.10.1.3, 10.10.1.5, 10.10.1.7, 10.10.1.9</td>
<td>Certified medical personnel, RX_DB</td>
</tr>
<tr>
<td>VLAN_13</td>
<td>Dynamic (RADIUS)</td>
<td>10.13.0.0/16</td>
<td>10.10.1.2, 10.10.1.3, 10.10.1.5, 10.10.1.7, 10.10.1.9</td>
<td>Uncertified medical personnel</td>
</tr>
</tbody>
</table>

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. Furthermore, you have VoWLAN telephones that operate at 802.11b/g; 802.11n telephones are not yet available. 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 802.11b/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 VSCs. You will set other radios to support pure-802.11n in the 5 GHz frequency. These radios support the private and ERS_Cart VSCs.

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 (MSM422) 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**

<table>
<thead>
<tr>
<th>System</th>
<th>Physical Layer</th>
<th>Frequency (GHz)</th>
<th>Channels</th>
<th>VSCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hospital MSM422 radios 1</td>
<td>802.11n</td>
<td>5</td>
<td>36</td>
<td>private</td>
</tr>
<tr>
<td>Hospital MSM422 radios 2</td>
<td>802.11b/g</td>
<td>2.4</td>
<td>1,6,11</td>
<td>RFID, private, public</td>
</tr>
<tr>
<td>Radios that support the local mesh</td>
<td>802.11n</td>
<td>5</td>
<td>52 &amp; 56</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>802.11a turbo</td>
<td>5</td>
<td>152</td>
<td></td>
</tr>
</tbody>
</table>

(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. The RFID tags and ERS carts will be roaming throughout the entire hospital, so you want to maintain consistency throughout the site for the access point settings, and you want to allow the APs to forward all traffic directly onto the network. However, you want to use the controller’s 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.
Select the Equipment

Although you can manage both the PCUMC hospital and office building networks with a single service controller because you are connecting the two networks with a local mesh, to provide network independence you choose to deploy a MultiService Mobility Controller in each building. You select the MSM750 for your controller because it can control the largest number of users and controlled APs, ensuring that your wireless network has room to grow without requiring a new controller.

To work alongside the MSM750s, you will deploy both MSM422s and MSM320s. The MSM422s will provide the 802.11n coverage for your wireless network, whereas the MSM320s will collaborate with the HP ProCurve RF Manager 100 IDS/IPS system to protect your wireless network with an intrusion prevention system (IPS) and provide additional 802.11b/g coverage.

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’s 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’s hardware is recorded in Table 2-12.
Example WLAN Installation
Plan the Equipment Layout

Table 2-12. Initial WLAN Hardware Decisions

<table>
<thead>
<tr>
<th>Location</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hospital</td>
<td>MSM Mobility Controller</td>
</tr>
<tr>
<td></td>
<td>MSM422s</td>
</tr>
<tr>
<td></td>
<td>MSM320s</td>
</tr>
<tr>
<td>Office Building</td>
<td>MSM Mobility Controller</td>
</tr>
<tr>
<td></td>
<td>MSM422s</td>
</tr>
<tr>
<td></td>
<td>MSM320s</td>
</tr>
<tr>
<td>Local Mesh</td>
<td>MSM422s</td>
</tr>
</tbody>
</table>

(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 CardBus 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 CardBus NICs that support 802.11b/g/n or 802.11a/n and have a receiver sensitivity of –71 to –94 dBm. Those laptops that are already wireless enabled will need 802.1X supplicants loaded on them if they do not already have them.

The university has already purchased VoWLAN telephones for the office building that support 802.11b/g and 802.1X.

For the local mesh, you will choose antennas according to HP ProCurve RF Planner’s 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 Internet Authentication Service (IAS) server 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 configure the hospital’s RADIUS servers as well as the office building’s RADIUS servers.

To manage the wireless network, you will use the MSM750 to manage the APs.
As mentioned earlier, you have also chosen to purchase an HP ProCurve RF Manager 100 IDS/IPS system 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 access devices.

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 HP ProCurve Multiservice Mobility Implementation Guide for information on how to perform each of these steps.

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. The 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 the HP ProCurve RF Manager 100 IDS/IPS system 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.
Example WLAN Installation
Plan Coverage and Capacity with RF Planner

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.

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.

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's redundancy. Every point of your layout should be covered by at least two APs (or more if your site requires).

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.

![Figure 2-21. RF Planner—Access Point Link Speed View](image-url)
Example WLAN Installation
Plan Coverage and Capacity with RF Planner

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 radios’ 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.
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.

Figure 2-23. RF Planner—Access Point Interference View
Cross-Floor Interference. After adjusting the floor’s radio settings to minimize interference, you should check the cross-floor interference by adjusting RF Planner’s 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 APs’ 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 the HP ProCurve RF Manager 100 IDS/IPS system 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.
Example WLAN Installation
Plan Coverage and Capacity with RF Planner

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, and a second local mesh to link the office building and the university. You can use RF Planner to plan these links and ensure that the APs will have the signal strength to support the necessary user applications’ requirements.

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 local mesh. However, the same process should be followed for each local mesh.

To plan the local meshes, 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’s local mesh between the office building and the hospital after the APs have been manually placed in their initial positions.

Note
If your outdoor layout is meant for users, you should follow the same method you used for the indoor layout.
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's 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. Because the local mesh APs will operate in 802.11n mode, which uses three antennas for Multiple-Input, Multiple Output (MIMO), you must install three external antennas on each AP.
Figure 2-26 shows the Access Point Link Speed View after the external antennas have been added to all four APs.

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.
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’s VSCs, you also need to take the following into account:

- You must comply with the HIPAA and FERPA standards as described in “Observe Relevant 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 or student 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>
<thead>
<tr>
<th>Security Requirement</th>
<th>Compliance Measure</th>
<th>Adequate?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical access to electronic information systems is limited while properly authorized access is allowed.</td>
<td>TBD</td>
<td></td>
</tr>
<tr>
<td>Technical policies and procedures grant access to EPHI only to those persons or software programs that should be allowed such access rights.</td>
<td>TBD</td>
<td></td>
</tr>
<tr>
<td>A mechanism encrypts and decrypts EPHI during transmission.</td>
<td>TBD</td>
<td></td>
</tr>
<tr>
<td>The network can verify that a person or entity seeking access to EPHI is the one claimed.</td>
<td>TBD</td>
<td></td>
</tr>
<tr>
<td>RFID tags cannot become a back door for unauthorized access.</td>
<td>TBD</td>
<td></td>
</tr>
<tr>
<td>The ERS carts require thumbprint authentication and a 30-second timeout.</td>
<td>TBD</td>
<td></td>
</tr>
</tbody>
</table>
Account for 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 access devices. 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.

Designate Access Zones

On the first level of the hospital, you designate the cafeteria, waiting areas, lobby, gift shop, and chapel as public zones. In these zones, you want to limit access to sensitive information. However, given the nature of wireless signals, you cannot entirely stop a wireless signal at the door of a public area. Users may be able to see private VSCs in a public area.

You should try to design your RF coverage so that the signal carrying these private VSCs is very weak or non-existent in public areas. However, if it is impossible to physically prevent access to private VSCs in public areas, you should instruct users not to access sensitive information in public areas.
You decide to permit both public and private access in Rehabilitation, and you decide to allow public access in the waiting areas, chapel, cafeteria, main lobby, and gift shop. The rest of the first level is restricted to private access.
On the second level, the patient rooms and Intensive Care are dual public/private zones, the waiting areas are again public only, and the surgical areas are private.
The third level is mostly dual public/private, except for the waiting area, which is public only.
In the office building, the waiting areas are public zones and the rest of the building is a private zone. You may not be able to prevent the private VSC from being accessed in these public zones, so again, employee training is essential.

Design the VLANs

When evaluating the existing VLANs at PCUMC, you realize that to accommodate the new network resources you need to create a few VLANs specifically for the wireless network. These VLANs will be referred to as wireless-only VLANs.

The first wireless-only VLAN to create is a guest VLAN (VLAN 16) that provides Internet access to patients and visitors. Likewise, the new VLAN_RFID (VLAN 5) is for the RFID tags and their server. You also create VLAN_ERS (VLAN 27) for the ERS.

In the office building, you need to create a new VLAN for student and faculty users on the third level. This VLAN will not be part of the PCUMC LAN or WLAN; instead, it will be part of the PCU LAN/WLAN. After consulting with the network administrators at the university, you create VLAN_1001 for student and faculty access from the office building. All traffic on this VLAN will be routed over the link to the university.
Extending the new VLANs through the wired infrastructure to routing switches can be time consuming. You decide to have the MSM controller act as the router for the wireless-only VLANs. You must enable access control on the VSCs that support wireless-only VLANs, and set up the controller as either a DHCP server or a DHCP relay. (The controller supports both capabilities.)

**Design the VSCs**

Table 2-14 lists PCUMC’s VSCs and the information required to begin planning VSC settings.

<table>
<thead>
<tr>
<th>VSC (SSID)</th>
<th>Access Zones</th>
<th>Security Level</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guests</td>
<td>Public</td>
<td>Low</td>
<td>Visitors and patients</td>
</tr>
<tr>
<td>RFID</td>
<td>Public, private</td>
<td>Low</td>
<td>RFID tags</td>
</tr>
<tr>
<td>VoWLAN</td>
<td>Public, private</td>
<td>Medium</td>
<td>VoWLAN telephones</td>
</tr>
<tr>
<td>PCUMC</td>
<td>Private</td>
<td>High</td>
<td>Certified and uncertified medical personnel</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Office doctors and staff</td>
</tr>
<tr>
<td>PCU</td>
<td>Private</td>
<td>High</td>
<td>Medical school faculty and staff</td>
</tr>
</tbody>
</table>

The Guests and RFID VSCs have the same security level, but they must be two separate VSCs because the RFID tags cannot log on to a VSC the same way that a human user can. VoWLAN security is set at Medium to take advantage of subscriber identity module (SIM)-card authentication methods in the phones, and the PCUMC VSC is set at High security. The PCU VSC, also high-security, is for the faculty and students on the third level of the office building.

(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. You can use VLANs in four different ways.

- **Egress, or 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. This is the VLAN on which the AP forwards traffic.

- **Dynamic, or User-Based, VLANs**
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's egress VLAN.

- **VSC-based VLANs**

  The VSC egress VLANs determine the VLAN that the controller uses to forward users' traffic onto the wired network for VSCs with centralized access control. You can assign different VSC-based VLANs to different types of traffic.

- **General VLANs**

  These are VLANs that are not assigned to a VSC, which means that:
  - Access control does not apply to traffic on these VLANs.
  - An IP address must be assigned to the VLAN through either DHCP or a static assignment.
  - VLAN traffic is routed according to its destination and the routing tables on Service Controller >> Network > IP Routes.

In this example, you are using the network's RADIUS server to authenticate some clients. The RADIUS server will provide dynamic VLAN assignments, depending on the user's login credentials, so you do not need to configure any of these VLANs on the wireless devices.

For the VSCs that use the controller for authentication and access control, you want the controller to route the traffic according to its routing table. This way, it will route all guest traffic out of the Internet port. When you configure DHCP on the VSC, the VLAN is automatically created. Therefore, you do not need to configure any of these VLANs either.

<table>
<thead>
<tr>
<th>VSC</th>
<th>Trusted</th>
<th>VLAN</th>
<th>Dynamic VLANs (assigned by RADIUS server)</th>
<th>VLAN IP</th>
<th>Policy and Data Store</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guests</td>
<td>No</td>
<td>General: VLAN_16*</td>
<td>N/A</td>
<td>10.16.0.0/16</td>
<td>Controller</td>
</tr>
<tr>
<td>RFID</td>
<td>No</td>
<td>General: VLAN_RFID*</td>
<td>N/A</td>
<td>10.5.0.0/16</td>
<td>Controller</td>
</tr>
<tr>
<td>VoWLAN</td>
<td>No</td>
<td>General: VLAN_VOIP</td>
<td>N/A</td>
<td>10.250.0.0/16</td>
<td>Controller</td>
</tr>
<tr>
<td>PCU</td>
<td>Yes</td>
<td>Egress: VLAN_1001</td>
<td>N/A</td>
<td>10.251.0.0/16</td>
<td>RADIUS (IDM agent)</td>
</tr>
</tbody>
</table>
Example WLAN Installation

Create a Security Plan

Choose the Security Protocols

From the options in “Create a Security Plan” on page 2-52, you next specify the VSC security settings, as shown in Table 2-16.

Table 2-16. VSC Security Assignments—Hospital and Office Building

<table>
<thead>
<tr>
<th>VSC (SSID)</th>
<th>SSID Broadcast</th>
<th>Encryption</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guests</td>
<td>Enabled</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>RFID</td>
<td>Enabled</td>
<td>None</td>
<td>MAC-Auth</td>
</tr>
<tr>
<td>VoWLAN</td>
<td>Enabled</td>
<td>Wi-Fi Protected Access (WPA)</td>
<td>802.1X (Extensible Authentication Protocol [EAP]-SIM)</td>
</tr>
<tr>
<td>PCUMC</td>
<td>Disabled</td>
<td>WPA/WPA2</td>
<td>802.1X (Protected EAP [PEAP] with Microsoft Challenge Handshake Authentication Protocol version 2 [MS-CHAPv2])</td>
</tr>
<tr>
<td>PCU</td>
<td>Disabled</td>
<td>WPA/WPA2</td>
<td>802.1X PEAP with MS-CHAPv2</td>
</tr>
<tr>
<td>ERS_Cart</td>
<td>Enabled</td>
<td>WPA/WPA2</td>
<td>802.1X (EAP-Generic Token Card [GTC])</td>
</tr>
</tbody>
</table>

(Table C-15 in Appendix C, “Site Survey Forms and Tables” is blank so that you can use it to record decisions for your organization.)
For the Guests VSC, 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 keep the system open for association by all RFID tags, VoWLAN devices, 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 the Guests and RFID VSCs because the traffic will not contain sensitive or private data, nor will the VSCs provide a means to invade the rest 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 patient and visitor NICs support.

For authentication, you choose not to authenticate the Guests VSC because you do not have control over guests’ devices, and because it is the simplest way to allow guests to access the Internet.

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.

For VoWLAN users, you choose 802.1X as the authentication method, because the VoWLAN phones that the university purchased have native 802.1X supplicants, and the SIM cards in the phones mandate that the Extensible Authentication Protocol (EAP) method be EAP-SIM. The phones also natively support Wi-Fi Protected Access (WPA/WPA2).

The PCUMC and PCU VSCs will have the highest degree of security. All users must log on with user credentials, using 802.1X, and WPA/WPA2 encryption will also be used.

(To select the EAP method, consult Figure D-1 of Appendix D, “Supplementary Information” for an EAP decision flow chart. Because the hospital and university use IAS as the RADIUS server, and because most of the 802.1X supplicants are native Windows supplicants, you choose Protected EAP [PEAP] with Microsoft Challenge Handshake Authentication Protocol version 2 [MS-CHAPv2] as the EAP method.)

Because you have decided to use biometric authentication with the ERS carts, you must create a new VSC—ERS_Cart—to accommodate the other EAP method, which is EAP-Generic Token Card (GTC). This new VSC will support only the ERS_VLAN, and can be accessed only in the hospital by certified medical personnel.
Table 2-17. Summary of VSC Characteristics

<table>
<thead>
<tr>
<th></th>
<th>Guests</th>
<th>RFID</th>
<th>VoWLAN</th>
<th>PCUMC</th>
<th>PCU</th>
<th>ERS_Cart</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID broadcast</td>
<td>Open</td>
<td>Open</td>
<td>Open</td>
<td>Closed</td>
<td>Closed</td>
<td>Open</td>
</tr>
<tr>
<td>Validation</td>
<td>Open</td>
<td>Open</td>
<td>Open</td>
<td>Open</td>
<td>Open</td>
<td>Open</td>
</tr>
<tr>
<td>(802.11 authentication)</td>
<td>None</td>
<td>None</td>
<td>WPA</td>
<td>WPA/WPA2</td>
<td>WPA/WPA2</td>
<td>WPA/WPA2</td>
</tr>
<tr>
<td>Encryption</td>
<td>Web-Auth</td>
<td>MAC-Auth</td>
<td>802.1X (EAP-SIM)</td>
<td>802.1X (PEAP with MS-CHAPv2)</td>
<td>802.1X (PEAP with MS-CHAPv2)</td>
<td>802.1X (EAP-GTC)</td>
</tr>
<tr>
<td>Access zones</td>
<td>Public</td>
<td>Public, private</td>
<td>Public, private</td>
<td>Private</td>
<td>Private</td>
<td>Private, public</td>
</tr>
<tr>
<td>Dynamic VLANs</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>VLAN_ERS</td>
<td>VLAN_11</td>
<td>Disabled, Disabled</td>
</tr>
<tr>
<td>Dynamic VLANs</td>
<td>VLAN_11</td>
<td>VLAN_12</td>
<td>VLAN_13</td>
<td>VLAN_59</td>
<td>VLAN_103</td>
<td>VLAN_ERS</td>
</tr>
<tr>
<td>Policy and datastore</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>RADIUS (IDM agent)</td>
<td>RADIUS (IDM agent) on PCU campus</td>
<td>RADIUS (IDM agent)</td>
</tr>
<tr>
<td>Locations</td>
<td>Hospital L1, L2, L3</td>
<td>Hospital L1, L2, L3</td>
<td>Office L1, L2, L3</td>
<td>Hospital L1, L2, L3</td>
<td>Office L1, L2</td>
<td>Hospital L1, L2, L3</td>
</tr>
<tr>
<td>Users</td>
<td>Patients, visitors</td>
<td>RFIDs</td>
<td>VoWLAN phones</td>
<td>Certified medical personnel</td>
<td>Office doctors</td>
<td>Certified medical personnel</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Administrative personnel</td>
<td>Office staff</td>
<td>Office staff</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Uncertified medical personnel</td>
<td>Office staff</td>
<td>Office staff</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Office staff</td>
<td>Office staff</td>
<td>Office staff</td>
</tr>
</tbody>
</table>
Security Settings for the Local Mesh Links

To configure the local mesh, you must complete the following tasks:

- **Configure the APs’ radios**
  
  You must ensure that the radios are using the same operating mode (Local mesh only or Access point and local mesh) and 802.11 wireless mode. Also, if you are not using DFS, you must ensure that all of the APs in each mesh are using the same channel on each radio. For example, each AP’s radio 1 must have the same operating mode, wireless mode, and channel, and each AP’s radio 2 must have the same operating mode, wireless mode, and channel.

- **Configure the local mesh profile**
  
  You must configure a local mesh profile on each master AP. This is where you set the master AP’s local mesh security settings. The security settings for the master MSM422s are shown in Table 2-18.

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Radios</th>
<th>Security</th>
<th>Encryption Key</th>
<th>Mesh ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hospital-to-Office</td>
<td>Both</td>
<td>WPA2-PSK</td>
<td>PCUMC@10101</td>
<td>1</td>
</tr>
<tr>
<td>Office-to-Uni</td>
<td>Both</td>
<td>WPA2-PSK</td>
<td>PCUMC@20202</td>
<td>2</td>
</tr>
</tbody>
</table>

- **Provision the connectivity settings**
  
  You must provision the connectivity of all APs that connect to the network through a local mesh. These settings specify that the AP will use a local mesh to connect to the network as well as which local mesh settings it should use when connecting. Because the local mesh participants will connect to the office building through the local mesh, and connect to their respective buildings through their LAN ports, you must provision the AP to use both interfaces.

  Table 2-19 shows the local mesh settings on mesh participants.
You will have to tag the ports on the switch to which the MSM422s connect according to the VLANs on which the MSM422s send traffic. In this example, you must tag ports on the switch that connect to the MSM422s for VLAN_E, VLAN_RFID, or VLAN_1001.

### Determine User Restrictions

Because the hospital decided to install PCM+ with IDM, 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*.

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.

---

#### Table 2-19. Connectivity Provisioning

<table>
<thead>
<tr>
<th>Provisioning Option</th>
<th>Uni A</th>
<th>Uni B</th>
<th>Hospital A</th>
<th>Hospital B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Local Mesh Port 1</td>
<td>Local Mesh Port 1</td>
<td>Local Mesh Port 1</td>
<td>Local Mesh Port 1</td>
</tr>
<tr>
<td>Assign IP Address via</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• IP Address</td>
<td>Static 10.10.1.17</td>
<td>Static 10.10.1.18</td>
<td>Static 10.10.1.19</td>
<td>Static 10.10.1.20</td>
</tr>
<tr>
<td>• Subnet Mask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>• Default Gateway</td>
<td>10.10.1.1</td>
<td>10.10.1.1</td>
<td>10.10.1.1</td>
<td>10.10.1.1</td>
</tr>
<tr>
<td>Automatically find mesh ID</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Mesh ID</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>AES/CCMP</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Country</td>
<td>United States</td>
<td>United States</td>
<td>United States</td>
<td>United States</td>
</tr>
<tr>
<td>Local mesh radio configuration</td>
<td>Wireless Mode</td>
<td>Wireless mode</td>
<td>Wireless Mode</td>
<td>Wireless mode</td>
</tr>
<tr>
<td>• Radio1</td>
<td>802.11n (5 GHz)</td>
<td>802.11n (5 GHz)</td>
<td>802.11n (5 GHz)</td>
<td>802.11n (5 GHz)</td>
</tr>
<tr>
<td>• Radio2</td>
<td>802.11a turbo</td>
<td>802.11a turbo</td>
<td>802.11a turbo</td>
<td>802.11a turbo</td>
</tr>
</tbody>
</table>
Notice that the administrative staff is not allowed to access financial resources (ACC_DB) over wireless connections. Access to less-sensitive information (scheduling and human resources information) is restricted to the first level of the hospital, and the time is restricted to office hours only.
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:

■ Laptop with PCM+ client and RF maps loaded
■ 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 PCM+ client)

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.

The new network devices for the first level are shown in Figure 2-31.
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 2-32.
On the hospital's 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:
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’s 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 the users and user groups. Set up the access controls as shown in Table 2-20 on page 2-65. If necessary, create new user accounts in Active Directory.

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.

The VSCs are assigned as shown in Figure 2-34, Figure 2-35, Figure 2-36, and Figure 2-37.
You want to support the Guests VSC in the public areas, the PCUMC VSC in the private areas, the RFID and VoWLAN VSCs in all areas, and the ERS_Cart VSC only in those areas where patient care takes place.

In the public areas, all 802.11b/g radios support the Guests, VoWLAN, and RFID VSCs only. This is to increase the available bandwidth for guests in those areas. Similarly, in the private areas, the PCUMC VSC is supported on both radios, also for increased coverage.
On the second level, you also support the Guests VSC in the public areas, the PCUMC VSC in the private areas, the RFID and VoWLAN VSCs in all areas, and the ERS_Cart VSC only in those areas where patient care takes place. You want to ensure that in the public zones one radio supports that VSC, in case a rolling cart needs to maintain a connection while moving from one area to another.
Example WLAN Installation
Perform the Initial Setup and Survey

In the waiting area, you want all 802.11b/g radios to support the Guests, VoWLAN, ERS_Cart, and RFID VSCs only.

However, because of the placement of your APs, each AP’s signal will propagate to both public and private areas, and to patient-care areas as well. Therefore, you will support the PCUMC VSC on each MSM422’s radio 1, and the RFID, ERS_Cart, VoWLAN, and Guests VSCs on radio 2.

Figure 2-36. Hospital L3—Radio Locations and VSC Settings
Example WLAN Installation
Perform the Initial Setup and Survey

As with the second floor, because of the placement of the APs and their cell coverage, you will support all VSCs on each AP. You will support the PCUMC VSC on each MSM422’s radio 1, and the RFID, VoWLAN, ERS_Cart, and Guests VSCs on radio 2.

![Figure 2-37. Office Building—Radio Locations and VSC Settings](image)

On the third floor of the office building, only the PCU and VoWLAN VSCs are supported. On the lower two levels, the Guests, RFID, VoWLAN, and PCUMC VSCs are supported by every AP.

The ERS_Cart VSC is not supported in the office building because the carts will not be in the office building, and the doctors will access the ERS on laptops, PC tablets, or handheld devices using the PCUMC VSC.

Mount the Access Devices

The next step is to mount the access devices 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 arrester. 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. If you can see a VSC in an area where you do not want it to be available, 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 the ERS through a wireless connection in the office building to ensure that the local mesh is working correctly.
Apply Additional Layers of Security

Once you have set up and tested the network that you planned, you can decide whether additional security measures are needed.

First, check the Security Compliance table to see if your organization is compliant yet:

Table 2-21. Security Compliance

<table>
<thead>
<tr>
<th>Security Requirement</th>
<th>Compliance Measure</th>
<th>Adequate?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical access to electronic information systems is limited while properly authorized access is allowed.</td>
<td>APs are mounted inside ceilings or locked rooms, and cages are installed with locks; console access is disabled; access devices are required to authenticate with 802.1X.</td>
<td>Yes</td>
</tr>
<tr>
<td>Technical policies and procedures grant access to EPHI only to those persons or software programs that should be allowed such access rights.</td>
<td>802.1X authentication and IDM user access policies (which include dynamic VLANs and access control lists [ACLs]) prevent unauthorized access of the ERS.</td>
<td>Yes</td>
</tr>
<tr>
<td>A mechanism encrypts and decrypts EPHI during transmission.</td>
<td>WPA/WPA2 is used for all ERS transmissions.</td>
<td>Yes</td>
</tr>
<tr>
<td>The network can verify that a person or entity seeking access to EPHI is the one claimed.</td>
<td>802.1X provides mutual authentication.</td>
<td>Yes</td>
</tr>
<tr>
<td>RFID tags cannot become a back door for unauthorized access.</td>
<td>IDM policies place all traffic from the RFID VSC in the RFID VLAN and restrict routing out of that VLAN.</td>
<td>Yes</td>
</tr>
<tr>
<td>The ERS carts require thumbprint authentication and a 30-second timeout.</td>
<td>ERS carts must authenticate over the “ERS_Cart” VSC, which requires 802.1X with EAP-GTC authentication and a thumbprint reader. Settings on the OS changed to time out and lock station after 30 seconds of inactivity.</td>
<td>Yes</td>
</tr>
<tr>
<td>ERS, prescription, financial, and human resources databases are not accessible in general public access areas.</td>
<td>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.</td>
<td>Yes</td>
</tr>
<tr>
<td>Rogue APs are eliminated.</td>
<td>802.1X device authentication is supported, and RF manager and sensors are in place on the network.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
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 access devices 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.
Example WLAN Installation
Finalize the Wireless Network
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 ProCurve Networking Elite Partners

HP ProCurve Networking recommends that customers use ProCurve 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

ProCurve Elite Partners have the highest level of training available from ProCurve, based on the number of ProCurve Accredited System Engineers (ASE) on staff. These ASEs are certified by ProCurve 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* will provide step-by-step instructions for creating a wireless network solution that meets the needs of a particular environment. It will also cover ongoing maintenance of a site, including adjusting the radio frequency (RF) signal.

The implementation guide will include switch configurations and step-by-step processes for the components of wireless network solutions:
- HP ProCurve MultiService Mobility (MSM) Controller Series
- HP ProCurve MultiService Mobility (MSM) Access Points (APs)
- HP wireless management products

The implementation guide will be released in the second quarter of 2009.

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 [http://www.procurve.com/solutions/mobility/resources.htm](http://www.procurve.com/solutions/mobility/resources.htm).
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.
Glossary

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's 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](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 NICs 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 access devices. 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.
Glossary

**authentication** The process of confirming an endpoint's or an end user's identity 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.

**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 PANs 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's 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's beacon frame.

**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’s size is determined by the transmitter’s 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’s 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 frames and stations cannot associate and authenticate with the access device unless they already know the SSID. Also see open system.

coordinated architecture  See architecture.
Glossary

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’s or user’s 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.


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](http://www.ietf.org/rfc/rfc3748.txt).


**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](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](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 endpoints 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's name. Although ESSID is more precise, the industry commonly uses the general term SSID to signify the network name.

**Extensible Authentication Protocol** See EAP.

**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).


**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.


**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](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](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](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’s 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.
Glossary

**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.

**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 **ACLs**, **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 APs, 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’s 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.
Glossary

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's 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 *keys* 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](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 *physical* 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.
Glossary

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’s 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 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.*
Glossary

**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.


**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.
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.*


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](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](http://tools.ietf.org/html/draft-funk-eap-ttls-v1-01).

Tx  *Transmit*. As opposed to **Rx**, which is *receive*.

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](http://www.3gpp.org/ftp/Specs/html-info/21101.htm).
Glossary

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](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](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/](http://www.wimaxforum.org/).

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](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](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.
Glossary

**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.
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**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Frequency Range</th>
<th>Maximum Rate (Mbps)</th>
<th>Indoor Range* (m)</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>5 GHz</td>
<td>54</td>
<td>35</td>
<td>WLAN</td>
</tr>
<tr>
<td>802.11b</td>
<td>2.4 GHz</td>
<td>11</td>
<td>45</td>
<td>WLAN</td>
</tr>
<tr>
<td>802.11g</td>
<td>2.4 GHz</td>
<td>54</td>
<td>40</td>
<td>WLAN</td>
</tr>
<tr>
<td>802.11n</td>
<td>2.4 and 5 GHz</td>
<td>248; 600 with channel bonding</td>
<td>70</td>
<td>WLAN</td>
</tr>
<tr>
<td>802.11y</td>
<td>3.65–3.70 GHz</td>
<td>54</td>
<td>50</td>
<td>Fixed P2P, point-to-mobile</td>
</tr>
<tr>
<td>802.15</td>
<td>2.4 GHz</td>
<td>1</td>
<td>10</td>
<td>PAN</td>
</tr>
<tr>
<td>802.15.4</td>
<td>868 MHz 902–928 MHz 2.4 GHz</td>
<td>0.1</td>
<td>10</td>
<td>Low-rate PAN</td>
</tr>
<tr>
<td>802.16</td>
<td>2–66 GHz</td>
<td>40</td>
<td>10,000</td>
<td>LAN/MAN broadband wireless (WiMAX)</td>
</tr>
<tr>
<td>802.20</td>
<td>&lt; 3.5 GHz</td>
<td>&gt; 1</td>
<td>n/a</td>
<td>Mobile broadband wireless access (MBWA) (vehicular mobility)</td>
</tr>
<tr>
<td>802.22</td>
<td>54–862 MHz</td>
<td>unknown</td>
<td>n/a</td>
<td>Wireless regional area network (WRAN) point-to-multipoint</td>
</tr>
</tbody>
</table>

*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

<table>
<thead>
<tr>
<th>MCS Index</th>
<th>Spatial Streams</th>
<th>Modulation</th>
<th>Coding Rate</th>
<th>CBPS 20 MHz</th>
<th>CBPS 40 MHz</th>
<th>Data Rate (Mbps) GI=800ns</th>
<th>Data Rate (Mbps) GI=400ns</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>BPSK</td>
<td>1/2</td>
<td>52</td>
<td>108</td>
<td>6.5</td>
<td>13.5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>QPSK</td>
<td>1/2</td>
<td>104</td>
<td>216</td>
<td>13</td>
<td>27</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>QPSK</td>
<td>3/4</td>
<td>104</td>
<td>216</td>
<td>19.5</td>
<td>40.5</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>16-QAM</td>
<td>1/2</td>
<td>208</td>
<td>432</td>
<td>26</td>
<td>54</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>16-QAM</td>
<td>3/4</td>
<td>208</td>
<td>432</td>
<td>39</td>
<td>81</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>64-QAM</td>
<td>2/3</td>
<td>312</td>
<td>648</td>
<td>52</td>
<td>108</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>64-QAM</td>
<td>3/4</td>
<td>312</td>
<td>648</td>
<td>58.5</td>
<td>121.5</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>64-QAM</td>
<td>5/6</td>
<td>312</td>
<td>648</td>
<td>65</td>
<td>135</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>BPSK</td>
<td>1/2</td>
<td>104</td>
<td>216</td>
<td>13</td>
<td>27</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>QPSK</td>
<td>1/2</td>
<td>208</td>
<td>432</td>
<td>26</td>
<td>54</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>QPSK</td>
<td>3/4</td>
<td>208</td>
<td>432</td>
<td>39</td>
<td>81</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>16-QAM</td>
<td>1/2</td>
<td>416</td>
<td>864</td>
<td>52</td>
<td>108</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>16-QAM</td>
<td>3/4</td>
<td>416</td>
<td>864</td>
<td>78</td>
<td>162</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>64-QAM</td>
<td>2/3</td>
<td>624</td>
<td>1296</td>
<td>104</td>
<td>216</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>64-QAM</td>
<td>3/4</td>
<td>624</td>
<td>1296</td>
<td>117</td>
<td>243</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>64-QAM</td>
<td>5/6</td>
<td>624</td>
<td>1296</td>
<td>130</td>
<td>270</td>
</tr>
<tr>
<td>16</td>
<td>3</td>
<td>BPSK</td>
<td>1/2</td>
<td>156</td>
<td>324</td>
<td>19.50</td>
<td>40.50</td>
</tr>
<tr>
<td>17</td>
<td>3</td>
<td>QPSK</td>
<td>1/2</td>
<td>312</td>
<td>648</td>
<td>39</td>
<td>81</td>
</tr>
<tr>
<td>18</td>
<td>3</td>
<td>QPSK</td>
<td>3/4</td>
<td>312</td>
<td>648</td>
<td>58.5</td>
<td>121.5</td>
</tr>
<tr>
<td>19</td>
<td>3</td>
<td>16-QAM</td>
<td>1/2</td>
<td>624</td>
<td>1296</td>
<td>78</td>
<td>162</td>
</tr>
<tr>
<td>20</td>
<td>3</td>
<td>16-QAM</td>
<td>3/4</td>
<td>624</td>
<td>1296</td>
<td>117</td>
<td>243</td>
</tr>
<tr>
<td>21</td>
<td>3</td>
<td>64-QAM</td>
<td>2/3</td>
<td>936</td>
<td>1944</td>
<td>156</td>
<td>324</td>
</tr>
<tr>
<td>22</td>
<td>3</td>
<td>64-QAM</td>
<td>3/4</td>
<td>936</td>
<td>1944</td>
<td>175.5</td>
<td>364.5</td>
</tr>
<tr>
<td>23</td>
<td>3</td>
<td>64-QAM</td>
<td>5/6</td>
<td>936</td>
<td>1944</td>
<td>195</td>
<td>405</td>
</tr>
<tr>
<td>24</td>
<td>4</td>
<td>BPSK</td>
<td>1/2</td>
<td>208</td>
<td>432</td>
<td>26</td>
<td>54</td>
</tr>
<tr>
<td>25</td>
<td>4</td>
<td>QPSK</td>
<td>1/2</td>
<td>416</td>
<td>864</td>
<td>52</td>
<td>108</td>
</tr>
<tr>
<td>26</td>
<td>4</td>
<td>QPSK</td>
<td>3/4</td>
<td>416</td>
<td>864</td>
<td>78</td>
<td>162</td>
</tr>
<tr>
<td>27</td>
<td>4</td>
<td>16-QAM</td>
<td>1/2</td>
<td>832</td>
<td>1728</td>
<td>104</td>
<td>216</td>
</tr>
<tr>
<td>28</td>
<td>4</td>
<td>16-QAM</td>
<td>3/4</td>
<td>832</td>
<td>1728</td>
<td>156</td>
<td>324</td>
</tr>
<tr>
<td>29</td>
<td>4</td>
<td>64-QAM</td>
<td>2/3</td>
<td>1248</td>
<td>2592</td>
<td>208</td>
<td>432</td>
</tr>
</tbody>
</table>

CBPS = Coded Bits per Symbol; GI = Guard Interval
Table B-3. Protection Mechanism Overhead

<table>
<thead>
<tr>
<th>Protection Mechanism</th>
<th>Channel Bandwidth (MHz)</th>
<th>Aggregated Frame Size (Bytes)</th>
<th>PHY Data Rate (Mbps)</th>
<th>Link-Layer Throughput (Mbps)</th>
<th>Protection Overhead (Percent)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTS-CTS</td>
<td>40</td>
<td>1500</td>
<td>300</td>
<td>36.84</td>
<td>88</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>66535</td>
<td>300</td>
<td>258</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>1500</td>
<td>144</td>
<td>32.5</td>
<td>77</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>66535</td>
<td>144</td>
<td>133.9</td>
<td>7</td>
</tr>
<tr>
<td>CTS-to-Self</td>
<td>40</td>
<td>1500</td>
<td>300</td>
<td>44.6</td>
<td>85</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>1500</td>
<td>600</td>
<td>48.22</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>66535</td>
<td>600</td>
<td>475.47</td>
<td>21</td>
</tr>
<tr>
<td>L-SIG TXOP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt; 0.1</td>
</tr>
</tbody>
</table>

CBPS = Coded Bits per Symbol; GI = Guard Interval
Table B-4. Wireless Modes; Shaded Cells = MSM422 Only

<table>
<thead>
<tr>
<th>Standard</th>
<th>Frequency (GHz)</th>
<th>Bit Rates (Mbps)</th>
<th>Channel Widths (MHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b</td>
<td>2.4</td>
<td>11</td>
<td>20</td>
</tr>
<tr>
<td>802.11g</td>
<td>2.4</td>
<td>54</td>
<td>20</td>
</tr>
<tr>
<td>802.11 b/g</td>
<td>2.4</td>
<td>11, 54</td>
<td>20</td>
</tr>
<tr>
<td>802.11a</td>
<td>5</td>
<td>54</td>
<td>20</td>
</tr>
<tr>
<td>802.11a Turbo</td>
<td>5</td>
<td></td>
<td>40</td>
</tr>
<tr>
<td>802.11n</td>
<td>5</td>
<td>300</td>
<td>40</td>
</tr>
<tr>
<td>802.11n</td>
<td>2.4</td>
<td>300</td>
<td>40</td>
</tr>
<tr>
<td>802.11n/a</td>
<td>5</td>
<td>270, 54</td>
<td>40, 20</td>
</tr>
<tr>
<td>802.11n/g</td>
<td>2.4</td>
<td>270, 54</td>
<td>40, 20</td>
</tr>
<tr>
<td>802.11n/b/g</td>
<td>2.4</td>
<td>270, 11, 54</td>
<td>40, 20</td>
</tr>
</tbody>
</table>
WLAN Frequencies

The frequencies available for wireless networks varies, depending on the region or country. The regulators for each region or country are the ultimate arbiters of how frequencies are assigned.

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 download the new software, visit the HP ProCurve Web site at http://www.procurve.com.)

Depending on your country some channels may be restricted to indoor use. In addition, although this information was accurate when this Design Guide was published, countries sometimes change their channel assignments. For example, Japan recently changed its channel assignments to conform to world usage. IEEE 802.11j is the standard for equipment that conforms to the old Japanese channel set. When you plan a network, check the current regulations for your country.
Calculations for Transmission Range

RSL Formula

To calculate received signal level (RSL) between site A and site B, use the following formula:

\[ \text{RSL} = (\text{EIRP of site A (dBi)}) - (\text{path loss between sites (dBm)}) + (\text{receiver sensitivity of site B (dBi)}) \]

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 isotropic 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:

\[ \text{EIRP} = (\text{transmit power (dBm)}) - (\text{cables and connectors (dB)}) + (\text{antenna gain (dBi)}) \]

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:

\[ 15 \text{ dBm} - (1 \text{ dB} + .25 \text{ dB} + .22 \text{ dB} + .25 \text{ dB}) + 6.5 \text{ dBi} = 19.78 \text{ dBm} \]

**Path-Loss Formula**

The path-loss equation uses these variables:

- \( L_p \) = free-space path loss in dBi
- \( F \) = frequency in GHz
- \( D \) = distance in meters

\[ L_p = 32.4 + 20 \log_{10} F + 20 \log_{10} D \]

Wireless networks use one of two frequencies, so you can use these simplified equations:

- **2.4 GHz**
  \[ L_p = 40.0 + 20 \log_{10} D \]

- **5 GHz**
  \[ L_p = 46.4 + 20 \log_{10} D \]

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**

<table>
<thead>
<tr>
<th>Type of Space</th>
<th>Scattering Exponent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open outdoors spaces</td>
<td>2 for short distances; add .5 for each 200 m</td>
</tr>
<tr>
<td>Outdoors with trees or buildings</td>
<td>3 or 4</td>
</tr>
<tr>
<td>Indoors with open spaces</td>
<td>2.5</td>
</tr>
<tr>
<td>Indoors with cubicles or other partitions</td>
<td>3.5</td>
</tr>
<tr>
<td>Indoors with walls</td>
<td>4 or 5</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Material</th>
<th>Thickness in Inches</th>
<th>Thickness in Centimeters (Approximation)</th>
<th>Attenuation, dB 2.4 GHz</th>
<th>Attenuation, dB 5 GHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red brick</td>
<td>3.5</td>
<td>9</td>
<td>7–8</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>18</td>
<td>13</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>10.5</td>
<td>27</td>
<td>20</td>
<td>33</td>
</tr>
<tr>
<td>Concrete(^1)</td>
<td>4</td>
<td>10</td>
<td>15–22</td>
<td>18–25</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>20</td>
<td>36–44</td>
<td>45–55</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>30</td>
<td>50–65</td>
<td>74–85</td>
</tr>
<tr>
<td>Reinforced concrete</td>
<td>8</td>
<td>20</td>
<td>42–46</td>
<td>53–57</td>
</tr>
<tr>
<td>Masonry block</td>
<td>8</td>
<td>20</td>
<td>15</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>40</td>
<td>22</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>60</td>
<td>32</td>
<td>39</td>
</tr>
<tr>
<td>Cinder block</td>
<td>7.5</td>
<td>19</td>
<td>6–7</td>
<td>9–10</td>
</tr>
<tr>
<td>Stucco(^2)</td>
<td>1</td>
<td>2.5</td>
<td>14–15</td>
<td>12–13</td>
</tr>
<tr>
<td>Brick-faced concrete</td>
<td>4 (concrete)</td>
<td>10</td>
<td>29</td>
<td>41</td>
</tr>
<tr>
<td>(Brick veneer 3.5 in./90 mm.)</td>
<td>8 (concrete)</td>
<td>20</td>
<td>48</td>
<td>67</td>
</tr>
<tr>
<td>Glass</td>
<td>0.25–0.75</td>
<td>0.6–1.9</td>
<td>0.5–1</td>
<td>1–2</td>
</tr>
<tr>
<td>Ceiling tile (suspended)</td>
<td>0.6</td>
<td>1.5</td>
<td>0.1</td>
<td>0.2</td>
</tr>
<tr>
<td>Drywall</td>
<td>0.25–0.625</td>
<td>0.6–1.6</td>
<td>0.5–1</td>
<td>0.5–1</td>
</tr>
<tr>
<td>Plywood</td>
<td>0.25–1.25</td>
<td>0.6–3.2</td>
<td>1.5–2</td>
<td>1.5–2</td>
</tr>
<tr>
<td>Solid wood(^3)</td>
<td>1.5–2</td>
<td>4–5</td>
<td>3–4</td>
<td>4–6</td>
</tr>
<tr>
<td>(Spruce, pine, and fir)</td>
<td>3</td>
<td>8</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>4.5</td>
<td>12</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>16</td>
<td>15</td>
<td>20</td>
</tr>
</tbody>
</table>

\(^1\)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.

Receiver Sensitivities and Transmit Powers of HP ProCurve Products

Table B-7 and Table B-8 show the receiver sensitivity and transmit powers of HP ProCurve access points.

**Table B-7. Receiver Sensitivity of HP ProCurve Access Points**

<table>
<thead>
<tr>
<th>Operating Mode</th>
<th>Data Rate</th>
<th>Receiver Sensitivity (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11n (20 MHz channels)</td>
<td>MCS 0 / MSC 8</td>
<td>–82</td>
</tr>
<tr>
<td></td>
<td>MCS 7 / MSC 15</td>
<td>–64</td>
</tr>
<tr>
<td>802.11n (40 MHz channels)</td>
<td>MCS 0 / MSC 8</td>
<td>–79</td>
</tr>
<tr>
<td></td>
<td>MCS 7 / MSC 15</td>
<td>–67</td>
</tr>
<tr>
<td>802.11a, j</td>
<td>6 Mbps</td>
<td>–87</td>
</tr>
<tr>
<td></td>
<td>54 Mbps</td>
<td>–67</td>
</tr>
<tr>
<td>802.11g</td>
<td>6 Mbps</td>
<td>–87</td>
</tr>
<tr>
<td></td>
<td>54 Mbps</td>
<td>–70</td>
</tr>
<tr>
<td>802.11b</td>
<td>1 Mbps</td>
<td>–94</td>
</tr>
<tr>
<td></td>
<td>11 Mbps</td>
<td>–87</td>
</tr>
</tbody>
</table>
Table B-8. Transmit Power of HP ProCurve Access Points

<table>
<thead>
<tr>
<th>Operating Mode</th>
<th>Data Rate</th>
<th>Transmit Power</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>dBm</td>
<td>mW</td>
<td></td>
</tr>
<tr>
<td>802.11n (20 MHz channels @ 5 GHz)</td>
<td>MCS 0 / 8</td>
<td>18</td>
<td>63</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCS 7/15</td>
<td>10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>802.11n (20 MHz channels @ 2.4 GHz)</td>
<td>MCS 0 / 8</td>
<td>19</td>
<td>79</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCS 7/15</td>
<td>10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>802.11n (40 MHz channels @ 5 GHz)</td>
<td>MCS 0 / 8</td>
<td>17</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCS 7/15</td>
<td>10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>802.11n (40 MHz channels @ 2.4 GHz)</td>
<td>MCS 0 / 8</td>
<td>17</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCS 7/15</td>
<td>10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>802.11a, j</td>
<td>6 – 24 Mbps</td>
<td>18 ± 2</td>
<td>70 ± 30</td>
<td></td>
</tr>
<tr>
<td></td>
<td>54 Mbps</td>
<td>12 ± 2</td>
<td>17.5 ± 7.5</td>
<td></td>
</tr>
<tr>
<td>802.11g</td>
<td>6 – 24 Mbps</td>
<td>18 ± 2</td>
<td>70 ± 30</td>
<td></td>
</tr>
<tr>
<td></td>
<td>54 Mbps</td>
<td>13 ± 2</td>
<td>22 ± 9.5</td>
<td></td>
</tr>
<tr>
<td>802.11b</td>
<td>1 – 11 Mbps</td>
<td>18.5 ± 2</td>
<td>78 ± 34</td>
<td></td>
</tr>
</tbody>
</table>

Table B-9 and Table B-10 show the receiver sensitivity and transmit powers of the HP ProCurve M111 client bridge.

Table B-9. Receiver Sensitivity of the HP ProCurve M111 Client Bridge

<table>
<thead>
<tr>
<th>Operating Mode</th>
<th>Data Rate (Mbps)</th>
<th>Receiver Sensitivity (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>6</td>
<td>−90</td>
</tr>
<tr>
<td></td>
<td>54</td>
<td>−72</td>
</tr>
<tr>
<td>802.11g</td>
<td>6</td>
<td>−92</td>
</tr>
<tr>
<td></td>
<td>54</td>
<td>−72</td>
</tr>
<tr>
<td>802.11b</td>
<td>11</td>
<td>−90</td>
</tr>
</tbody>
</table>
Table B-10. Transmit Power of the HP ProCurve M111 Client Bridge

<table>
<thead>
<tr>
<th>Operating Mode</th>
<th>Data Rate (Mbps)</th>
<th>Transmit Power</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>dBm</td>
</tr>
<tr>
<td>802.11a</td>
<td>6–24</td>
<td>20±2</td>
</tr>
<tr>
<td></td>
<td>54</td>
<td>16±2</td>
</tr>
<tr>
<td>802.11g</td>
<td>6–24</td>
<td>20±2</td>
</tr>
<tr>
<td></td>
<td>54</td>
<td>16±2</td>
</tr>
<tr>
<td>802.11b</td>
<td>1–11</td>
<td>20±2</td>
</tr>
</tbody>
</table>

Conversion between Milliwatts and Decibels

To convert between dBm and mW, use these formulas.

Convert dBm to mW:

\[
\frac{X_{dBm}}{10} = Y_{mW}
\]

For example:

\[
\frac{18\, dBm}{10} = 63\, mW \approx 10
\]

Convert mW to dBm:

\[
X_{dBm} = 10\log_{10}(Y_{mW})
\]

For example:

\[
18\, dBm \approx 10\log_{10}(63\, mW)
\]
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-11. Path Loss at 2.4 GHz

<table>
<thead>
<tr>
<th>Environment</th>
<th>High-End Loss</th>
<th>Low-End Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entirely open, no interference or obstructions</td>
<td>40 + 25 log D</td>
<td>40 + 20 log D</td>
</tr>
<tr>
<td>Open indoors</td>
<td>40 + 25 log D</td>
<td>42 + 25 log D</td>
</tr>
<tr>
<td>Outdoor, urban environment</td>
<td>40 + 40 log D</td>
<td>40 + 30 log D</td>
</tr>
<tr>
<td>Indoor, semi-open</td>
<td>40 + 40 log D</td>
<td>40 + 25 log D</td>
</tr>
<tr>
<td>Indoor, closed</td>
<td>40 + 40 log D</td>
<td>40 + 40 log D</td>
</tr>
</tbody>
</table>

Table B-12. Path Loss at 5 GHz

<table>
<thead>
<tr>
<th>Environment</th>
<th>High-End Loss</th>
<th>Low-End Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entirely open, no interference or obstructions</td>
<td>46 + 25 log D</td>
<td>46 + 20 log D</td>
</tr>
<tr>
<td>Open indoors</td>
<td>46 + 25 log D</td>
<td>48 + 25 log D</td>
</tr>
<tr>
<td>Outdoor, urban environment</td>
<td>46 + 40 log D</td>
<td>46 + 30 log D</td>
</tr>
<tr>
<td>Indoor, semi-open</td>
<td>46 + 40 log D</td>
<td>46 + 30 log D</td>
</tr>
<tr>
<td>Indoor, closed</td>
<td>46 + 40 log D</td>
<td>46 + 40 log D</td>
</tr>
</tbody>
</table>
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:

\[
\lambda = \frac{c}{f}
\]

\[
\lambda = \frac{3 \times 10^{10}}{2.4 \times 10^{9}}
\]

\[
\lambda = 12.5
\]

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Wavelength</th>
<th>1/2 Wavelength</th>
</tr>
</thead>
<tbody>
<tr>
<td>in</td>
<td>cm</td>
<td>1/2 Wave</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inches</td>
</tr>
<tr>
<td>2.4 GHz</td>
<td>4.92</td>
<td>2.46</td>
</tr>
<tr>
<td>5 GHz</td>
<td>2.36</td>
<td>1.18</td>
</tr>
</tbody>
</table>

Table B-13. Wavelengths of WLAN Frequencies
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-14 shows the Colubris product names and the new, HP ProCurve names.

Table B-14. Colubris-to-HP ProCurve Product Name Converter

<table>
<thead>
<tr>
<th>Colubris Product Name</th>
<th>HP ProCurve Product Name</th>
<th>HP ProCurve Product Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSC-5100 Enterprise Mobility (US/CA, UK, EUR, AUS/NZ, ARG)</td>
<td>MSM710 Mobility Controller</td>
<td>J9325A</td>
</tr>
<tr>
<td>MSC-5200 (US/CA, UK, EUR, AUS/NZ, ARG)</td>
<td>MSM730 Mobility Controller</td>
<td>J9326A</td>
</tr>
<tr>
<td>MSC-5500 (US/CA, UK, EUR, AUS/NZ, ARG)</td>
<td>MSM750 Mobility Controller</td>
<td>J9327A</td>
</tr>
<tr>
<td>MSC-5100 Access Service (US/CA, UK, EUR, AUS/NZ, ARG)</td>
<td>MSM710 Access Controller</td>
<td>J9328A</td>
</tr>
<tr>
<td>MSC-5200 Access Service (US/CA, UK, EUR, AUS/NZ, ARG)</td>
<td>MSM730 Access Controller</td>
<td>J9329A</td>
</tr>
<tr>
<td>MSC-5500 Access Service (US/CA, UK, EUR, AUS/NZ, ARG)</td>
<td>MSM750 Access Controller</td>
<td>J9330A</td>
</tr>
<tr>
<td>MSC-3300 US (JAPAN, KOREA, ROW)</td>
<td>MSM323 US Access Point</td>
<td>J9337A</td>
</tr>
<tr>
<td>MSC-3300 (JAPAN, KOREA, ROW)</td>
<td>MSM323 WW Access Point</td>
<td>J9341A</td>
</tr>
<tr>
<td>MSC-3300R US (JAPAN, KOREA, ROW)</td>
<td>MSM323-R US Access Point</td>
<td>J9342A</td>
</tr>
<tr>
<td>MSC-3300R (JAPAN, KOREA, ROW)</td>
<td>MSM323-R WW Access Point</td>
<td>J9345A</td>
</tr>
<tr>
<td>MSC-3200 US (JAPAN, KOREA, ROW)</td>
<td>MSM313 US Access Point</td>
<td>J9346A</td>
</tr>
<tr>
<td>MSC-3200 (JAPAN, KOREA, ROW)</td>
<td>MSM313 WW Access Point</td>
<td>J9350A</td>
</tr>
<tr>
<td>MSC-3200R US (JAPAN, KOREA, ROW)</td>
<td>MSM313-R US Access Point</td>
<td>J9351A</td>
</tr>
<tr>
<td>MSC-3200R (JAPAN, KOREA, ROW)</td>
<td>MSM313-R WW Access Point</td>
<td>J9354A</td>
</tr>
<tr>
<td>Visitor Management Software</td>
<td>Guest Management software</td>
<td>J9355A</td>
</tr>
<tr>
<td>MAP-630 US</td>
<td>MSM335 US Access Point</td>
<td>J9356A</td>
</tr>
<tr>
<td>MAP-630 ROW</td>
<td>MSM335 WW Access Point</td>
<td>J9357A</td>
</tr>
</tbody>
</table>
## Reference Tables
### New Colubris Product Names

<table>
<thead>
<tr>
<th>Colubris Product Name</th>
<th>HP ProCurve Product Name</th>
<th>HP ProCurve Product Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAP-625 US</td>
<td>MSM422 US Access Point</td>
<td>J9358A</td>
</tr>
<tr>
<td>MAP-625 ROW</td>
<td>MSM422 WW Access Point</td>
<td>J9359A</td>
</tr>
<tr>
<td>MAP-330 US (JAPAN, KOREA, ROW)</td>
<td>MSM320 US Access Point</td>
<td>J9360A</td>
</tr>
<tr>
<td>MAP-330 (JAPAN, KOREA, ROW)</td>
<td>MSM320 WW Access Point</td>
<td>J9364A</td>
</tr>
<tr>
<td>MAP-330R US (JAPAN, KOREA, ROW)</td>
<td>MSM320-R US Access Point</td>
<td>J9365A</td>
</tr>
<tr>
<td>MAP-330R (JAPAN, KOREA, ROW)</td>
<td>MSM320-R WW Access Point</td>
<td>J9368A</td>
</tr>
<tr>
<td>MAP-330 AP+Sensor US (JAPAN, KOREA, ROW)</td>
<td>MSM325 Access Point</td>
<td>J9369A</td>
</tr>
<tr>
<td>MAP-330 AP+Sensor (JAPAN, KOREA, ROW)</td>
<td>MSM325 WW Access Point</td>
<td>J9373A</td>
</tr>
<tr>
<td>MAP-320 US (JAPAN, KOREA, TAIWAN, ROW)</td>
<td>MSM310 US Access Point</td>
<td>J9374A</td>
</tr>
<tr>
<td>MAP-320 (JAPAN, KOREA, TAIWAN, ROW)</td>
<td>MSM310 WW Access Point</td>
<td>J9379A</td>
</tr>
<tr>
<td>MAP-320R US (JAPAN, KOREA, ROW)</td>
<td>MSM310-R US Access Point</td>
<td>J9380A</td>
</tr>
<tr>
<td>MAP-320R (JAPAN, KOREA, ROW)</td>
<td>MSM310-R WW Access Point</td>
<td>J9383A</td>
</tr>
<tr>
<td>WAP-200 US (KOREA, TAIWAN, ROW)</td>
<td>M110 US Access Point</td>
<td>J9385A</td>
</tr>
<tr>
<td>WAP-200 (KOREA, TAIWAN, ROW)</td>
<td>M110 WW Access Point</td>
<td>J9388A</td>
</tr>
<tr>
<td>WCB-200 (US/CA, UK, EUR, KOREA, TAIWAN)</td>
<td>M111 Client Bridge</td>
<td>J9389A</td>
</tr>
<tr>
<td>RF Manager 1500 Enterprise</td>
<td>RF Manager 100 IDS/IPS system</td>
<td>J9397A</td>
</tr>
<tr>
<td>RF Manager 1300 Basic</td>
<td>RF Manager 50 IDS/IPS system</td>
<td>J9398A</td>
</tr>
<tr>
<td>RF Planner</td>
<td>RF Planner</td>
<td>J9400A</td>
</tr>
<tr>
<td>CNMS-200 Software for RHEL and CentOS</td>
<td>CNMS 200 Software</td>
<td>J9428A</td>
</tr>
<tr>
<td>CNMS-500 Software for RHEL and CentOS</td>
<td>CNMS 500 Software</td>
<td>J9429A</td>
</tr>
</tbody>
</table>
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 APs’ intended location? 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.

<table>
<thead>
<tr>
<th>Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone/email:</td>
</tr>
<tr>
<td>Department/position:</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Device</th>
<th>User Type</th>
<th>Applications</th>
<th>Bandwidth</th>
<th>Sensitive Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Network Resource</th>
<th>Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Network Resource</th>
<th>Users</th>
<th>Access Type</th>
<th>Location</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## 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

<table>
<thead>
<tr>
<th>System</th>
<th>Location</th>
<th>Frequency</th>
<th>Range</th>
<th>WLAN Interference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Network Infrastructure Devices

Use these tables to record your existing network infrastructure devices.

**Table C-5. Network Infrastructure Devices—Switches**

<table>
<thead>
<tr>
<th>Vendor/Model Number</th>
<th>Layer 3 Switching</th>
<th>PoE</th>
<th>Gig PoE</th>
<th>Free PoE Ports</th>
<th>802.1X Port Speeds</th>
<th>Uplink Speeds</th>
<th>Location</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Use this table to record your existing 802.1X infrastructure devices.

**Table C-6. 802.1X Infrastructure Devices**

<table>
<thead>
<tr>
<th>802.1X Infrastructure Device</th>
<th>RADIUS servers</th>
<th>Type:</th>
<th>IP address:</th>
<th>IP address:</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS servers</td>
<td>Type:</td>
<td>IP address:</td>
<td>IP address:</td>
<td></td>
</tr>
<tr>
<td>Directory services</td>
<td>Type:</td>
<td>IP address:</td>
<td>IP address:</td>
<td></td>
</tr>
<tr>
<td>Integrated with RADIUS?</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>no</td>
<td>no</td>
<td></td>
</tr>
</tbody>
</table>
Use this table to record existing servers.

**Table C-7. Existing Servers**

<table>
<thead>
<tr>
<th>Server Name</th>
<th>Function or Contents</th>
<th>IP Address</th>
<th>Switch</th>
<th>Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Existing VLANs

Use this table to record existing VLANs.

**Table C-8. Existing VLANs**

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Static or Dynamic</th>
<th>IP Address</th>
<th>Switches</th>
<th>Users and Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Physical Layer Decisions

Use this table to record your decisions about the VSC's Physical Layer.

Table C-9. Physical Layer Decisions

<table>
<thead>
<tr>
<th>System</th>
<th>Physical Layer</th>
<th>Frequency (GHz)</th>
<th>Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Architecture Decisions

Use this table to record your decisions about WLAN architecture.

Table C-10. Architecture Decisions

<table>
<thead>
<tr>
<th>Location</th>
<th>Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Hardware Decisions

Use this table to record your hardware decisions.

**Table C-11. WLAN Hardware Decisions**

<table>
<thead>
<tr>
<th>Location</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Security Requirement</th>
<th>Compliance Measure</th>
<th>Adequate?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VSCs

Use these tables to record your initial VSC settings.

Table C-13. Initial VSC Settings

<table>
<thead>
<tr>
<th>VSC (SSID)</th>
<th>Access Zones</th>
<th>Security Level</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VSC-to-VLAN Assignments

Use this table to record your VSC to VLAN assignments.

Table C-14. VSC-to-VLAN Assignments

<table>
<thead>
<tr>
<th>VSC</th>
<th>Trusted</th>
<th>VLAN</th>
<th>VLAN IP</th>
<th>Linkage</th>
<th>Datastore</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VSC Security Assignments

Use this table to record your VSC security assignments.

**Table C-15. VSC Security Assignments**

<table>
<thead>
<tr>
<th>VSC (SSID)</th>
<th>SSID Broadcast</th>
<th>Validation</th>
<th>Encryption</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>User Access Group</th>
<th>Network Resources</th>
<th>Days</th>
<th>Times</th>
<th>Locations</th>
<th>VSCs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Radio</th>
<th>IEEE 802.11</th>
<th>Channel</th>
<th>Tx Power</th>
<th>VSCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This appendix provides additional information about the following topics:

- EAP methods
- Super G
- HIPAA security standards

**EAP Methods**

Use Figure D-1 to decide which Extended Authentication Protocol (EAP) method you should use. You can then read the text that follows for more information about each EAP method.
EAP-Message Digest 5 (MD5)

EAP-MD5 is a base-level authentication protocol; for credentials, an endpoint submits a one-way hash of a random challenges and its password.

This method has the advantage of simplicity, which makes implementation and configuration straightforward. But it is vulnerable to:

- Automated cracking tools and dictionary attacks
- Attackers that pose as the authentication server and steal credentials

Thus, EAP-MD5 affords only a low level of protection and is not regarded as suitable for wireless networks. Another reason this method is unsuitable for wireless networks is that it does not provide material necessary for generating encryption keys and securing the connection.
EAP-TLS (Transport Level Security)

EAP-TLS is highly secure because it uses PKI digital certificates for authentication credentials. It also provides mutual authentication: both the supplicant and the server must possess valid certificates.

EAP-TLS is impervious to the attacks that affect EAP-MD5 but can be difficult to implement. Managing significant numbers of certificates requires specialized software and human expertise, which makes EAP-TLS substantially more expensive than password-based methods.

EAP-Tunneled TLS (TTLS)

Created by Funk Software as an extension to EAP-TLS, EAP-TTLS removes the obstacle of certificate management.

Like EAP-TLS, EAP-TTLS enforces mutual authentication. But with EAP-TTLS, only authentication servers, not supplicants, authenticate with digital certificates, reducing the number of necessary certificates perhaps a thousandfold. For this reason, EAP-TTLS is significantly easier to deploy than EAP-TLS.

Although supplicants authenticate with usernames and passwords, EAP-TTLS preserves much of the security of EAP-TLS by establishing a two-step procedure for tunneling those credentials.

In the first step—the initial TLS handshake—the server authenticates to the supplicant. The two devices use the public key in the server certificate to exchange cipher keys and create a symmetric encryption tunnel. In the second step—the secondary handshake—the supplicant submits credentials over the secure tunnel using a secondary authentication protocol.

The secondary protocol can be another EAP method, but is typically a form of the RADIUS CHAP/PAP protocols. You can use a relatively insecure—but easy to implement—secondary protocol because the tunnel secures the messages.

The encryption tunnel is maintained only for the duration of the secondary handshake; once the handshake is complete, the tunnel is destroyed.
**Protected EAP (PEAP)**

PEAP is Microsoft’s extension of EAP-TLS and is very similar to EAP-TTLS. Like EAP-TTLS, PEAP uses a two-step authentication architecture, in which the supplicant and server create a symmetric tunnel over which the supplicant then sends its credentials.

Unlike EAP-TTLS, EAP-PEAP does not support the RADIUS CHAP/PAP protocols; it generally supports MS-CHAPv2 instead. The level of security, however, is approximately the same.

**Lightweight EAP (LEAP)**

A Cisco proprietary EAP method, LEAP authenticates users by means of passwords; it also provides keying material, which is important for wireless networks. However, although LEAP provides mutual authentication, it is vulnerable to man-in-the-middle attacks and is not recommended.

**EAP-Subscriber Identity Module (SIM)**

A SIM is a smart card installed on a mobile device, which stores the device’s unique International Mobile Subscriber Identity (IMSI) and authentication key (Ki). The SIM uses the IMSI and Ki to authenticate, in a secure manner, to an authentication server, which has access to a database of legitimate IMSIs and the corresponding KIs. The SIM might also negotiate encryption keys with the authentication server to secure future transmissions.

EAP-SIM is primarily used as a secure authentication method for headless devices such as wireless phones.

**EAP-Generic Token Card (GTC)**

While EAP-GTC is similar in design to EAP-MD5, this method was originally designed to work with token cards, devices that store one-time passwords (OTPs), which are less susceptible to cracking than traditional, static passwords. However, EAP-GTC can be used with a traditional password, in which case it is vulnerable to many of the attacks to which EAP-MD5 is also prey. In contemporary networks, EAP-GTC is most often used as the inner protocol for EAP-TTLS or PEAP.
Some wireless network interface card (NIC) vendors include on their cards a specialized chipset from Atheros that features a faster data rate for 802.11g, called “Super G” (108 Mbps). Super G features are available only when the wireless NIC is paired with a Super G AP from the same vendor. The higher rate is a proprietary solution, not part of 802.11g, and involves one or more of the following techniques:

- **Channel bonding**—Channel 6, half of channel 1, and half of channel 11 are bonded together and centered on channel 6, thereby transmitting on a channel that is 40 MHz wide instead of 20 MHz. This can cause substantial interference with channels 1 and 11 in any nearby 802.11b/g network. Some implementations will not go into channel-bonding mode if a conventional 802.11b/g network is detected.

- **Packet bursting**—More than one packet can be sent at a time, thereby reducing the number of interpacket intervals.

- **Fast packets**—Packets can contain a longer data payload in each packet.

- **Data compression**—The Lempel Ziv algorithm (used with data compression utilities such as WinZip) is used to compress data.

Super G-enabled wireless clients are backward-compatible with standards-based 802.11g access devices such as ProCurve APs and controllers, but the 108 Mbps data rate is not available.
HIPAA Security Standards

The information for this section was taken from the HIPAA Security Series of papers that were produced by the Centers for Medicare and Medicaid Services (CMS), which are found at www.cms.hhs.gov. This section addresses only those standards that directly apply to the network on which electronic protected health information (EPIH) is stored and made accessible. Except where noted, all specific implementations are “addressable” rather than required. You can find the full text of the HIPAA Security Standard at http://aspe.hhs.gov/admnstimp/FINAL/FR03-8334.pdf.

Physical Safeguards

The Security Rule defines physical safeguards as “physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.”

Facility Access Controls

Entities must “implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.”

Questions to consider:

- Are policies and procedures developed and implemented that address allowing authorized and limiting unauthorized physical access to electronic information systems and the facility or facilities in which they are housed?
- Do the policies and procedures identify individuals (workforce members, business associates, contractors, etc.) with authorized access by title and/or job function?
- Do the policies and procedures specify the methods used to control physical access such as door locks, electronic access control systems, security officers, or video monitoring?
Workstation Use

Entities must “implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.”

Questions to consider:

■ Are policies and procedures developed and implemented that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI?

■ Do the policies and procedures identify workstations that access EPHI and those that do not?

■ Do the policies and procedures specify where to place and position workstations to only allow viewing by authorized individuals?

■ Do the policies and procedures specify the use of additional security measures to protect workstations with EPHI, such as using privacy screens, enabling password protected screen savers or logging off the workstation?

■ Do the policies and procedures address workstation use for users that access EPHI from remote locations (i.e., satellite offices or telecommuters)?

Workstation Security

Entities must “implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.”

Questions to consider:

■ Are physical safeguards implemented for all workstations that access EPHI, to restrict access to authorized users?

■ Have all types of workstations that access EPHI been identified, such as laptops, desktop computers, personal digital assistants (PDAs)?

■ Are current physical safeguards used to protect workstations with EPHI effective?

■ Are additional physical safeguards needed to protect workstations with EPHI?

■ Are the physical safeguards used to protect workstations that access EPHI documented in the Workstation Use policies and procedures?
Device and Media Controls

Entities must “implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information, into and out of a facility, and the movement of these items within the facility.”

Questions to consider:

- Are policies and procedures developed and implemented that govern the receipt and removal of hardware and electronic media that contain EPHI, into and out of a facility, and the movement of these items within the facility?

- Do the policies and procedures identify the types of hardware and electronic media that must be tracked?

- Have all types of hardware and electronic media that must be tracked been identified, such as, hard drives, magnetic tapes or disks, optical disks or digital memory cards?

The Device and Media Controls standard has four implementation specifications, two required.

1. **Disposal (Required)**—Entities must “implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.”

Questions to consider:

- Are policies and procedures developed and implemented that address disposal of EPHI, and/or the hardware or electronic media on which it is stored?

- Do the policies and procedures specify the process for making EPHI, and/or the hardware or electronic media, unusable and inaccessible?

- Do the policies and procedures specify the use of a technology, such as, software or a specialized piece of hardware, to make EPHI, and/or the hardware or electronic media, unusable and inaccessible?

- Are the procedures used by personnel authorized to dispose of EPHI, and/or the hardware or electronic media?
2. **Media Re-Use (Required)**—Entities must “implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.”

Questions to consider:
- Are procedures developed and implemented for removal of EPHI from electronic media before re-use?
- Do the procedures specify situations when all EPHI must be permanently deleted or situations when the electronic media should only be reformatted so that no files are accessible?

3. **Accountability**—Entities must “maintain a record of the movements of hardware and electronic media and any person responsible therefore.”

Questions to consider:
- Is a process implemented for maintaining a record of the movements of, and person(s) responsible for, hardware and electronic media containing EPHI?
- Have all types of hardware and electronic media that must be tracked been identified, such as hard drives, magnetic tapes or disks, optical disks or digital memory cards?

4. **Data Backup and Storage**—Entities must “create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.”

Questions to consider:
- Is a process implemented for creating a retrievable, exact copy of EPHI, when needed, before movement of equipment?
- Does the process identify situations when creating a retrievable, exact copy of EPHI is required and situations when not required before movement of equipment?
- Does the process identify who is responsible for creating a retrievable, exact copy of EPHI before movement of equipment?

**Technical Safeguards**

The Security Rule defines technical safeguards as “the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.”
Access Control

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 as specified in § 164.308(a)(4)[Information Access Management].”

Four implementation specifications are associated with the Access Controls standard.

1. **Unique User Identification (Required)***—Entities must “assign a unique name and/or number for identifying and tracking user identity.”
   
   Questions to consider:
   - Does each workforce member have a unique user identifier?
   - What is the current format used for unique user identification?
   - Can the unique user identifier be used to track user activity within information systems that contain EPHI?

2. **Emergency Access Procedure (Required)***—Entities must “establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.”
   
   Questions to consider:
   - Who needs access to the EPHI in the event of an emergency?
   - Are there policies and procedures in place to provide appropriate access to EPHI in emergency situations?

3. **Automatic Logoff**—Entities must “implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.”
   
   Questions to consider:
   - Do current information systems have an automatic logoff capability?
   - Is the automatic logoff feature activated on all workstations with access to EPHI?
4. **Encryption and Decryption**—Entities must “implement a mechanism to encrypt and decrypt electronic protected health information.”

Questions to consider:

- Which EPHI should be encrypted and decrypted to prevent access by persons or software programs that have not been granted access rights?
- What encryption and decryption mechanisms are reasonable and appropriate to implement to prevent access to EPHI by persons or software programs that have not been granted access rights?

**Integrity**

An entity must “implement policies and procedures to protect electronic protected health information from improper alteration or destruction.”

**Person or Entity Authentication.** An entity must “implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.”

There are a few basic ways to provide proof of identity for authentication. A covered entity may:

- Require something known only to that individual, such as a password or PIN.
- Require something that individuals possess, such as a smart card, a token, or a key.
- Require something unique to the individual such as a biometric. Examples of biometrics include fingerprints, voice patterns, facial patterns or iris patterns.

Questions to consider:

- What types of authentication mechanisms are currently used?
- What level or type of authentication is reasonable and appropriate for each information system with EPHI?
- Are other authentication methods available that may be reasonable and appropriate?

**Transmission Security.** An entity must “implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.”
This standard has two implementation specifications:

1. **Integrity Controls**—An entity must “implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.”

   Questions to consider:
   - What security measures are currently used to protect EPHI during transmission?
   - Has the risk analysis identified scenarios that may result in modification to EPHI by unauthorized sources during transmission?
   - What security measures can be implemented to protect EPHI in transmission from unauthorized access?

2. **Encryption**—An entity must “implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.”

   Questions to consider:
   - How does the organization transmit EPHI?
   - How often does the organization transmit EPHI?
   - Based on the risk analysis, is encryption needed to protect EPHI during transmission?
   - What methods of encryption will be used to protect the transmission of EPHI?

**Security Guide for Offsite Users of EPHI**

**Accessing EPHI.** Covered entities must develop and implement policies and procedures for authorizing EPHI access in accordance with the HIPAA Security Rule at §164.308(a)(4) and the HIPAA Privacy Rule at §164.508. It is important that only those workforce members who have been trained and have proper authorization are granted access to EPHI.
### Table D-1. Risks Associated with Accessing EPHI

<table>
<thead>
<tr>
<th>Risk</th>
<th>Possible Risk Management Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log-on/password information is lost or stolen, resulting in potential unauthorized or improper access to or inappropriate viewing or modification of EPHI.</td>
<td>Implement two-factor authentication for granting remote access to systems that contain EPHI. This process requires factors beyond general usernames and passwords to gain access to systems (e.g., requiring users to answer a security question such as “Favorite Pet’s Name”). Implement a technical process for creating unique user names and performing authentication when granting remote access to a workforce member. This may be done using RADIUS or other similar tools.</td>
</tr>
<tr>
<td>Employees access EPHI when not authorized to do so while working offsite.</td>
<td>Develop and employ proper clearance procedures and verify training of workforce members prior to granting remote access. Establish remote access roles specific to applications and business requirements. Different remote users may require different levels of access based on job function. Ensure that the issue of unauthorized access of EPHI is appropriately addressed in the required sanction policy.</td>
</tr>
<tr>
<td>Home or other offsite workstations left unattended, risking improper access to EPHI.</td>
<td>Establish appropriate procedures for session termination (time out) on inactive portable or remote devices. Covered entities can work with vendors to deliver systems or applications with appropriate defaults.</td>
</tr>
<tr>
<td>Contamination of systems by a virus introduced from an infected external device used to gain remote access to systems that contain EPHI.</td>
<td>Install personal firewall software on all laptops that store or access EPHI or connect to networks on which EPHI is accessible. Install, use and regularly update virus-protection software on all portable or remote devices that access EPHI.</td>
</tr>
</tbody>
</table>

**Storing EPHI.** Covered entities must develop and implement policies and procedures to protect EPHI that is stored on remote or portable devices, or on potentially transportable media (particularly backups).
Table D-2. Risks Associated with Storing EPHI

<table>
<thead>
<tr>
<th>Risk</th>
<th>Possible Risk Management Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop or other portable device is lost or stolen, resulting in potential unauthorized/improper access to or modification of EPHI housed or accessible through the device.</td>
<td>Identify the types of hardware and electronic media that must be tracked, such as hard drives, magnetic tapes or disks, optical disks or digital memory cards, and security equipment, and develop inventory-control systems.</td>
</tr>
<tr>
<td></td>
<td>Implement process for maintaining a record of the movements of, and person(s) responsible for, or permitted to use hardware and electronic media containing EPHI.</td>
</tr>
<tr>
<td></td>
<td>Require use of lockdown or other locking mechanisms for unattended laptops.</td>
</tr>
<tr>
<td></td>
<td>Password-protect files.</td>
</tr>
<tr>
<td></td>
<td>Password-protect all portable or remote devices that store EPHI.</td>
</tr>
<tr>
<td></td>
<td>Require that all portable or remote devices that store EPHI employ encryption technologies of the appropriate strength.</td>
</tr>
<tr>
<td></td>
<td>Develop processes to ensure appropriate security updates are deployed to portable devices such as smart phones and PDAs.</td>
</tr>
<tr>
<td></td>
<td>Consider the use of biometrics such as fingerprint readers on portable devices.</td>
</tr>
<tr>
<td>Use of external device to access corporate data, resulting in the loss of operationally critical EPHI on the remote device.</td>
<td>Develop processes to ensure backup of all EPHI entered into remote systems.</td>
</tr>
<tr>
<td></td>
<td>Deploy policy to encrypt backup and archival media; ensure that policies direct the use of encryption technologies of the appropriate strength.</td>
</tr>
<tr>
<td>Loss or theft of EPHI left on devices after inappropriate disposal by the organization.</td>
<td>Establish EPHI deletion policies and media-disposal procedures. At a minimum this involves complete deletion, via specialized deletion tools, of all disks and backup media prior to disposal. For systems at the end of their operational lifecycles, physical destruction may be appropriate.</td>
</tr>
</tbody>
</table>
Transmitting EPHI. Covered entities must establish and implement appropriate policies and procedures to secure EPHI that is being transmitted over an electronic communications network.

### Table D-3. Risks Associated with Transmitting EPHI

<table>
<thead>
<tr>
<th>Risk</th>
<th>Possible Risk Management Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data is left on an external device (accidentally or intentionally)</td>
<td>Prohibit or prevent download of EPHI onto remote systems or devices without an operational justification.</td>
</tr>
<tr>
<td>(such as in a library or hotel business center.)</td>
<td>Ensure workforce is appropriately trained on policies that require users to search for and delete any files intentionally or unintentionally saved to an external device.</td>
</tr>
<tr>
<td></td>
<td>Minimize use of browser-cached data in web-based applications which manage EPHI, particularly those accessed remotely.</td>
</tr>
<tr>
<td>Contamination of systems by a virus introduced from a portable storage device.</td>
<td>Install virus-protection software on all portable or remote devices that store EPHI.</td>
</tr>
<tr>
<td>Data intercepted or modified during transmission.</td>
<td>Prohibit transmission of EPHI via open networks, such as the Internet, where appropriate.</td>
</tr>
<tr>
<td></td>
<td>Prohibit the use of off-site devices or wireless access points (e.g. hotel workstations) for non-secure access to email.</td>
</tr>
<tr>
<td></td>
<td>Use more secure connections for email via SSL and the use of message-level standards such as S/MIME, SET, PEM, PGP etc.</td>
</tr>
<tr>
<td></td>
<td>Implement and mandate appropriately strong encryption solutions for transmission of EPHI (e.g. SSL, HTTPS etc.). SSL should be a minimum requirement for all Internet-facing systems which manage EPHI in any form, including corporate web-mail systems.</td>
</tr>
<tr>
<td>Contamination of systems by a virus introduced from an external device used to transmit EPHI.</td>
<td>Install virus-protection software on portable devices that can be used to transmit EPHI.</td>
</tr>
</tbody>
</table>
Index

Numerics
802.11a ... 1-27, 2-32
  interference with ... 1-23, 1-24
802.11b ... 1-21, 1-27, 2-5
  interference with ... 1-23, 1-24
802.11g ... 1-27
  FHSS ... 1-21
  interference with ... 1-23, 1-24
802.11n
  channel bonding ... 1-31
  compatibility ... 1-31
  existing infrastructure ... 1-26
  frame aggregation ... 1-31
  A-MPDU ... 1-31
  A-MSDU ... 1-31
  interference with ... 1-23, 1-24
  MIMO (Multiple-Input, Multiple-Output) ... 1-30
  network upgrade ... 1-98
  protection mechanisms ... 1-31
802.11r ... 1-91
802.15 ... 1-22
802.1X ... 1-67, 1-89, 2-61
  fast roaming ... 1-92
  supplicant ... 1-67

A
access control ... 1-72
access control zones ... 1-57, 1-58
ACLs ... 1-72
AES (Advanced Encryption Standard) ... 1-70
AM band ... 1-25
antennas
  directional ... 1-48
  external ... 1-48, 1-52
  omnidirectional ... 1-48
AP detection
  neighbor ... 1-74
APC (Automatic Power Control) ... 1-97
aquariums ... 1-19, 2-25
architecture ... 1-32
  autonomous ... 1-32
  centralized access control ... 1-34
combined ... 1-41
optimized WLAN ... 1-34
  centralized intelligence ... 1-36, 1-40, 1-78
  distributed intelligence ... 1-38, 1-40, 1-78
attenuation ... 1-19
authentication ... 1-66, 1-69, 1-71

B
barcode scanners ... 1-11
beamforming ... 1-30
Bluetooth ... 1-22
Bundesdatenschutzgesetz ... 1-17

C
CardBus ... 1-49
cell phones ... 1-25
cells
  size ... 1-51, 1-53
ceramic tile ... 1-19
certificates ... 1-67
channels
  overlapping ... 1-29
closed system ... 1-64
CNMS software ... 1-50
cordless telephones ... 1-22
coverage ... 1-51
  multi-level ... 1-54
customer information ... 1-14

data loss ... 1-21
Data Protection Act of 1998 ... 1-17
density ... 1-10
DFS (Dynamic Frequency Selection) ... 1-7
digital certificates ... 1-67
Directive 95/46/EC ... 1-16
directory services ... 1-61

downtime, cost of ... 1-14
DSRC (Dedicated Short Range Communications) ... 1-23
dSSS (Direct Sequence Spread Spectrum) ... 1-21
dynamic VLAN ... 1-72
dynamic WEP ... 1-69, 1-71
EAP (Extensible Authentication Protocol) … 1-68
Elevator shafts … 1-19, 2-21, 2-25
encryption … 1-66, 1-71
endpoint integrity … 1-18
ERS (Electronic Records System) … 2-4, 2-13, 2-33, 2-52

FERPA (Family Educational Rights and Privacy Act of 1974) … 1-16, 1-66
FHSS (Frequency Hopping Spread Spectrum) … 1-21, 1-22
floor plan … 2-36
FM band … 1-25
frame aggregation … 1-31
  A-MPDU … 1-31
  A-MSDU … 1-31
frame retransmission … 1-21
frequencies
  Bluetooth … 1-22
  cordless telephones … 1-22
  high-voltage power … 2-27
  interference … 1-20
  ISM band … 1-20
  medical telemetry … 1-22, 2-23
  microwave oven … 1-23
  non-interfering … 1-25
  radar … 1-24
  RFID … 1-23
  WiMAX … 1-24
FTP … 1-10

GLBA (Gramm-Leach-Bliley Act) … 1-16
GPS (Global Positioning System) … 1-25
GSM (Global System for Mobile Communications) … 1-25

H
heat maps … 2-36
high availability … 1-96
high-voltage frequencies … 2-27
  power lines … 1-19
HIPAA (Health Insurance Portability and Accountability Act) … 1-15, 1-66
HiperLAN … 1-24

IDS/IPS
  See also RF Manager … 1-82
infrared … 1-25
interference
  existing APs … 1-25
  non-interfering systems … 1-25
  obstacles … 1-19
IP stack … 1-91
ISM (Industrial, Scientific, Medical) bands … 1-20

Law 78-17 … 1-17
lighting … 1-19
LMDS (Local Multipoint Distribution Service) … 1-25
local mesh
  dynamic … 1-7
  DFS (Dynamic Frequency Selection) … 1-7
  increased reliability … 1-97
  static … 1-6
local meshing … 1-6

M
M111 Client Bridge … 1-43
MAC lockout
  MSM700 series … 1-77
  RF Manager … 1-77
MAC spoofing … 2-52, 2-61
MAC-Auth … 1-64
  local … 1-65
  RADIUS … 1-65
management solutions … 1-50
medical telemetry … 1-22, 1-25
Michael … 1-70
microwave ovens … 1-23
MIMO (Multiple-Input, Multiple-Output) … 1-30
mirrors … 1-19
mobility … 1-12
MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2) … 2-61
MSM APs … 1-46
  initial settings … 1-86
  MSM313 … 1-45
  MSM323 … 1-45
  rogue APs … 1-81
  specifications … 1-45, 1-47
MSM313 access point … 1-44
MSM323 access point … 1-44
MSM700 series
  access controller … 1-41
  features … 1-43
  initial settings … 1-85
  internal firewall … 1-76
  Layer 3 mobility … 1-43
  MAC lockout … 1-77
  mobility controller … 1-43
  rogue APs … 1-80
  WPA2 opportunistic key caching … 1-43
multi-level coverage … 1-54
MultiService Mobility Access Points
  See MSM APs … 1-56
MultiService Mobility Controller
  See also MSM700 series … 1-56

N
NAC (network access control) … 1-72
NAC 800 … 1-73
NFC (Near Field Communication) … 1-25

O
obstacles … 1-19, 1-20
OFDM (Orthogonal Frequency Division Multiplexing) … 1-21, 1-30
open system … 1-64
opportunistic key caching … 1-93

P
PAN (personal area network) … 1-22
PCI card … 1-49
PCI DSS (Payment Card Industry Data Security Standard) … 1-16
Personal Information Protection Law … 1-17
Physical Layer … 1-21
  for wireless networks … 1-27
pine needles … 1-19, 2-26
PIPEDA (Personal Information Protection and Electronic Documents Act) … 1-17
plenum
  ceiling … 1-20
PMM (ProCurve Mobility Manager) … 2-36
pre-association … 1-65
printers … 1-67
private access zone … 1-57, 2-57
Private Sector Provisions of the Privacy Act 1988 (Cth) … 1-17
ProCurve Switches
  2626 … 2-28
  3500yl … 2-28, 2-67, 2-68
  5304xl … 2-69
  8212zl … 2-28
propagation modeling … 1-52
provisioning … 1-86
public access zone … 1-57, 2-53

R
radar … 1-24
RADIUS … 1-61, 1-70, 2-31
MAC-Auth … 1-65
receiver sensitivity … 1-49, 1-51
redundancy … 1-96
  local mesh … 1-97
regulations … 1-15
RF Manager … 1-82
  MAC lockout … 1-77
  rogue APs … 1-81
RF Planner … 1-52
  rogue APs … 1-82
RFID … 1-23, 1-25, 2-5, 2-32, 2-33, 2-52
  active tags … 1-23, 2-5
risk tolerance … 1-14
roaming … 1-12
algorithm … 1-12
fast … 1-90
with 802.1X … 1-92
Layer 2 … 1-91
fast … 1-40
Layer 3 … 1-93
Wireless Edge Services Modules … 1-95
not seamless … 1-90
seamless … 1-90
rogue AP detection … 1-74
rogue APs … 1-80
detect with
  autonomous AP … 1-81
  MSM controller … 1-80
  RF Manager … 1-81
  RF Planner … 1-82

S
security … 1-56
  additional layers … 1-73
  appropriate access … 1-17
  compliance … 1-14
  endpoint integrity … 1-18
  filters … 1-77
  MSM products … 1-75
  physical … 1-56
service set … 1-58
shielded walls … 1-19
SIM (Subscriber Identity Module) … 1-67
SIM card … 2-61
site survey … 1-84
smart phone … 1-67
SNR (sound-to-noise ratio) … 1-13
SOX (Sarbanes-Oxley) … 1-15, 1-66
spaces, types of … 1-18
spectrum analyzer … 2-66
spoofing, MAC … 2-52, 2-61
sprinklers … 1-19, 1-20
SSID broadcast … 2-61
SSIDs … 1-64, 1-72, 1-92
static VLAN … 1-72
static WEP … 1-71
STBC (Space-Time Block Coding) … 1-30
subnets … 2-30
Super G … 1-50
switches
  See ProCurve Switches

T
throughput … 1-28, 1-51
TKIP (Temporal Key Integrity Protocol) … 1-70
traffic analyzer … 1-87, 2-66
transmit power … 1-49, 1-52

U
UHF-VHF bands … 1-25
upgrade to 802.11n … 1-98
user access … 1-6
user needs … 1-9
  density … 1-10
  device used … 1-11
  mobility … 1-12
  security … 1-13
  risk tolerance … 1-14
user types … 1-8
  employees … 1-9
  temporary … 1-9

V
validation
  open … 1-64
  shared-key … 1-64
VLANs … 2-30
  dynamic … 1-60, 1-72
  static … 1-59, 1-72
VoIP … 1-10
VoWLAN … 1-51, 1-91, 2-4
VSCs … 1-58
  access controls … 1-72
  authentication method … 1-68
  configure … 1-87
  filters … 1-77
  security … 1-63
  trust levels … 1-59
  user restrictions … 1-72

W
walls
  shielded … 1-19
Web-Auth … 1-66
WEP (Wired Equivalent Privacy)
  dynamic … 1-69, 1-71
  static … 1-71
Wibree … 1-22
WiMAX … 1-24
wireless bridging … 2-26
wireless clients … 1-49, 1-90
wireless devices … 1-11
    authentication support … 1-12
wireless filters … 1-77
wireless point-to-point … 1-24
wireless USB … 1-24
WMTS (Wireless Medical Telemetry Service) … 1-22, 1-25, 2-23
WPA (Wi-Fi Protected Access) … 1-70
    802.1X … 1-70
WPA/WPA2 … 1-71
WPA2 … 1-70
WPA-PSK … 1-71
X
X-rays … 2-19, 2-23
Z
ZigBee … 1-22
zones
    access … 1-57
    private … 1-57
    public … 1-57
Technology for better business outcomes

To learn more, visit www.hp.com/go/procurve/

© Copyright 2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. 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 will not be liable for technical or editorial errors or omissions contained herein.

May 2009

Manual Part Number
5900-0251

HP ProCurve Networking