



Wireless Hotspot Deployment Guide

Intel in
Communications

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. Intel products are not intended for use in medical, life saving, life sustaining applications.
Intel may make changes to specifications and product descriptions at any time, without notice.

*Other names and brands may be claimed as the property of others.

Copyright © 2003, Intel Corporation

Table of Contents

- 1. PURPOSE AND ORGANIZATION OF THIS GUIDE..... 6**
- 1.1 ORGANIZATION OF THIS GUIDE 6
- 2. HOTSPOT OVERVIEW 7**
- 2.1 WHAT MAKES UP A HOTSPOT? 8
- 2.2 UNDERSTANDING YOUR USER’S EXPECTATIONS 8
 - 2.2.1 *Customer cost expectations* 9
 - 2.2.2 *Performance expectations* 9
 - 2.2.3 *Security expectations* 9
 - 2.2.4 *Availability and reliability expectations* 9
- 2.3 UNDERSTANDING THE HOTSPOT ENVIRONMENT 10
 - 2.3.1 *Physical size* 10
 - 2.3.2 *Number of users*..... 10
 - 2.3.3 *Usage models*..... 10
 - 2.3.4 *Examples*..... 11
- 3. HOTSPOT FUNCTIONALITY AND NETWORK COMPONENTS..... 12**
- 3.1 THE ACCESS POINT 14
 - 3.1.1 *Important access point features and functionality*..... 14
 - 3.1.2 *Choosing your AP*..... 16
- 3.2 SWITCH/HUB 17
- 3.3 NETWORK ACCESS CONTROLLER 18
- 3.4 IP ADDRESS ALLOCATION MANAGER 18
- 3.5 NETWORK ADDRESS/PORT TRANSLATOR 19
- 3.6 WAN ACCESS GATEWAY/ROUTER 20
- 3.7 LAN 20
- 3.8 WAN BACKHAUL 20
- 3.9 INTERNET SERVICE PROVIDER – ISP 21
- 3.10 WIRELESS INTERNET SERVICE PROVIDER – WISP 21
- 3.11 AUTHENTICATION AUTHORIZATION AND ACCOUNTING (AAA) SERVER 22
- 3.12 INTEGRATION AND CONSOLIDATION 23
- 4. UNDERSTANDING WIRELESS ENVIRONMENTS 23**
- 4.1 PERFORMING AN RF SITE SURVEY 24
- 4.2 TYPES OF RF INTERFERENCE 24
 - 4.2.1 *Direct interference*..... 24
 - 4.2.2 *Indirect interference* 25
 - 4.2.3 *Path interference* 25
 - 4.2.4 *Line of Sight interference* 26
- 4.3 PERFORMANCE CONSIDERATIONS 26
- 4.4 SITE COVERAGE 27
 - 4.4.1 *Roaming*..... 27
 - 4.4.2 *AP cell size, layout, and placement* 28
 - 4.4.3 *AP density*..... 28
 - 4.4.4 *Channel infrastructure layout considerations* 29
- 4.5 CHOOSING YOUR AP 29
 - 4.5.1 *Types of APs* 29
 - 4.5.2 *AP features to look for*..... 30
- 4.6 HOTSPOT SECURITY IN BRIEF 31

4.7 SUMMARY 32

5. WIRELESS SECURITY..... 32

5.1 WIRED VERSUS WIRELESS..... 33

5.2 WHAT IS BEING PROTECTED?..... 33

 5.2.1 *Types of Attacks*..... 33

5.3 SECURITY TECHNOLOGIES BACKGROUND..... 34

5.4 SECURITY OPTIONS 36

5.5 WIRE EQUIVALENT PRIVACY (WEP)..... 37

 5.5.1 *WEP Weaknesses*..... 40

 5.5.2 *Dynamic Key Exchange (DKE)*..... 41

5.6 802.11i..... 41

 5.6.1 *Advanced Encryption Standard (AES)* 42

 5.6.2 *Temporal Key Integrity Protocol (TKIP)* 42

 5.6.3 *Framework - 802.1X*..... 43

 5.6.4 *Authentication Framework - EAP* 45

 5.6.5 *EAP Authentication Methods*..... 45

5.7 WPA..... 47

 5.7.1 *WPA Benefits* 48

 5.7.2 *WPA Deployment Issues*..... 48

5.8 WPA2..... 48

 5.8.1 *WPA2 Limitations*..... 49

5.9 BEST PRACTICES 49

6. MANAGING THE HOTSPOT 50

6.1 MANAGEMENT CONSIDERATIONS..... 51

6.2 MANAGEMENT TOOLS..... 51

7. ENTERPRISE APPLICATIONS..... 52

7.1 VPN AND SECURITY APPLICATIONS..... 52

 7.1.1 *PPTP* 53

 7.1.2 *L2TP* 53

 7.1.3 *IPSEC/ESP* 53

 7.1.4 *SST*..... 53

7.2 REAL-TIME APPLICATIONS..... 53

 7.2.1 *MSN/Windows Messenger (WM)*..... 53

 7.2.2 *Yahoo Messenger (YM)* 54

 7.2.3 *AOL Instant Messenger (AIM)* 54

 7.2.4 *Internet Relay Chat (IRC)*..... 54

 7.2.5 *Voice over IP (VoIP)* 55

 7.2.6 *Other common protocols to consider* 55

7.3 REAL-TIME BATCH APPLICATIONS..... 55

7.4 SUMMARY 56

8. BILLING..... 56

8.1 SOME BILLING MODELS 56

 8.1.1 *Time-Based Billing*..... 56

 8.1.2 *Usage-Based Billing*..... 57

9. COMMON INFRASTRUCTURE AND APPLICATION ISSUES..... 58

9.1 LACK OF ON-SITE DOCUMENTATION AND ASSISTANCE..... 58

9.2 BROWSER ISSUES 58

 9.2.1 *Proxy settings* 58

 9.2.2 *Corporate intranet pages* 59

 9.2.3 *Cached pages*..... 59

9.3 CLIENT MANAGER APPLICATIONS 59

9.4 IP ADDRESSES 60

 9.4.1 Static IP addresses 60

 9.4.2 NATs 60

 9.4.3 Other IP address issues 60

9.5 ETHERNET PACKET PROBLEMS 61

 9.5.1 Preamble length 61

 9.5.2 Packet fragmentation 61

9.6 BILLING ISSUES 61

9.7 GEOGRAPHIC ISSUES 62

10. HOTSPOT BLUEPRINTS 63

10.1 INTRODUCTION 63

10.2 A WORD ABOUT THE PROCESS 65

10.3 COLLECTING REQUIREMENTS 66

10.4 SMALL HOTSPOT – THE COFFEE SHOP 68

 10.4.1 User Requirements 69

 10.4.2 Location Owner/Service Provider Requirements 70

 10.4.3 Physical Environment Requirements 72

 10.4.4 Special Requirements 73

 10.4.5 Network Requirements 73

 10.4.6 Network Design 75

 10.4.7 Equipment Selection 76

 10.4.8 Summary 76

10.5 CONVENTION CENTER HOTSPOT 77

 10.5.1 Site Goals and User Model 77

 10.5.2 Site Survey 77

 10.5.3 AP Layout 78

 10.5.4 Security/Authorization 79

 10.5.5 Site Management 79

 10.5.6 Billing 79

 10.5.7 Design Issues 80

10.6 CONCLUSIONS 80

11. APPENDIX A: COMMONLY USED TERMINOLOGY 81

 11.1 GENERAL TERMINOLOGY 81

 11.2 HOTSPOT COMPONENTS 81

 11.3 SECURITY TERMINOLOGY 82

12. APPENDIX B: TABLE OF ACRONYMS AND ABBREVIATIONS 84

List of Figures

Table 3-1 IANA Address allocation for Private Networks	19	5
Table 5-1: WEP, WAP, WAP2 and 802.11i (RSN)	37	5
Table 10-1: HotSpot Characteristics	65	5
Table 10-2 Coffee Shop Layout	69	5
Figure 10-1: Network Diagram for the Coffee Shop HotSpot	75	5
Figure 3-1 Reference HotSpot Architecture		14
Figure 4-1: Interference Types		26
Figure 4-2: AP Cell Layout for Three Channels		28
Figure 5-1 Shared Key Authentication Sequence		38
Figure 5-2 WEP Encryption Sequence for Transmission		39
Figure 5-3 Clear and encrypted frame areas		40
Figure 5-5-4 802.1X Architecture		43
Figure 5-5: 802.1X Port-based Access Control		44
Figure 5-6: EAP Framework		45

List of Tables

Table 3-1 IANA Address allocation for Private Networks	19
Table 5-1: WEP, WAP, WAP2 and 802.11i (RSN)	37
Table 10-1: HotSpot Characteristics	65
Table 10-2 Coffee Shop Layout	69
Figure 10-1: Network Diagram for the Coffee Shop HotSpot	75

1. Purpose and Organization of this Guide

The intention of this guide is to discuss the implementation of a Public Wireless HotSpot as well as bring to light many of the issues with designing, building, and deploying a HotSpot. This guide is not intended to be a comprehensive guide for 802.11 wireless technologies, but will give a brief overview of the pertinent subjects. We will leave more thorough discussions of wireless technologies to the wide variety of available books on the subject.

It is assumed that the reader of this guide has working knowledge of both LAN and WAN technologies and has had “hands on” experience in designing, implementing and/or managing LANs. A familiarity with WAN technologies and their interfaces to LAN environments is also assumed.

1.1 Organization of this Guide

This guide is organized around the major research and development areas and activities involved in building and deploying a public wireless HotSpot. The topics covered in this guide include:

- HotSpot Overview
- HotSpot Functions and Network Components
- Understanding Wireless Environments
- Wireless Security
- HotSpot Management
- Enterprise Applications
- Billing
- Common Infrastructure and Application Issues
- HotSpot Blueprints

The guide is divided into the following sections:

- Chapter 1, “Purpose and Organization of this Guide”, provides an introduction and overview of this guide.
- Chapter 2, “HotSpot Overview” takes a look at user expectations and environmental requirements.
- Chapter 3, “HotSpot Functionality and Network Components”, introduces the functionality of a HotSpot and a high level overview of the components required to implement said functions.

- Chapter 4, “Investigating Wireless Capability”, covers the requirements of the wireless connection and radio frequency (RF) related issues, such as multipath interference, that can arise in HotSpot implementations.
- Chapter 5, “Wireless Security”, addresses securing the wireless portion of HotSpot networks and discusses security options: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2 and Robust Security Network (RSN).
- Chapter 6, “Managing the HotSpot”, presents ideas for effectively managing HotSpots
- Chapter 7, “Enterprise Applications” reviews applications commonly used by enterprise users.
- Chapter 8, “Billing”, describes various HotSpot billing models, and the requirements for implementation and support.
- Chapter 9, “Common Infrastructure and Application Issues”, presents some of the more common and recurring issues that the authors have encountered in numerous public HotSpots.
- Chapter 10, “HotSpot Blueprints” presents two examples of HotSpot implementations. These HotSpot types were selected to outline some of the issues you might encounter when implementing HotSpots.
- Appendix A provides definitions for commonly used terms
- Appendix B defines all the acronyms and abbreviations used in this document.

2. HotSpot Overview

Functionally, a public HotSpot is a readily available wireless network connection where users with compatible wireless network devices such as PDAs, cell phones, notebook computers, or handheld games can connect to the Internet or private intranet, send and receive email, and download files all without being encumbered by Ethernet cables. You may ask, “Why would I want to deploy a Public Wireless HotSpot?” The answer to this question is “to enhance a customer’s experience”.

With the number of people emailing, chatting, shopping, uploading and downloading files, surfing the web, and playing games across the Internet increasing, offering Wireless network connections will bring customers into a place of business and/or lead them to choose one place of business over another. For example, business travelers can work from their hotel rooms, special events staff can update schedules, locations, results, and specialized content to their customers without installing kiosks and having lines queued up waiting for a terminal to become available. Employees can work from a local coffee shop while enjoying a café latte or cup of tea. These benefits offer a revenue opportunity for both the service provider and the owner of the site.

2.1 What makes up a HotSpot?

Functionally, a public HotSpot is a readily available wireless network connection where users with compatible wireless network devices such as PDAs, cell phones, notebook computers, or handheld games can connect to the Internet or private intranet, send and receive email, and download files all without being encumbered by Ethernet cables. The HotSpot can be temporary or permanent in nature: a trade show that runs over 3 days or at a local coffee shop, respectively, but should always mimic the user's native environment with respect to functionality and security. In other words, the HotSpot should be invisible to the user in every respect, other than making the initial connection to the network.

A HotSpot is made up of some or all of the following components:

- Mobile Station(s)
- Access Point(s)
- Switches, Routers, Network Access Controller
- Web Server
- AAA Server
- High speed Internet connection such as DSL or T1/T3 (WAN backhaul)
- Internet Service Provider (ISP)
- Wireless ISP

Some of these elements may be implemented by the "owner" of the HotSpot while others may be purchased services. Please refer to Chapter 10 for more specific information regarding HotSpot configurations and blue prints.

2.2 Understanding your User's Expectations

HotSpot user expectations can vary greatly based on the environment. For instance, a user on the floor of an industry trade show will have different expectations of the HotSpot than does a user at a coffee shop. A business (or leisure) traveler staying at a HotSpot-enabled hotel will have a different set of expectations. If the user's expectations are not fully understood, the success of the HotSpot will be in question. The highest consideration should be given to the user requirements when designing and implementing a HotSpot.

2.2.1 Customer cost expectations

How to bill, or if to bill, is also a function of the HotSpot environment. For instance, a permanent HotSpot at a coffee shop or hotel would most likely bill for the service (specific billing schemes are discussed in further detail in Chapter 8) whereas a HotSpot at a trade show or special event would likely offer the service free-of-charge, especially if event information and real-time updates are available, such as shuttle bus times, and/or seminar times and locations. However, a location, such as a hotel, can differentiate itself from its competition by offering the HotSpot service for free. The location owner must understand the value a customer places on the HotSpot availability and charge accordingly.

2.2.2 Performance expectations

HotSpots have been heavily touted as providing high-speed connectivity to the Internet and enterprise LANs. It is no surprise that high-speed Internet access is what end-users have come to expect. When designing a HotSpot you should consider providing your users a minimum 100Kb/s transfer rate. Depending on the type of users (business, gamers, video watchers, etc.) and the number of simultaneous users expected, you will need to adjust your minimum supplied bandwidth accordingly. For example, a 500Kbps DSL line may be fine for a coffee shop expecting 2 or 3 active users at any given time, but it would not be sufficient for a hotel or other large venue. You will want to design your HotSpot to provide the maximum bandwidth possible in the given environment and business context: trade-offs between cost of bandwidth and the expected revenue must be examined.

2.2.3 Security expectations

More and more, computer users are becoming aware that all computers and networks are vulnerable to malicious acts. It should be the responsibility of the wireless service provider to secure the link and is the responsibility of the user to provide security at the application level through personal firewalls or other means. In reality, most users, unless backed up by an enterprise, will not have a personal firewall, yet they will expect that the HotSpot provider will supply a secure connection. The HotSpot service provider should strive to protect the end-user from malicious acts (purposeful or not) from other users on the WLAN and Internet. Even the most basic and easily implemented security practices can make the difference between a secure and non-secure environment. Security is discussed in greater detail in Chapter 5 of this document.

2.2.4 Availability and reliability expectations

Customers will expect that the wireless connection “just works”: the user’s experience is most affected by the ease of network connectivity. Connectivity problems are usually due to improper

or incorrect configurations and unexpected hardware resets. New network loads can also cause problems that were not seen when the HotSpot was initially deployed. Another reason for inconsistent network performance is a change to the environment such as a neighbor business installing an AP transmitting on a conflicting channel.

To maintain consistent HotSpot availability, the most important thing to do is monitor the network frequently. You will want to look for usage patterns and watch how your network performs under different usage scenarios to fully comprehend the availability and reliability of the HotSpot. Managing the HotSpot is discussed in more detail in Chapter 6.

2.3 Understanding the HotSpot Environment

It is important to understand the HotSpot environment in order to deploy a configuration that meets the users' requirements. There are three key factors that determine what type of HotSpot environment to create: the physical size of the location, the number of simultaneous users, and the types of usage expected.

2.3.1 Physical size

The physical size of the location is the first key factor to consider. This is one element (along with user density) that will determine how many wireless Access Points (APs) must be deployed. A typical AP covers a circular area roughly 300 feet in all directions. Multiple APs are required to provide coverage for large sites. AP deployment is discussed in more detail in chapters 3 and 4.

2.3.2 Number of users

The next key factor in determining HotSpot layout is the number of users and the user density: number of users per unit of area. The number of users (along with their usage patterns) will determine the bandwidth required to provide a pleasurable user experience. A minimum target for bandwidth is 100Kbps per active user. You will need to determine from the usage models how many of the connected users will be simultaneously active. For example, an environment with 5 active users will require 500Kbps or better Internet connectivity, i.e. a DSL line or connection with equivalent capacity.

The number of users in a given area can impact the number of APs required due to the resource limitations of the AP. In an environment with many users, like a hotel conference room or convention hall, more APs may be required to handle the load, even though a single AP can provide coverage for the physical area: 20-25 users per AP is a good guideline.

2.3.3 Usage models

The third key factor is the types of applications the users will run while connected to the HotSpot. The expected usage will be different at different sites. For example, a coffee shop's typical user might be small and home business owners and students, while a hotel would likely have more enterprise-class business travelers. Students would be more likely to run applications like on-line chat, Internet games and streaming audio while business travelers are more likely to connect to corporate intranets to read email and run business applications.

What needs to be determined is the minimum bandwidth required to provide a user running the "typical" applications at the site, with enough capacity to have a good experience. This number, multiplied by the number of simultaneous users, determines the minimum Internet bandwidth required. For example, if you determine the typical usage at your site requires 200Kbps of bandwidth for adequate performance and you expect no more than 5 users to be actively using this bandwidth at any one time (out of a potentially larger population of connected users), a 1Mbps Internet connection would be required.

200Kbps X 5 simultaneous users = 1,000Kbps = 1.0 Mbps bandwidth needed

2.3.4 Examples

The following examples illustrate how HotSpot size, number of users, and usage types affect HotSpot deployments.

2.3.4.1 Coffee shop

A typical coffee shop is relatively small. The number of simultaneous users is also going to be small: probably fewer than five. In this environment, a single AP would be sufficient to provide adequate coverage and service. Usages would include e-mail, web surfing, and on-line chat; all of which have relatively low bandwidth requirements. An Internet connection with a bandwidth of ~500Kbps (e.g. a DSL line) would be sufficient.

2.3.4.2 Hotel

For a hotel, the first question to address would be "What is the coverage area?". Is it strictly the lobby, or the lobby and conference rooms, or the lobby, conference rooms and all guest rooms? If the coverage area is just the lobby, a single AP may be sufficient. To cover everything (lobby, conference center and guest rooms) may require 20 or more APs. The user base will be larger than a coffee shop, on the order of 10-50 simultaneous users, depending on the hotel size, but the user density would be very small if 10 or more APs were deployed. User density in the conference rooms might be high and could potentially warrant increasing the number of APs located there. Typical users are likely business travelers who would be focused on email, access

to corporate intranets, web-surfing and file downloads. A T1 (1.5 Mbps) or higher bandwidth Internet connection will most likely be required.

2.3.4.3 Convention center

A convention center environment combines a large space with a large user population with the possibility of high user density in the conference sessions. Many APs, possibly 50 or more, would be required, both to cover the physical space and to provide the performance needed to support the large number of users. Usage would be similar to the hotel environment: email, corporate intranet access, web-surfing and file downloads along with the potential for event-specific content. 10s to 100s of Mbps of bandwidth would be required to support this usage scenario.

3. HotSpot Functionality and Network Components

We can summarize HotSpot user expectations as being able to access the Internet and everything that comes with it. Customers may also want the added benefits of a wireless connection and a secure network environment. In this chapter we take a look at the technical aspects of the HotSpot environment and the functionality that a HotSpot must have implemented in order to fulfill a user's expectations. The network hardware and software components needed to provide these functions are also discussed.

Below is a list of some important features and functionality that a HotSpot needs to provide.

- Enabling access to the wireless link
 - 1) Providing the mobile station with information about the wireless network
 - 2) Creating an association with the mobile station
 - 3) Providing access to the local network
 - 4) Providing data packet transfer services
 - 5) Disassociation from with the mobile station
- Provisioning the HotSpot
 - 1) Page redirection function
 - 2) Mobile station authentication
 - 3) User authorization
- Layer 3 (IP) Address Management

- 1) Providing an IP address for the mobile device
 - 2) Private to public address translation if necessary
 - 3) Providing Domain Name Services (DNS)
 - 4) Providing information about gateways
- Providing access to HotSpot LAN
 - Providing access to the WAN
 - Protecting user data privacy
 - Provide accounting information (keep track of user network usage)

Some of these functions are provided by a single HotSpot network component while others are implemented through the collaboration or combination of two or more components. To illustrate these functions, we'll reference the HotSpot architecture shown in Figure 3-1. Please keep in mind that this is one of many possible HotSpot configurations.

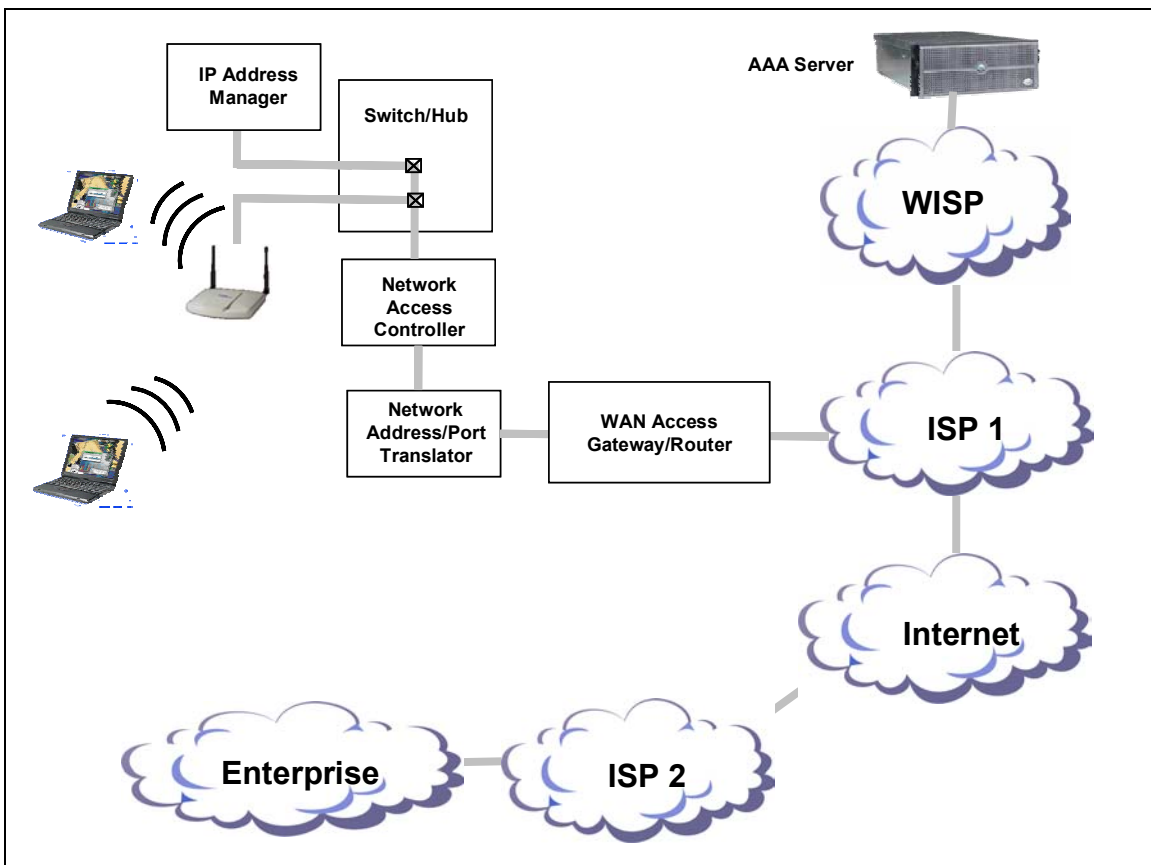


Figure 3-1 Reference HotSpot Architecture

3.1 The Access Point

The main purpose of the Access Point is to provide wireless access to the HotSpot network. The AP is typically tasked with securing access to the network. However, due to known vulnerabilities with the current security standard, Wired Equivalent Privacy (WEP), and lack of key management, most deployed APs should not be relied upon to secure network access. Those that are, have done so by including non-standard enhancements made by manufacturers. For the sake of completeness, we will mention some of those functions here as advances in wireless network security that will allow APs to participate in network security tasks.

3.1.1 Important access point features and functionality

This section describes what the authors consider to be the most important Access Point features and functionality to be considered when implementing a HotSpot. This is not a full list of features currently available, but rather the minimum needed to deploy a successful HotSpot.

3.1.1.1 Providing the mobile device with information about the wireless network

On a regular basis, APs will broadcast the wireless network parameters through a message called the beacon. The purpose of this message is to make it easier for end-users to determine what networks they can connect to and to let the mobile device know about the wireless network characteristics (channel in use, frequency hopping information, etc.). Beacons are always sent by the AP and cannot be disabled in any way.

Another method used in device association is advertising. In advertising itself and the network, an AP broadcasts a message that includes the SSID of the network (in addition to the information sent in the beacon). Advertising is not mandatory or necessary for a mobile station (MS) to establish a connection with the AP. If a wireless network is not advertised, the user needs to know the SSID in order to connect to the AP. This is one of the most easily implemented security methods although it is not a robust one.

Tidbit: *Whether or not a wireless network is advertised is a configuration setting on the AP. If you don't see your wireless network advertised, check the AP configuration. You always want to advertise the wireless network of a public HotSpot to make it easier for potential users to find it.*

3.1.1.2 Responding to mobile station requests for information

The mobile station does not have to wait for the AP to advertise its presence. As a matter of fact, if it did, the mobile station would never be able to connect to networks that don't advertise. The mobile station can proactively get information from an AP in one of two ways; it can send a probe

request to discover nearby 802.11 networks or it can send a request for association to a specific AP. In either case, the AP includes the necessary information about the wireless network in its response to the mobile station.

3.1.1.3 Privacy and security considerations

802.11 can provide data privacy by encrypting frames as they get transmitted over the wireless medium. The first data encryption specification for use with 802.11 is the WEP encryption specification. When using WEP, the administrator of an AP enters in a key, and the user must program the same key into the client. Once the two are matched, packets can be exchanged. Since the keys have to be changed and managed manually, you would have to notify any and all of your customers every time you decide to change your network's secret key. If you don't change the key, then you can bet that soon after you have established one, everyone in your neighborhood would know what it is. WEP's lack of automatic key management is a major barrier to practical use in HotSpots.

In acknowledgment of WEP's vulnerabilities, the IEEE 802.11 Task Group set out to develop a more secure encryption mechanism for wireless networks. The result is "Robust Secure Network" (RSN). While RSN addresses all of WEP's vulnerability, the industry felt it needed an immediate solution to resolve 802.11 security problems. The Wi-Fi* Alliance developed an interim solution by using finished portions of the un-ratified RSN specification. This solution is called Wi-Fi* Protected Access (WPA). WPA and RSN (a.k.a. 802.11i) include key management and better encryption. These authentication standards will slowly become more prevalent as hardware for client NICs and APs become available. Both of these specifications, WPA (and WPA2) and RSN are addressed in more detail in chapter 5.

Tidbit: HotSpots typically do not use WEP due to its lack of key management and encryption vulnerabilities unless required by law, as in Japan. Prior to WPA, HotSpots only had the alternatives of proprietary solutions or no encryption at all for securing the wireless link.

3.1.1.4 Device and user authentication

802.11 uses WEP in two ways; one is to authenticate the device and the other is to provide confidentiality by encrypting the data packets. It is important to understand the distinction; newcomers to 802.11 often confuse the two uses. You have the option of using or not using WEP for authentication and for encryption but there is a simple rule; you can use WEP for authentication only if you also use it for encryption. The converse is not true. You can use WEP for encryption and not use it for authentication. In 802.11 parlance, not using WEP for authentication is called "Open Authentication" while using WEP for authentication is called "Pre-shared key Authentication".

Before a device can get connected to the AP as a conduit to the network, it must be authenticated. WEP only provides device authentication. That is, no information is provided about the user of the mobile device. In Pre-Shared Key Authentication, the assumption is that if you know the shared-secret then you must be OK to use the network. Once the mobile station has been authenticated, it is allowed to associate with the AP.

Once again, Pre-Shared Key Authentication can only be used when WEP is enabled for data encryption. In this case, the key used for authentication is the same key used by WEP for data encryption. When other encryption specifications are used (TKIP or AES), Open Authentication is the only authentication mode allowed.

While WEP does not provide user authentication, WPA and RSN do include user authentication mechanisms as part of their infrastructure (802.1X and EAP). Further discussion of 802.1X, EAP, WPA and RSN can be found in Chapter 5.

3.1.1.5 Device authorization

Authorizing the mobile station (MS) to connect to the network means that the MS is able to associate with the AP and send and receive packets through that association (connection). In the 802.11 standard, authentication is required for authorization and positive authorization enables association. It is not necessary to be associated with an AP in order to exchange management frames. Association is required to pass packets through the AP addressed to other network components.

In a WEP-enabled wireless network, authorization is the job of the AP. As was mentioned earlier, many HotSpots do not use WEP and therefore only use Open Authentication. Using Open Authentication means the MS will be authorized and associate with the AP almost immediately after requesting the association since there is no need to check the credentials of the MS. When HotSpots use WPA or RSN, authorization generally comes from an AAA server.

3.1.1.6 Providing access to the local network

Once the MS has an association to the AP, it can send and receive data frames on the local HotSpot network. The AP serves as a bridge between the wireless and wired networks, providing access to the HotSpot wired network.

3.1.2 Choosing your AP

The AP is the direct means of communication between the HotSpot LAN and the user's device. The quality of the AP and its feature set is a determining factor in the success of HotSpot deployment.

Consistent interoperability of the AP with 802.11 wireless network cards from diverse vendors is the most critical AP feature. For this reason an important consideration when choosing an AP is whether or not it is Wi-Fi* Alliance certified. The Wi-Fi* Alliance is an independent organization that serves the 802.11 wireless industries by offering a set of interoperability tests that must be passed by a given AP or client wireless NIC to be Wi-Fi* Alliance certified. Vendors design their hardware to 802.11 specifications and then, for a fee, submit their products to the Wi-Fi* Alliance for certification.

Wi-Fi* certification serves to instill a level of confidence that a Wi-Fi CERTIFIED* client device will work with a similarly Wi-Fi CERTIFIED* Access Point. It is important to remember that it is unlikely that two Access Points from different manufacturers will work together. Wi-Fi* Alliance is working to add the Inter Access Point Protocol (IAPP) 802.11f standard to their test suite, but at this time it is not included. Unless Access Points support IAPP, it is not possible to roam from one Access Point to another if the manufacturers are different. In some cases even different AP models from the same manufacturer do not support roaming between them. Please refer to section 4.5 for more in-depth information regarding Access Points.

3.2 Switch/Hub

The purpose of the switch or hub is to provide multiple ports for connectivity from APs and other network components to the HotSpot's backhaul. This component can be a simple hub or a sophisticated switch with VLAN capabilities. If the component is a smart, VLAN-capable switch, it can participate in the task of controlling network access. Let's take a look at some of the things a VLAN-capable switch can do.

- Physically separate ports. In other words, traffic traveling through specific port(s) does not and cannot reach other port(s).
- Connect two or more ports together, essentially put all traffic traveling through the connected ports on the same backhaul.
- Route packets from one port to another based on MAC address or IP address.
- Tag packets based on source or destination port, MAC address or IP address.

All of this capability gives you the ability to control the routing of packets to certain destinations based on certain packet properties (port, MAC address, IP address) that the switch supports. If you couple this capability with some intelligence (usually implemented by another network component) to determine the state of MS authentication, you can control access to the network in many different ways. Once you know the identity of the user, you can also provide specific quality of service (QoS) by giving certain users' packets special treatment. With a smart switch and a

network access controller you have many different options available for provisioning your network.

3.3 Network Access Controller

The purpose of the Network Access Controller (NAC), as its name implies, is to control access to the network. A NAC functions as the gatekeeper to the network by implementing smart filters used to select what is let through onto the gated network. The main function of the NAC is to perform user authentication or to assist in the authentication and to control network access based on the authentication state. A NAC generally has a single data port in and a single data port out. Since NACs process all packets on their way to the HotSpot's backhaul, they are required to have sufficient processing power to maintain the desired performance.

NACs have been used for a long time in wired networks. Recently; a new breed has emerged that works especially well for wireless HotSpots; the "Wireless Gateway". Besides controlling access to the network, Wireless Gateways provide several integrated functions into a single network component such as AP management, page redirection capabilities and tracking of network usage for accounting and billing purposes. Two very popular Wireless Gateways are sold by Bluesocket* and Nomadix*.

3.4 IP Address Allocation Manager

In order for mobile stations and/or other network components to communicate with each other they need to have unique IP addresses within the HotSpot. The universal method of providing such an address is through a Dynamic Host Configuration Protocol (DHCP) server. DHCP is an Internet protocol for automating the configuration of computers that use TCP/IP. A DHCP server will not only provide the MS with an IP address but will also provide the IP addresses of the gateway and DNS servers to use. DHCP servers provide other services which are not relevant for a HotSpot so they will not be discussed here.

Critical to the functionality of the HotSpot is the choice of IP address used for assignment to the mobile stations. You have the choice of using either public or private IP addresses. Public IP addresses allow you direct communication with other devices on the Internet. They are public routable addresses so anyone needing to find the mobile station will be able to do so using the assigned public IP address. Public IP addresses can be hard to obtain and are costly when leased from an ISP. Most HotSpots will choose to use private IP addresses for the mobile stations on their LANs. The Internet Assigned Numbers Authority (IANA) reserved a pool of IP addresses for use in private networks. The set of reserved IP addresses for use in private networks is described in RFC 1918. Table 4-1 lists these addresses:

10.0.0.0 – 10.255.255.255	24-bit block Single class A network number
172.16.0.0 – 172.31.255.255	20-bit block 16 contiguous class B network numbers
192.168.0.0 – 192.168.255.255	16-bit block 255 contiguous class C network numbers

Table 3-1 IANA Address allocation for Private Networks

Private IP addresses can be used in any private network and are not routable on the Internet. Since these addresses are not routable, they can't be used to directly communicate with other devices on the Internet. So how can devices that use private IP addresses communicate with devices outside the HotSpot? The answer is through a Network Address/Port Translator.

3.5 Network Address/Port Translator

When IP packets are sent over the Internet, those packets must use public (unique) IP addresses. So how can a networked device that uses a private IP address send a packet over the Internet? The answer is that you switch to using a public IP address while the packet traverses the Internet. Any organization that implements a private network using private addresses must also own (or lease) one or more public IP addresses to allow internal traffic to move over the Internet. Any packet that needs to cross from a private network to a public network needs to have its source IP address changed to a public IP address. The device that performs the translation from private address to public address is called the Network Address Translator or NAT.

A variation of this translation exists that also translates the IP port. These devices are called Network Address Port Translators or NAPT devices. NAPT devices have an advantage over NAT devices in that you can map many private IP addresses onto a single public IP address by just changing the IP port that is used with the public address. NAPT devices are fairly common; they are even used in home networks. For example, if you have multiple computers in your home accessing the Internet through a DSL line then you are likely to have a NAPT capable device. Rarely does a DSL provider give the home user more than one IP address for home use (unless

the user requests it and is willing to pay for it). Most DSL routers sold for the home such as LinkSys* routers have NAPT capability.

As in home networks, HotSpots commonly include the use of a NAPT device. You can choose to purchase public IP addresses from your ISP but, how many will you need and at what price? Some HotSpot service providers do choose to use public IP addresses at their HotSpots because they have fewer problems when VPNs are used. There are well known interoperability problems that exist getting VPNs to pass through a NAT or NAPT device. Most vendors, but not all, have overcome these interoperability issues in their products. The most frequently recurring problem is when multiple mobile stations try to connect to the same VPN server. As an example, multi-VPN usage might happen at a convention or a hotel where employees from the same company are staying when they attempt to read their corporate email around the same time.

Tidbit: Make sure that your NAPT device supports multiple simultaneous VPN connections to the same VPN server. This service will be important to your enterprise customers. When testing the NAPT device or when specifying it for purchase, make sure that this requirement is met when using the most popular tunneling protocols (GRE, PPTP, L2TP, IPSec). If possible, test multiple VPN support using the most popular VPN products (e.g. Cisco*, Microsoft*, CheckPoint*, Nortel*, Netstructure*).

3.6 WAN Access Gateway/Router

The WAN Access Gateway/Router is the point of exit from the HotSpot to the ISP. This component fulfills the function of providing access to a WAN. The type of gateway depends on the type of backhaul to the ISP. Examples of types of backhaul include ADSL, T1, T3, E1 and E3.

Tidbit: Consult your ISP for advice on best WAN Access Router choices to match the ISP's service and equipment.

3.7 LAN

The HotSpot LAN is typically implemented with CAT5 Ethernet cable and network interfaces that support Fast Ethernet or even Gigabit Ethernet. APs and other HotSpot network components can be connected together through switches if they are on one common subnet or routers if on separate subnets. It is important to distinguish these requirements early on, as APs configured for L2 roaming cannot pass network traffic through a router.

3.8 WAN Backhaul

There are several options for connecting the HotSpot to the Internet. The most common WAN connection is some configuration of DSL. These types of connections are relatively cheap and will provide, in most cases, sufficient bandwidth for a small HotSpot. Leased lines are the best alternative if the HotSpot provider is concerned with controlling the quality of service (QoS) of the HotSpot. Leased lines avoid many of the variables associated with DSL service: committed information rate (CIR) from the DSLAM to the Internet on a per-channel basis can be as low as 10Kbps!

In order to decide what kind of backhaul service is required, a service provider needs to determine how many users are likely be logged in at the HotSpot at any one time.

For broadband service, a data transfer rate of 100Kbps is considered the minimum. Depending on the size of the HotSpot, the number of simultaneous users using 100Kbps may vary between 1 and a few hundred. When determining the requirements of the backhaul you will need to have an idea of, statistically, how many users will be requiring the full 100Kbps simultaneously. Your first estimate might be based on data collected at existing HotSpots or based on customer information (for example, knowing the number of customers that sign up for Internet access at a hotel). After the HotSpot is functional, the best thing to do is monitor network usage trends in order to forecast future bandwidth requirements.

3.9 Internet Service Provider – ISP

The Internet Service Provider (ISP) provides the connection between the HotSpot and the Internet or other WAN. ISPs can provide WISP services and in some cases do. Examples of these types of ISPs are AT&T*, T-Mobile*, and Verizon*. When the ISP and WISP are not the same company, the WISP generally selects the appropriate ISP for the HotSpot. The connection to the ISP from a HotSpot, i.e. the backhaul, should be a high speed connection such as DSL, T1 or T3.

3.10 Wireless Internet Service Provider – WISP

The advent of 802.11-based communications brought new business opportunities, among them the requirement for a new kind of Internet Service Provider; the Wireless Internet Service Provider or WISP. ISPs can also provide WISP type services, and in some cases do, but there is enough independence in the requirements for non-ISP businesses to provide WISP services. Among the services provided by WISPs are:

- HotSpot Design

- Management
 - Remote HotSpot Health Monitoring
 - Managing hardware/software updates
 - Network Configuration Management
 - User Account Management
- Access control and monitoring
 - Provisioning
 - Authentication
 - Security
- Accounting & Billing: Pre-paid, post-paid, and roaming settlements
- WAN Access

HotSpots can be implemented in locations such as cafes, hotels, and airports. WISPs do not necessarily have to own the physical HotSpot locations. WISPs and location owners will establish business relationships to deliver wireless communications through HotSpots. In some cases, owners of physically dispersed locations will establish service contracts with several WISPs to deliver wireless services to their areas. One example is that of large hotel chains. A hotel chain might choose different WISPs based on geographical locations or for other business reasons.

3.11 Authentication Authorization and Accounting (AAA) Server

Authentication, Authorization and Accounting (AAA) Server is a generic term used to identify a network component that provides the services, as implied by its name, of authentication, authorization and accounting.

Authentication is the process of identifying a unit (device or user) that wishes to engage in a network-based transaction. The authentication can be mutual and it can take place using any one of several authentication protocols such as EAP-TTLS or PEAP.

Authorization is the enablement of access to specific resources once a unit (device or user) has been authenticated. As an example, Authorization can take place by enabling a port on a switch. The port enabled might provide access to Web services, databases etc.

Accounting refers to tracking resource utilization. The utilization data can be used for the purpose of creating charges, performance tuning or other reasons. Typically, the AAA server resides on

site at the WISP location. The AAA server can also reside at the headquarters of the HotSpot location owner. This might be the case for location owners such as large hotel chains. In other cases, the AAA services are distributed between servers that reside at multiple locations. The distributed servers communicate with each other to provide a complete set of services.

RADIUS (Remote Authentication Dial In User Service) is a standardized protocol used to communicate with and between AAA servers and AAA agents. Support for this protocol is widely available in the industry. Some AAA servers also support proprietary protocols which might be more efficient than RADIUS; of course, their use will limit interoperability with client components (generally the AP).

3.12 Integration and Consolidation

Public Wireless LANs (HotSpots) are a new concept and, as such, the technology and business models to support it are still evolving. From the technology point of view, the trend is to integrate as many of the network services required for a HotSpot into the fewest number of network components. The term “HotSpot-in-a-box” is generally used for turn-key solutions that consist of a single network component combined with the most common HotSpot functions. There are pros and cons to this type of solutions but both keep changing in step with new the technology.

This document assumes certain architectural choices have been made for the purpose of illustration. Please keep in mind that there are many possible HotSpot configuration choices and the technology is still evolving. Consolidation of business models and service choices should also be considered. The ISP, WISP, and mobile phone services can all be provided by the same enterprise or supplied separately. Once again, our choice of business model in this document is used only to illustrate points of interest.

4. Understanding Wireless Environments

The mobile station's (MS) wireless connection is typically the most ignored aspect of HotSpot implementations. It is tempting to make assumptions regarding a given environment without doing the necessary upfront work to insure complete RF coverage and high network throughput. Careful thought and upfront work must be completed in order to implement a successful wireless network.

A wireless network can be successfully implemented by performing the following.

- Investigate your site requirements regarding the type of HotSpot you are implementing
- Perform a Site Survey in order to assess the challenges involved in installing a new wireless network

- Evaluate the site for coverage and placement of APs.
- Choose your equipment carefully to match the environment you are in.
- Take the appropriate precautions to insure the proper level of wireless security.

4.1 Performing an RF Site Survey

Site Surveys are the most important part of any wireless implementation and require three pieces of equipment to perform; a Test/Standard AP, RF Analyzer, and a notebook computer.

The Test AP should be a representative sample of what you plan on implementing in your environment. If you are not sure of which access point to use, a Wi-Fi* CERTIFIED AP should be sufficient in most cases.

RF Analyzers come in many shapes and sizes. Some of the most well-known are Airmagnet*, AiropEEK*, and Network Instruments* Observer. If you are planning on implementing an 802.11b-only environment, Airmagnet* has a good solution for PDAs (making the site survey much easier to complete). There are also many freely downloadable software solutions like Netstumbler*, Mini-stumbler* (for PDAs), Kismet* (Linux), and Airtraf* (Linux). The downside to the freely downloadable programs is that they take a significant level of expertise and patience to run, and many times are not quite as full-featured as the commercial products.

RF site surveys require patience and a keen eye for detail. Many times items like microwave ovens, portable phone systems, wireless video monitors, and metal walls may be overlooked as they do not usually appear in the RF analysis tool. Cordless phones systems usually cause interference only when they are in use, as do microwave ovens. This RF noise may appear to be negligible in the analysis tool, but if an AP frequency (channel) is configured to operate near the emission frequency of the appliance, the radiated noise can present a more serious problem than initially predicted.

Tidbit: You should perform a site survey at a time when the network will most likely be in use. If possible, several visits to the site will help in making sure that no additional sources of interference are present. Make a log of any activity including channel, MAC address, and signal strength.

4.2 Types of RF Interference

In general, RF interference can be broken down into four categories; direct interference, indirect interference, path interference (multipath), and Line of Sight (LoS) interference.

4.2.1 Direct interference

802.11b networks operate in the ISM band on distinct channels. The channel plan, however, offers only three non-overlapping channels – meaning that two adjacent channels will actually be overlapping as the bandwidth of the 802.11b signal is wider than the channel spacing. Direct interference is caused by other 802.11 devices operating on the same frequency/channel within the surveyed area. Because 802.11b devices can negotiate and coordinate their transmissions, performance will be the most noticeable problem with this type of interference.

Primarily, this interference will come from existing Access Points and Ad-Hoc networks. Existing access points are the easiest to detect unless they happen to be powered off while the survey is being performed. For instance, a coffee shop may only leave their APs on while the store is open, a college student renting the apartment upstairs may turn his AP on only in the evening. These are just two of the many non-continuous usage scenarios.

Ad-Hoc networks are much more difficult to detect as they are temporal by nature. While more common in environments like college campuses and areas with lots of teenagers, ad-hoc networking is becoming more popular and easier to implement every day. This is the primary reason why regular auditing and monitoring of your HotSpot is important.

4.2.2 Indirect interference

Indirect interference refers to devices that are not specified as 802.11 but operate in the same spectrum used by 802.11. 802.11 devices operate in the unlicensed spectrum space in the 2.4 and 5 GHz range. Other non-802.11 devices are also free to operate in this spectrum. Since these are primarily burst devices, seeing them from any standard survey tool like Airmagnet* or Netstumbler* is very difficult. Many times they will just show up as an unusually high noise floor.

When surveying a facility you must take care to inspect the phone system in use, check for locations of microwave ovens, and look to see if they have any wireless monitoring systems in place.

4.2.3 Path interference

Another difficult problem in the site survey is gauging Path Interference. Path Interference comes in four categories; Reflection, Refraction, Diffraction, and Scattering. For a full treatment of path interference please refer to *Certified Wireless Network Administrator Study Guide* from Planet3 Wireless*.

RF (especially in the 5 GHz range) has a strong tendency to reflect off of metal objects, mirrors, foil-backed insulation, and other dense, reflective objects. Since the full network infrastructure is not in place when you are surveying the site, it is very helpful to set up your test AP to run some tests to look for possible signal issues. In general, the installer needs to use a lot of experience and intuition in order to appropriately place Access Points. Other behaviors like signal scattering

off of the décor, refracting through windows, or diffracting around metal cabinets may add to the amount of interference present.

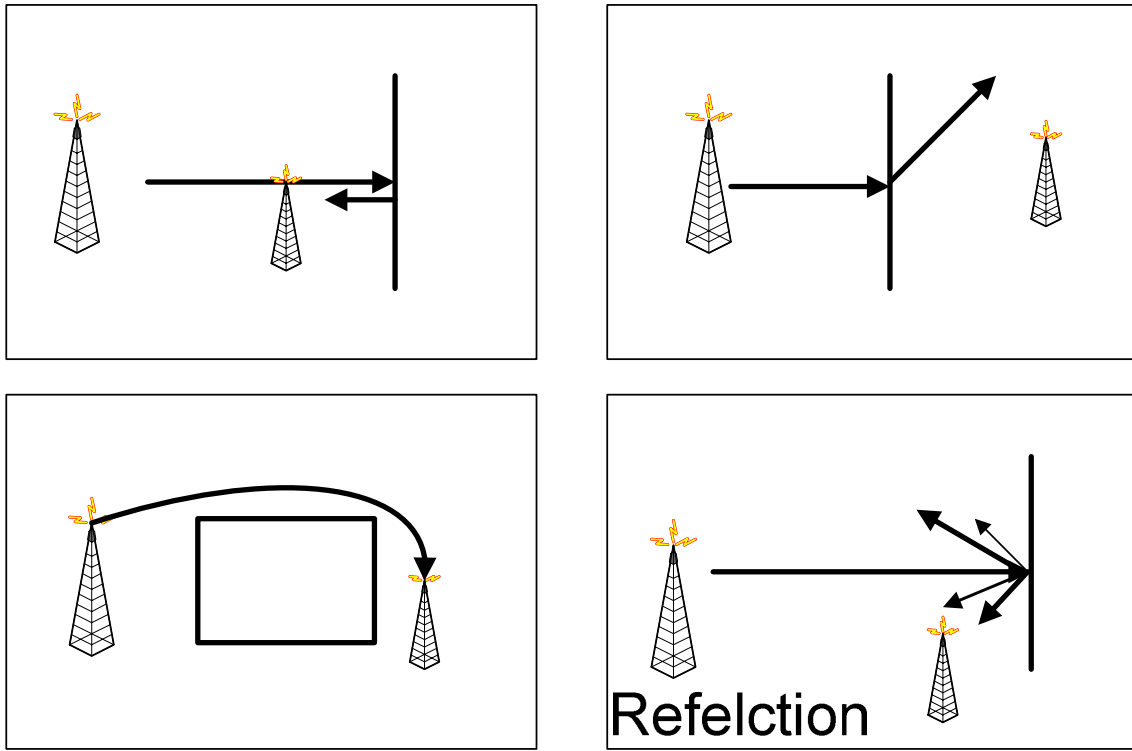


Figure 4-1: Interference Types

4.2.4 Line of Sight interference

Walls, furniture and trees are common Line of Sight (LoS) interference sources that must be addressed any time a wireless network is being installed. Most line of sight issues come from signal absorption from interfering objects. These can be as obvious as wall hangings and as subtle as vehicles passing through the line of sight. The most common Line of Sight problem is caused when using “point to point” long distance wireless links.

Tidbit: Once the installation is complete, the survey should be completed again to look for possible problems that were missed during the initial survey. It is quite likely that once saturated with RF, the environment will become much more complex and noisy.

Sender

Recei

4.3 Performance Considerations

While 802.11b's maximum data rate is 11Mbps and 802.11a and 802.11g's maximum is 54Mbps, there are several factors that can affect data rate performance.

Aside from the design considerations of the hardware, the two most influential factors affecting performance are distance (between transmitter and receiver) and the pro-active methods used by the protocols to deal with signal interference. There are mechanisms outlined in the 802.11 specification that compensate for possible transmission errors that might result from lower signal strength and/or higher interference. For example, as the distance between the transmitter and receiver gets larger, the data rate can be automatically stepped down from 11Mbps to 5.5, 2, or even 1 Mbps. The lower data rates act to insure fewer errors are generated as the RF signal gets weaker.

Another way to decrease error rates is to use special 802.11 control messages (RTS/CTS) to reserve the channel before transmission of data frames. The transmitter can automatically switch to using these messages when it detects a high packet error rate. After taking into consideration the overhead of error recovery mechanisms and protocol headers, the effective throughput will be much lower.

The 802.11 protocol also requires every packet sent to be acknowledged, further reducing the effective data transmission rate. A good rule of thumb is the actual data rate will be roughly half the maximum specified. So the maximum data rate of an 802.11b network will be around 5.5Mbps, while an 802.11a or 802.11g network will be around 27Mbps.

4.4 Site Coverage

Determining the needs of the facility is often thought of as just concerning yourself with backhaul networks or overall throughput. Many people forget about the complexities in making sure the site is adequately covered and that roaming is working correctly. Often it is assumed that complete coverage of facility is required, which leads to over-coverage. In a business environment it may be necessary to cover stairwells and hallways, but is it necessary to cover a bathroom in a coffee shop? Whatever the answer may be it is important to make these decisions prior to performing the site survey and installing Access Points.

4.4.1 Roaming

Roaming requires a flat network or Mobile IP in order to function appropriately. Since Mobile IP is rarely implemented, it is important to maintain a flat network in areas where you expect users to roam. The term "flat network" implies a single subnet in which all Access Points and users are connected. When a user moves from one area, like a conference room, to another, like the cafeteria, the APs will pass the user along maintaining the user's session persistence. This is especially important with connection sensitive applications like VPNs, email, and SSL connections. In some instances it may be impractical to implement roaming, such as when

buildings are long distances away from each other, though a thorough assessment of user needs should be done before making these decisions.

4.4.2 AP cell size, layout, and placement

While you may be tempted to solve site coverage issues by adding more Access Points, care should always be taken before making such decisions. In many cases, wireless networks are used to attract people into a place of business. If this is the strategy, placing an Access Point near an exterior wall or window may lead to undesirable users sitting outside and using, or worse, hacking the network. Access Point placement needs to be carefully considered using the data from the RF survey coupled with security considerations to place Access Points in the most appropriate places. Placing Access Points where they can bleed RF outside of the intended location can also cause problems with other wireless networks and alter coverage expectations.

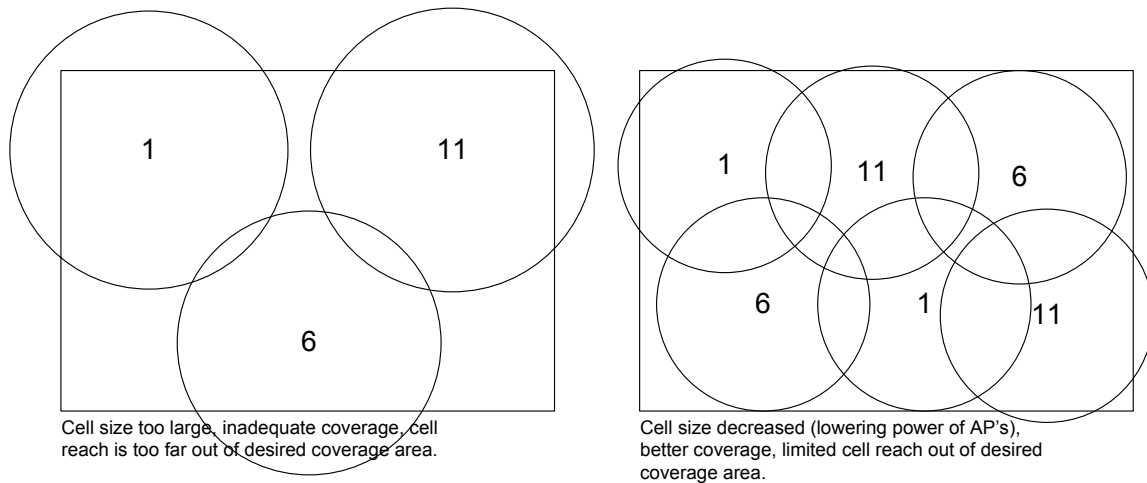


Figure 4-2: AP Cell Layout for Three Channels

When implementing Access Points you must take into consideration channel layout and cell size (see figure 4-2). Due to the restrictive nature of the ISM band there are only 3 non-interfering (non-overlapping) channels available for usage in 802.11b. The resulting pattern needs to resemble figure 4-2: no same channel AP's overlapping. In order to implement an appropriate channel layout you must be familiar with the sphere of RF radiated by a given Access Point. Please consult your Access Point documentation or manufacturer's support web site to determine the typical irradiated area by your access point for a given power setting.

4.4.3 AP density

In small environments like coffee shops and homes, cell size is not a major concern as the usage areas are usually well-covered and the backhaul is most often the limiting factor, not the AP throughput. In large installation environments like hotels, airports, and offices, AP density may

need to be increased to allow more APs to service a larger set of users. Most enterprise equipment will ship with data regarding the effective radiated RF area for their access points at a given power (usually in milliWatts). This should always be double-checked in the site survey and implementation. In many cases lowering the power output of the access point will allow for an increase in the number of APs in a given area, allowing for more users to be serviced with higher throughput.

4.4.4 Channel infrastructure layout considerations

When utilizing different 802.11 capabilities it is important to remember the impact they may have in your layout. Today, many Access Points currently on the market ship with multiple frequency capabilities like 802.11b/g and 802.11a/g. It is important to remember that the effective cell size of Access Points that support different frequencies (802.11a versus 802.11g, 802.11g infers 802.11b) are quite different and if supplying both connection types, must be taken into consideration.

Tidbit: 802.11a utilizes the 5 GHz frequency spectrum and is more limited in the effective coverage distance than 802.11g (2.4 GHz) due to the frequency and power limitations. You will need about 3 times as many 802.11a access points to cover the same area as 802.11g.

4.5 Choosing Your AP

Cost is almost always the driving factor in purchasing equipment for a wireless network. Combined with the broad array of enterprise, SOHO, and switched access point technology it can often be quite challenging to choose the proper equipment.

4.5.1 Types of APs

Access Points come in three primary varieties: Small Office/Home Office (SOHO), Enterprise, and Switched. Great care should be taken in selecting an AP for a particular application; while price is important it can be far more expensive to implement the wrong solution and then attempt to ameliorate it than to spend a little more money up front and avoid many post-deployment issues.

SOHO APs are primarily low-manageability products that are designed to work by themselves and do not possess the same feature and functionality sets that you would find in Enterprise class APs. For example, it is unlikely that you need Radius support or SNMP management capabilities in your home. However, it is more likely that you would need DHCP or basic routing and NAT capabilities in your SOHO AP. In many cases SOHO class APs may not have the latest or most robust security capabilities, though they will almost always support the basic standards. Major manufacturers of SOHO APs are LinkSys*, D-Link*, Buffalo* (Melco), and Netgear*.

Enterprise class APs are designed for a very demanding user set and tend to be high-manageability and highly-interoperable devices. Enterprise APs are designed to work in very large networks with multiple APs supporting roaming users, various security capabilities, and supply detailed real-time data. The Enterprise AP market is dominated by Cisco*, but Symbol*, Agere*, and 2Wire* are significant players in this market.

A new category of AP is the Enterprise Wireless Switch. These types of APs are known as Fat Devices because of the abundance of processing power and individuality that the APs possess. Companies like Symbol* with their Mobius* line and Extreme* with their Summit 300-48* line are centralizing the AP function while distributing the RF-to-LAN bridge.

Instead of a full suite of APs being laid out, you can instead have small antenna/bridge combinations that convert the RF signal down a standard Ethernet protocol that uses CAT 5 cable to transmit the data to the header device. These switches can support dozens of antennas spread throughout an area and significantly reduce the number of devices that need to be managed. They also improve load balancing and roaming since the switch and antennas act as a single device. In addition, many of these devices support auto-configuration of the RF environment and can put themselves into a lower power state if no MS is detected. However, they are relatively expensive and require a lot of power and maintenance.

4.5.2 AP features to look for

AP features to look for depend mostly on the type of implementation. In general, the following capabilities are ideal for a usable and supportable environment.

RF Power should be adjustable

In many SOHO Access Points this feature is not available. The lack of this feature leads to problems in implementing a multi-AP environment. Typically, an Enterprise AP will support a power range of 5-100 milliWatts.

Multiple Antenna Types

APs should support a variety of antenna types and be adjustable to turn antenna diversity on or off. Antenna diversity is a method of minimizing multipath fading by using multiple antennas. The radio system chooses the signal from the antenna with the best reception; this is especially useful in areas of high interference. In some 802.11a/b SOHO APs you will be unable to turn diversity on as they physically split the two antennas. Some APs even have the antennas hardwired, making it impossible to switch to a directional or remote antenna.

Remote Management

Access Points should have some form of remote manageability access that is secure from hacking, such as SSH2 or HTTPS. If these are not available, other methods will have to be put into place to prevent hacking into the manageability interface. Some tactics for preventing intrusion include putting the APs on a restricted subnet and to control access by ACLs.

SNMP Support

SNMP support is a must for any Enterprise-level solution. Always make sure that SNMP is disabled by default and remember to change default community strings and passwords.

Power Over Ethernet (PoE)

PoE can be the difference between a cost effective HotSpot implementation and an ineffective one. PoE allows power to be run directly to the remote device over the CAT5 Ethernet cable. Since Access Points are often put in places where power is hard to get (ceilings and long hallways) PoE is a much more desirable solution than having new, costly, power access installed. Since PoE was just recently ratified as an IEEE standard (802.3af) many devices still have custom power requirements and therefore may require vendor specific PoE equipment.

Long and Short Preamble Support

The first generation of the 802.11 specification indicated the use of a 144-bit preamble that was used to help wireless receivers prepare for the acquisition of wireless signals. As 802.11 addressed higher transmission rates and considered new usage models such as VoIP, a shorter, more efficient 56-bit preamble was also introduced. After the introduction of short preambles, the first APs and NICs on the market included a configuration option to use either short or long preambles. This caused interoperability problems for users of Mobile Stations that do not offer such options. If the AP communicated using short preamble and the MS used long preamble, they would not be able to associate and the MS could not connect.

Recognizing the interoperability problem created by the choice of short or long preambles, hardware manufacturers developed systems that could automatically support either setting. In the process, the option for administrators or users to select short or long preambles disappeared from the device configuration interfaces. Today, you can still find hardware that is configurable for either long or short preambles. In choosing between long and short preamble, we recommend using long preamble as this provides the ability to provide services to customers with legacy Mobile Stations.

Tidbit – When an AP provides a configuration choice of long or short preamble, choosing long preambles will provide interoperability with mobile stations that still use legacy NICs.

4.6 HotSpot Security in Brief

Since data transmitting over an RF link is available to anyone with the equipment that enables the data to be viewed, it is important to make sure that your HotSpot supports the appropriate level of security. Remember that any encryption will have processing overhead associated with it, requiring more powerful and capable devices to handle the additional load. RF encryption technologies include WEP (Wired Equivalency Protocol), Dynamic WEP, TKIP, WPA, and soon AES (please refer to Chapter 5 for more in-depth information).

4.7 Summary

Wireless networks present unique challenges due to the complex characteristics of Radio Frequency transmissions. Most network administrators have little history planning, installing, and managing RF networks and therefore must be careful to always;

- Understand the environment and its needs
- Perform site surveys to spot potential trouble areas and clarify layout
- Chose the appropriate equipment to complement the site
- Keep in mind the unique requirements of wireless networks such as security

5. Wireless Security

This Chapter provides an overview of the different protocols used to secure the wireless segment of a HotSpot. It does not however, delve into the details of each protocol. The intent is to provide the reader with enough practical information to understand options for protecting the wireless network and how the choice of protection affects the network (and the pocketbook) itself. In this chapter you will learn:

- What is being secured
- Types of attacks
- Security options
- Performance considerations
- Interoperability issues
- Hardware/software upgrade requirements

- What packet sequence to expect given the protection mode chosen. This is useful when troubleshooting the network.

5.1 Wired versus Wireless

In a wired network, the first method of authentication is implemented by physical barriers that a user has to overcome in order to access the network: physically gaining access to a building and getting on the network. Such barriers are not available in a wireless network where signals can travel beyond the walls of a building. A security mechanism has to be put in place to guard a 802.11 wireless network. Security on the wireless network has been 802.11's "Achilles' Heel". There has been much publicity regarding how easy it is to break 802.11's main security mechanism, WEP. The WEP protocol is 802.11's original security mechanism. Due to its weaknesses, WEP is rarely¹ used in public HotSpots to provide encryption: instead, proprietary methods are used to control access.

802.11i is the IEEE's replacement for WEP that addresses the weaknesses in the WEP protocol. However, it will require new and more powerful APs and possibly new Mobile Station hardware developed to support this change. For this reason, the Wi-Fi* Alliance defined an interim security solution called the Wi-Fi* Protected Access (WPA). WPA is a subset of 802.11i: both are based on 802.1X. The rest of this chapter describes the major features of WEP, WPA, and 802.11i. At the end of this chapter, the reader will find some practical pointers for addressing HotSpot security.

5.2 What is being protected?

The security defined in the 802.11 specification addresses protection for the radio link layer only; the communications link between the mobile station and the AP. The 802.11 specification does not specify network security beyond the AP. It is the responsibility of the HotSpot provider to insure that the wireless links are secure.

5.2.1 Types of Attacks

The following is a short list of types of attacks that can occur via a wireless network. Note that this is not a comprehensive list of all attack types, but rather a list of the more common attack types.

- Unauthorized association to the AP

¹ In certain countries such as Japan and parts of Europe, WEP is used due to government requirements. However, in those cases, WEP is complemented with other security measures.

- Rogue APs
- Man-in-the-middle
- Eavesdropping
- MAC Spoofing
- Denial of Service

Unauthorized association to APs and rogue Access Points are problems specific to wireless networks. Eavesdropping, MAC Spoofing and Denial of Service are also found in wired networks. Knowing that these types of attacks are possible helps drive the decisions regarding network set up and security.

5.3 Security Technologies Background

The primary requirements for a secure network include controlling access, maintaining user privacy and data integrity, and protecting against well-known types attacks. To fulfill these requirements, the network must provide technology (either hardware or software) that implements the following functions.

- Overall framework to bring together the implementation of the functions mentioned below
- Authentication
- Authorization
- Confidentiality
- Data Integrity
- Key management
- Protection against well known attacks: MAC spoofing, man-in-the-middle attacks, etc.

Let's take a brief look at these functions.

Access Control Framework

The access control framework provides the glue for the implementation of all the other services. The original specification of WEP did not include a framework for authentication and authorization. With WAP, WAP2 and RSN, the 802.11i Task Group introduced the use 802.1X as the authentication and authorization framework. We describe 802.1X in more detail in a later section.

Authentication

Authentication refers to the verification of the credentials provided by an entity which seeks authentication on the network. The authentication method used in a network implementation is

dependent on several factors, such as whether or not the network is an enterprise or a public network and what the intent of the network is in serving its users. For this reason, you need a way to support multiple authentication methods. 802.1X uses Extensible Authentication Protocol (EAP) as a means to support multiple authentication methods. EAP and the authentication methods it supports are addressed in later sections.

Authorization

This function refers to allowing the authenticated unit access to specific network resources. 802.1X specifies port-based authorization. Once an authorized client (a laptop or a network component) has been authenticated, the ports through which it can gain access to network resources are enabled. Elaborate access mechanisms can be derived from this basic capability by using VLAN-enabled (Virtual LAN) switches.

Confidentiality

This function addresses how to keep the information exchanged between one or more communicating units confidential. In other words, only the units to which the messages are intended are able to read the messages. This function is accomplished by encrypting the wireless frames with a strong encryption algorithm. WEP uses a pre-shared key for encryption and has weaknesses that the 802.11 Task Force did not realize until after the standard was delivered to the general public. 802.11i uses the Advanced Encryption Standard (AES) which thus far has no known weaknesses.

Data Integrity

This function insures that the recipient of a message has a way to detect if a message has been tampered with while in route to its destination. In WEP, data integrity is implemented through use of a Cyclic Redundancy Check (CRC) which is not cryptographically secure since the results are predictable, meaning that one can mathematically predict the CRC when one or more bits in the message are changed. WAP and WAP2 use "Message Integrity Check" (MIC), 802.11i uses Counter Mode with **CCB MAC** (CCM).

Key Management

Key management refers to the capability to automate how authentication and encryption keys are generated, transferred, and used in the system to secure the communications link. With WEP, 802.11 provided no automated key management. In WEP, a pre-shared key is entered manually and remains the same until it is manually changed on the APs and all the mobile stations that use those APs. Obviously the lack of automatic key management is a hole in the specification. 802.11i plugs this hole by relying on the 802.1X key management functions. To provide a migration path for deployed hardware, 802.11i specifies the use of WEP as one of the two new protocols defined in 802.11i. To be able to use WEP in 802.11i, some enhancements have been

made to the protocol. These enhancements are provided by the Temporal Key Integrity Protocol (TKIP). We'll revisit TKIP and 802.1X in the section titled "802.1X".

Protection against well known attacks

A well designed security system will guard against well known attacks. 802.11i includes guards against well know attacks such as MAC spoofing and man-in-the-middle attacks. The resistance to these attacks is usually the result of combining the authentication, authorization, confidentiality and key management features.

The following sections in this chapter present the major 802.11 and Wi-Fi* security specifications; WEP, 802.11i, WAP and WAP2, and address how the functions mentioned above are addressed within each of these specifications.

5.4 Security Options

802.11's first security specification was the "Wired Equivalent Privacy" (WEP) protocol. Soon after its completion, WEP was determined to have serious weaknesses that rendered it virtually unusable in environments where security is critical. The 802.11 Task Force has moved ahead to provide a more robust security specification for the 802.11 standard. The 802.11 Task Force formed the 802.11 Task Group i (TGi) to define the next generation security standard for 802.11. The new standard is called "Robust Secure Network" (RSN) and is also known as 802.11i.

RSN has increased computational requirements from the basic WEP standard. This requirement comes from the use of a more complex encryption algorithm and from the inclusion of automatic key management. The new requirement also means that already deployed equipment can not be upgraded since it lacks the power to handle these requirements. The Wi-Fi* Alliance concluded that it was necessary to provide a migration path through which wireless service providers could make their networks more secure without requiring them to completely replace all their APs, a costly investment. This path was also necessary since it would be unreasonable to expect all clients to be upgraded simultaneously.

To provide this path, the Wi-Fi* Alliance, in a joint effort with the IEEE 802.11 Task Force, developed the "Wi-Fi Protected Access" (WPA) specification and later WPA2. These two specifications were developed by using finished portions of the yet unratified 802.11i specification. Table 6-1 shows the major characteristics of the four security specifications, WEP, WPA, WPA2 and 802.11i (RSN).

Feature	WEP	WPA	WPA2	802.11i (RSN)
---------	-----	-----	------	---------------

Access Control Framework	None	802.1x	802.1x	802.1x
Authentication Framework	None	EAP	EAP	EAP
Encryption Algorithm	RC4	RC4	AES	AES
Key Size	40 bits or 104 bits	128 bits for encryption and 64 for authentication	128 bits	128 bits
Packet Key	Concatenation	Mixing Function	Not Needed	Not Needed
Key Management	Static	802.1X + TKIP	802.1X + CCMP	802.1X + CCMP
Key Lifetime	24 bit IV	48 bit IV	48 bit IV	48 bit IV
Authentication Methods	Shared Key	Shared Key, EAP-based Methods	Shared Key, EAP-based Methods	Shared Key, EAP-based Methods
Header Integrity	None	Michael	Michael	CBC-MAC
Data Integrity	CRC32	Michael	Michael	CBC-MAC
Pre-Authentication	No	No	No	Yes
Roaming	Limited (limited to APs from same manufacturer)	Limited (limited to APs from same manufacturer)	Limited (limited to APs from same manufacturer)	Yes

Table 5-1: WEP, WAP, WAP2 and 802.11i (RSN)²

To better understand the differences between the security options, the following sections provide background information on the requirements of a secure wireless link.

5.5 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the original 802.11 security specification. It was designed to secure the radio link layer by protecting the data as it traverses the wireless portion of the network. WEP does not provide protection beyond the AP and applies equally to 802.11a, 802.11b and 802.11g.

² Table 5-1 shows some functions that are not specific to security (e.g., roaming). These functions are shown for the sake of completeness; otherwise there would be no difference between the WPA2 and 802.11i columns

WEP's limitations stem not just from lack of a secure encryption method but also from lack of a practical key management protocol. WEP is based on knowledge, by the communicating parties, of a secret key. The secret key can be used as credential in the authentication phase and also to encrypt packets for the purpose of confidentiality. The key is entered manually into the AP and in all the clients that wish to communicate with that AP. Once a shared key is in place, it remains the same until it is manually changed in each of the network components that use the wireless network in question. This lack of automatic key management makes WEP easy prey for hackers looking to uncover and exploit the secret encryption key.

WEP has three major security objectives; provide device authentication, confidentiality, and message integrity. Authentication must take place before a mobile station is allowed to associate with and send traffic through an AP. This authentication is not mutual; only the mobile station is required to authenticate with the AP, the AP does not reciprocate. Authentication is provided through two modes of operation: Open Authentication and Shared-Key Authentication.

Open Authentication allows any wireless device to associate with an AP. For Shared-Key Authentication, the AP sends a text string to the MS in a challenge message. The MS is required to encrypt the string using its WEP key and to send it back to the AP. The encryption key used by the mobile station is the same WEP key that is used for regular traffic when in WEP mode. Once the mobile station has been authenticated, it is ready to associate with the AP and subsequently exchange messages with other entities on the network. Figure 6-1 illustrates the Shared-Key authentication sequence.

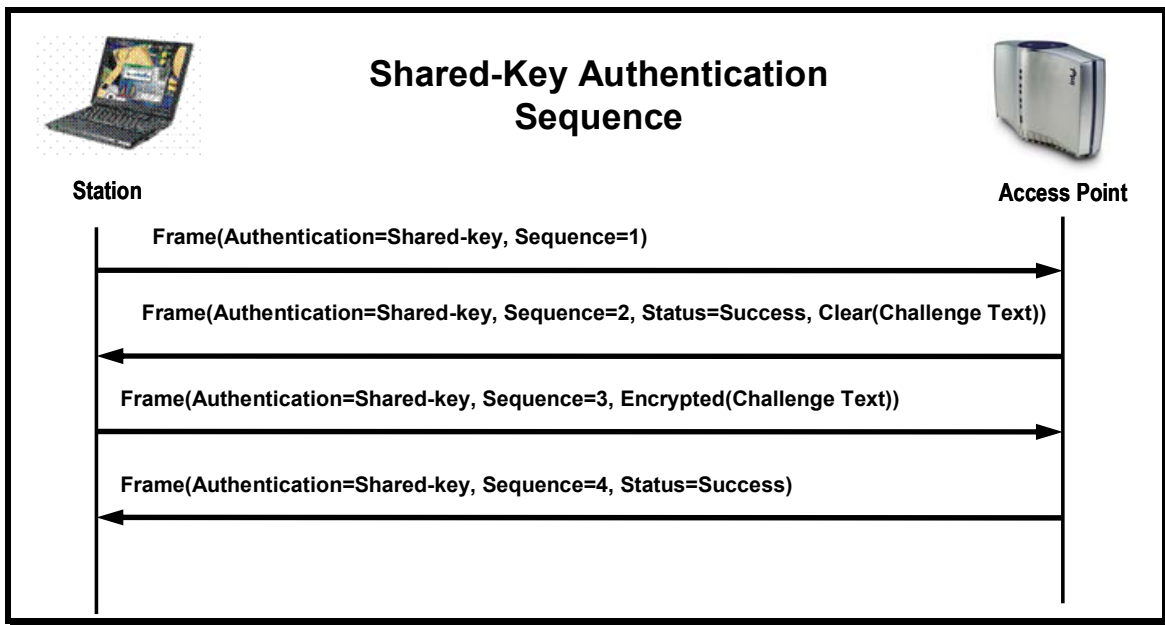


Figure 5-1 Shared Key Authentication Sequence

When WEP is enabled, it provides confidentiality by encrypting the messages exchanged between the mobile station and the AP over the wireless link. To encrypt the message, the sending unit first generates a 24-bit Initialization Vector (IV). The IV is used in conjunction with the 40-bit or 104-bit WEP secret key to form the WEP encryption key. The WEP key is then fed to an RC4 engine which uses it to generate an encryption keystream the same length as the body of the frame plus the length of the IV, 64 or 128 bits respectively (24 bits + 40 bits = 64 bits or 24 bits + 104bits = 128 bits). Finally, the keystream is XORed with the frame's body (the frame header is not included) and the IV to generate the ciphered stream. Because the IV is generated by the sending unit, it must be sent to the receiver outside of the encrypted area of the frame. Figure 5-2 illustrates the encryption process. Refer to Figure 5-3 for frame composition details.

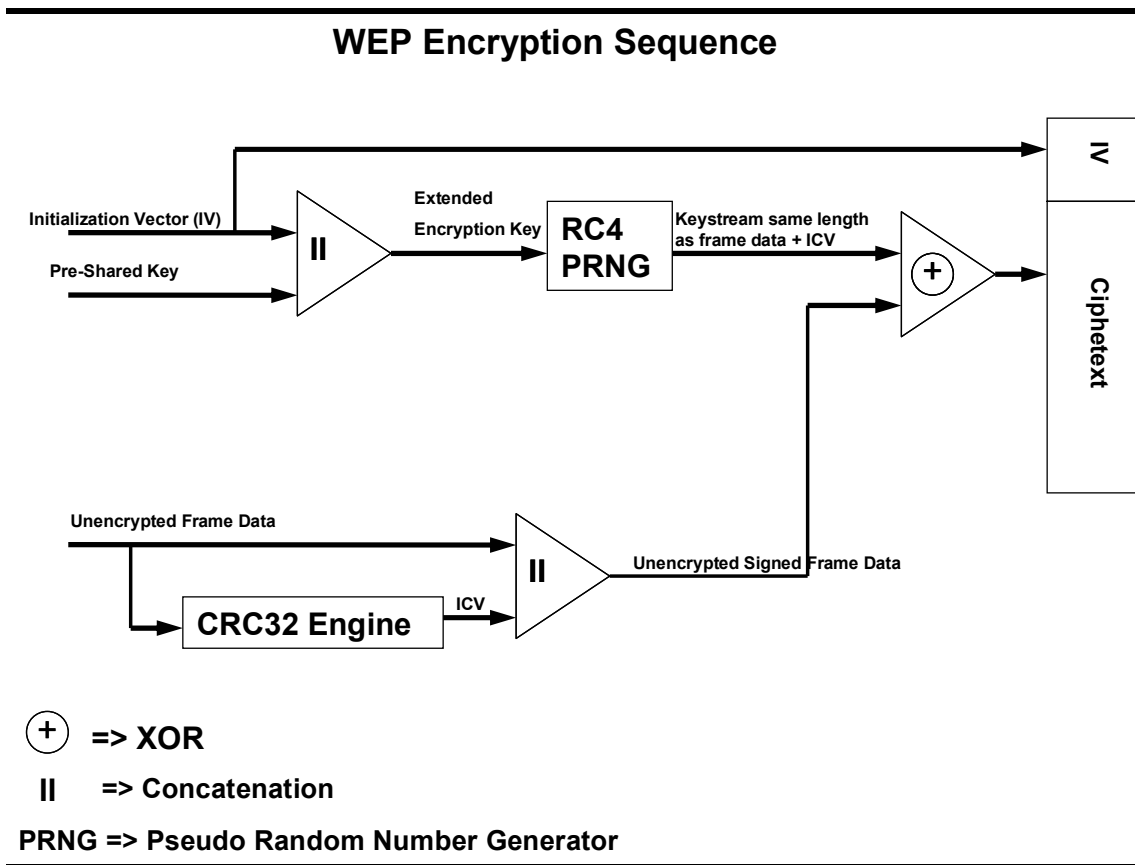
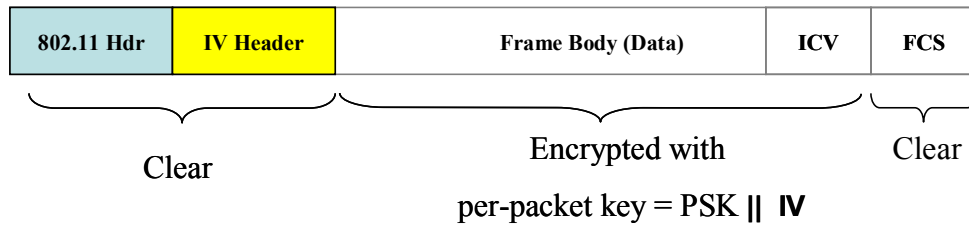


Figure 5-2 WEP Encryption Sequence for Transmission

The goal of WEP's integrity feature is to provide a way for a frame receiver to determine whether or not the frame has been tampered during transmission. To accomplish this goal, the frame sender is required to calculate a hash value (32-bit CRC) of the data frame and to append it prior to frame encryption. The hash value is called the Integrity Check Value (ICV). Because the ICV is encrypted it is not visible to the casual observer.



IV = Initialization Vector
 ICV = Integrity Check Value (CRC32)
 FCS = Frame Check Sequence
 PSK = Pre-Shared Key

Figure 5-3 Clear and encrypted frame areas

5.5.1 WEP Weaknesses

The well-publicized security problems with 802.11 come from the use of WEP as the primary means of securing the wireless link. As mentioned earlier, WEP was designed to provide authentication, confidentiality, and integrity but unfortunately, it has flaws in all these areas. The first area of weakness comes from WEP's inability to maintain the shared key secret. The most obvious reason for this problem is the lack of automated key management. WEP's key distribution is manual; every user needs to know the same secret key. Once you have distributed the key to a large user community, changing it means updating every known user; not a practical situation. The result is that in most environments where WEP is used, the key stays the same for extended periods of time. When a large community knows the secret key, you can guarantee it will not stay a secret for very long.

Another weakness in WEP is that its secret key can be easily cracked from captured packets. This is possible because WEP reuses the encryption keys after approximately 20,000 packets have been exchanged and lets eavesdroppers know when the reuse is taking place. The exposure occurs because part of the key, the IV, is sent unencrypted. An eavesdropper can tell when a key is being reused by keeping track of the IV. Knowing when the key is being reused allows a hacker to obtain multiple packets that have been encrypted with the same key. Through the process of XORing the captured messages, the eavesdropper can recover the encrypting key.

A second way to crack WEP keys is when a key is used in the authentication phase. The 802.11 specification describes two authentication modes; Shared Key and Open Authentication. When using Shared key, the key used for authentication is the same key used by WEP for packet encryption. Unfortunately, this mode of operation exposes the text used to challenge the MS in both clear and encrypted modes, giving a hacker enough information to crack the key.

The third way WEP keys are exposed occurs when certain keys, called weak keys, are used in the RC4 algorithm. Weak keys have patterns in the first and third bytes of the key that cause corresponding patterns in the first few bytes of the generated RC4 key stream. Armed with this knowledge, a hacker can use the IV and exposed key stream to identify potential weak keys. Other weaknesses include lack of forgery and replay protection. The lack of automatic key management alone makes WEP not appropriate for public HotSpot usage.

5.5.2 Dynamic Key Exchange (DKE)

DKE is an attempt by several companies with interest in improving wireless security to overcome the lack of automatic key management in WEP. There are two major draw backs for DKE, it lacks interoperability and all implementations require an AAA server, meaning that it does not provide a solution for small sites and SOHO networks. For these reasons, we do not recommend the use of DKE unless all your equipment comes from the same vendor: interoperability is not a concern and you only deal with sites that have an AAA server.

Tidbit: WEP, by itself, is not appropriate for HotSpots. Even if WEP used a strong encryption algorithm, WEP's lack of an automated key management mechanism makes it impractical to use in HotSpots. DKE does not help either due to its lack of adoption and interoperability issues.

5.6 802.11i

802.11's solution to WEP's flaws is the Robust Security Network (RSN). RSN is being developed by the IEEE 802.11 Task Group "i" (a.k.a, 802.11i). This standard is scheduled to be ready for implementation in the first half of 2004. RSN is based on the Advanced Encryption Standard (AES) for encryption of wireless frames and 802.1X for authentication, authorization, and key management. AES is a very strong encryption algorithm with no known flaws: so far it has resisted all forms of cryptanalysis. AES, however, is computationally intensive and would consume most of the computational power available in many APs currently on the market. Notebook computers that use NIC cards and offload the encryption to the main processor would be able to support AES. Entry-level PDAs would most likely not have the necessary computational power required to support AES.

To provide a migration path for improved security at sites with less powerful APs, the 802.11i task force has also developed a set of software-based updates for WEP-based security to work on devices with lower computational capability. This solution is called Wi-Fi Protected Access (WPA). WPA was developed by the Wi-Fi* Alliance as an interim solution to 802.11 security requirements and is based on Draft 3.0 of the 802.11i standard. WPA is not part of the 802.11i standard and will be discussed in "section 5.7.

5.6.1 Advanced Encryption Standard (AES)

AES is the result of efforts by the National Institute of Standards and Technology (NIST) in conjunction with industry and the cryptographic community to develop a Federal Information Processing Standard (FIPS) that specifies an encryption algorithm(s) capable of protecting sensitive government information. This standard is designed to replace current FIPS encryption specification, DES. AES is mandatory for government information and voluntary for the industry. AES specifies the use of the Rijndael algorithm; an encryption algorithm that was selected from submissions made to NIST's AES development efforts.

802.11i selected AES as its basis for providing encryption for 802.11i. AES is a very robust encryption algorithm with no known flaws that has resisted all cryptanalysis tests to which it has been exposed thus far. AES has high computational requirements (much higher than WEP alone) and will require hardware assistance be in place on network components. The use of AES as an encryption algorithm will require using computationally capable APs, i.e. APs with some sort of processor on board. On the Mobile Station side, notebook computers will be able to handle AES's increased computational and power requirements, entry-level PDAs will not. For this reason, the 802.11 committee developed the TKIP specification to provide a solution for existing hardware.

5.6.2 Temporal Key Integrity Protocol (TKIP)

Designed as a wrapper around WEP, TKIP was developed to address WEP's weaknesses and to provide a migration path to more secure WLANs using existing hardware. TKIP requires more computing power than WEP but less than AES-based RSN and WPA2. TKIP can be implemented as an upgrade to software and/or firmware. TKIP, while it uses RC4 (the same algorithm as WEP), it adds the following security improvements:

- New per-packet key mixing function
- New message integrity check (MIC) named Michael
- Longer initialization vector (from 24 bits in WEP to 48 bits in TKIP)
- New re-keying mechanism (session key renewed on a regular basis)

TKIP begins a session with a 128-bit temporal key that is known to the mobile station and the AP that changes after every 10,000 packets transmitted. The session key is used as a basis to generate per-packet keys. Per-packet keys are generated using a combination function that uses the temporal session key, the mobile station's MAC address, and the IV.

5.6.3 Framework - 802.1X

802.1X is a specification that describes an architectural framework for an authentication and authorization mechanism that is based on port access control. 802.1X is part of a family of standards for local and metropolitan area networks and is being adapted by the IEEE 802.11's Task Group "i" as the basis for Wi-Fi's new security model. 802.1X is based on the Extensible Authentication Protocol (EAP). EAP provides the ability for network administrators to choose from several authentication methods as appropriate for their environments. Figure 5-4 shows a simple 802.1X architecture diagram.



Figure 5-5-4 802.1X Architecture

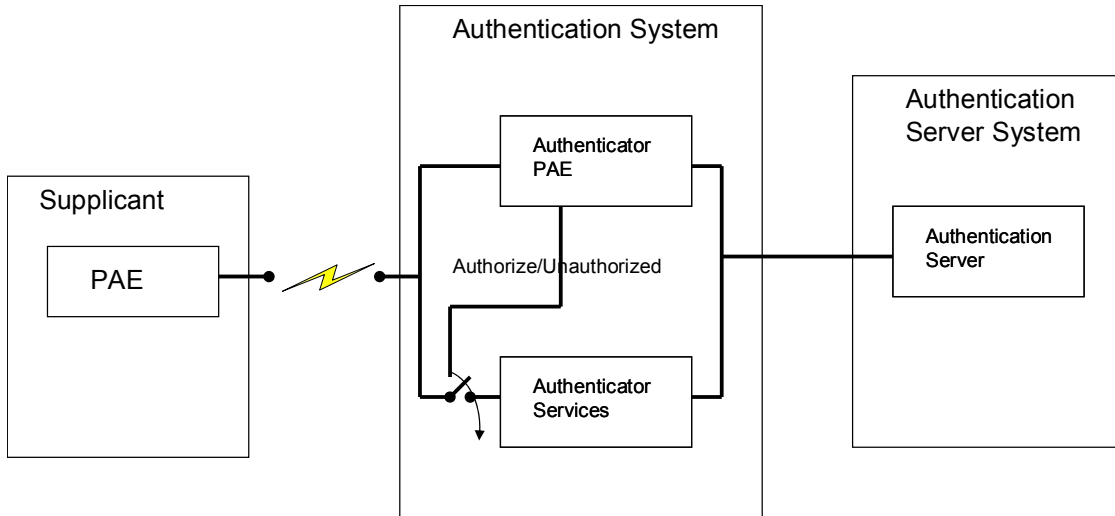
For the purpose of authentication and authorization, 802.1X provides the following specifications:

- How the access control mechanism operates
- Levels of access control supported as well as port behavior at each level
- Requirements for protocol between supplicant and authenticator
- Requirements for protocol between authenticator and authentication server

- Procedure for how authentication and authorization are used to support network access control
- Encoding of Protocol Data Units (PDUs) used in authentication and authorization protocol exchanges
- Requirements for port-based access control management (identifies managed objects and management operations)
- Requirements for remote management using SMT
- Requirements for equipment claiming conformance to the 802.1X standard.

5.6.3.1 Port-based Network Access Control

802.1X controls access to a network by limiting what services a client system (e.g. a notebook computer) can access from another system (e.g. an AP) through a specific port. In this context, a port is a point of attachment to the LAN. In a wired network, an example of a port would be a MAC bridge port or the physical ports in a router. In a wireless network, an example of a port is an “association” between a station (notebook computer) and an AP. Examples of services which can be restricted through a port-based access control include the routing functions of a network layer router and access to DHCP server. By controlling such functions, a device connected to a specific port can be limited to services that perform authentication and authorization only. Once a device/user has been authenticated, the port can be enabled to access other services such as access to the Internet. Please refer to Figure 5-5 for an illustration of port-based access.



PAE = Port Access Entity

Figure 5-5: 802.1X Port-based Access Control

5.6.4 Authentication Framework - EAP

The Extensible Authentication Protocol (EAP) is a generic authentication framework that, as its name implies, supports a wide variety of authentication protocols. Figure 5-6 is a block diagram of the EAP framework. EAP was originally developed for use with PPTP. 802.1X uses EAP as part of its network access control mechanism for wireless networks. For this reason, EAP can be used over a wide variety of data links.

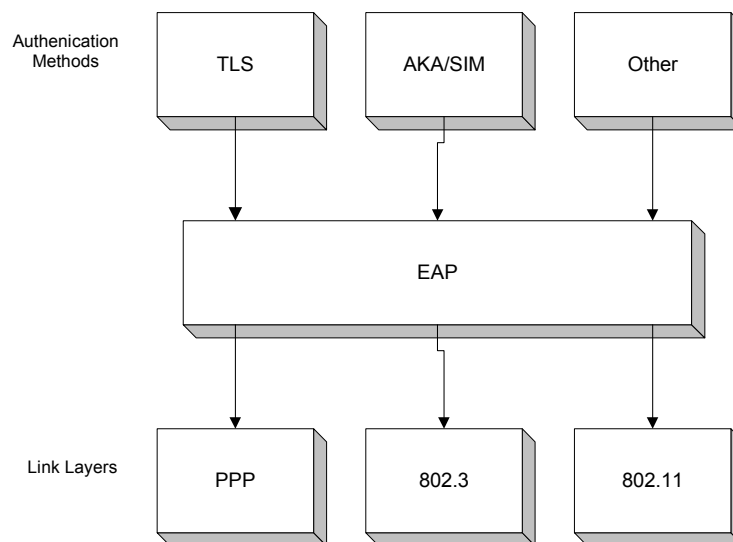


Figure 5-6: EAP Framework

The actual authentication method used is determined through a negotiation process between the MS to be authenticated and the authentication server.

5.6.5 EAP Authentication Methods

As mentioned earlier, EAP is a framework that supports multiple authentication protocol selection. The actual protocol to be used for authentication is selected through a negotiation process between the mobile station and the AP. Peer devices make the authentication method selection based on the protocols they support and policies that may have been configured into the device by an administrator. An example of a policy would be the selection of specific authentication protocol for connections within the enterprise network and another protocol for connections outside the enterprise network.

Tidbit: Support for authentication selection policies is implementation-dependent and some devices may not support this at all while others may have extensive support. There are many EAP authentication protocols, the most prevalent being: MD5, LEAP, TLS, TTLS, and PEAP.

5.6.5.1 MD5 - Message Digest 5

MD5 is the simplest of EAP's authentication methods, but when used over a wireless network it is the least secure. MD5 is a one-way authentication method of supplicant (Mobile Station) to network (AP) that uses a hash of a password and challenge string to provide proof of identity. MD5's main drawbacks include storage of the password in clear text mode for the authenticator to access and being a one-way authentication method. Only the Mobile Station is authenticated leaving it vulnerable to man-in-the-middle attacks.

Tidbit: MD5 provides no key management so attackers can still sniff your network and crack WEP keys. Support for MD5 is mandatory in the EAP specification.

5.6.5.2 LEAP - Lightweight EAP

LEAP is an EAP authentication method developed by Cisco* that supports mutual authentication. It uses the MS username and password and AP credentials for authentication by a RADIUS server. Upon authentication, LEAP generates one-time WEP keys for session usage. Using LEAP, each user connected to a wireless network uses a unique WEP key. Session keys can be renewed by using the RADIUS timeout feature that causes the user to re-login. Re-logins can take place without user intervention or knowledge. LEAP's vulnerability comes from its use of MS-CHAPv1 for mutual authentication. MS-CHAPv1 is known to be vulnerable to attacks. LEAP's drawback is that it works end-to-end on Cisco*-based networks only. Other vendors have added support for LEAP to their server ends broadening LEAP's interoperability. This however, does not help in a HotSpot environment where you want to support a broad set of customer system configurations.

5.6.5.3 TLS - Transport Level Security

TLS is an IETF standardized authentication method that uses X.509 certificates to provide mutual authentication. TLS's generation, distribution and general management of certificates requires a Public Key Infrastructure (PKI) to be in place. To transmit PKI information, TLS relies on Secure Sockets Layer (SSL). TLS generates per session WEP keys and provides for MS re-authentication and re-keying without user intervention. The main TLS drawback comes from its requirement for the client to hold a certificate. Managing certificates for large numbers of clients can be a very difficult task and is sufficient reason for many to avoid this authentication method.

5.6.5.4 TTLS – Tunneled TLS

TTLS, pioneered by Funk Software* and now an IETF standard, is one of two authentication methods (the other being PEAP) developed to overcome TLS's demanding requirement for client certificates. In TTLS, the mobile station identifies itself with username/password while the AP continues to use certificates as in TLS. TTLS is able to transmit credentials in a secure manner by using an SSL established tunnel between the client and the authentication server. Because it uses this secure tunnel, TTLS is able to support multiple challenge-response mechanisms (PAP, CHAP, MS-CHAPv1, MS-CHAPv2, PAP/Token Card or EAP). TTLS implements the different authentication methods by exchanging "attribute-value-pairs" (AVPs) that are similar to what is used in the RADIUS protocol. Another advantage of TTLS over TLS is that the user identity is not exposed to eavesdroppers as this information is sent to the server over the established tunnel. TTLS is considered very secure, has been implemented by several vendors and is widely

deployed. Nonetheless, it has not been embraced by all as the definitive 802.11 authentication method. TTLS' main rival is Protected EAP (PEAP) which we'll talk about next.

5.6.5.5 Protected EAP - PEAP

PEAP, pioneered by Microsoft*, Cisco*, and RSN is now an IETF standard, and is one of two authentication methods (the other one being TTLS) developed to overcome TLS' demanding requirement for client certificates. In PEAP, as in TTLS, the mobile station identifies itself with username/password while the AP continues to use certificates. The main difference between TTLS and PEAP is that PEAP uses the client-to-RADIUS tunnel to establish a second EAP exchange. This allows PEAP to support all of EAP authentication methods.

Tidbit – PEAP is a Cisco developed protocol that only works when Cisco provided protocols are available on the client and the server. However, several companies have licensed PEAP and incorporated it into their authentication servers.

5.7 WPA

While 802.11i resolves all the security shortcomings encountered with WEP, the completion of this new security specification was not meeting the time demands in the WLAN industry. The Wi-Fi* Alliance, using preliminary specifications for the 802.11i standard, developed the Wi-Fi* Protected Access (WPA) specification as an interim solution. WPA is a subset of the 802.11i standard leaving out only the specifications for Independent Basic Service Set, pre-authentication, and the use of AES. For encryption, WPA supports WEP with TKIP enhancements, both of which can be implemented in software and/or firmware.

For authentication, WPA supports two modes of operation; Enterprise and Pre-Shared Key (PSK). Enterprise mode requires a RADIUS server for authentication and key distribution. PSK was introduced as a means of authentication in small wireless sites (home, SOHO, small HotSpots) that lack an authentication server. In PSK mode, the pre-shared key is used only for authentication and not for packet encryption.

For data privacy, WPA uses TKIP. Session keys are generated from this pre-shared (master) key and renewed on a regular basis to deter hackers. Per-packet keys are in turn generated from the session keys using a mixing function. Wi-Fi* equipment certification that occurs after September 2003 must include an implementation of WPA. For data integrity, WPA adds a message integrity check (MIC) called Michael. This feature is provided through the use of TKIP.

5.7.1 WPA Benefits

WPA has several major benefits over WEP and RSN:

- Provides better security than WEP
- Requires changes to software/firmware only
- Provides a solution that can be implemented with existing hardware
- Allows WEP-based clients to operate in mixed-WPA/WEP networks (however, this compromises security).
- Support will be integrated into most major Operating Systems. There has been a download for MS Windows available at Microsoft's Web site since June 2003.

5.7.2 WPA Deployment Issues

Some of the most noted issues you should consider when deploying WPA include:

- Requires firmware upgrades for stations. This means that HotSpots will need to support customers who have upgraded their device to WPA and those who have not.
- WPA does not support pre-authentication
- Roaming with WPA is not possible, stations must re-authenticate. This can take on the order of 600 milliseconds. Vendors will probably support roaming by caching credentials but this solution will most likely not work across different vendor's hardware.
- Requires new client capabilities (802.1X and WPA) in supplicant
- Requires firmware upgrades for stations and APs

5.8 WPA2

The Wi-Fi* Alliance has also defined a specification called WPA2 that adds support for AES and roaming and uses CCM for header and data integrity. WPA2 also supports pre-authentication, reducing the AP-to-AP re-authentication process time from about 600 milliseconds to 30 milliseconds.

5.8.1 WPA2 Limitations

Some of the most noted issues you should consider when deploying WPA2 include:

- Requires hardware accelerated AES. This will require new APs, and in some cases, new NICs/wireless client hardware.
- Requires new client capabilities (802.1X and WPA2) in supplicants

5.9 Best Practices

Securing a HotSpot requires some finesse. If you implement one of the new standards such as WPA or 802.11i, you may end up disabling those customers that haven't upgraded their systems to the new security standard. Make sure to provide a solution for your customers that will not upgrade right away by installing mixed-mode APs. Mix-mode APs support both legacy WEP as well as the newer WPA requirements and thus provide a transition path to full WPA support. However, be aware that this mode of operation is not endorsed by the Wi-Fi* Alliance because it compromises WPA security. In an enterprise environment, where a single IT department controls deployment, it is easier to deploy WPA. Public HotSpots must take a more diverse set of customer requirements into consideration.

For public HotSpots, stay away from cheaper, SOHO APs. This type of AP tends to lack processing power for newer encryption algorithms as well as support for simultaneous use of legacy and newer authentication methods (mixed-mode APs).

Install access points that support VLANs. This will facilitate the support of multiple access methods. This is especially important to continue to support legacy clients as well as clients with newer security schemes.

Use SSL (Secure Socket Layer) or SHTTP (Secure HTTP) to protect against theft of personal information or credit card information at the application level. This is especially useful when asking the user to purchase network access time on their first connection attempt. Note: Wireless Gateways tend to enforce this security mode.

For users needing to access corporate networks, VPNs will still be the best method to secure their connections. VPNs provide end-to-end encryption and authentication. 802.11i will only protect the wireless connection from the mobile station to the AP.

Purchase equipment that can be easily upgraded to the new WPA, WPA 2.0 and RSN (802.11i) standards.

6. Managing the HotSpot

Managing HotSpots takes discipline and plenty of thought in order to manage effectively. The cost of designing and initially deploying your HotSpot configuration can be easily exceeded by ongoing maintenance costs if the HotSpot is not implemented properly. An ineffective site management model can cause poor response to issues effecting customers and non-scalable models can limit growth, both of which impact the success of your venture.

Compounding the problem is the growing feeling among consumers that 802.11 connectivity is no longer just a luxury. It is seen as a mission critical service for business travelers in airports, hotels, coffee shops, etc. Consumers will make decisions about which location and service provider to use based on their expectations of reliability and performance. With the fierce competition among wireless providers today, HotSpots with a reputation for problems will rapidly lose business.

Since a given service provider's HotSpots will potentially exist across a broad geographic area, being able to physically visit the sites can be an expensive and time-consuming proposition. A HotSpot design should include a remote management capability that provides monitoring and direct access to equipment. However, some activities, such as replacing equipment, will require a physical presence. Your management model must account for this. Options include contracting to 3rd parties, sourcing locally by hiring regional specialists, or allocating an appropriate travel budget.

In addition to performing basic management, a strategy to rollout upgrades for bug fixes and new technologies and capabilities needs to be established. If a firmware upgrade is necessary for your APs but you can't upgrade all of them remotely, you could quickly find yourself with an unexpected financial burden and unhappy customers. Having an appropriate change control policy and upgrade path is essential for being able to implement changes as the needed.

Tidbit: The key to any site management strategy is to have well-established goals and find cost-effective ways to meet them. Also, the RF environment can change from day to day, often without your knowledge or control. Active monitoring is important for finding rogue APs, conflicts from new devices like microwaves or phones, and attempts to bypass your site's security.

6.1 Management Considerations

The primary goal of any HotSpot provider's management strategy is to have data on a day to day basis that a site is still up and running. It's amazing how often we visit a HotSpot that is not in service and the service provider is unaware. In addition to performing management procedures remotely, it is highly recommended that you or a contracted 3rd party periodically audit some of your sites in order to verify they are functioning as planned. While remote management tools give some insight into the basic functionality, nothing is as effective as a person sitting down at the actual site and using the network.

One of the surest ways of ensuring proper functioning of HotSpots is to follow a "Copy Exact" policy. Using a Copy Exact approach, all of your procedures, installation methodologies,

equipment, revision control, and maintenance processes are the same regardless of location. This makes management and maintenance much easier by removing differences, and therefore potential new problems, at each site. As problems are found and fixed, all sites will benefit.

Increasingly, Internet providers are being held responsible for many of the activities that occur on their networks. This may include actions like illegal file trading, hacking, and virus prevention. Having said this, security and monitoring of sites for access and activity becomes paramount in avoiding litigation.

6.2 Management Tools

Site management tools need to address both the health of the network from the traditional wired networking side, as well as from the RF side. Many tools exist today based on SNMP or proprietary methods for querying network equipment such as routers, DHCP server, access points, and switches. Strategies need to be implemented to allow visibility into your remote network environments.

Since most HotSpots are implemented with private IP addresses behind a NAT device, it is important to design a strategy to reach your equipment in the private address space. One way this can be done is by mapping public address to private address, though there are rarely enough addresses available for this capability. A more common option would be to map a port through the single available public IP address for each device located in the private address space. This will allow products such as What's Up Gold* to gather data from network equipment, like Access Points, that are typically hidden behind a NAT.

Many of the more capable APs gather some general statistics regarding performance on the RF interface, though for critical locations it is still recommended that distributed monitors like Airmagnet* Distributed or Wildpacket's* RF Grabber be used to monitor your environments.

Many mistakes are made in monitoring sites remotely. One example is pinging an external interface from the wireless gateway. The ability to ping a device is not a sufficient measure to insure it is operating properly. Without visibility into your network to the device level you can never be sure of the state of the network. Implementing proper monitoring capabilities will all but assure that you can perform upgrades and remote changes to your configurations when needed.

7. Enterprise Applications

Enterprise business users make up the majority of recurring revenue for HotSpots. In addition, business class users are the most demanding on a wireless infrastructure due to their use of products like VPNs, Personal Firewalls, and Real-Time Applications. It is the demanding

business user that should be taken into consideration before making any decisions to restrict activities in a wireless infrastructure.

Business user applications can be separated into three categories; VPN and security, Real-Time Applications, and Real-Time Batch Applications.

7.1 VPN and Security Applications

The primary application of the business user is the virtual private network (VPN). The VPN allows the business user to utilize network resources from their Enterprise network as though they were sitting in their office. Well known throughout the industry as the most secure way to connect to the enterprise network, VPNs utilize an array of IP Ports and Protocols.

Non-enterprise consumers are becoming aware of the need to protect their systems with personal firewalls, intrusion detection, application monitors, and virus protection. Many times these applications are combined together in a hybrid application similar to ZoneLabs* Zone Alarm*, or ISS* Black ICE*. These applications learn what is “normal” for a given system and in their default states restrict behavior that is outside these lines.

What does this mean to a service provider? The key is to remember that many activities which may be intended for harmless or even well meaning reasons are seen as possible intrusions to one of these applications. Loading Java applications to track user’s logins or logouts, using ICMP to ping a device to see if it’s still there, excess SNMP traffic, and other extraneous activities can appear as threats to a Personal Security Application. The following four sections describe some VPN protocols and the ports they use. Blocking these ports will prevent the client from these protocols for VPN access.

7.1.1 PPTP

Point to Point Tunneling Protocol (PPTP) utilizes TCP port 1723 for call setup and management. Once the call is setup all encrypted data is communicated via IP Protocol 47 (GRE). In order to support PPTP VPN connections the wireless infrastructure must support outbound connections over both TCP port 1723 and IP Protocol 47.

7.1.2 L2TP

Layer 2 Tunneling Protocol utilizes UDP Port 1701 to establish a tunnel that simulates a layer two connection for the client. L2TP is most commonly utilized to tunnel IPSEC connections for remote users. Since it is simulating a layer 2 connection you need not worry about the various IPSEC protocols listed below.

7.1.3 IPSEC/ESP

IPSEC utilizes UDP Port 500 for call setup, tear down, and maintenance. The actual data connection is most commonly handled via IP Protocol 51 (ESP – Encapsulation Service Payload) and occasionally IP Protocol 50 (AH – Authentication Header).

7.1.4 SST

A proprietary protocol utilized by the Intel Netstructure VPN (once known as Shiva and recently sold to a company that will rename it to Shiva) SST Utilizes UDP Port 2233. It is important to note that SST can be configured to use other ports though 2233 is the registered port.

7.2 Real-Time Applications

In today's business and consumer environments, batch applications have given way to more and more need for real-time connectivity. From Internet Chat Programs like Microsoft* MSN*/Windows* Messenger (WM), Yahoo* Messenger (YM), AOL* Instant Messenger (AIM), and various Internet Relay Chat (IRC) applications like mIRC and FIRC, real-time applications such as these provide a challenge to network security.

Another group of real-time applications includes remote control or real-time data access over secure tunnels like SSL. Remote Desktop (RDP) has been popularized to the extent that it is now included in all new versions of Window*s 2000, Windows* XP, and Windows* 2003 Server. These types of applications can cause connectivity and usage issues if the HotSpot configuration/network engineer and/or user are over-exuberant about blocking ports and port access.

7.2.1 MSN/Windows Messenger (WM)

MSN* Messenger/Windows* Messenger is an aggressive application that utilizes many ports and functions. Windows Messenger primarily uses the Session Initiation Protocol (SIP IETF RFC 2543) for opening and closing connections. By default, SIP will use UDP Port 5060 (with a failover to TCP Port 5060) though it can be manually configured to be any TCP/UDP port or SSL connection. In the case of Windows Messenger, it will usually be an SSL session to the Windows* Messenger Server for the SIP negotiation.

Chatting can be tunneled over any TCP/UDP port or via SSL. Windows Messenger contacts a WM Server via HTTP over port 80 or through whatever HTTP proxy is available. This makes basic connectivity for chatting and updates a simple process.

Other Messenger capabilities require the use of SIP for negotiating call setup and tear down based on the following functions and ports. For Audio and Video connectivity the Real-Time

Protocol (RTP) uses UDP Ports 5003-65535. For Application Sharing TCP Port 1503 is used. For File Transfer TCP Ports 6891-6900 is negotiated. For Remote Assistance TCP Port 3389 is used for the Remote Desktop Protocol.

Reference Articles

<http://www.microsoft.com/WindowsXP/pro/techinfo/administration/inside/communicates.asp#im>

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/evaluate/worki01.asp>

<http://www.ietf.org/rfc/rfc2543.txt?number=2543>

7.2.2 Yahoo Messenger (YM)

The basic Yahoo* Messenger connection is initiated primarily via HTTP but can also be established over TCP Ports 20, 23, 25, 80, 119, 5050, 8001, or 8002. Yahoo also allows for connecting a web cam via TCP Port 5100, File Transfer and File Sharing via HTTP TCP Port 80, and Voice Chat via TCP/UDP Ports 5000-5010.

Reference Articles

<http://help.yahoo.com/help/us/mesg/twin/twin-36.html>

7.2.3 AOL Instant Messenger (AIM)

All AIM* servers listen to all ports for an AIM client connection. However the default port is TCP/UDP 5190. The most common configuration is to tunnel to the AIM server via HTTP TCP Port 80.

7.2.4 Internet Relay Chat (IRC)

TCP Port 6667 is the most commonly used port for IRC. TCP Ports 6660-6670 is the general range used by most IRC Servers. It is important to remember that IRC can be configured to use any port; as an example DALNET uses Port 7000. For file transfer via Direct Client Communication (DCC) IRC clients will use TCP ports ranging from 1024 to 5000. Once again they can be configured for just about any port.

7.2.5 Voice over IP (VoIP)

Voice over IP is a fast growing market that allows remote users to make, receive, and route voice calls into the Public Telephone Network. Working remotely can now be as simple as having your desk calls routed over the Internet to wherever your current location is, removing the need for high cell phone use or being tied to a phone line.

VoIP utilizes SIP and H.323 for connection negotiation and transfer respectively. H.323 utilizes TCP Port 1720 and as discussed earlier SIP utilizes primarily UDP Port 5060 with failover to other mechanisms.

7.2.6 Other common protocols to consider

- SSH and SSH2: TCP Port 22
- SSL: TCP Port 443
- Remote Desktop Protocol: TCP Port 3389
- NNTP (Network News Transfer Protocol): TCP Port 119
- Microsoft* SQL Server: TCP/UDP Port 1433
- Citrix* ICA: TCP Port 1494
- Microsoft* Terminal Server: UDP Port 1604

7.3 Real-Time Batch Applications

Many applications today only send/receive data in short bursts. The best example is SMTP/POP3. Simple Mail Transfer Protocol (SMTP) sessions are established over TCP port 25 and are used to send email from an SMTP client application to an SMTP relay server. POP3 (Post Office Protocol 3) is used primarily for retrieval and maintenance of an email account on a POP3-compliant server. POP3 sessions are established via TCP port 110 and are also generally short in nature as it is a batch based protocol.

Another common real-time batch application is SSL-based email. Today it is very common for business users (and consumers) to utilize an SSL based email account accessible via a web browser. Offering a highly portable mail solution, a web interface is updated either at regular intervals, otherwise known as a refresh, or updated when the user manually refreshes the page through an action like send, or through a request for a refresh. SSL email is most commonly run via TCP port 443 though many businesses will change this port in order to make the server more difficult to hack.

7.4 Summary

While it is tempting to restrict utilization of Internet connectivity down to the bare minimum via the controlled restriction of TCP/IP ports and protocols, the impact of doing this must first be considered. Many customers have sincere business reasons for utilizing many of the mentioned services. If these services are blocked, or degraded in any way, customers will react quickly. When restricting TCP/IP ports and protocols, make sure to take the time to consider the possible ramifications of the restrictions by carefully weighing the pros and cons of such an action.

8. Billing

There are many billing models (including not charging for the service): it is not the intention of this document to describe them all in detail or to recommend one over the other. Having said that, there are architectural considerations that must be understood in order to properly implement the billing system, whichever model is used.

8.1 Some Billing Models

Billing models come in many shapes and sizes. They can be bundled into two large categories for the purposes of this document: those that require knowing when the user has logged out, and those that do not. In other words the billing may be time period-based, where a user is billed for a defined time period with no limit on the number of logins within that timeframe, or usage-based where the user is billed per time period used (per minute, per hour, etc.) and/or each time the user logs in.

8.1.1 Time-Based Billing

Some examples of time-based billing are:

- A monthly charge that provides unlimited access to the network. There would be no limits on the number of logins or on how long the network was used.
- A 24 hour billing cycle (typically found in hotels) where service is provided from noon on the first day until noon on the next day, with unlimited logins and usage in between.
- An hourly rate where the user is charged a set fee for one hour of usage, even if actual usage is less, with no limit on the number of logins

Time-based billing is easy to implement and support because the service provider does not need to track the current status (connected or not) of the user. The user is charged the same amount if they use the system for 1 minute or the full time period, or in the case of monthly billing, whether or not they use the network at all. The only tracking required is the fact that this particular user has connected and when, so that subsequent connections can be allowed without further charge until the time period has expired. This can be done by tracking the MAC address of the user (or some other unique identifier) and the time they logged in.

8.1.2 Usage-Based Billing

Some examples of usage-based billing are:

- Pre-paid minutes. The user buys a “bank” of minutes which is reduced by each minute the service is used
- Per-minute charging, similar to cell-phone usage

- A charge for each login, with some number of minutes included in the initial charge, then a per-minute charge for each minute exceeding the initial block.

In usage-based models, the service provider must know whether the user is currently connected, and needs to determine the user has disconnected relatively quickly to avoid over-billing. If the user disconnects “gracefully” using a mechanism supplied by the service, this is straightforward. But, the user may disconnect unexpectedly for any number of reasons, including a system crash, shutting down the system without logging off, or simply leaving the location.

What may appear to be simple solutions to tracking user connectivity do not always work. For example, pinging the client machine at regular intervals. If the user launches a VPN session, the pings will fail, even though the user is still connected. Or, pinging the client can also fail if the user has implemented a personal firewall that blocks ICMP packets. Any mechanism that relies on Layer 3 network protocols can fail due to VPN or firewall issues. Another example would be using a JavaScript applet in the client’s browser that communicates back to a server on the service provider’s network. To avoid these problems, a solution must be implemented that uses Layer 2 protocols.

Commercial solutions are available that address this issue. For example, access/gateway controllers like the Nomadix* HotSpot Gateway, the Cisco* Broadband Service Manager and a host of others, have a built-in mechanism for tracking user connections that are not impacted by VPNs or firewalls.

Tidbit: When implementing a custom solution, insure the connection detection algorithm uses a layer 2 protocol, such as ARP, to avoid problems.

9. Common Infrastructure and Application Issues

This section highlights some of the typical issues that can cause problems at public HotSpots. In some cases, these issues can be addressed proactively by the service provider or mitigated with documentation. Others are caused by configuration issues on user’s machines. In these cases, there’s nothing the service provider can do but be aware of the issue and train their support staff to respond.

9.1 Lack of On-site Documentation and Assistance

The most obvious piece of on-site documentation, but one often missing, is an indication to the passerby that the HotSpot even exists. HotSpots need to be well marked and include

documentation that describes for the user where and how to get login credentials, the name of the service provider providing the service, what the SSID for the HotSpot is and how to get technical support if there is a problem.

Depending on your authentication model, the user may be required to obtain a scratch card at another location, or purchase time through means other than at the HotSpot or on the HotSpot network. It is frustrating for users to get their system set up to use the HotSpot, only to discover they must pack up and go somewhere else first. Understanding where and how to get login credentials is essential to a good customer experience. Knowing the service provider allows the user to determine if they have existing login credentials they can use. The SSID lets users easily determine which network to select if there are multiple SSIDs visible at the HotSpot (or none visible).

The on-site documentation should also clearly describe how to reach the login page, for example, launch the browser or network client, and describe potential problem areas such as those listed below.

Tidbit: At a minimum the on site staff should be aware that the HotSpot exists, know the basic coverage area, the SSID, and where to direct users who have connectivity problems.

9.2 Browser Issues

9.2.1 Proxy settings

One of the most common problems users will experience at public HotSpots is the inability to reach the service provider's login page because of incorrect proxy settings in the browser. A typical enterprise user's environment will include a proxy server. The browser will be configured to use this proxy to reach the Internet. At the HotSpot, the proxy will be unreachable and attempts to access the Service Provider's login page will fail. Users must be directed to modify their browser settings to turn off the proxy.

This problem is further complicated by the use of VPNs. The proxy must be turned off to reach the initial login page. Then it must be turned on after the VPN is launched to correctly navigate the user's enterprise environment. Then it must be turned off again after exiting the VPN to allow the user to continue to access the Internet or to use a web-based logoff mechanism.

Tidbit: Inform the user that they should make a note of their proxy settings prior to changing them so they can be restored correctly.

9.2.2 Corporate intranet pages

In some cases, when the user's home page is set to an intranet site (e.g. the company's home intranet page); the redirect to the service provider's login page fails because the network address of the intranet page isn't valid. Users must be directed to either change the home page, or enter a valid Internet page into the browser (e.g. www.intel.com).

9.2.3 Cached pages

When checking to see if the connection is established, if the user launches a web page that has been cached locally in the browser, the page will be presented correctly but the connection may not be established. The user will see what will appear to be intermittent connections, with cached pages showing up, while uncached locations give an error. This is a user education issue. For this type of checking, a news page (e.g. www.cnn.com) should be used, where the information changes rapidly allowing the user to easily see if the data is "stale".

9.3 Client Manager Applications

Client managers are applications that make it easier for the user to control the wireless (and wired in some cases) network device. Microsoft* provides a simple client manager with Windows* XP. NIC vendors often supply a client manager. Intel* PROSet* is an example of a client manager application. Additionally, some computer OEMs provide them as well as some wireless service providers. With this array of possible applications, it is easy for a user to inadvertently have multiple client managers installed and running on their system. These client managers can conflict with each other, causing problems for the user. There is nothing that the service provider can do to prevent this, but it is important for support staff to be aware of the issue.

Client managers each have their individual quirks that can cause problems for users as well. Again, there isn't anything specifically the service provider can do about this other than to be aware of them when helping users debug problems. Some common quirks include:

- The client manager chooses the access point generating the strongest radio signal, not the one with the SSID specified by the user as highest priority
- The SSID isn't displayed on a scan, even though the access point is available and broadcasting
- There is no mechanism to connect to an access point that is not broadcasting its SSID, even though the user knows the SSID

9.4 IP Addresses

9.4.1 Static IP addresses

If the user's system is configured with a static (pre-defined) IP address rather than set to obtain an IP address automatically from a DHCP server, the user will not be able to get access to the HotSpot network. To fix this, the user must modify the TCP/IP properties on the wireless network device by changing the setting to "obtain an IP address automatically" and "obtain DNS server address automatically". As with changing the proxy settings, the user should be reminded to save the existing settings, (IP address, DNS server addresses) so they can be reset afterwards.

9.4.2 NATs

While NATs can be a great solution for the public IP address space problem and various firewall problems, they can be detrimental in a network if the customer doesn't know they exist. For example, if a DSL line is used for service it will typically be deployed with a DSL modem/router. This router would be configured to provide a NAT environment. If the other end of the DSL network happens to be NATed as well, then you have a situation of a "Double NAT". The problematic areas of NATing (VPNs for example) won't only be of concern to the local router but will need to be addressed for the remote. This means a service provider must know the network thoroughly from the HotSpot connection through the entire network to the Internet, whether it's a localized or a centralized architecture environment.

9.4.3 Other IP address issues

As most HotSpots use private addressing it is important to note that, for an enterprise user, their VPN gateway may be on the same network, or subnet as the client. If this were to happen, no routing would occur in the client. Hence it is best to use as small as subnet as practical and then, use the space in the Class that makes the most sense. In other words, if all you need is a sub-C, then use a 192.168 subnet rather than a 10.0.0.0 (A) network. If multiple Class C subnets are required, then you will want to use the next larger network. This will reduce the possibilities of creating a problem.

Take, for an example, a VPN gateway with the address of 10.0.1.1 and a mask of 255.255.255.0. This is a Class A subnet address, but masked to a C. If a HotSpot were to issue an address of 10.0.2.x with a class A mask of 255.0.0.0, then both the HotSpot and the VPN gateway would have an overlap condition.

9.5 Ethernet Packet Problems

9.5.1 Preamble length

The preamble synchronizes the transmitting and receiving radios and allows them to derive common timing relationships. One of two formats can be used: long or short. Short format is more efficient, but is not required to be supported on all devices. The wireless Access Point at a HotSpot will be configured to either short or long preamble. For the client NIC and access point to communicate, the client NIC must be configured to match.

Most NIC cards can be set to detect the preamble length of the AP and automatically set the client appropriately, but some cannot. And not all cards with the “automatic” setting correctly set preamble. If the preamble lengths don’t match, the user will not be able to associate with the AP. Some network client managers provide a convenient way to set preamble, while others don’t. In some cases, it may require making modifications in the NIC driver configuration via the operating system interface. To reduce the potential for this problem, APs in public HotSpots should be configured for long preamble.

9.5.2 Packet fragmentation

Packet fragmentation occurs when the packet frame size is larger than a pre-determined level. When this occurs, the MAC controller will split the packet across frames. To maintain network efficiency, the frame size between two devices should be the same. Normally this is negotiated but it is possible to change this through a driver interface. Problems will occur when the frame size of the AP is dramatically different from that of the router. When configuring an AP for use in a HotSpot, the service provider should ensure the frame size of the AP matches that of the backhaul network.

9.6 Billing Issues

The mechanisms for logging in and out can be very confusing for the user. The login mechanism is usually easier to understand since typically the user is automatically directed to the login page, and can’t do anything else until login credentials are provided. Logging out is often more problematic. The process by which the user disconnects must be clearly described and easy to use, and something the user can remember easily after a period of time doing something else. Good documentation is necessary in addressing these issues.

The billing mechanism must also handle the case where the user does not follow normal logout procedures, but disconnects abruptly either because of a system failure or simply because they

shut down the machine or leave the location. If not, users may be over-billed (or feel they were over-billed), creating support problems.

One mechanism for handling network disconnection is to create a small web browser window with a “logout” button or link. This is a separate window from the primary browser window. While providing a clean logout mechanism, it also provides a place where the logout process can be explained.

There are some potential problems with this model. Some web sites and applications create their own separate browser windows. Sometimes these elements will detect that a window is already open and direct their content to that window. This can cause the logout window to be overwritten with new content, leaving the user with no obvious way back to the logout page. (A “Back” option is available via a right-mouse click on the web page, but not everyone is aware of this.)

Another problem is if the user accidentally closes the logout window. Since the window is automatically launched and typically does not include an address bar, the user has no way of knowing the URL to return to, leaving them with no way to generate the logout command.

VPNs can also cause problems because of the proxy issue described previously. If the user has enabled a proxy while using VPN and forgets to reset it after exiting, the links on the logout page may not work.

9.7 Geographic Issues

While the 802.11 standard is widely adopted and used worldwide, the channels available for use vary between geographical areas. In the United States, channels 1 through 11 are approved for usage. In Europe (except for France), channels 1 through 13 are allowed. France restricts usage to channels 10 through 13. Japan allows 1 through 14. Depending on the location of your HotSpot, these channel differences can have an impact on whether a user can see your access point. Client NICs designed for the US market may not be able to “see” an Access Point transmitting on channels 12 or 13. If the customer population at a given HotSpot is likely to include foreign visitors (e.g. airports and hotels), the AP should be set on channel 11 or below to insure that all users will be able to see it.

If it is likely that foreign travelers will visit a HotSpot, steps should be taken to inform the user of local laws and processes and to provide instructions in non-local languages. The HotSpot login page should be written in the predominant local language(s) and, at a minimum, an English version. In some locations, login credentials cannot be obtained via a credit card on the Internet.

In these cases, a scratch card must be obtained from a licensed vendor. This process is not typical in the US and one that a US traveler may not be familiar with.

Another geographically-based difference to consider is the use of encryption in Japan. Encryption (typically WEP today) is required to be implemented and supported in Japanese public HotSpots. This is usually not the case in other areas of the world and users may not be familiar with the process for using encryption to get associated with the AP and connected to the Internet.

Tidbit: It is important to look at the configurations and methodologies used when developing, deploying, and supporting a HotSpot through the eyes of someone unfamiliar with local customs and local languages.

10. HotSpot Blueprints

10.1 Introduction

In this section we present two HotSpot implementations: a small coffee shop and a very large convention center. Given the available types of hardware for HotSpots and the multitude of external factors that can affect its performance, there isn't one single design that will work for all HotSpots. The examples presented in this section are just two of many possible implementations that work within the constraints and requirements that we have defined. Use these examples to guide you when building your own HotSpot.

The two examples presented here are a small and very large HotSpot. There is no standard way to classify a HotSpot as a small or very large so these definitions are our own arbitrary definitions for purpose of illustration, see section 2.3 for more details on HotSpot size descriptions. The implementation locations were chosen for illustrative purposes as well. The small and very large examples were chosen because they each present unique challenges. Table 11-1 shows some of the characteristics of the HotSpots.

Feature	Coffee Shop	Convention Center
---------	-------------	-------------------

Feature	Coffee Shop	Convention Center
Number of Users	< =10	500 - 3000
User Density (Users/AP)	10 Max	25 Max
Horizontal Physical Coverage	< 1500 sq.ft.	200,000 sq.ft.
Vertical Physical Coverage	1 Floor - 6 feet (MS max elevation)	1 Floor x 20 ft. = 40 ft.
Indoors	Yes	Yes
Outdoors	Yes	No
Security	User Authentication, No Encryption	No user authentication No encryption
Billing	Credit Card, Subscription, One time card	Free

Feature	Coffee Shop	Convention Center
Special Considerations	<p>Neighbor businesses can also implement HotSpots which create RF interference.</p> <p>Use of microwave ovens creates RF interference.</p> <p>Mixture of power users and unsophisticated users</p>	<p>Usage bursts – from 10 to 500 users in 30 seconds or less.</p> <p>Sub-areas can change physical layout during conference. For example, conference rooms get expanded or compressed based on the popularity of a topic of presentation.</p> <p>Convention Center administration personnel should be on separate WLAN.</p> <p>Many users will use VPN connections to the same enterprise network.</p> <p>At trade shows, other WLANs might be implemented for purpose of demonstrations.</p> <p>Many power users.</p>

Table 10-1: HotSpot Characteristics

10.2 A Word about the Process

The process that we will follow for the purpose of getting our HotSpots deployed consists of the following phases:

- 1) Collect requirements³
 - User Requirements
 - Service Provider Requirements
 - Physical Environment Requirements

³ HotSpots operate in unlicensed frequencies, however, there may be other requirements such as business licenses and so on that we have chosen to omit as they are not relevant to the purpose of this discussion.

- Network Requirements
- Special Requirements
- 2) Perform the site survey
- 3) Develop the initial design
- 4) Deploy
 - Install hardware
 - Test the HotSpot (connectivity and performance)
- 5) Go online and turn it on!
- 6) Monitor performance and make corrections as appropriate

As with any other project, the first thing to do is understand what is needed to make the project a success. You do this by collecting requirements for the system. You'll gather requirements through interviews with stake holders and also performing a site survey. Next, you'll need to layout the initial HotSpot design on paper. After this step you should have an idea of the equipment, cabling and AP layout needed for your HotSpot implementation.

After you have installed the hardware, you should run another site survey to determine if you are getting the coverage you had planned on. You will also need to run tests to determine how easy it is to connect to your system, get to the enterprise network, and perform the expected user tasks (email, web surfing, etc.). As a last step, monitor your network usage to catch any unforeseen problems with your system (conflicts with external APs, RF interference from non-802.11 devices, etc.). Make corrections to your network configuration as necessary. Now you are ready for prime time!

10.3 Collecting Requirements

As mentioned earlier, you'll gather requirements and then perform a site survey to get an idea of the physical limitations and issues. For the purpose of this discussion, we have split the requirements into the following categories:

- User Requirements
 - Performance requirements
 - Maximum number of concurrent users in HotSpot
 - Maximum number of concurrent users per AP
 - Access to enterprise
 - Roaming/mobility requirements
 - Security requirements
 - Link level security
 - VPN requirements

- Location Owner/service provider requirements
 - Access control
 - Billing support
 - Maintenance requirements
 - Network performance monitoring
 - Automatic software upgrade capability
 - Remote management capabilities
 - Availability

- Physical environment requirements
 - Expected coverage area
 - Special antenna requirements
 - Special outdoor equipment

- Special requirements

- Network requirements
 - Provisioning
 - Provided by wireless gateway
 - Backhaul requirements (derive from collected requirements)
 - Backbone requirements (usually CAT 5 10/100 Ethernet, might consider 1Gb if lots of media streaming is expected)
 - AP Requirements
 - Power control
 - Antenna type
 - Maximum number of users supported
 - Maximum performance
 - RF requirements: 802.11 a, b, and/or g
 - Coverage requirements
 - IP address management
 - How many addresses are required
 - Who provides DHCP services
 - How long to lease addresses for
 - NAT requirements

User requirements

User requirements stem from the type of users you want to provide service to and their expectations of the service. This also includes requirements that are derived from the number and concentration of users: lots of users in a small area will require that your APs are able to handle a large number of users or a denser deployment of APs.

Location Owner/Service Provider Requirements

The HotSpot location owner and the service provider are usually not the same. However, they tend to have the same goal, to provide the best service for the value. For this reason we have grouped the location owner and the service provider requirements together.

Physical Environment Requirements

These requirements are used to understand the environmental factors for which you have no control: a location might contain a lot of RF reflective material for which you might have to adjust the type of antennas you use as well as the amount power needed.

Special Requirements

These are unusual requirements that don't show up in most HotSpot designs. For example, a University might have special requirements for how they track access to the wireless network by their student and faculty population.

Network Requirements

These requirements are essentially derived from the other requirements and include characteristics that you must have on your network.

10.4 Small HotSpot – the Coffee Shop

The coffee shop in this scenario resides in a shopping mall or strip mall. To make the scenario interesting, we assume a neighboring business also offers wireless access to the Internet. The two wireless offerings and locations are not owned by the same entity so they are assumed to rely on a different WISP and ISP. For a coffee shop with an area of approximately 1500 sq.ft. (30ftx50ft), ample coverage may be provided with just a single AP. A single AP in a HotSpot of this size will also send the RF signal into the street and neighboring businesses. This will cause interference problems with neighboring HotSpots if they transmit on the same channel. It behooves both HotSpot administrators to cooperate in their efforts by making sure that their APs don't interfere with each other. This problem can get more complicated when more of the surrounding businesses provide wireless Internet access. The general characteristics of this HotSpot are described in Table 11-1. Figure 11-1 depicts the layout for the coffee shop HotSpot.

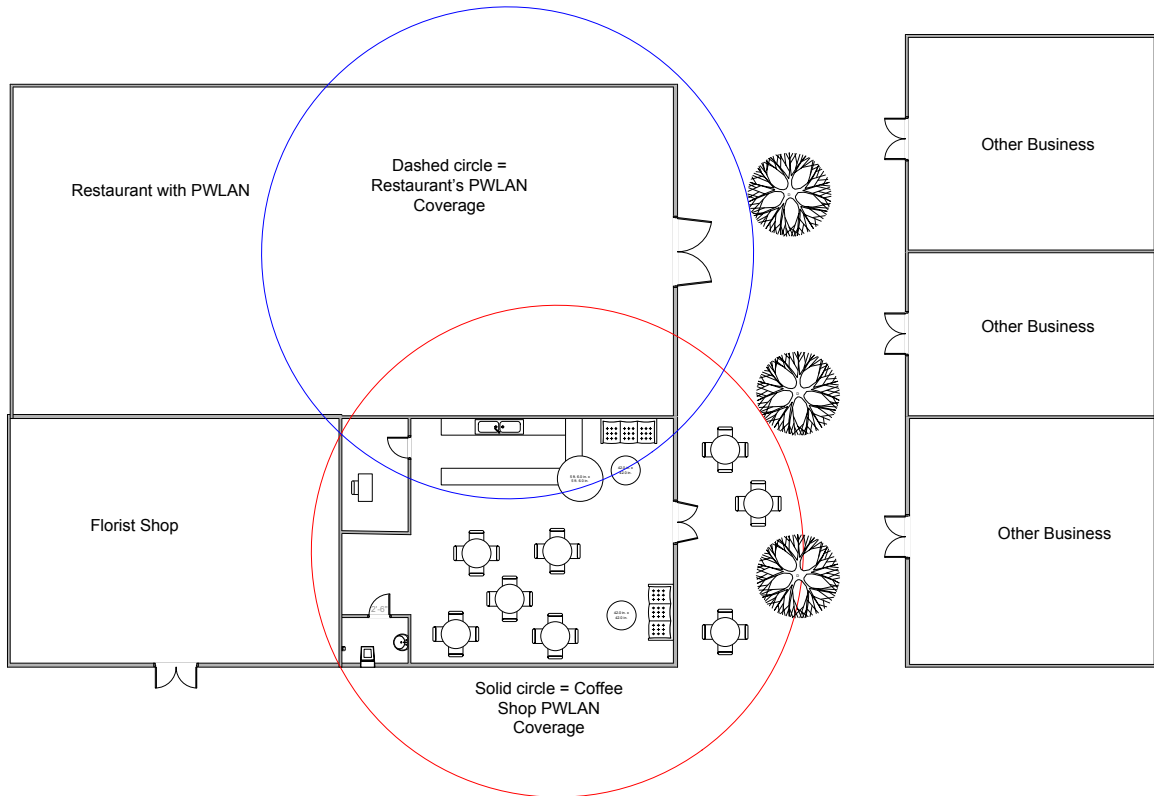


Table 10-2 Coffee Shop Layout

10.4.1 User Requirements

The table below shows the requirements for the user. These requirements can also be seen as requirements from the HotSpot owner in terms of services s/he wants to provide to his/her customers.

Requirement	Resolution
<u>Performance</u>	The network will provide a minimum of 100 Kbps
<u>Maximum number of concurrent users</u>	All network components including the AP shall support a minimum of 10 simultaneous users.
<u>Maximum number of concurrent users per AP</u>	The AP shall support a minimum of 10 simultaneous users.
<u>Access to Enterprise</u> The network must allow	Yes, the network will provide support for multiple concurrent VPN connections to the enterprise. All currently existing

enterprise user access to enterprise resource through use of VPN connection	VPN protocols shall be supported but only the following VPN products shall be tested: NetStructure*, Cisco*, CheckPoint* and Microsoft*.
<u>Roaming/Mobility</u> If more than one AP is used in the design, it shall be possible to roam between the APs.	The APs shall support roaming
<u>Security</u> Link level encryption of packets is not required. The user can use VPN for access to the enterprise and SSL for secure internet transactions in the Internet.	Link level encryption of packets is not supported. The user be able to use VPN for access to the enterprise and SSL for secure internet transactions in the Internet. Furthermore, the user will be encouraged to use a personal firewall to protect his or her system from intrusion.

Table 10-3: User Requirements for Coffee Shop HotSpot

10.4.2 Location Owner/Service Provider Requirements

The table below shows the requirements that the HotSpot owner must take into consideration in providing HotSpot services.

Requirement	Resolution
Access Control Only authorized users shall be allowed use of the HotSpot network. Upon connection for the first time, the user will be required to supply valid user credentials. It shall be possible to provide the credentials using an Internet browser.	Access control shall be the function of the wireless gateway. The wireless gateway shall support the Universal Access Method (UAM) whereby the user can gain access to the authentication process through a standard browser. The wireless gateway shall block access to all other resources until the user has successfully logged in or has purchase access time.
Billing Support The network shall keep track of per user usage time. The network shall support the use of credit card to purchase access	Billing functions shall be supported by the wireless gateway. The wireless gateway must support the billing model stipulated in the requirement. Furthermore, the wireless gateway must provide an interface to automatically request and get authorization for charges to a user's credit card. The

<p>to the HotSpot. The billing model is as follows. There are two types of users: 1) Regular users – These users have an account with your company and get charged a fixed amount of \$20.00 for unrestricted use on a monthly basis. 2) Transient users – These users are allowed to use their credit card to purchase time in one hour increments. The first five hours are billed at \$5.00 per hour. After the sixth hour, the user will pay for a full day at a rate of \$30.00 per day. In a per-hour billing model, all the hours must be used within a 24 hour period. All the hours will be purchased in a single transaction, i.e. the user can't add hours to a previous purchase and you cannot apply additional hours to a previous transaction.</p>	<p>wireless gateway must also keep track of the user's network usage.</p>
<p><u>Maintenance Requirements:</u> Provide performance monitoring Support software upgrades</p>	<p><u>Network Monitoring:</u> Network monitoring will be provided by ensuring that the APs and wireless gateway support SNMP and provide the capability to return statistical data gathered during network usage. <u>Automatic Software Upgrades:</u> The APs and wireless gateway shall have the ability to have software and firmware upgraded over the wire.</p>
<p><u>Remote Management Capabilities</u> It shall be possible to perform basic management functions on the HotSpot network components from a remote location (e.g., the</p>	<p>It shall be possible to access the AP and the wireless gateway to perform functions such as retrieve statistics or messages transmitted and received, error counters, and upgrades to firmware and software.</p>

WISP)	
<p>Availability</p> <p>Failover is not a requirement. However, there should be a mechanism that alerts administrators that the HotSpot has gone down.</p>	<p>The network components will exist in a single instance with no failover capability. That is, there will be no on-line backup of the network components. The software shall support a hart beat or a polling function that will allow a central control unit to determine if the HotSpot is on-line or down.</p>

Table 10-4: Location Owner/Service Provider Requirements

10.4.3 Physical Environment Requirements

Requirement	Resolution
<p>Coverage Area</p> <p>The Coffee Shop area is 30 ft wide by 50 feet long. There shall be access to the wireless network from any area in the Coffee Shop. Furthermore, the wireless signal shall reach up to 15 ft in front and side (side facing the street) of the Coffee Shop to service customers that sit on the outside tables. Tolerance for performance is 1Mbps at the furthest table outside.</p>	<p>A single AP shall be sufficient to cover the required area.</p>
<p>Outdoor Requirements</p> <p>The wireless signal shall reach up to 15 ft. in front and side (side facing the street) of the Coffee Shop to service customers that sit at the outside tables. Tolerance for performance is 1Mbps at the furthest table outside. There shall be no outdoor wireless equipment installed in</p>	<p>Clients that sit at the outside tables will be serviced by the single AP residing inside. It is estimated that an AP with a transmission diameter of 150 ft. and transmit through one outside wall will satisfy this requirement.</p>

<p>the Coffee Shop. All outdoor patrons shall be serviced with the APs located inside the location.</p>	
---	--

Table 11-4: Physical Environment Requirements

10.4.4 Special Requirements

Requirement	Resolution
<p><u>Coexistence with administration network for the Coffee Shop.</u> The Coffee Shop uses a PC and printer for shop administration purposes. The PC is used to upload sales information to the headquarter’s database. There is a local printer that is occasionally used to print business related communications. It is critical that both networks; the local administration network and the public wireless access are maintained separately.</p>	<p>Both, the public and the administration networks, shall be run over the same backbone. The networks will be kept separate through the use of a VLAN supporting switch.</p>

Table 11-5: Special Requirements

10.4.5 Network Requirements

Requirement	Resolution
<p><u>Provisioning</u> The user shall be able to provide credentials for the purpose of login into the system by using the Internet browser in the user’s mobile system. Alternatively,</p>	<p>The provisioning of the system shall be implemented within the wireless gateway. Upon detection of a new mobile station attempting to access the Internet through the local wireless network, the wireless gateway shall redirect the user’s browser to a local page, or a page at the service provider’s network which will allow the user to either login or</p>

Requirement	Resolution
<p>should the user not have a pre-existing account with the provider, it shall be possible for the user to purchase access time from the provider using the same Internet browser means. The network must provide a time out mechanism such that the user does not have to re-login if the</p>	<p>purchase access time using a credit card. The user credentials will be checked by an AAA server that resides on the WISP network.</p>
<p><u>Backhaul Requirements</u> The requirement to support 10 users with a sustained transfer rate of 100Kbps requires that the backhaul connections to the Internet bet at least 1Mps.</p>	<p>The backhaul shall be a 1Mbps DSL line, at a minimum. This will allow for 100Kpbs/user at max utilization, with increased performance with a lower number of users.</p>
<p><u>Backbone Requirements</u> 100Mbps</p>	<p>The backbone for the Coffee Shop HotSpot shall be a 100Mbps Ethernet. All equipment attached to this network must support this transfer rate.</p>
<p><u>AP Requirements</u> AP must have a range of 150 ft going through a single 6" wall. It must be software and firmware upgradeable over the wired network connection. It must be Wi-Fi certified.</p>	<p>The AP shall meet the stipulated requirements</p>
<p><u>IP Address Management</u> Requirements – The HotSpot shall use one public IP address and be able to allocate a minimum of 15 IP private addresses from a local pool of addresses.</p>	<p>The network shall include a DHCP server that allocates addresses from the following pool: Start Address: 192.168.1.100 End Address: 192.169.1.115 The wireless gateway shall implement the DHCP server. The address lease time shall be 24 hours The wireless gateway shall use two public IP addresses to communicate with the WAN. One address will be used for translation of private IP addresses and the other is used for maintenance/management of the wireless gateway.</p>

Requirement	Resolution
	The wireless gateway shall implement the NATP protocol. Private addresses shall be translated to one of the public IP address used by the wireless gateway.
Special Antenna Requirements	No special antennas are required

Table 11-6: Network Requirements

10.4.6 Network Design

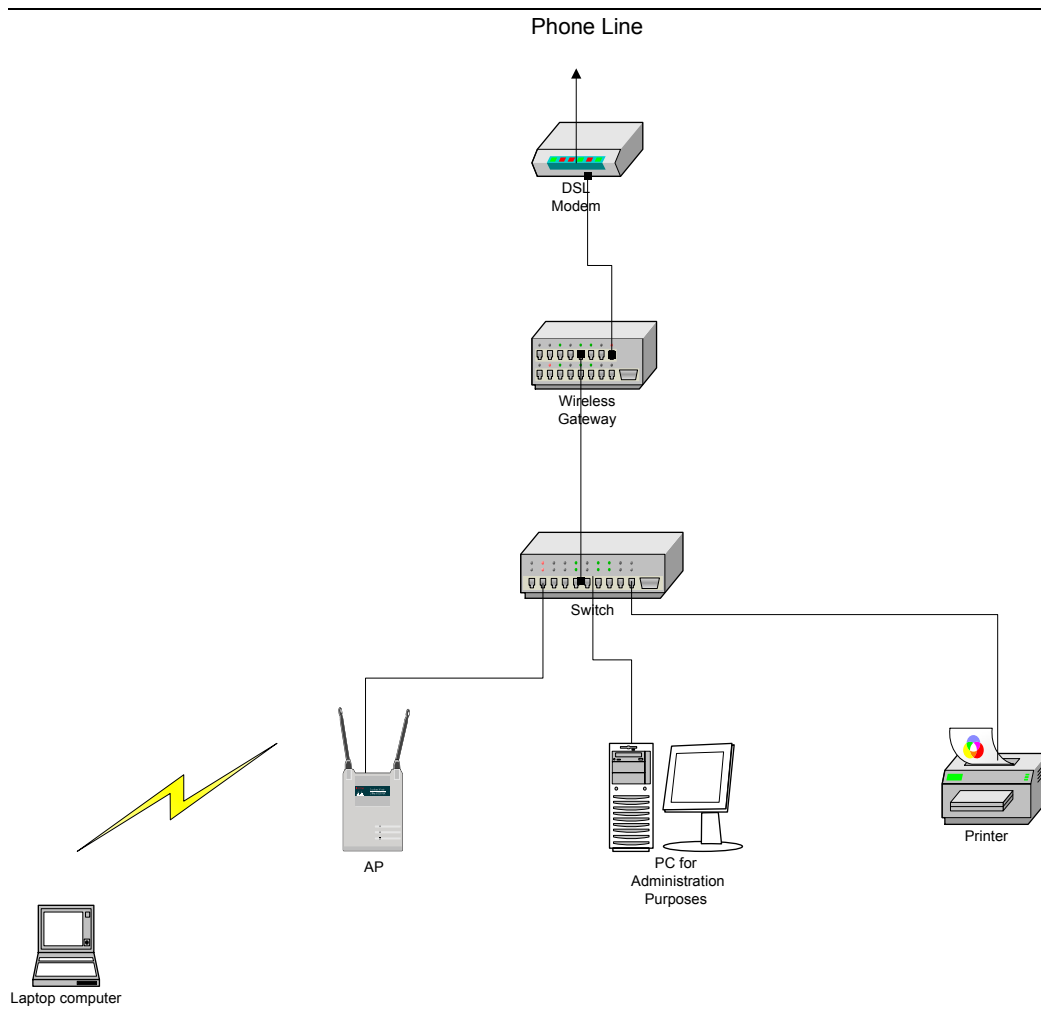


Figure 10-1: Network Diagram for the Coffee Shop HotSpot

10.4.7 Equipment Selection

There are only four major hardware components in the coffee shop HotSpot:

1. AP
2. Switch
3. Wireless Gateway
4. DSL Router

The model of the DSL Router is normally determined by the service provider so you only have to research and buy three of the four hardware components. The table below shows some choices. These choices are not an endorsement on these products only presented as examples. Many more exist that meet our requirements.

Network Components	Choices
Access Point	Cisco* 1200 Nomadix* AG-2000w (HotSpot in a box) D-Link* AirPlus Xtreme G™ HP* ProCurve 420 802.11g AP LinkSys* WRT55AG
Switch	Cisco* Catalyst 3100 HP* ProCurve Switch 2626
Wireless Gateway	BlueSocket* WG-1100 Nomadix* AG-2000w (HotSpot in a box) Nomadix* HSG

Table 11-7: Network Components

10.4.8 Summary

The small coffee shop HotSpot provides a simple and straightforward example of how to implement a HotSpot. It also highlights the fact that the industry is moving towards total hardware integration. For example, the Nomadix* AG-2000w is a network component that provides most of the functions required in a HotSpot. The next example we show is for a more complex HotSpot, a convention center.

10.5 Convention Center HotSpot

The convention center HotSpot is a lot more complex than the small coffee shop HotSpot previously presented. Rather than attempt to completely describe the deployment as we did above, we'll instead provide an overview of the steps required and the design decisions that will need to be made..

10.5.1 Site Goals and User Model

In this scenario, we are setting up a wireless network for the attendees at a conference/tradeshaw. The conference organizers would like attendees to be able to get wireless network service in all session rooms, in the keynote hall, and in the front entryway where tables and seating have been set up, but not in the exhibition hall areas, to avoid conflicting with wireless demos being shown. The expected number of attendees is around 3000. Each individual conference session may hold upwards of 100 people. Users should be able to move between session rooms without losing their wireless network connection.

In this scenario, we are making the assumption that 65% of the attendees have a wireless device with them, and at any given time, 40% of them will be using the network: 26% of the total attendees. Overall just under 800 people active at one time, with about 25 people active in any individual conference session.

$3,000 \text{ total attendees} \times 0.65 = 1,950 \text{ attendees with wireless access}$

$1,950 \text{ attendees with wireless access} \times 0.40 = 780 \text{ attendees with access on the network}$

$780 \text{ attendees with access on the network} / 3,000 \text{ total attendees} = 0.26 \rightarrow 26\%$

The expected network usage is web browsing to the convention's information site, general web surfing, and accessing corporate e-mail (requiring VPN to connect to the corporate intranet).

10.5.2 Site Survey

Step one is to do a site survey of the location. Here we want to determine whether there are any existing wireless networks, or wireless networks from neighboring sites that might overlap, or any devices, like microwave ovens or portable phones that may cause signal conflicts. We need to look for barriers, such as walls or other obstacles that might impact signals, and for areas that might be difficult to cover with the circular coverage area of a typical AP antenna, such as long, narrow hallways.

This will help us determine where the APs can be located. With the APs we also need to consider placing them where they are not easily accessible, to avoid tampering or theft and we need to consider accessibility of power and network connectivity.

In this example, the convention center has no existing wireless network. The food service area is well away from the hot spot, so there are no issues with microwaves. The building is far enough away from other buildings that no external wireless networks present a conflict. This means that all 3 802.11b channels will be available for us to use. This will be critical to provide the AP density we need.

There are pillars in the main hallways where the APs can be mounted. In the session rooms, they will be hung from the ceiling. The venue provides an Ethernet drop in each of the session rooms but we'll have to string our own Ethernet cable to the APs in the main hallway. This can be a "quick and dirty" cable run since it will be temporary

10.5.3 AP Layout

You can see the convention center layout in figure 11-5. There is a long narrow front entryway, with session rooms on either side of large exhibit halls. The left-most exhibit hall will hold the keynote sessions. The exhibit halls on the right (2) are for exhibitors and demos.

There will be large numbers of users concentrated in small areas (e.g. session rooms or the front entryway). While a small number of APs might cover the physical area of the HotSpot, they would not provide the capacity needed for the expected number of users. For this reason, more APs will be used with their signal strength reduced, to allow a higher density of APs in one area. Multiple channels (1, 6, and 11) are used to avoid conflicts with overlapping AP zones. The keynote area is not fully covered because of the location of the presenter's stage. We will only need to cover the seating area. But even with 6 APs, if most of the attendees come to the keynote, and our usage percentages are accurate, we may not have the capacity necessary to service all the users. However, we are constrained by the number of available channels and how much we can reduce the power of the APs.

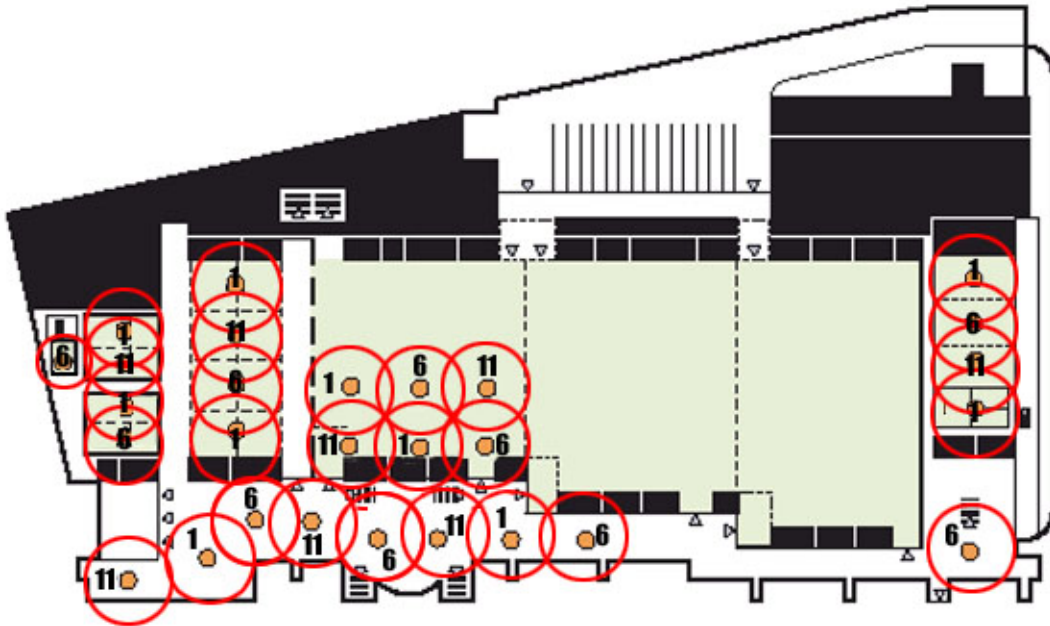


Figure 11-3: Convention Center Wireless Coverage

10.5.4 Security/Authorization

Wireless network access will be free to attendees. There will be no login/authorization required since badges are required to enter the building, so only registered attendees will have physical access to the HotSpot (except for maybe the sidewalks in front of the building). There will be no WEP or other security required.

10.5.5 Site Management

We want to be able to monitor the health of the network, bandwidth usage, watch for introduction of viruses and malicious users. We will want to choose APs, network gateways, and other network components that include an SNMP capability to facilitate this. Then use a network manager, such as HP OpenView*, to provide a centralized management console. It would also be a good idea during the course of the event to do regular RF audits using tools like AirMagnet Wireless LAN Analyzer or WildPackets Airopeek.

10.5.6 Billing

Wireless service will be provided to the conference attendees for free.

10.5.7 Design Issues

Network Topology

The user base for this HotSpot will be highly mobile. Attendees will go from room to room as they attend sessions. To allow roaming (moving from AP to AP) to work, a “flat” network is required. This will require the use of VLANs to allow enough network capacity. We will also need to use a NAT device since the number of users is much too large to assign public IP addresses to each.

Power

This network will only exist for a short time, during the duration of the event. It would not be cost-effective to run power to new locations where we want to install the APs. But we also don't want to be limited by the location of existing power. So we'll select an AP model that gets power over the network (PoE) to overcome any power access and distribution issues. We will still need to run Ethernet cables to the AP locations to provide access to the backhaul network.

Performance

To give the users a “broadband” experience doing the types of applications we expect, roughly 100Kbps of bandwidth is desired. An AP's maximum bandwidth is roughly 5Mbps of real throughput, which does not include TCP/IP overhead. This means about 50 users per AP. There are 28 APs in the convention center design in figure 11-5. If there is a perfect distribution of users and APs (which there won't be), this means 1,400 simultaneous users at 100Kbps. The target is 780 users (26% of 3,000). Depending on how accurate the numbers are, we are currently providing nearly double the capacity we think we'll need. This gives us plenty of breathing room if our assumptions turn out to be incorrect.

If all 28 APs are operating at 5Mbps, then an OC-3 (155Mbps) backhaul will be required. This assumes that all 50 users on the AP are simultaneously downloading at all times. If we assume half are actively downloading (vs. just reading content), then we'll need about 70Mbps which can be achieved (plus extra) with two T3 lines. Using two T3s (or equivalent) also would provide redundancy. Ideally, each T3 would come from a different service provider, in order to avoid possible outages due to service provider downtime.

10.6 Conclusions

HotSpots came in many sizes and shapes and usually with their own set of challenges. Gathering requirements, doing a site survey and choosing the right equipment are the three most important factors for success. As in any other worthwhile project, make sure you spend enough time getting an understanding of what you need to deliver. As wireless HotSpots become more popular, the number of users at your HotSpot is likely to increase. Make sure you plan for the next revolution

in communications.

11. Appendix A: Commonly Used Terminology

11.1 General Terminology

This section lists some of the general term used in the 802.11 specification.

- 802.11 – IEEE specification for wireless communication in the unregulated radio spectrum
- Antenna diversity – A method of minimizing multipath fading by using multiple antennas. The radio system chooses the signal from the antenna with the best reception. Especially useful in areas of high interference.
- Channels – frequencies within the unregulated radio spectrum that are available for use by wireless devices. Channel usage for wireless devices is regulated by each individual country and varies worldwide.
- Cell size – the amount of area that can be affectively covered by an Access Point
- Coverage – the amount of area in which the wireless network is available
- Line of Sight – the ability to see one network component from another with not obstacles in between.
- RF Interference – noise within the radio band that causes communication and connectivity issues between components on the network
- Roaming – the ability of a mobile station to seamlessly switch between Access Points on a network and maintain connectivity

11.2 HotSpot Components

While wireless networks and HotSpots share some of the same components and terminology as a wired network, there are some hardware and software differences between the two paradigms. The following list describes terminology commonly used when discussing wireless HotSpot components.

- Access Point(s) – provide wireless access to the HotSpot network.

- Authentication Authorization and Accounting (AAA) Server – network component that provides the services, as implied by its name, of authentication, authorization and accounting. Basically controls user and device access to the HotSpot.
- Authenticator – device that allows mobile stations to gain access to the wireless network.
- Internet Service Provider (ISP) – entity that provides the connection to the Internet.
- IP Address Manager – controls and allocates IP addresses within the HotSpot.
- Mobile station – any 802.11 wireless client device located within the HotSpot.
- Network Access Controller – the gatekeeper to the network; determines what traffic to let through to the protected network by implementing smart filters and policies.
- Network Address/Port Translator – provides mapping from public to private IP addresses to allow a HotSpot to use a single public IP address for its Internet connection.
- Router, Switch, or Hub – provide multiple ports for connectivity from APs and other network components to the HotSpot's backhaul and the interface to the Internet.
- Supplicant – mobile station trying to gain access to the wireless network.
- WAN Backhaul – high speed, high bandwidth (typically) connection to the Internet. Connects the HotSpot to the Internet.
- Web Server – network component that provides access to the HotSpot's login page(s).
- Wireless ISP – ISP with wireless service support such as HotSpot design and network monitoring.

11.3 Security Terminology

Following are many of the acronyms used when talking about 802.11 security. The acronyms are listed and briefly described here, with more in-depth discussion of security in Chapter 5.

- 802.1X – describes an architectural framework for an authentication and authorization mechanism that is based on port access control.
- 802.11i – IEEE task force designated to address security issues with 802.11 technology. This is also the name given to the resulting security specification produced by this task force.
- AES – Advanced Encryption Standard, encryption standard used by the 802.11i specification.

- **DKE** – Dynamic Key Exchange, automatic key management feature for WEP.
- **EAP** – Extensible Authentication Protocol, a generic authentication framework that, as its name implies, supports a wide variety of authentication protocols
- **EAP-MD5** – EAP using MD5: a one-way authentication method of supplicant (Mobile Station) to network (AP) that uses a hash of a password and challenge string to provide proof of identity.
- **EAP-TLS** – EAP using TLS: an IETF standardized authentication method that uses X.509 certificates to provide mutual authentication.
- **EAP-TTLS** – EAP using TTLS: an IETF standard, is one of two authentication methods (the other being PEAP) developed to overcome TLS's demanding requirement for client certificates.
- **LEAP** – EAP authentication method developed by Cisco* that supports mutual authentication.
- **PEAP** – an IETF standard, is one of two authentication methods (the other one being TTLS) developed to overcome TLS' demanding requirement for client certificates. In PEAP, as in TTLS, the mobile station identifies itself with username/password while the AP continues to use certificates.
- **RSN** – Robust Security Network, developed by 802.11 Task Force "i" (typically called 802.11i), based on the Advanced Encryption Standard (AES) for encryption of wireless frames and 802.1X for authentication, authorization, and key management.
- **TKIP** – Temporal Key Integrity Protocol, protocol developed using RC4 algorithm with new per-packet key mixing function, new message integrity check (MIC) named Michael, longer initialization vector (from 24 bits in WEP to 48 bits in TKIP), and new re-keying mechanism (session key renewed on a regular basis).
- **WEP** – Wired Equivalent Privacy, security of the radio link layer protecting data as it traverses the wireless portion of the network.
- **WPA/WPA2** – Wi-Fi Protected Access, a subset of the 802.11i standard leaving out only the specifications for Independent Basic Service Set, pre-authentication, and the use of AES. For encryption, WPA supports WEP and TKIP, both of which can be implemented in software and/or firmware. WPA2 adds support for AES and roaming and uses CCM for header and data integrity.

12. Appendix B: Table of Acronyms and Abbreviations

Acronym	Description
AAA	Authentication, Authorization and Accounting
ADSL	Asynchronous DSL
AES	Advanced Encryption Standard
AIM	AoL Instant Messenger
AP	Access Point
CAT5	Category 5
CIR	Committed Information Rate
CCM	Counter Mode with CBC-MAC
CRC	Cyclic Redundancy Check
DCC	Direct Client Communication
DHCP	Dynamic Host Configuration Protocol
DES	Data Encryption Standard
DKE	Dynamic Key Exchange
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
GRE	Generic Routing Encapsulation
GHz	GigaHertz
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
IANA	Internet Assigned Numbers Authority
IAPP	Inter Access Point Protocol
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers

Acronym	Description
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security
IRC	Internet Relay Chat
ISP	Internet Service Provider
IV	Initialization Vector
Kbps	Kilobits per second
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
LEAP	Lightweight EAP
LoS	Line of Sight
MAC	Media Access Controller
Mbps	Megabits per second
MD5	Message Digest 5
MIC	Message Integrity Check
MS	Mobile Station
NAC	Network Access Controller
NAT	Network Address Translator
NAPT	Network Address Port Translator
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NNTP	Network News Transfer Protocol
OEM	Original Equipment Manufacturer
PAE	Port Access Entity
PDA	Personal Digital Assistant
PDU	Protocol Data Units
PEAP	Protected EAP
PKI	Public Key Infrastructure
PoE	Power over Ethernet
POP3	Post Office Protocol 3
PPTP	Point-to-Point Tunneling Protocol

Acronym	Description
PSK	Pre-Shared Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RDP	Remote Desktop ?
RF	Radio Frequency
RSN	Robust Security Network
RTP	Real-Time Protocol
SIP	Session Initiation Protocol
SMT	Station Management
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOHO	Small Office Home Office
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSH2	Secure Socket Shell version 2
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled TLS
UDP	User Datagram Protocol
VoIP	Voice over IP
VLAN	Virtual LAN
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WISP	Wireless ISP
WLAN	Wireless LAN
WM	Windows Messenger
WPA	Wi-Fi Protected Access
XOR	Exclusive OR

Acronym	Description
YM	Yahoo Messenger