Wireless Hotspot Deployment Guide

Application Note

September 2005

Authors:

John Hammond
H. Dean Lee
Christopher Anderson
Prakash Kripalani
Greg Meyer
Chad Skinner
Juan Rivero
Bart Kessler
Tim Sweeney

Revision: 003
September 2005

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, critical control or safety systems, or in nuclear facility applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

Intel Corporation may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter. The furnishing of documents and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights.

Designers must not rely on the absence or characteristics of any features or instructions marked “reserved” or “undefined.” Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See http://www.intel.com/products/processor_number for details.

The Wireless Hotspot Deployment Guide may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

This Application Note as well as the software described in it is furnished under license and may only be used or copied in accordance with the terms of the license. The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document.

Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature may be obtained by calling 1-800-548-4725 or by visiting Intel's website at http://www.intel.com.

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

Copyright © 2005, Intel Corporation. All Rights Reserved.

Contents

Figures

Tables

Revision History

Date	Revision	Description
December 2003	001	Initial release.
September 2004	002	Added 802.11 Standards Basics section Expanded Managing a Hotspot section
September 2005	003	Added Broadband Backhaul section Updated Wireless Security section Added Emerging Wireless Technologies section Added IEEE 802.11 Wireless Standards appendix Added Details of Wireless Security appendix

1.0 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/development areas and activities involved in building and deploying a public wireless hotspot.

The guide is divided into the following sections:

- Section 1.0, “Purpose and Organization of this Guide” on page 12 provides an introduction and overview of this guide.
- Section 2.0, “Hotspot Overview” on page 14 takes a look at user expectations and environmental requirements.
- Section 3.0, “Hotspot Functionality and Network Components” on page 18 introduces the functionality of a hotspot and a high level overview of the components required to implement said functions.
- Section 4.0, “Broadband Backhaul” on page 27 provides information about how to connect hotspots to the Internet using various common backhaul services.
- Section 5.0, “802.11 Standards Basics” on page 37 provides an overview of the fundamental features specified by the 802.11 standards that are likely to influence hotspot implementation.
- Section 6.0, “Understanding Wireless Environments” on page 52 covers the requirements of the wireless connection and radio frequency (RF) related issues, such as multi-path interference, that can arise in hotspot implementations.
- Section 7.0, “Wireless Security” on page 62 addresses securing the wireless portion of hotspot networks and discusses security options: Wireless Equivalence Protocol (WEP), Wi-Fi Protected Access (WPA), WPA2 and 802.11i.
- Section 8.0, “Managing a Hotspot” on page 75 presents ideas for effectively managing hotspots
- Section 9.0, “Enterprise Applications” on page 82 reviews applications commonly used by enterprise users while in public hotspots.
- Section 10.0, “Billing” on page 86 describes various hotspot billing models, and the requirements for implementation and support.
- Section 11.0, “Common Infrastructure and Applications Issues” on page 88 presents some of the more common and recurring issues that the authors have encountered in numerous public hotspots.

- Section 12.0, “Hotspot Blueprints” on page 94, presents two examples of hotspot implementations. These hotspot types were selected to outline some of the issues you might encounter when implementing hotspots.
- Section 13.0, “Emerging Wireless Technologies” on page 108 provides an overview of emerging wireless technologies.
- Appendix A, “IEEE 802.11 Wireless Standards” briefly describes the appendices of the 802.11 standard.
- Appendix B, “Commonly Used Terms” provides definitions for commonly used terms.
- Appendix C, “Acronyms and Abbreviations” defines all the acronyms and abbreviations used in this guide.
- Appendix D, “Details of Wireless Security” provides technical details of WEP and 802.11i.

2.0 Hotspot Overview

Public hotspots provide an easy method for customers to connect to the Internet. With the increasing number of people emailing, chatting, shopping, uploading and downloading files, surfing the web, and playing games across the Internet, wireless network access is an attractive draw for customers and could potentially lead them to choose one place of business over another. Business travelers can work from their hotel rooms, and 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, 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
- Authorization, Authentication and Accounting (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 Section 12.0, “Hotspot Blueprints” on page 94 for more specific information.

2.2 Understanding User 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 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 Section 10.0, “Billing” on page 86) 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 of 200 Kbps transfer rate from the hotspot to the ISP and Internet. 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 500 Kbps DSL line may be fine for a coffee shop expecting 2 or 3 active users at any given time, but it would likely 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. Also, consider that the bandwidth requirement is not as simple as the maximum number of users multiplied by 200 Kbps. This would only be required if all users are simultaneously downloading large files. Of course, it's always better to err on the side of more bandwidth, but you may find that 500 Kbps provides each user with more than 200 Kbps for up to four users. Again, the venue and clientele will play important parts in determining your bandwidth requirement.

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 it 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. 802.11i provides the best means for a service provider to secure the wireless link. Wi-Fi Protected Access (WPA) provides a good migration path to 80211i. 802.11i, WPA and security in general are discussed in greater detail in Section 7.0, “Wireless Security” on page 62 of this guide.

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. Unexpected hardware resets can occur as a result of power glitches or as a response to software exceptions. When reset this way, some hardware revert to a default configuration that is not appropriate for the network setup. New network loads such as new APs or new virtual networks can also cause problems that were not seen when the hotspot was initially deployed. New network loads can come about as a result of a site

becoming popular with more users. The new users can also have different web surfing habits such as viewing videos, playing music or online games. 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 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 Section 8.0, “Managing a Hotspot” on page 75.

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. The following three key factors that determine what type of hotspot environment to create

- physical size of the location
- number of simultaneous users
- 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 Section 3.0, “Hotspot Functionality and Network Components” on page 18 and Section 6.0, “Understanding Wireless Environments” on page 52.

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 200Kbps 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 1 Mbps 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 (e.g. 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 1 Mbps 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.

3.0 Hotspot Functionality and Network Components

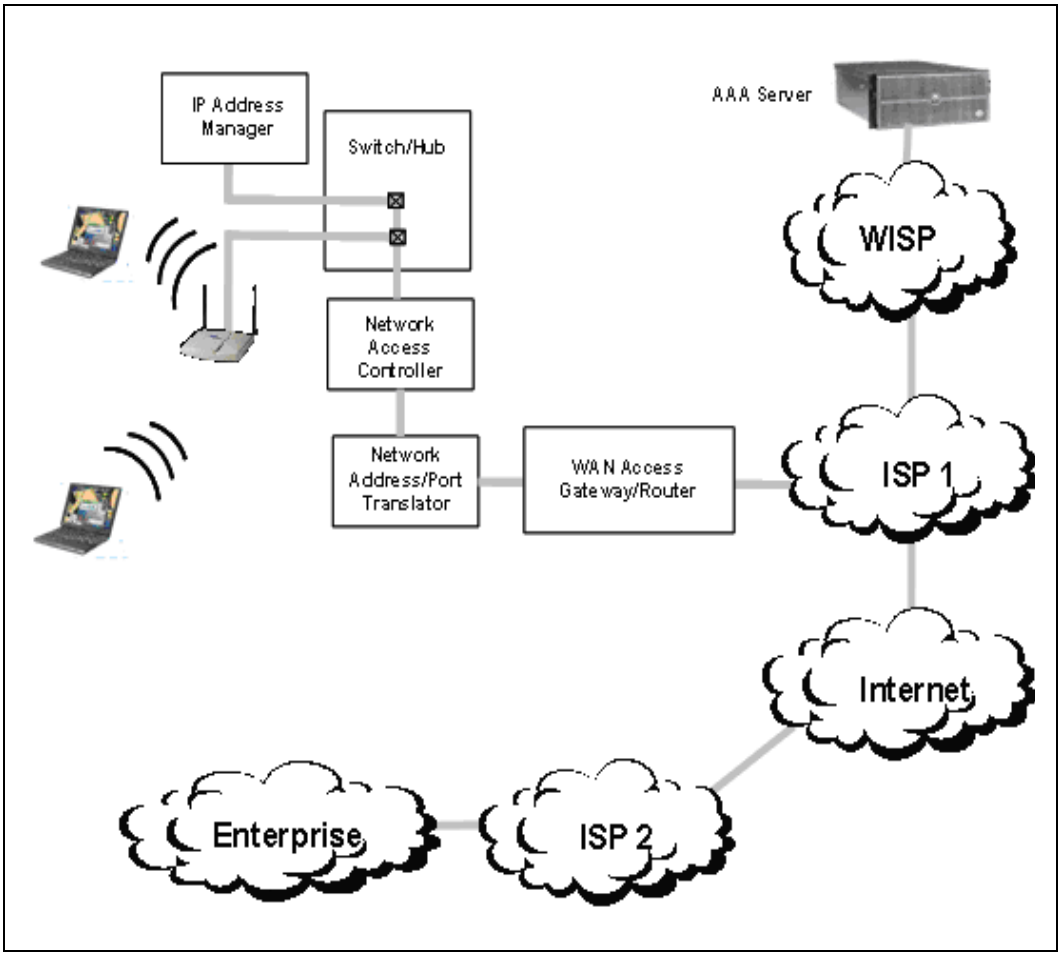
We can summarize hotspot user expectations as being able to access the Internet and everything that comes with it. Customers may also want the added benefits of a wireless connection and a secure network environment. In this section we take a look at the technical aspects of the hotspot environment and 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.

Some important features and functionality that a hotspot needs to provide are listed below:

- Enabling access to the wireless link
  - — Providing the mobile station with information about the wireless network
  - — Creating an association with the mobile station
  - — Providing access to the local network
  - — Providing data packet transfer services
  - — Disassociation from the mobile station
- Provisioning the hotspot
  - — Page redirection function
  - — Mobile station authentication
  - — User authorization
- Layer 3 (IP) Address Management
  - — Providing an IP address for the mobile device
  - — Private to public address translation if necessary
  - — Providing Domain Name Services (DNS)
  - — 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 1. Please keep in mind that this is one of many possible hotspot configurations.

Figure 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 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 Broadcasting Wireless Network Information

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. If the SSID is not broadcast, the WLAN may not appear in the user's list of available networks.

Note: Whether or not a wireless network (SSID) 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 SSID of a public hotspot to make it easier for 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 pro-actively 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 was 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 (TGi) developed a more secure encryption mechanism for wireless networks. The result is 802.11i. While 802.11i addresses all of WEP's vulnerabilities, the ratification of the standard would take many months and the industry felt it needed an immediate solution to resolve 802.11 security problems. So the Wi-Fi Alliance developed an interim solution by using finished portions of the then un-ratified 802.11i specification. This solution, called Wi-Fi Protected Access (WPA) includes key management and better encryption. These authentication standards will slowly become more prevalent as hardware for client NICs and APs become available. The specifications for WPA, WPA2 and 802.11i are addressed in more detail in Section 7.0, "Wireless Security" on page 62.

Note: 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, most hotspots used no encryption for securing the wireless link after the authentication process (user log-in).

3.1.1.4 Device and User Authentication

802.11 uses WEP in two ways; one is to securely authenticate the device and the other is to provide confidentiality by encrypting the data packets. It is important to understand the distinction between these 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 data packet encryption. The converse is not true. You can use WEP for encryption and not use for it 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 WPA2 do include user authentication mechanisms as part of their infrastructure (802.1X and EAP). Further discussion of 802.1X, EAP, WPA and WPA2 can be found in Section 7.0, “Wireless Security” on page 62.

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, the authorization is the job of the AP. As was mentioned earlier, many hotspots do not use WEP and only use Open Authentication. Using Open Authentication means the mobile station (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 WPA2, 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 two Access Points from different manufacturers may not work together. Wi-Fi 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 6.5, “Choosing your Access Point (AP)” on page 57 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 addresses 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 1 lists these addresses:

Table 1. IANA Address Allocation for Private Networks

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 256 contiguous class C network numbers

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 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 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.

Note: 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.

Note: 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 and Chapter 4.0, “Broadband Backhaul” describes them in more detail. The most common WAN connection is xDSL (see Section 4.1.2, “Digital Subscriber Line (DSL)” on page 28). These types of connections are relatively inexpensive 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 because the committed information rate (CIR) from the DSLAM to the Internet on a per-channel basis can be as low as 10 Kbps!

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 200 Kbps per user is considered the minimum. Depending on the size of the hotspot, the number of simultaneous users using 200 Kbps 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 200 Kbps 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 network 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 these services.

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. Please see Section 7.3.2, “WPA Authentication” on page 65 for more information about secure authentication methods.

Authorization is the enabling 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. The AAA server can reside 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 standard 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

The technology and business models to support public hotspots 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 guide 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.

4.0 Broadband Backhaul

To a large extent, the hotspot's backhaul to the Internet has a significant impact to the users' experience at the wireless hotspot. Users have come to expect broadband connections and associated quick download speeds. There are many options for connecting hotspots through the wide area network (WAN) to the Internet, ranging from low-cost Digital Subscriber Lines to high-speed wireless canopies. The types of backhaul options depend on locality and what services are available to that area. The options described in this section are not an exhaustive list but rather the more common types of wired and fixed wireless solutions.

Section 3.8, "WAN Backhaul" on page 24 outlines methods of calculating the minimum backhaul bandwidth for the expected number of hotspot users. This section will describe different backhaul options and compare them, primarily from a technical and performance aspect. An easy reference table is included near the end of this section.

4.1 Wired Backhaul Solutions

4.1.1 Leased Lines, Digital Signal (DS)

Digital Signal Level (DS) is a broad, generic designator for several types of multiplexed telecommunications carrier systems including T-Carrier in North America, J-Carrier in Japan and E-Carrier in Europe and most of the world. These are commonly referred to as Leased Lines.

T-Carrier Trunk Level 1 (T-1) lines are divided into 24 synchronized channels, each channel is 64 Kbps for a total signaling speed of 1.544 Mbps. There are more Trunk Levels available that are listed in Table 2 below. Leased T-Carrier lines can be "fractioned" by dividing the lines into virtually any number of channels, which are also known as DS-0's. Ordering "fractional" T-Carrier lines allows the subscriber to customize the exact amount of bandwidth needed for their operations. T-Carrier lines may be delivered on fiber optic transmission systems where fiber is available (you should insist on it being installed as part of your order).

While T-1 was developed and is optimized for uncompressed voice communications, it can also be used for data communications. The signal and bit transmissions are required to be synchronized and therefore, the subscriber is guaranteed the bandwidth that is purchased. If you lease a T-1 line, you could, for example, split it (fraction it) into 12 voice grade channels to support 12 voice conversations, and use the remaining 768 Kbps for reasonably high-speed access to the Internet. The telephone carrier will install the T-1 line with what is known as a DS-1X (RJ-45) terminator on the customer premise. It is then up to the subscriber how to split the bandwidth, which is usually provisioned on the subscriber's point-of-entry router.

J-Carrier is identical to T-Carrier in signaling and framing. However, E-Carrier uses separate channels for framing and signaling and so the method of splitting/fractioning the E-1 line is slightly different. An E-1 line consists of 32 DS-0 channels with 30 channels fully dedicated to data, resulting in 2.048 Mbps. The remaining two channels consist of signaling and framing with one channel for each. Table 2 shows common carrier rates for each of the carrier types:

Table 2. Common Carrier Data Rates

North American T-Carrier	Data Rate	# DS-0 Channels
DS-0	64 Kbps	1
T-1 (DS-1)	1.544 Mbps	24
T-1C	3.152 Mbps	48
T-2 (DS-2)	6.312 Mbps	96
T-3 (DS-3)	44.736 Mbps	672
T-4 (DS-4)	274.176 Mbps	4032
Japan J-Carrier	**Data Rate**	**# DS-0 Channels**
J-1	1.544 Mbps	24
J-2	6.312 Mbps	96
J-3	32.064 Mbps	480
J-4	97.728 Mbps	1440
J-5	397.000 Mbps	5760
European E-Carrier	**Data Rate**	**# DS-0 Channels**
E-1	2.048 Mbps	32
E-2	8.448 Mbps	128
E-3	34.368 Mbps	512
E-4	139.264 Mbps	2048
E-5	565.148 Mbps	8192
E-6	2200.000 Mbps	32,768

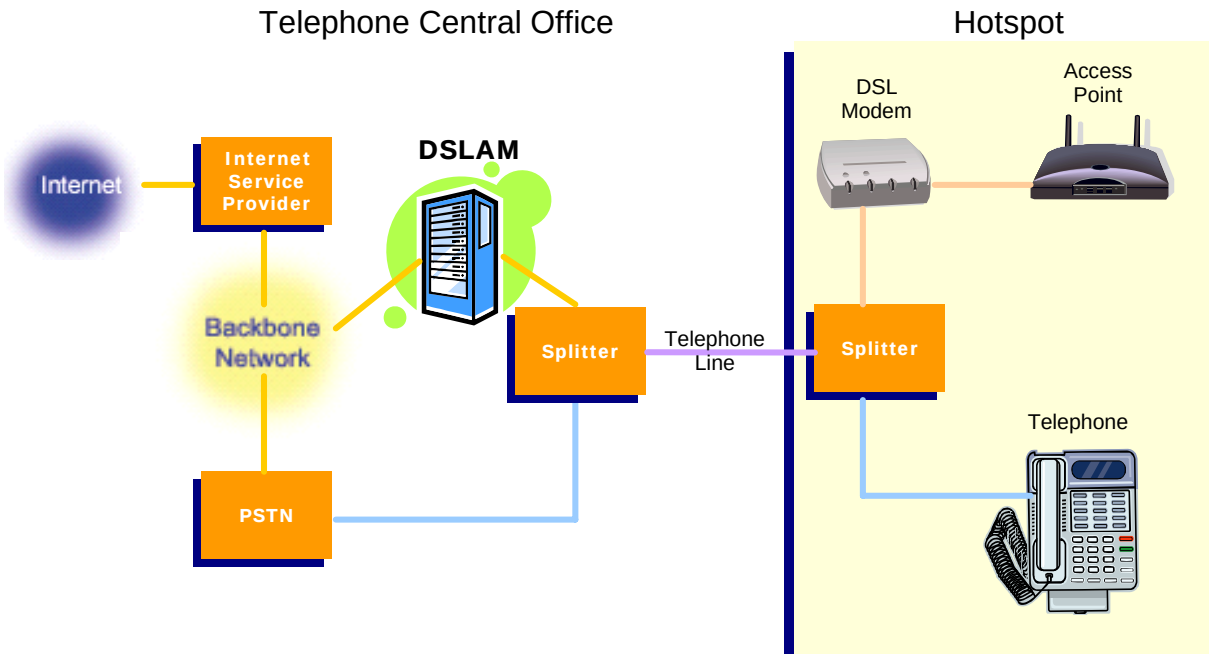
4.1.1.1 Pros and Cons

Leased Lines, or Digital Signal Level lines, support synchronous data transmissions that guarantees the minimum data rates for both the upstream and downstream directions. Users are assured that data rates will be maintained at those levels. In addition, users are able to configure the lines, "fractioning" the DS-0 channels to suit their individual needs using appropriate network routers. However, leased lines are costly in relation to other types of wired services (see below).

4.1.2 Digital Subscriber Line (DSL)

Digital Subscriber Line (DSL) is a broadband, packet data access technology for the Public Switched Telephone Network (PSTN) copper lines. xDSL refers collectively to all types of DSL, such as ADSL (and G.Lite), VDSL, IDSL, SDSL and HDSL. This "last-mile" technology connects homes or offices to the telephone switching stations and is not used between switching stations.

Figure 2. DSL Topology



xDSL operates over existing copper telephone lines using sophisticated modulation schemes and requires short runs to a central telephone office, usually less than 20,000 feet. The closer the subscriber is to the telephone central (switch) office, the higher possible data rates. xDSL offers much higher speeds than previous methods such as ISDN - up to 52 Mbps for downstream traffic, and from 32 Kbps to over 2 Mbps for upstream traffic.

The carriers use Digital Subscriber Line Access Multiplexers (DSLAM's) to interconnect multiple DSL lines to a high-speed backbone network. The DSLAM multiplexes (aggregates) data transmissions from all DSL lines and connects them to the Backbone Network, an Asynchronous Transfer Mode (ATM) network. Consequently, all subscribers connected to the DSLAM vie for the bandwidth that connects the DSLAM to the ATM Backbone. Carriers will usually over-subscribe the DSLAM to utilize as much available bandwidth as possible. For example, if 20 customers subscribe at 2 Mbps each and if the ATM network bandwidth is only 10 Mbps and all 20 customers are online, they will only get 500 Kbps each (assuming they are all active at once). For this reason, xDSL prescribed data rates are a maximum rate and actual rates will vary. You can determine how much the carrier over subscribes by asking for the "minimum commitment rate". Of course, there are many other potential bottle-necks in determining the overall hotspot bandwidth, such as the ISP's backhaul bandwidth.

Most DSL technologies require that a signal splitter (filter) be installed at the customer premise to separate voice signals from data signals. However, it is possible to manage the splitting remotely from the central office. This method is known by many names, splitterless DSL, "DSL Lite," G.Lite, or Universal ADSL. Splitterless DSL gives up some performance for the convenience of installation which can be accomplished by most customers so that a service truck does not need to be dispatched.

Table 3 provides a summary of various DSL specifications:

Table 3. DSL Specification Summary

Type	Description	Data Rate	Distance	Application
ADSL	Asymmetric Digital Subscriber Line	1.5 - 9 Mbps down 16 - 640 kbps up	Up to 18k ft on 24 gauge wire	Internet access, video on-demand, simplex video, remote LAN access, interactive multimedia
DSL Lite (G.Lite)	Splitterless DSL	1.5 Mbps - 6 Mbps down 16 - 640 kbps up	18k ft on 24 gauge wire	The standard ADSL; sacrifices speed for not having to install a splitter at the user premise.
HDSL	High data rate Digital Subscriber Line	1.5 Mbps - 42 Mbps duplex	12k ft on 24 gauge wire	T1/E1 service Feeder plant, WAN, LAN access, server access
SDSL	Symmetric Digital Subscriber Line	1.5 Mbps - 2 Mbps duplex	12k ft on 24 gauge wire	Same as HDSL plus premises access for symmetric services
VDSL	Very high data rate Digital Subscriber Line	13 - 52 Mbps down 1.5 - 2.3 Mbps up	1k to 4.5k ft depends on data rate	Same as ADSL plus HDTV

4.1.2.1 Pros and Cons

Digital Subscriber Lines offer high-speed data rates and are inexpensive when compared to other types of services, making them good choices for a hotspot backhaul. xDSL data rates vary despite the subscribed rate because the rate depends on the distance from the Central Office (CO) to the customer premise (called the local loop) and how much the carrier has subscribed the DSLAM's available backbone bandwidth. While carriers advertise the maximum data rate for a given service, the rates are usually lower and variable. Subscribers should ask the carrier what the "minimum commitment rate" is for the xDSL service.

4.1.3 Cable Modem

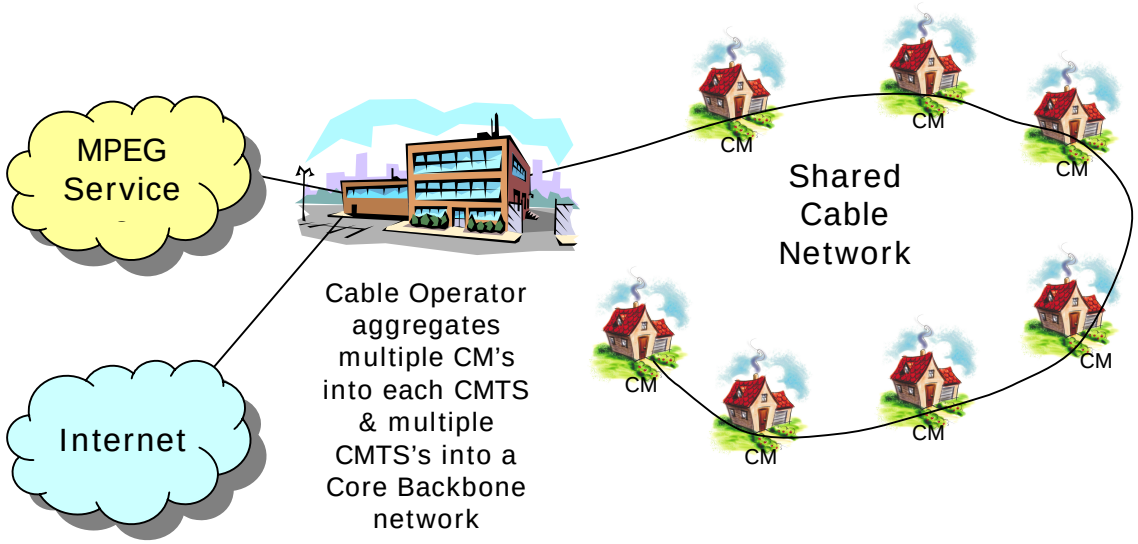
Data Over Cable Service Interface Specification (DOCSIS), developed by CableLabs* and approved by the ITU, defines interface requirements for cable modems involved in high-speed data distribution (both MPEG and IP data) over cable television system networks.

The DOCSIS architecture has the following two key components:

- Cable Modem (CM), which is located at the customer premise
- Cable Modem Termination System (CMTS), which is located at the head-end of service providers and used to aggregate traffic from multiple Cable Modems and then communicate with the backbone network.

DOCSIS specifies modulation schemes and the protocol for exchanging bidirectional signals between these two components over cable.

Figure 3. Cable Modem Network Topology



There are three versions of DOCSIS implemented and deployed, as shown in Table 4:

Table 4. DOCSIS Versions†

DOCSIS Version	Description and Features
1.0	High Speed Internet Access. Key features: Downstream traffic transfer rates between 27 and 36 Mbps over a radio frequency (RF) path in the 50 MHz to 750+ MHz range, and upstream traffic transfer rates between 320 Kbps and 10 Mbps (Average 5 Mbps) over a RF path between 5 and 42 MHz. But, because data over cable travels on a shared loop, individuals will see transfer rates drop as more users gain access.
1.1	Data, Voice, Gaming and Streaming. Key features: DOSCIS 1.1 is interoperable with DOCSIS 1.0. It enhanced QoS for multiple services such as voice and streaming; Improved security over DOCSIS 1.0; and more robust upstream data transmission (average 10 Mbps).
2.0	Added capacity for symmetric services by operating at 64 QAM and having new 6.4 MHz wide channel. It increased bandwidth for IP traffic by using enhanced modulation and improved error correction. The result for upstream transmission is 30 Mbps, which is 3 times better than DOCSIS 1.1 and 6 times than DOSCIS 1.0. DOSCIS 2.0 is interoperable and backward compatible with DOCSIS 1.x.

The latest DOCSIS specification, eDOCSIS, has been published to the industry. eDOCSIS stands for embedded DOCSIS, which will provide a subordinate function at the core chip level to the host device. And, rather than leveraging a home networking protocol, an eDOCSIS device will feed directly into a cable network's DOCSIS channel. eDOCSIS is intended to solve end device (and traffic) management, configuration and security issues to significantly reduce cost in the service operation and to improve speed and quality of end customer services.

†DOCSIS information courtesy of Javvin Technologies* (www.javvin.com)

4.1.3.1 Pros and Cons

Cable modems offer high-speed data rates and are inexpensive when compared to other types of services, making them good choices for a hotspot backhaul. Subscribers on the cable network share the same local network bandwidth so data rates vary, sometimes significantly, depending on how many subscribers are active and what kind of applications (bandwidth) they are using.

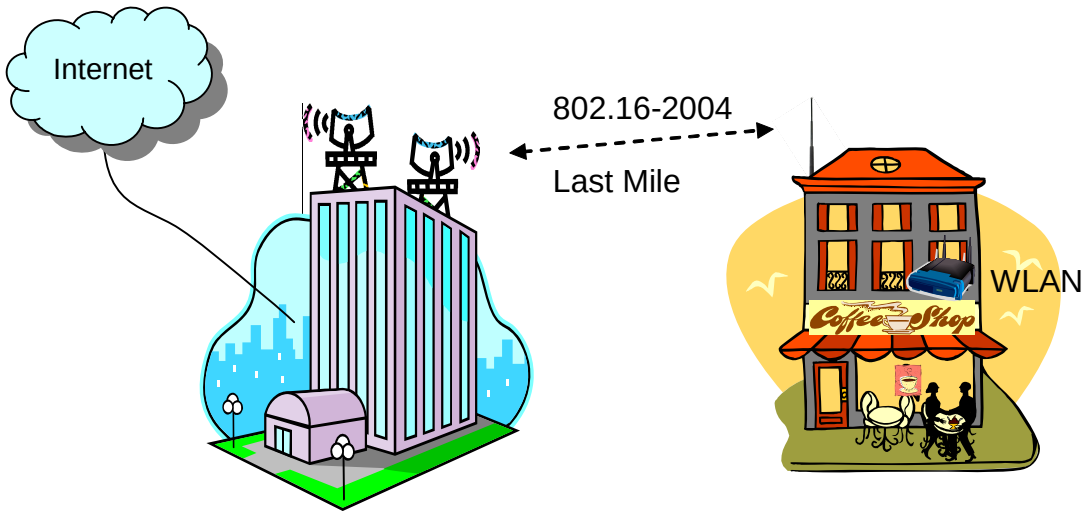
4.2 Wireless Backhaul Solutions

Wireless broadband solutions are required when wired broadband is not available, such as remote or rural locations. Typically, wireless solutions cost more than wired solutions and some do not perform as well. Also, as with any wireless solution, wireless backhaul is prone to frequency interference even when special high-gain, directional antennas are used. For these reasons, hotspot owners and operators usually favor wired backhaul solutions unless none are available.

4.2.1 WiMAX

WiMAX technology is a worldwide wireless networking standard that addresses interoperability across IEEE 802.16 standard-based products. WiMAX technology offers a wireless alternative to wired backhaul and last mile deployments that use other wired backhaul techniques described in this section.

Figure 4. WiMAX Last Mile to Hotspot



WiMAX technology can reach a theoretical 30-mile coverage radius and achieve data rates up to 75 Mbps, although at long range, throughput is closer to 1.5 Mbps. The IEEE 802.16 standard, with addendums, addresses two types of usage models: a fixed wireless wide area usage model (IEEE 802,16-2004) and a portable, mobile usage model (802.16 REV E, scheduled for ratification in 2005).

WiMAX has been designed to address challenges associated with traditional wired last-mile deployments. Last mile deployments use a point-to-multipoint topology to connect residential or business subscribers to a base station. Base stations are generally configured to cover a sector or sectors. Sectors are geographical segments which can have one or more radio base station(s) for the covered area.

To meet global regulatory requirements and allow providers to use all available spectrums within the allocated bands, the 802.16-2004 standard supports channel bandwidth sizes between 1.5 MHz and 20 MHz. Governments around the world have established frequency bands available for use by licensed and license-exempt WiMAX technologies as well as power requirements for high-power and low-power operations. There are advantages associated with licensed and licensed-exempt bands as outlined in Table 5:

Table 5. Benefits of Licensed and License-exempt Solutions

Licensed Solution Advantages	License-exempt Solution Advantages
Better quality of service	Fast rollout
Better non-line-of-sight (NLOS) reception at lower frequencies	Lower costs
Higher barriers for entrance	More world-wide options

A consortium of industrial leaders formed the non-profit organization, WiMAX Forum*. The WiMAX Forum's responsibilities are parallel to the efforts of the Wi-Fi* Alliance's efforts of 802.11. Equipment that is WiMAX Forum Certified™ is tested for specification compliance and vendor interoperability.

4.2.1.1 Pros and Cons

WiMAX (IEEE 802.16) is a new standard and service providers are beginning to deploy last mile services. The implications of interoperable, standards-based equipment means WiMAX service providers can have lower operating costs which will translate to lower subscriber fees for hotspot operators and other customers over other types of wireless services, such as LMDS and MMDS discussed below. Low costs combined with high performance makes WiMAX a good choice for any hotspot operator.

4.2.2 Local Multipoint Distribution Service (LMDS)

Local Multipoint Distribution Service (LMDS) uses microwave signals to transmit voice, video, and data signals using low power transmissions which can reach distances no greater than a five mile (nominal three mile) range. It is a fixed wireless broadband service that relies on microwave radios to send large amounts of information between each of the radios at very high speeds. In the U.S., the FCC has allocated LMDS 1.15 GHz in the 28-GHz, 30-GHz and 31-GHz frequency bands. At this high of frequency, line of sight between the transmit and receive antennas is critical.

The high frequency and large band allows data speeds of more than 150 Mbps but low transmit power limits the range and the cost is relatively high.

Some LMDS services only transmit the downlink from the base stations to the customer premise, relying on other means such as PSTN for the uplink. Be sure to order bi-directional LMDS.

4.2.2.1 Pros and Cons

LMDS offers very high speed data rates and installation can be accomplished quickly since lines do not have to be provisioned or installed at the customer premise. However, the antennas must be close (within 5 miles) and have line of sight, and the service is relatively expensive.

4.2.3 Microwave Multipoint Distribution Service (MMDS)

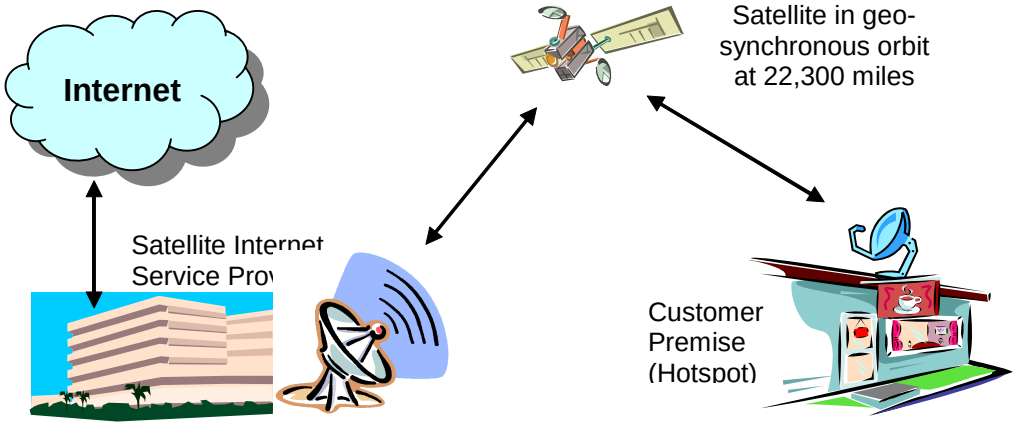
Microwave Multipoint (or Multichannel) Distribution Service (MMDS) is also known as Wireless Cable and similar to LMDS but with a smaller licensed frequency spectrum and a longer range. This fixed wireless system is used primarily to distribute cable television in digital form, providing more than 100 channels to a radius of approximately 35 miles from the transmitter. The licensed microwave signal is received by an antenna (line of sight) on the subscriber's home or office, then sent down coaxial cable to a set-top box on the customer's TV or to a cable modem. Data speeds are approximately 10 Mbps and the cost is "medium" compared to the higher cost of LMDS and the lower cost of WiMAX wireless services.

4.2.3.1 Pros and Cons

While MMDS is similar to LMDS and requires antennas be line-of-site, its range is greater and cost is lower than LMDS. However, bandwidth is limited to 10 Mbps for each transmitter antenna's geographic sector which is shared amongst the subscribers in those sectors.

4.2.4 Satellite Internet Service

Figure 5. A typical satellite service solution



Satellite Internet service works by transmitting signals to geosynchronous orbiting satellites located 22,300 miles (42,165 km) above the Earth's equator. Once the signal reaches the satellite, it is relayed to the subscribers' ground stations. Each satellite is capable of up to 5000 simultaneous channels (streams) of communications when using IP multicast.

Satellite services are available virtually world-wide, except at extreme latitudes. The subscriber simply needs to have a clear line of site towards the Earth's equator. The satellite service provider will install a small dish usually on the rooftop, two modems (downlink and uplink) and coaxial cable between the dish and modems.

Typical downlink speeds are 500 Kbps and uplink speeds are limited to 50 Kbps. Some services only transmit from the satellite to the subscriber (downlink) and the uplink is provided by regular PSTN phone lines. Advanced services offered by the service providers, such as data compression and "acceleration", may improve data throughput but only for files and data streams that can be compressed.

In addition to a slow uplink speed, performance is also affected by the long signal path, which causes high latency. Even though signals travel at the speed of sound, they must travel about 45,000 miles up to the satellite and back down to the ground station. Typical latency will delay delivery of data by about one second in each direction. Consequently, a web request will have an additional two seconds of delay, one second for the request and one second for the response. Each of these request/response round trips adds up to a noticeable delay for interactive, time-critical applications.

Satellite Internet technology does allow hotspots to move, such as commercial airplanes, commuter trains and ferry ships. Advanced (smart) satellite antennas rotate and track the satellite as the hotspot moves. This allows continuous connection as long as the antenna has continuous sight of the satellite (the connection will break when the train enters a tunnel, for instance). Although the performance of the system remains lower than wired solutions, the "captured" customers of these hotspots are tolerant knowing that they are able to access the Internet to complete business transactions that would otherwise be delayed until they arrived at their destinations.

4.2.4.1 Pros and Cons

The cost of satellite services are about twice that of xDSL or cable services and the data rates are about half on the downlink and about one-tenth of the uplink. When poor data rates are combined with long latency (due to the long signal path), the user experience degrades considerably. Although satellite Internet services can provide faster access for rural residence as compared to dial-up services, this solution is not recommended for hotspot owners servicing multiple clients at a time due to its poor performance.

4.3 Summary

Table 6 compares the different types of broadband backhaul discussed in this section.

Table 6. Comparison of Broadband and Backhaul Methods

Service	Capacity	Range	Deployment	Deploy Costs
Leased Lines	300+ Mbps	--	Dense	Medium to High
xDSL	52 Mbps	18k - 1k feet on local loop	Very dense	Low
Cable Modem	30 Mbps	--	Very dense	Low
WiMAX	75 Mbps	30 miles	Sparse	Low - Medium
LMDS	150+ Mbps	3 - 5 miles	Very limited	High
MMDS	10 Mbps	35 miles	Sparse	Medium
Satellite	0.5 Mbps	World-wide	Sparse	Low

Hotspot operators will need to decide which type of backhaul service they will use based on availability, performance and costs. Performance characteristics not only include bandwidth (capacity) but also latency and delay that all affect the end user experience. For instance, satellite systems allow for wide-spread coverage (it's available anywhere with line of sight to the satellite) but the latency of transmitting and receiving signals from 22,300 miles (42,165 km) very much impacts the overall speed of the connection and experience for the end users.

In general, wired backhaul methods are cost effective and wide spread. Leased Lines (T-Carrier, E-Carrier & J-Carrier) services are excellent choices. The hotspot is guaranteed the level of performance so this type of backhaul service helps ensure users receive a consistent experience. But of the wired services available, Leased Lines are most expensive.

On the other hand, DSL services are more cost-effective and perform reasonably well despite that carriers often over-subscribe the backbone bandwidth. This type of service, although more widely used, results in more sporadic connection experiences for the end users than Leased Lines.

Cable service is probably even more sporadic since this service is shared with other subscribers on the local service. If there are few users on the cable service, performance will be very good but as more users join the local cable network or use high bandwidth applications, performance declines. Like DSL, the service is very cost-effective and available in most populated areas of the world.

Wired services are limited to relatively short distances from the telephone or cable offices. Hotspots that are located in more remote areas will require other methods of connecting to the Internet infrastructure, such as wireless services or satellite.

The three types of wireless services discussed in this section, LMDS, MMDS and WiMAX are similar in their deployment methods. WiMAX equipment is gradually being certified and will eventually make fixed wireless, "last mile" backhaul more cost-effective. Until then, LMDS and MMDS are alternative wireless services that may be available to remotely located hotspots.

Although satellite data service has not proven to be a good choice for a standard hotspot because of the slower data rates and very high latency, it has proven to be a good method for hotspots that move, such as airplanes and trains. Business travelers and commuters are beginning to reap the benefits of wireless hotspots as they travel because of innovations on backhaul methods. Satellite tracking antennas provide connectivity to these highly mobile hotspots. Although the latency of the satellite connection degrades the user experience, users are more tolerant because of the moving environment and their ability to stay connected in what otherwise would be "down time."

While it is difficult to directly compare the different types of broadband backhaul options because of their differing architectures and technologies, there are several good choices of backhaul methods for hotspots. The hotspot's location will determine which backhaul options are available based on which services the providers have deployed in that area. The hotspot operators should shop around carefully and understand the differences being offered.

5.0 802.11 Standards Basics

The 802.11 standard was first adopted in 1997. The standard defines a Medium Access Control (MAC) sublayer along with management protocol and services and three physical (PHY) layers (Infrared, Frequency Hopping Spread Spectrum Radio and Direct Sequence Spread Spectrum Radio in the 2.4 GHz frequency).

The first 802.11 standard as ratified in 1997 operates at a rate of 1.0 and 2.0 Mbps in the 2.4 GHz band. The second and third 802.11 standards, the 802.11a and 802.11b respectively, came in 1999.

802.11b, 802.11a and 802.11g are addendums to the original specification. 802.11a specifies a new PHY layer that uses an orthogonal frequency domain multiplexing (OFDM) radio to achieve data rates up to 54 Mbps in the 5.8 GHz frequency range. 802.11b is an extension to the DSSS PHY achieving data rates up to 11 Mbps. 802.11g is an extension to 802.11b which uses an orthogonal frequency domain multiplexing radio to achieve data rates up to 54 Mbps while remaining in the 2.4 GHz frequency range and compatible with 802.11b devices. These addendums are an evolution towards faster data rates and also, in the case of 802.11a, an attempt to overcome the problems brought as a result of using the overcrowded 2.4GHz S-band ISM where microwave ovens, cordless phones, baby monitors and many other commercial devices operate.

The purpose of this section is to present a comparison of the three major 802.11 media types. To understand the comparison between 802.11a, 802.11b and 802.11g we'll need to first understand the key technologies that most influence the differences. The following sections present an introduction to the technologies that differentiate the standards the most followed by sections that make the actual comparison of the 802.11 media types.

5.1 What Makes the Standards Different?

Many amendments to the original 802.11 standard have been included with each of the new extensions to the standard. In this section, we only look at the key enhancements in the standards that are most likely to affect a hotspot implementation, mainly the rate, number of channels, AP coverage range and interoperability.

To maintain the compatibility and maximize reuse of the technology, major changes have been confined to the PHY layer of the 802.11 specification. Higher transmission rates have been accomplished by specifying the use of more efficient transmission technologies such as Orthogonal Frequency Division Multiplexing (OFDM) as well as more efficient signal encoding techniques. 802.11g and 802.11a use OFDM as the modulation technology to support rates up to 54 Mbps. OFDM is a more efficient transmission method than the 802.11b Direct Sequence Spread Spectrum (DSSS) transmission technology. Thus, 802.11 uses a combination of encoding and transmission techniques to support rates from 1 Mbps to 54 Mbps. Table 7 shows the encoding and transmission (modulation) technologies as they apply to each of the transmission rates:

Table 7. 802.11 Encoding and Modulation Techniques

Rate (Mbps)	Encoding	802.11b Modulation		802.11g Modulation		802.11a Modulation	
		Mandatory	Optional	Mandatory	Optional	Mandatory	Optional
1	DBPSK	Barker-DSSS		Barker-DSSS			
2	DQPSK	Barker-DSSS		Barker-DSSS			
5.5	DBPSK	CCK - DSSS	PBCC	CCK-DSSS	PBCC		
6	BPSK			OFDM	CCK-OFDM	OFDM	
9	BPSK				OFDM, CCK-OFDM		OFDM
11	DQPSK	CCK-DSSS	PBCC	CCK-DSSS	PBCC		
12	QPSK			OFDM	CCK-OFDM	OFDM	
18	QPSK				OFDM, CCK-OFDM		OFDM
22	8PSK				PBCC		
24	16 QAM				CCK-OFDM	OFDM	
33	8PSK				PBCC		
36	16 QAM				OFDM, CCK-OFDM		OFDM
48	64 QAM				OFDM, CCK-OFDM		OFDM
54	64 QAM				OFDM, CCK-OFDM		OFDM

5.2 802.11b

The main drive of the 802.11b standard was to increase the data transmission rate. Up until 802.11b, the transmission rates supported by 802.11 products were 1.0 and 2.0 Mbps. This was considered to be too low for speed hungry applications. 802.11b adds support for 5.5 and 11 Mbps rates. These higher rates are achieved by introducing an extension to the PHY specification. To provide the higher rates, 8-chip complementary code keying (CCK) is employed as the modulation scheme. Also, an optional mode replacing the CCK modulation with packet binary convolutional coding (HR/DSSS/PBCC) is provided (see the section below titled "What is PBCC). Table 8 shows the main characteristics of the 802.11b standard:

Table 8. 802.11b Basic Characteristics

Feature	Description
Radio Technology (Bandwidth Utilization Mode)	Mandatory: DSSS, FHSS, IR
Encoding/Modulation	Mandatory - CCK (Complementary Code Keying) Optional - PBCC (Packet Binary Convolutional Code)
Noise Sensing Technology	Clear Channel Assessment (CCA) capability
Media Access Method	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
Frequency Band	2400 ~ 2483.5 MHz for U.S., Canada, and ETSI 2400 ~ 2497MHz for Japan
Supported Rates	1, 2, 5.5 and 11 Mbps
Channels	1-11 - U.S., Canada 1-13 - ETSI 1-14 - Japan 10-11 - Spain 10-13 - France
Range	Indoors: 75-100 ft. Outdoors: ~ 1,000 ft.

5.2.1 What is PBCC?

When the 802.11b standard was being discussed, two encoding techniques emerged as primary contenders:

- Complementary Code Keying (CCK) proposed by Intersil*
- Packet Binary Convolutional Code (PBCC) proposed by Texas Instruments*

In the end, CCK was chosen as mandatory and PBCC as optional.

Note: The 802.11b standard includes several optional features. When selecting equipment which includes optional features of the standard, keep in mind that you will most likely only be able to take advantage of the optional features when the mobile client wireless card and the AP come from the same manufacturer.

5.2.2 Modulation Techniques

802.11b adds two higher data rates to the 802.11 standard; 5.5 Mbps and 11 Mbps. While it continues to use DSSS as the transmission technology, the higher rates are achieved through use of a different encoding method call Complementary Code Keying (CCK). 802.11b retains the Barker code encoding method specified in the 802.11 standard to transmit data at the 1 and 2 Mbps.

5.2.3 Channels

The 802.11b standard operates in the 2.4 GHz ISM (Industrial, Scientific and Medical) band. The 80 MHz band is divided into 14 channels. Regulatory domains control which channels are used in different countries for 802.11b communications. Table 9 shows the 802.11 channels allowed by each regulatory domain:

Table 9. Channel Allocation per Regulatory Domain

Regulatory Domain	Allowed Channels
U.S. (FCC)/Canada (IC)	1-11 in 2.412 - 2.462 GHz
Europe (ETSI) except France and Spain	1-13 in 2.412 - 2.472 GHz
France	10-13 in 2.457 - 2.472 GHz
Spain	10-11 in 2.457 - 2.462
Japan (MKK)	14 in 2.484 GHz

Adjacent channels have a separation of only 5 MHz and most of the energy for each channel spans, by design, a 22 MHz band. What this means is that adjacent channels do interfere with each other. Figure 6 shows that this channel allocation only permits three non-overlapping channels. For example in the U.S., these non-overlapping channels are 1, 6 and 11. In Europe, because of the extra two channels (12 and 13), 1, 7 and 13 is a better allocation (due to wider separation) of non-overlapping channels.

Figure 6. 802.11b Channels in 2.4 GHz

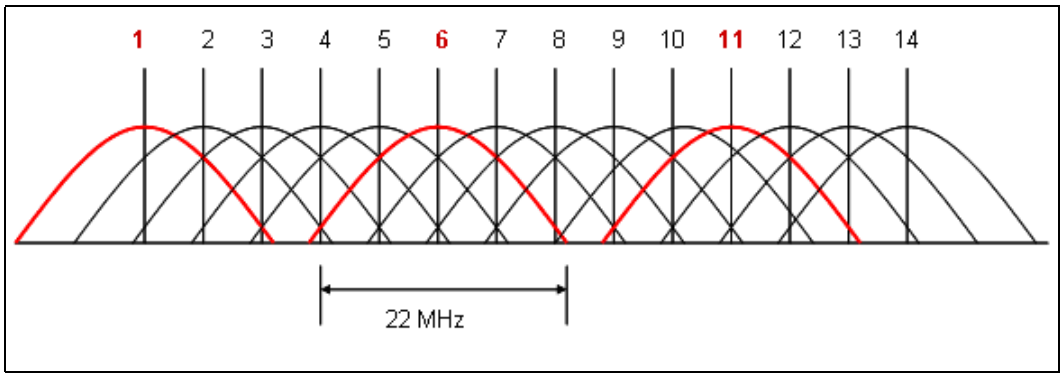
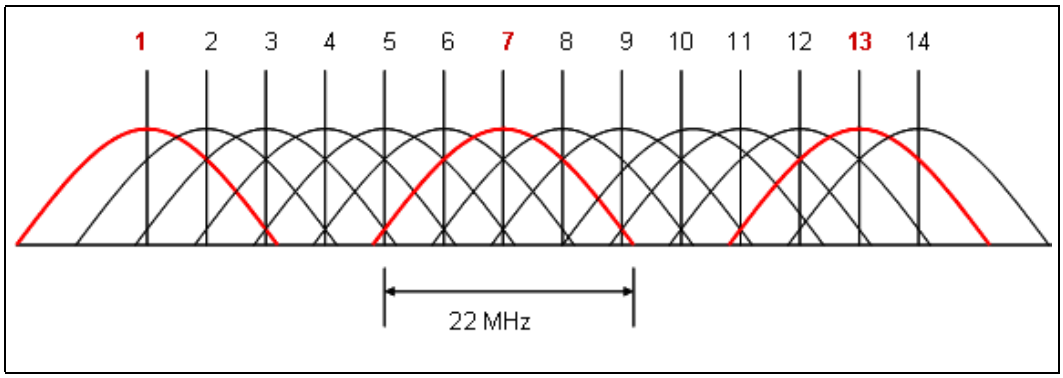


Figure 7 shows the best allocation for ETSI regulated countries:

Figure 7. 802.11b Optimal Channel Allocation for ETSI Regulated Countries

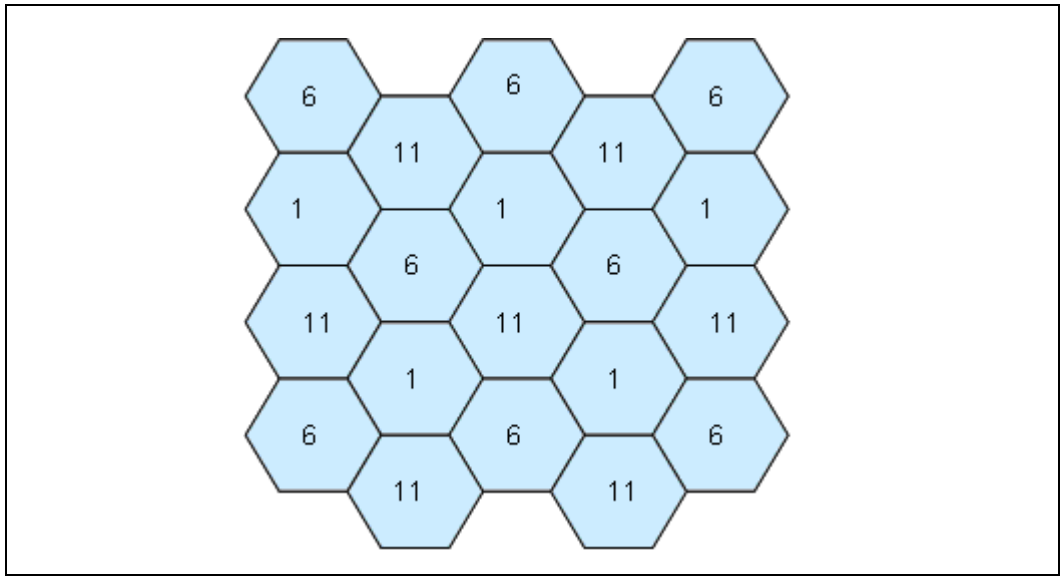


Note: Keep in mind that wireless cards manufactured for U.S. markets may not scan channels above channel 11. To ensure that you can provide the best service for those types of wireless clients, you might consider using channels 1, 6 and 11 in ETSI regulated countries.

5.2.3.1 Channel Re-use

Due to the small number of non-overlapping channels (3) in the 802.11b specification, deployments of wireless sites that use multiple APs require careful design consideration. In order to minimize interference between APs and maximize network throughput it is necessary to keep APs that communicate in the same channel away from each other. The honeycomb pattern shown in Figure 8 is a suggested configuration. Which channel is placed in each slot is not important as long as you keep APs operating in the same channel as far away from each other as possible.

Figure 8. 802.11b Honeycomb Placement



When implementing 802.11b wireless networks in multilevel sites with only three channels to work with, even the honeycomb pattern shown in Figure 8 does not provide you with a perfect solution. You can see from this honeycomb pattern that every channel slot is next to the other two non-overlapping channels. What this means is that having just three non-overlapping channels is not ideal to support three dimensional deployments. But not all is lost. In such cases you can try other techniques such as controlling the transmit power emitted by the APs so as to avoid interference from one level to the adjacent ones. Conversely, you can up the power level of certain APs and distribute the honeycomb pattern over multiple levels.

5.2.4 Transmission Rates

802.11b adds two more operational rates to the original 802.11 specification, 5.5 Mbps and 11 Mbps. These higher transmission rates are achieved by utilizing Height Rate DSSS (HR/DS) transmission technology and CCK as the modulation. The specification also supports dynamic rate switching with the objective of improving performance. The algorithm for performing rate switching is beyond the scope of the standard but in general, as the signal degrades either because of larger distances between the AP and the mobile station or due to noise or multi-path interference, the transmission rate drops. As a matter of physics, longer wave forms will travel further distances and for this reason dropping the data rate allows the AP to communicate with clients as they move further away. To ensure coexistence and interoperability between different equipment manufacturers, the standard defines a set of rules that must be followed by all the client stations (STAs). Transmission rates can also be selected as a matter of choice. For example it is possible to program most APs to negotiate only certain rates. Reasons to control the rate might

include controlling the APs range of operation or to allow only certain data rates to ensure specific quality level. When controlling the range, by eliminating the use of lower rates one essentially narrows the range/distance over which an AP will allow associations. Table 10 shows approximate indoor maximum range values for the four rates supported by 802.11b:

Table 10. 802.11b Rate vs. Approximate Maximum Range

Rate	Approximate Maximum Range
1 Mbps	350 ft.
2 Mbps	250 ft.
5.5 Mbps	180 ft.
11 Mbps	150 ft.

Note: You can limit the transmission rates supported by an AP as a way to control the range over which the AP will function. Rate control complements and provides an alternative to adjusting the transmission power as a way to control an AP's operational range.

5.2.5 Range

802.11b range is highly affected by its environment. Indoors, where RF signals need to travel through obstacles or where there are a lot of obstacles to bounce from, the signal reach will be smaller than outdoors with Line Of Sight (LOS) between the AP and mobile clients. Table 11shows typical values for three different environments, outdoors, office setting and residential setting. Note that the maximum values specified can only be reached at the lowest data rate of 1 Mbps. The table also shows what distances might be reached when operating at 11Mbps.

Table 11. Wi-Fi Range Estimates for Three Typical Environments

Environment/Setting	Maximum Range at 1Mbps	Maximum Range at 11 Mbps
Outdoors (open space with standard antenna)	750-1,000 ft	150-350 ft
Office setting	250-350 ft	100-150 ft
Residential setting	125-200 ft	60-80 ft

5.3 802.11g

The IEEE approved the 802.11g amendment to 802.11b in 1999. Of main interest to us in this section are the support for higher data rates (up to 54 Mbps) and the backwards compatibility with 802.11b. 802.11g works in the same 2.4GHz band as 802.11b. Higher rates were, once again, obtained by making changes to the PHY (called the Extended Rate Phy - ERP) layer of the 802.11 specification. Most notable are the change in transmission technology and the encoding techniques. For a more efficient utilization of the bandwidth, 802.11g uses Orthogonal Frequency Division Multiplexing (OFDM) as the transmission mechanism and adds a few more of encoding modes (BSK3, QPSK, QPSK1, CCK, 16 QAM, 64 QAM) which are used based on the transmission rate. For compatibility, 802.11b includes a handshake protocol that allows 802.11b stations to determine when other stations are about to send packets using the 802.11g higher data rates. More information on the interoperability effects is provided in the next section. Table 12 shows the basic characteristics of the 802.11g specification.

Table 12. 802.11g Basic Characteristics

Radio Technology (Bandwidth Utilization Mode)	Mandatory: DSSS, FHSS, IR
Encoding/Modulation	Mandatory - CCK (Complementary Code Keying) Optional - PBCC (Packet Binary Convolutional Code)
Noise Sensing Technology	Clear Channel Assessment (CCA) capability
Media Access Method	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
Frequency Band	2400 ~ 2483.5 MHz for U.S., Canada, and ETSI 2400 ~ 2497MHz for Japan
Supported Rates	1, 2, 5.5, 6, 9, 11, 12, 18, (22,) 24, (33,) 36, 48 and 54 Mbps
Channels	1-11 - U.S., Canada 1-13 - ETSI 1-14 - Japan 10-11 - Spain 10-13 - France
Range	Indoors: 75-100 ft. Outdoors: ~ 1,000 ft.

5.3.1 Transmission Rates

802.11g builds on the four 802.11b supported rates (1, 2, 5.5 and 11) adding ten more rates. Of the fourteen rates, only seven are mandatory (1, 2, 5.5, 11, 6, 12 and 24 Mbps) the other seven are optional. Of the seven optional rates, two (22 and 33) use the PBCC modulation mode. You will find that most equipment will support most of the optional rates except the PBCC-based ones. In general, the lack of PBCC support by some manufacturers is mainly a business decision (cost cutting) since it is not mandated by the standard.

5.3.2 802.11b and 802.11g Coexistence

The most talked about feature of the 802.11g standard has been its support for much higher speeds than 802.11b. 802.11g supports multiple transmission rates all the way to 54 Mbps.

The next most talked about feature was its backwards compatibility with 802.11b devices. Unfortunately, this backwards compatibility did not come for free. To reach the higher data rates, 802.11g uses a different modulation method, OFDM (and optionally, PBCC), combined with several encoding schemes depending on the rate. What this means is that 802.11g devices, while communicating in the same 2.4 GHz band as 802.11b, talk in a language or manner that 802.11b devices don't understand. Not being able to understand 802.11g lingo, 802.11b devices cannot participate in the handshaking required to keep the mobile stations from all talking at the same time.

So how is it possible for an 802.11g AP to maintain communications simultaneously without the clients trampling over each other? The answer lies in the use of a handshaking protocol that was defined for use in the 802.11b standard, the RTS/CTS handshake. RTS stands for "Request To Send" and CTS for "Clear To Send." This handshake was originally specified for 802.11b stations to use at their own discretion when they detect the communications degrading or the medium being crowded.

Rather than relaying on the retransmission of undelivered packets, the mobile stations can clear the channel for transmission by sending an RTS message to the AP. If the AP determines it is OK for the station to transmit, it broadcasts out a CTS message to the requesting station. Both the RTS and

CTS message contain information regarding how much time the client needs to deliver the packet in question. All clients that receive the CTS will then yield the channel to the requesting station by making sure they don't transmit during the requested time period.

802.11b stations are able to understand RTS/CTS requests from 802.11g units because these messages are sent using modulation schemes used in the 802.11b specification, DSSS. Once an 802.11g station has been granted the channel, it can switch back to OFDM if necessary. The bottom line on the interoperability handshake is that it generates overhead, so much that it can cut the 802.11g throughput by over 50%. We'll discuss the effects of the overhead in the sections that make the comparison of the three standards.

To lessen the effect of the RTS/CTS protocol, a second method of reserving the channel was specified. This method is called CTS-to-Self and consists of the sending station reserving the channel by bypassing the RTS and just sending a CTS message to itself. All stations that hear this message will refrain from transmitting, thus clearing the channel. This method of channel reservation reduces the overhead, increasing the throughput.

Unfortunately, this method is vulnerable to the "Hidden-Node" problem. In the "Hidden-Node" case, two mobile stations can be too far apart to hear each other's messages but not too far from the AP for association. When this situation occurs, one of the stations may not hear the CTS-to-Self messages sent by the other thus opening up the possibility for packet collisions. The situation gets worse the more stations that connect to the same AP and the further away they are from each other. Use of CTS-to-Self is a configuration option in some wireless cards. CTS-to-Self is not recommended in crowded wireless environments.

Note: Using CTS-to-Self messages may actually degrade the performance of a mixed-mode wireless network.

5.3.3 Channels and Data Rates

802.11g functions in the same 2.4 GHz band as 802.11b and supports the same number of channels, up to 14 (depending on country). As such, 802.11g has the same limitations as 802.11b with only three non-overlapping channels.

Data rates of 1, 2, 5.5 and 11 Mbps are implemented just as in the 802.11b specification, that is, the same transmission technology and modulation. Data rates of 6, 9, 12, 18, 22, 24, 36, 48 and 54 Mbps are implemented using OFDM and more efficient encoding techniques. Because of the advantages that OFDM has over DSSS, these rates can be reached at distances that are comparable to some of the lower rates in 802.11b. For example the 6 Mbps rate can go further than the 2 Mbps. We'll revisit this topic when we do a comparison of the three technologies in the following sections.

5.3.4 Range

There are several factors that influence the communications range you'll get out a wireless device. Some of these factors include signal obstruction objects in the environment, RF noise, distance between the AP and the mobile client, rate of transmission, transmission technology, radio-input sensitivity and transmission power. Most product literature tends to only list one or two ranges. Those ranges generally refer to the maximum distance, indoor and outdoors, the AP will be able to communicate with a mobile device when using the lowest data rate it supports.

You will find products that say 600 ft. outdoors and others that say 1000 ft. You might wonder, what does the 802.11 specification require? Well, the specification does not exactly tell you the maximum distance required for every rate supported. Instead, it specifies the minimum receiver

sensitivity and the maximum transmit power. Even then, when specifying the maximum transmit power, the 802.11 specification says that wireless devices shall adhere to the requirements specified by the appropriate regulatory institutions in their respective regulatory domains.

What this means is that there is no precise distance at which communications stops or at which rates switch. The distance will be influenced by the maturity of the technology (early generation devices tend to go shorter distances), the environment, the allowance made by regulatory bodies and in some cases deviations from the standard that gives a company an edge. A area which has improved distances as the technology matures has been receiver sensitivity. Receiver sensitivity can mean the difference between 600 and 1000 ft. communications range as announced by some products. Table 13 shows the rates supported by 802.11g vs. an approximate maximum indoor range. The gray rows show the original rates supported by 802.11b and the white rows the new rates added in 802.11g specification.

Table 13. 802.11g Rate vs. Approximate Maximum Range

Rate	Approximate Maximum Indoor Range
1 Mbps	350 ft.
2 Mbps	250 ft.
5.5 Mbps	180 ft.
6 Mbps	300 ft.
9 Mbps	250 ft.
11 Mbps	150 ft.
12 Mbps	200 ft.
18 Mbps	170 ft.
24 Mbps	140 ft.
36 Mbps	100 ft.
48 Mbps	95 ft.
54 Mbps	90 ft.

5.4 802.11a

Approved in 1999, 802.11a was the next standard developed after 802.11b. 802.11a's main purpose was to move towards a less crowded unlicensed frequency, 5 GHz, and to improve the data rates. 802.11a has been slow to gain acceptance in the market. One of the reasons was the lack of interoperability with the existing 802.11b and the fact that 802.11g was lurking in the background promising both interoperability with 802.11b and data rates comparable with those of 802.11a. 802.11a products first appeared in 2000 but it wasn't until the end of 2003 when 802.11a started to gain traction. 802.11a's main advantage over 802.11g comes from its frequency of operation which is not affected by the likes of cordless phones, microwave ovens and security equipment. The 802.11a standard also supports 12 non-overlapping channels. More non-overlapping channels mean higher network capacity. 802.11b and 802.11g on the other hand only support three non-overlapping channels. Table 14 shows some of the main characteristics of the 802.11a standard. The sections that follow provide more detail.

Table 14. 802.11a Basic Characteristics

Feature	Description
Transmission Types (Bandwidth Utilization Mode)	Mandatory: OFDM Optional: None
Encoding/Modulation	Mandatory - BPSK, QPSK, 16-QAM, 64-QAM
Noise Sensing/Media Busy Technology	Clear Channel Assessment (CCA) capability
Media Access Method	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
Frequency	5 GHz band - Subject to authorities responsible for geographic-specific regulatory domains.
Supported Rates	All: 6, 9, 12, 18, 24, 36, 48, 54 Mandatory: 6, 12, 24
Channels	U.S. - 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161 Europe - 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112,116, 120, 124, 128, 132, 136, 140 Japan - 34, 38, 42, 46

5.4.1 Transmission Rates and Range

802.11a supports eight transmission rates, from 6 Mbps to 54 Mbps. The ability to reach higher rates than 802.11b comes from utilizing OFDM which is a more efficient transmission mode. However, the utilization of higher frequency band comes at the price of shorter range. Table 15 shows the ranges supported and the approximate range at each rate.

Table 15. 802.11a Rate vs. Approximate Maximum Range

Rate	Approximate Maximum Indoor Range
6 Mbps	180 ft.
9 Mbps	165 ft.
12 Mbps	155 ft.
18 Mbps	130 ft.
24 Mbps	120 ft.
36 Mbps	105 ft.
48 Mbps	90 ft.
54 Mbps	60 ft.

5.4.2 802.11a Channels

What channels are defined for use by the 802.11a specification depends on regulations for a given region. In the United States, 802.11a utilizes 12 channels, spread across 3 bands. 8 of the channels are restricted to indoor use and 4 (52-64) can be used inside or outdoors. Table 16 shows the per-band channel distribution of the U.S.

Table 16. Valid Operating Channels in the U.S.

Regulatory Domain	Band (GHz)	Operating Channel Numbers	Center Frequencies (MHz)
United States	U-NII lower band (5.15-5.25)	36 40 44 48	5180 5200 5220 5240
United States	U-NII middle band (5.25-5.35)	52 56 60 64	5260 5280 5300 5320
United States	U-NII upper band (5.725-5.835)	149 153 157 161	5745 5765 5785 5805

A more complete list of channels that includes those supported in other regions of the world is shown in Table 17. If you are concerned that your equipment may not meet regulatory RF requirements, you should consult with the appropriate agencies for the regions in which you plan to deploy a hotspot. The information presented in this document was accurate at the time of writing but it is possible that changes in the spectrum usage have occurred since publication of this guide.

Table 17. 802.11a Channels Supported Throughout the World

Channel	Frequency (MHz)	Americas	ETSI (Europe)	Japan
34	5170	-	-	X
36	5180	X	X	-
38	5190	-	-	X
40	5200	X	X	-
42	5210	-	-	X
44	5220	X	X	-
46	5230	-	-	X
48	5240	X	X	-
52	5260	X	X	-
56	5280	X	X	-
60	5300	X	X	-
64	5320	X	X	-
100	5500	-	X	-
104	5520	-	X	-
108	5540	-	X	-
112	5560	-	X	-
116	5580	-	X	-
120	5600	-	X	-
124	5620	-	X	-
128	5640	-	X	-
132	5660	-	X	-
136	5680	-	X	-
140	5700	-	X	-
149	5745	X	-	-
153	5765	X	-	-
157	5785	X	-	-
161	5805	X	-	-

Figure 9 below depicts the channel spacing for the U-NII lower and mid bands. These channels are used for indoor communications.

Figure 9. Lower and Middle U-NII Bands

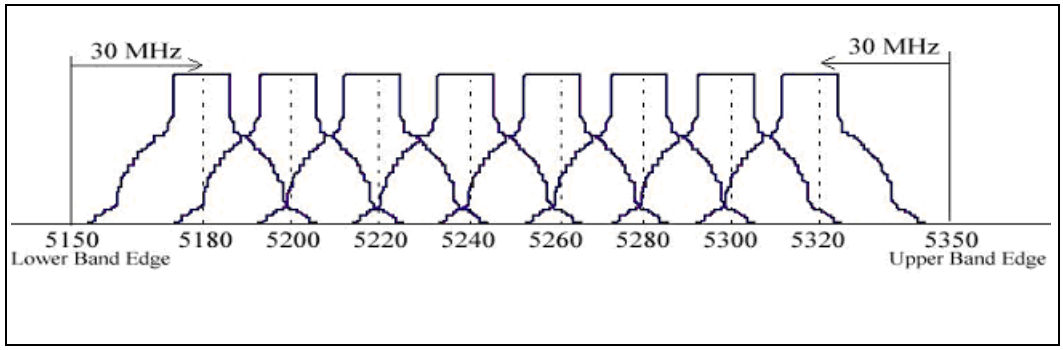
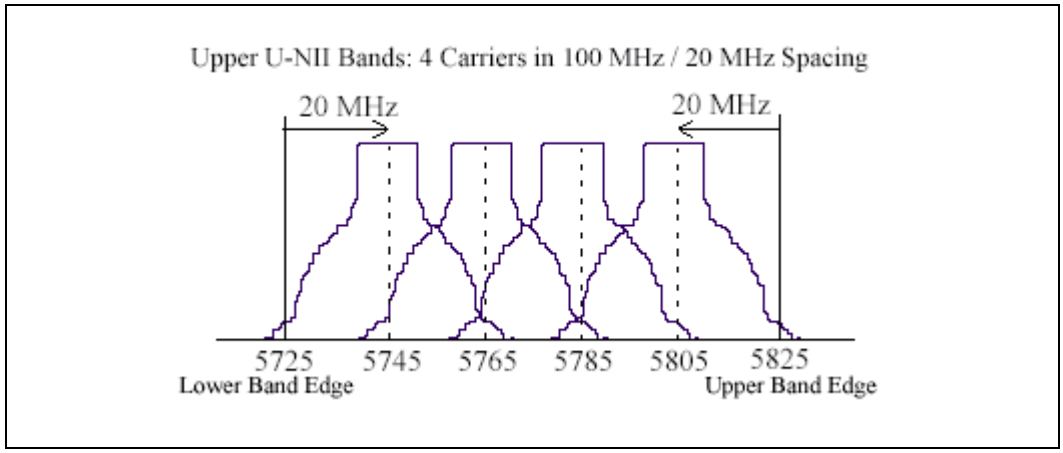


Figure 10 depicts the channel allocation for the upper U-NII band. This band is used for outdoor communications.

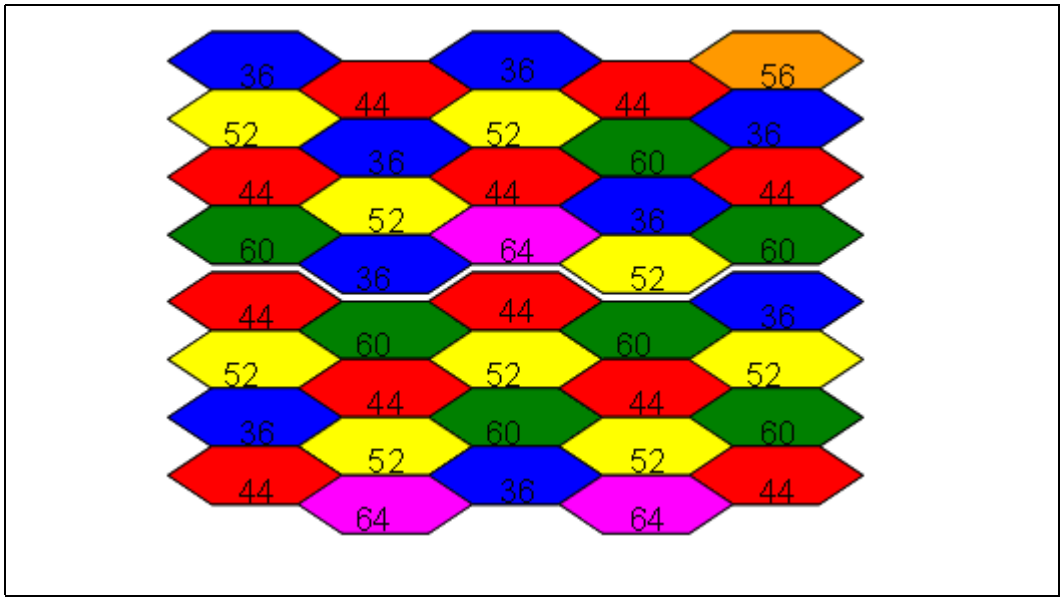
Figure 10. Upper U-NII Bands



5.4.2.1 802.11a Channel Reuse

While the figures above indicate some degree of overlap in the 802.11a channels, this overlap occurs at low energy levels. All twelve 802.11a channels are considered non-overlapping for purpose of communications. This brings a high level of flexibility when designing the layout of a wireless network. If your hotspot does not require the use of many channels, you should use channels that are not adjacent to further minimize any interference. Figure 11 shows an AP layout that does not resort to using all the channels:

Figure 11. 802.11a Sample Channel Configuration



5.4.3 802.11a/bg Throughput Comparisons

Throughput is obviously a big consideration when designing hotspots. As a service provider, you know that the larger throughput of your equipment, the more users you'll be able to service and the better support you'll be able to provide to hungry bandwidth services such as multimedia services. It is clear that the higher the data rate the higher the throughput. So, 802.11b and 802.11a have higher throughput than 802.11b. What may not be clear is that there are other parts of the specification that affect the throughput. The most important one is the backwards compatibility between 802.11g and 802.11b. The 802.11g specification requires 802.11g APs to support communications with 802.11b clients. As mentioned earlier, this support has come at the expense of throughput for both the 802.11b and 802.11g clients as well as the AP. Table 18 shows the approximate throughputs that can be obtained with all the 802.11 technologies as well as throughputs obtained when using an 802.11g AP while working in mix-mode using RTS/CTS and CTS-to-Self packet protection.

Table 18. Throughput Comparisons for 802.11a, 802.11b and 802.11g

Technology	Data Rate (Mbps)	Approximate Throughput (Mbps)	Throughput as Percentage of 802.11b
802.11b	11	6	100%
802.11g with 802.11b clients using CTS/RTS protection	54	8	133%
802.11g with 802.11b clients using CTS-to-self protection	54	12	200%
802.11g w no 802.11b clients	54	22	367%
802.11a	54	26	430%

5.5 Summary

This section presented the basic characteristics of the major 802.11 protocols; 802.11a, 802.11b and 802.11g. An understanding of the properties of each of these technologies is essential when determining which technology is right for your environment and the goals of your wireless site. The next section looks at how 802.11 technologies can be put to work to implement a public hotspot and how to gain a good understanding of the environment that affects its performance.

6.0 Understanding Wireless Environments

Maintaining good quality communications between the mobile station (MS) and the AP throughout the hotspot is typically the most ignored aspect of hotspot implementations. It is tempting to make assumptions regarding a given environment without doing the necessary up front work to ensure complete RF coverage and high network throughput. Careful thought and up front 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 the right technology
- Choose your equipment carefully to match the environment you are in
- Take the appropriate precautions to ensure the proper level of wireless security

6.1 Performing an RF Site Survey

Site Surveys are the most important part of any wireless implementation and require three pieces of equipment to perform:

- Test/Standard AP
- RF Analyzer
- 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.

Hotspot RF Analyzers come in many shapes and sizes. Some of the most well-known vendors are AirMagnet*, Wildpackets* and Network Instruments*. AirMagnet has a good solution for PDAs which makes the site survey easier to conduct. There are also many free downloadable solutions like NetStumbler*, MiniStumbler* (for PDAs), Kismet* (Linux), and Elixar* AirTraf* (Linux). The downside to the free 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.

Note: 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 to make sure that no additional sources of interference are present. Make a log of any activity including channel, MAC address, and signal strength.

6.2 Types of RF Interference

In general, RF interference can be broken down into four categories:

- direct interference
- indirect interference
- path interference (multi-path)
- Line of Sight (LoS) interference

6.2.1 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.

6.2.2 Indirect Interference

Indirect interference refers to devices that are not specified as 802.1, 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.

6.2.3 Path Interference

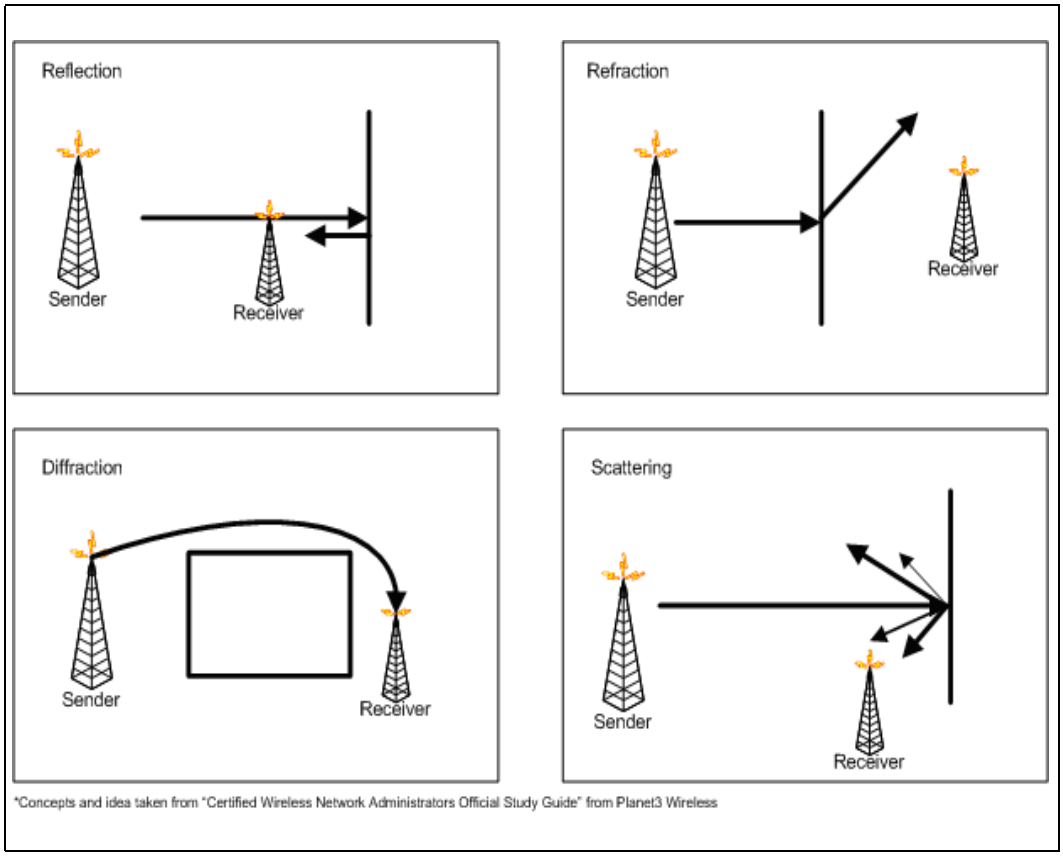
Another difficult problem in the site survey is gauging Path Interference. Path Interference comes in four categories:

- Reflection
- Refraction
- Diffraction
- Scattering.

For a full treatment of path interference, please refer to the *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 12. Interference Types



6.2.4 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.

Note: 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.

6.3 Performance Considerations

While 802.11b's maximum data rate is 11 Mbps and 802.11a and 802.11g's maximum is 54 Mbps, 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 11 Mbps to 5.5, 2, or even 1 Mbps. The lower data rates act to ensure 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 5.5 Mbps, while an 802.11a or 802.11g network will be around 27 Mbps.

6.4 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 the 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.

6.4.1 Roaming

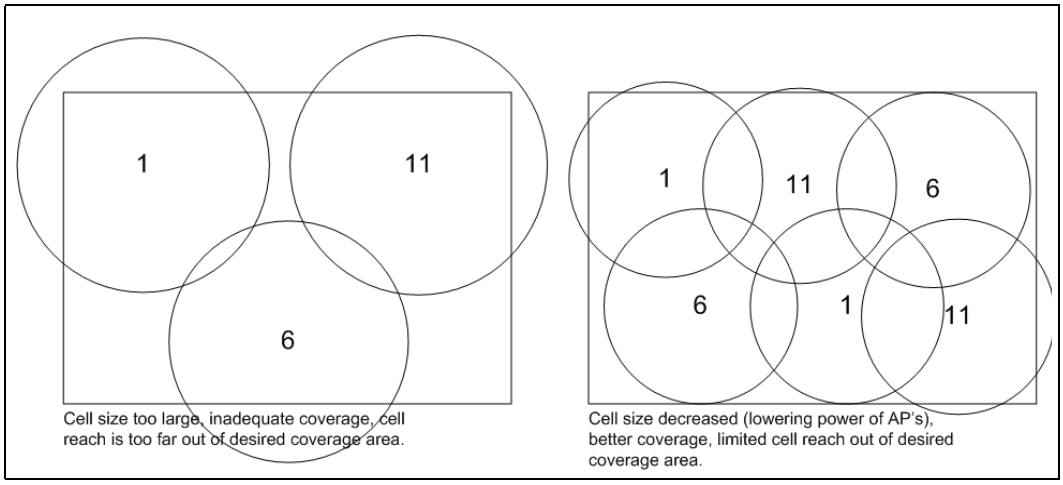
When a user moves from one area, like a conference room to the cafeteria, the APs will transfer the user’s data along maintaining the users session persistence. This is especially important with connection sensitive applications like VPNs, email, and SSL connections. In some instances it may be impractical 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. 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 were you expect users to roam. The term "flat network" implies a single subnet in which all Access Points and users are connected.

6.4.2 Access Point (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 13. AP Cell Layout for Three Channels



When implementing Access Points you must take into consideration channel layout and cell size (Figure 13). 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 13: 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.

6.4.3 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.

6.4.4 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 b/g and a/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.

Note: 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.

6.5 Choosing your Access Point (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.

6.5.1 Types of APs

Access Points come in three primary varieties:

- Small Office/Home Office (SOHO)
- Enterprise
- 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*, Colubris*, Agere*, and 2Wire* are significant players in this market segment.

A new category of AP is the Enterprise Wireless Switch. Wireless switches are known as fat devices because of the abundance of processing power and individuality that the switch possesses. Dumb APs connect to the wireless switch, which maintains client sessions and associations. The dumb APs in these configurations are simple radio devices. Companies like Aruba*, Symbol* and Extreme* 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 mobile station is detected. However, they are relatively expensive and require a lot of power and maintenance.

6.5.2 AP Features to Look For

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

6.5.2.1 RF Power should be adjustable

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

6.5.2.2 Multiple Antenna Types

APs should support a variety of antenna types and be able 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 not be able 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. See Section 13.3, “IEEE 802.11n MIMO” on page 118 for more information on new, emerging radio designs such as Multiple In, Multiple Out (MIMO).

6.5.2.3 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.

6.5.2.4 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.

6.5.2.5 Power Over Ethernet (PoE)

Power over Ethernet can make a hotspot more cost effective. 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.

6.5.2.6 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 (MS) 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.

Note: 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.

6.6 802.11a/b/g Choosing the Right Technology

In this section we'll take a look at reasons why you might want to pick one technology over the other, or, perhaps to use them simultaneously. First, given the background that we offered in the previous sections, the following statements about the technologies will help you understand the choices:

- 802.11a and 802.11g support higher data rates than 802.11b, up to 54 Mbps
- Signals transmitted in lower bands travel further than signals transmitted in higher bands. 802.11b and 802.11g function at a lower frequency, 2.4 GHz, than 802.11a, which functions in the 5 GHz band. Thus, 802.11b- and 802.11g-based communications can reach further distances.
- OFDM is a more efficient transmission means than DSSS allowing higher encodings and higher rates, thus, 802.11a and 802.11g provide higher rates, up to 54 Mbps.
- Compatibility requirements for 802.11g with 802.11b makes it so, when in the presence of 802.11b clients, 802.11g wireless communications will degrade in throughput by nearly fifty percent from the case where no "b" clients are present.
- OFDM mitigates multi-path better than DSSS making it a better technology for indoors. This means that OFDM-based technologies will reach higher rates at a given distance.
- Both 802.11g and 802.11a use the same transmission technology, OFDM, for the higher, non-802.11b rates. Thus the radio technology is the same and reusable in both designs.

6.6.1 Reasons to Use 802.11b

If your site is already implemented using 802.11b and you are happy with the level of service you provide then there is no reason for change. We'll assume in this section that you do have a reason to change/upgrade your AP and so the question is: Should you stick with 802.11b or change to support 802.11g and/or 802.11a? Pros and Cons are presented in the following sections.

6.6.1.1 802.11b Pros

- The most popular standard supported today by mobile clients
- Mature and less expensive technology

- Interoperates with 802.11g so your "b" APs will be able to support clients with this new technology

6.6.1.2 802.11b Cons

- Provides the slowest maximum data rate (11 MHz)
- Given the interoperability that "g" APs provide, b-only APs will eventually be a thing of the past posing maintenance issues
- Only three non-overlapping channels (same as 802.11g) makes it hard to deploy in complex environments
- Susceptible to multi-path interference
- Open to interference from many other commercial products that use same band such as microwave ovens, baby monitors, cordless phones, Bluetooth*-based products, etc.

6.6.2 Reasons to Use 802.11g

802.11g was developed to meet the higher speeds achieved by the 802.11a standard while maintaining compatibility with 802.11b. This meant that higher speeds could be obtained without obsoleting the investment on 802.11b equipment already done by so many. As stated before, such compatibility did not come for free. An 802.11g AP will change its operational mode to accommodate 802.11b clients the minute it detects the presence of the first client of such type. This mode of operation consists of protecting each packet sent on the wireless medium with an RTS and CTS combination message. As we discussed in the 802.11g section, this pair of guard packets adds a large overhead to the 802.11g communications but guards it from potential collisions caused by 802.11b clients which are not able to detect when "g" clients are communicating. Pros and Cons are presented in the following sections.

6.6.2.1 802.11g Pros

- Much higher data rates than 802.11b
- Supports larger number of clients than 802.11b
- Interoperates with 802.11b (this can be both a pro and a con)
- When using OFDM, it provides for better defense from multi-path interference than 802.11b

6.6.2.2 802.11g Cons

- Throughput not comparable with data rates when operating in protected (compatible) mode
- Only three non-overlapping channels (same as 802.11b) not enough for complex implementations
- Susceptible to interference from many other types of commercial products that use same band such as microwave ovens, baby monitors, cordless phones, Bluetooth-based products, etc.

6.6.3 Reasons to Use 802.11a

802.11a was designed to be faster and to avoid interference from multi-path and from other commercial products that operate in the 2.4 GHz band. Pros and Cons are presented in the following sections.

6.6.3.1 802.11a Pros

- Faster data rates than 802.11b
- More non overlapping channels (12) than 802.11b or 802.11g provide more flexibility in the layout of the network
- Offers the highest network capacity when operating at 54 Mbps over each of twelve non overlapping channels
- Better support for multimedia services (audio and video) due to higher network capacity and less chance for interference from other common RF devices
- More resilient to multi-path interference than 802.11b and non-OFDM operating 802.11g

6.6.3.2 802.11a Cons

- Does not support the more prevalent (as of today) 802.11b devices
- Shorter range requires more APs to cover the same footprint as 802.11b/g APs

6.7 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
- Choose the appropriate equipment to complement the site
- Keep in mind the unique requirements of wireless networks such as security
- Plan for the future; choose the appropriate technology

7.0 Wireless Security

This section provides an overview of the different security modes used to secure the wireless segment of a public hotspot, enterprise, and personal networks. The intent is to provide enough practical information to understand the options for protecting the wireless network and how the choice of protection affects the network (and the pocketbook) itself.

7.1 History of Wireless Security

Wireless security has improved since the original draft of 802.11. The security improvements make it possible to establish a more secure hotspot, protecting data and controlling access.

- WEP - Wired Equivalent Privacy is the original 802.11 security specification and was ratified in September 1999. As time progressed, there was a need for additional security, hence the IEEE committee worked on a new specification, 802.11i.
- WPA - A year before 802.11i was ratified the Wi-Fi Alliance decided to release an interim implementation of the current 802.11i specification called Wi-Fi Protected Access (WPA). WPA supports two flavors: enterprise (including public) and personal (SOHO). For enterprise authentication WPA supports 802.1X and RADIUS, whereas for personal authentication it uses a Pre-Shared Key (PSK). For the data encryption, WPA uses Temporal Key Integrity Protocol (TKIP) for both enterprise and personal modes. All the Wi-Fi certified hardware shipping after September 2003 was required to be WPA complaint.
- WPA2 - Wi-Fi Protected Access 2 is based on the final ratification of 802.11i, and is defined by the Wi-Fi Alliance. WPA2 and 802.11i are virtually identical. The 802.11i standard was ratified in June 2004. WPA2 supports two flavors: enterprise (including public) and personal (SOHO). WPA2 supports the same authentication framework as WPA, but has a new stronger encryption algorithm called AES (Advanced Encryption Standard) with CCMP (Counter Mode with CBC-MAC Protocol).

Table 19 below shows the major characteristics of the four security specifications, WEP, WPA, WPA2 and 802.11i.

Table 19. Wireless Security Timeline

Features	WEP	WPA	WPA2	802.11i
Timeline	September 1999	September 2003	September 2004	September 2004
Access Control	None	802.1X	802.1X	802.1X
Authentication	None	EAP	EAP	EAP
Key Size	40 bits or 104 bits	128 bits for encryption and 64 for authentication	128 bits	128 bits
Encryption Data	RC4	TKIP	AES	AES
Key Management	Static	802.1X + TKIP	802.1X + AES-CCMP	802.1X + AES-CCMP
Header Integrity	None	Michael	Michael	CBC-MAC
Data Integrity	CRC32	Michael	Michael	CBC-MAC
Pre-Authentication	No	No	No	Yes
Roaming	Limited to APs from same manufacturer	Limited to APs from same manufacturer	Limited (limited to APs from same manufacturer)	Yes

7.2 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the original authentication and encryption mechanism specified by the 802.11 standard. 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 access point.

WEP uses a secret key as a credential in the authentication phase and then to encrypt packets of data. The secret key is entered manually into the AP and by any 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 is provided through two modes of operation: open authentication and shared-key authentication. When WEP is enabled, it encrypts the messages exchanged between the mobile station and the AP over the wireless link. 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 with during transmission.

Please refer to Appendix D, “Details of Wireless Security” for further details related to WEP.

7.2.1 WEP Weakness

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; this lack makes WEP easy prey for hackers looking to uncover and exploit the secret encryption key. WEP's key distribution is manual; every user must use the same secret key. Once that key is distributed to a user community, changing it means updating every user, which is not a practical situation. This can result in the same secret key being shared for an extended period of time by a large community of users, compromising the security of the key and the network.

The WEP key is particularly vulnerable during the authentication phase. The 802.11 specification describes two authentication modes: open authentication and shared-key authentication. When using a shared key, the key used for authentication is the same as that used by WEP for packet encryption. Unfortunately, this mode of operation exposes the text used to challenge the mobile station in both clear and encrypted modes, giving a hacker enough information to crack the key. Shared-key authentication mode use is not recommended.

7.3 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 (Temporal Key Integrity Protocol) enhancements, both of which can be implemented in software and/or firmware.

For authentication, WPA supports two modes of operation: Enterprise and Personal. Enterprise mode requires a RADIUS or LDAP 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.

For data privacy, WPA uses TKIP. 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.

7.3.1 WPA Benefits

WPA offers several major benefits over WEP:

- Provides stronger security than WEP
- Allows WEP-based clients to operate in mixed-WPA/WEP networks (however this compromises security)
- Integrated in most major Operating Systems
- In most cases, existing Wi-Fi CERTIFIED* components can be upgraded to use WPA through relatively simple firmware upgrades. As a result, WPA is a good solution for providing enhanced security for the existing installed base of WLAN hardware.

7.3.2 WPA Authentication

WPA Enterprise authentication is a combination of open systems and 802.1X authentication, which uses two phases:

- The first phase uses open system authentication and indicates to the wireless client that it can send frames to the AP.
- The second phase uses 802.1X to perform a user-level authentication.

WPA Personal supports the use of pre-shared key in the environments that do not support RADIUS* implementation. With a RADIUS implementation, WPA Enterprise supports EAP authentication.

7.3.3 Key Management

With 802.1X, re-keying of unicast encryption keys is optional. With WPA, re-keying of both unicast and global encryption keys is required. The TKIP (Temporal Key Integrity Protocol) changes the unicast encryption key for every frame and each change is synchronized between the wireless client and the AP. For the global encryption key, WPA includes a facility for the AP to advertise changes to the connected wireless clients.

7.3.4 Michael

A new algorithm in WPA, known as Michael, calculates an 8-byte MIC (Message Integrity Code). The MIC field is encrypted along with the frame data and the Integrity Check Value (ICV). Michael also provides replay protection. A new frame counter in the 802.11 frame is used to prevent replay attacks.

7.3.5 Enterprise and Personal Modes for WPA

The following table lists the authentication and encryption methods used for WPA Enterprise and Personal modes:

Modes	Authentication	Encryption
Enterprise (Business, Government and Public)	802.1X/EAP	TKIP/MIC
Personal (SOHO/Personal)	PSK	TKIP/MIC

7.3.6 WPA Deployment Challenges

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

- Requires firmware upgrades to AP's. If that is not possible, then the AP itself might need to be replaced.
- The hotspots will need to support customers who have upgraded their device with WPA support and those that are still using WEP.
- As far as possible, use of a single AP broadcasting at least 2 SSIDs, each tied to a unique BSSID. This multiple VLAN feature support may not be commonly available today.
- Make the customers aware of WPA-based access availability at that location and part of the SP offering.

- Users will need to upgrade their wireless client to support 802.1X and WPA.
- Roaming with WPA will require re-authentication, and that can put limitations on seamless roaming between AP's.
- WPA does not support pre-authentication.

7.4 WPA2

WPA2 (Wi-Fi Protected Access 2) is based on the final ratification of IEEE 802.11i, and is defined by Wi-Fi Alliance. WPA2 and IEEE 802.11i are virtually identical. The IEEE 802.11i standard was ratified in June 2004. Refer to the Appendix D, “Details of Wireless Security” for additional details.

WPA2 requires the same level of authentication specification as defined for WPA. In addition, WPA2 supports much stronger key management (data encryption) standards when compared to WPA. Also, WPA2 adds support for AES and roaming and uses CCMP for header and data integrity. The AES-CCMP support is mandatory in both the 802.11i specification and WPA2. AES support is significant because it delivers the data privacy required by financial and government institutions. WPA2 supports two flavors: WPA2-enterprise and WPA2-personal (SOHO).

7.4.1 WPA2 Benefits

WPA2 benefits include:

- Provides added security over WEP and WPA
- WPA2 is backward compatible to WPA
- WPA2 provides improved encryption with AES and a high level of assurance that only authorized users can access the network
- WPA2 is able to meet government and enterprise security requirements

7.4.2 WPA2 Deployment Challenges

Some of the most important 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
- The cost of replacing existing WLAN hardware to support WPA2 can be fairly significant

7.4.3 WPA2 Mixed Mode

WPA2 includes an optional mixed-mode feature permitting the coexistence of WPA and WPA2 clients on the same SSID. WPA2 Mixed Mode is supported by Wi-Fi Alliance. This mode can be used when transitioning from WPA to WPA2. Unlike the WEP to WPA mixed mode, WPA to WPA2 mixed mode is a secure operating mode.

With WPA2 Mixed Mode, once the client selects the cipher, that cipher is used to encrypt all the unicast communications between the client and AP. This option does provide enterprise class security because it supports encryption with either TKIP or AES.

WPA2 does not allow WPA2 to WEP mixed modes due to security concerns with WEP which has been documented as a weakness.

7.4.4 Enterprise and Personal Modes for WPA2

The following table lists the authentication and encryption methods used for WPA2 Enterprise and Personal modes:

Modes	Authentication	Encryption
Enterprise (Business, Government and Public)	802.1X/EAP	AES-CCMP
Personal (SOHO/Personal)	PSK	AES-CCMP

7.4.5 Steps to Prepare for WPA/WPA2 Deployment

The following list describes the WPA/WPA2 deployment process and outlines the component requirements. This list will also prepare the technical team to implement 802.1X authentication and TKIP or AES encryption within the environment.

- Security Mechanism and Credentials

  Need to have a network security policy in place. Typically, the database is stored locally on the server, or externally, in Microsoft Active Directory, LDAP, iPlanet or Secure ID Token.

- Authentication Server and User Authentication Database

  Typically a RADIUS server is used. Check to see if the server you are about to deploy supports the EAP types and works with user credentials database.

- Client Operating Systems and Supplicants

  The selection of client OS, authentication server and EAP types are all interdependent on each other and should be considered in parallel when selecting a supplicant. The Zero Config in Windows XP service pack 2 supports some of the industry standard security parameters. If that does not support your needs, then you may look for an aftermarket supplicant.

- EAP Types

  The EAP type used needs to be supported by the authentication server and the user database. It should also be supported by the client OS and the supplicant. Some examples of EAP types: TLS, TTLS, MD5, PEAP, and LEAP.

- Access Points and Client Network Interface Cards

  You will need to confirm that all APs and client devices to be used in the deployment are WPA or WPA2 certified.

7.5 Methods of Connecting to Secure Hotspots

To connect to a secure hotspot, in most cases a client must be manually configured or provisioned by a user, with the security parameters provided by the service provider or captured from their Web site. This process is not only time consuming, but it could also require multiple tries to successfully connect to the secure site. It also requires the user to have the client configured prior to arriving at the hotspot. With the introduction of Wireless Provisioning Services (WPS) this process is simplified and mostly automated.

7.5.1 WPS Technology

WPS is designed to simplify, automate, and standardize initial sign-up and subscription renewal, so that the user does not have to perform a different set of steps for each wireless provider to which they want to connect.

Wireless Provisioning Services (WPS), which is included in Service Pack 2 (SP2) for Windows XP, is intended to make the wireless connectivity easier and more secure. This new technology for public hotspots provides automatic provisioning and sign-up capabilities to improve user experience and enhance security for mobile Windows customers. WPS builds upon Microsoft's existing support for wireless technology and connectivity in Windows* such as wireless auto configuration, connection wizards, and wireless security features such as Protected Extensible Authentication (PEAP) and Wi-Fi Protected Access (WPA) in Windows XP. WPS enables a wireless client computer running Windows XP Home Edition, Professional or Tablet PC Edition with Service Pack 2 (SP2), to connect and download network configuration information from a provisioning server.

A provisioning server is a computer running Windows 2003 with SP1 and running IIS or a third-party web server that maintains a collection of information files that are used to configure client computers during the connection and account sign-up process. After the client running Windows XP with SP2 has obtained network configuration information, it automatically configures the connection to your network.

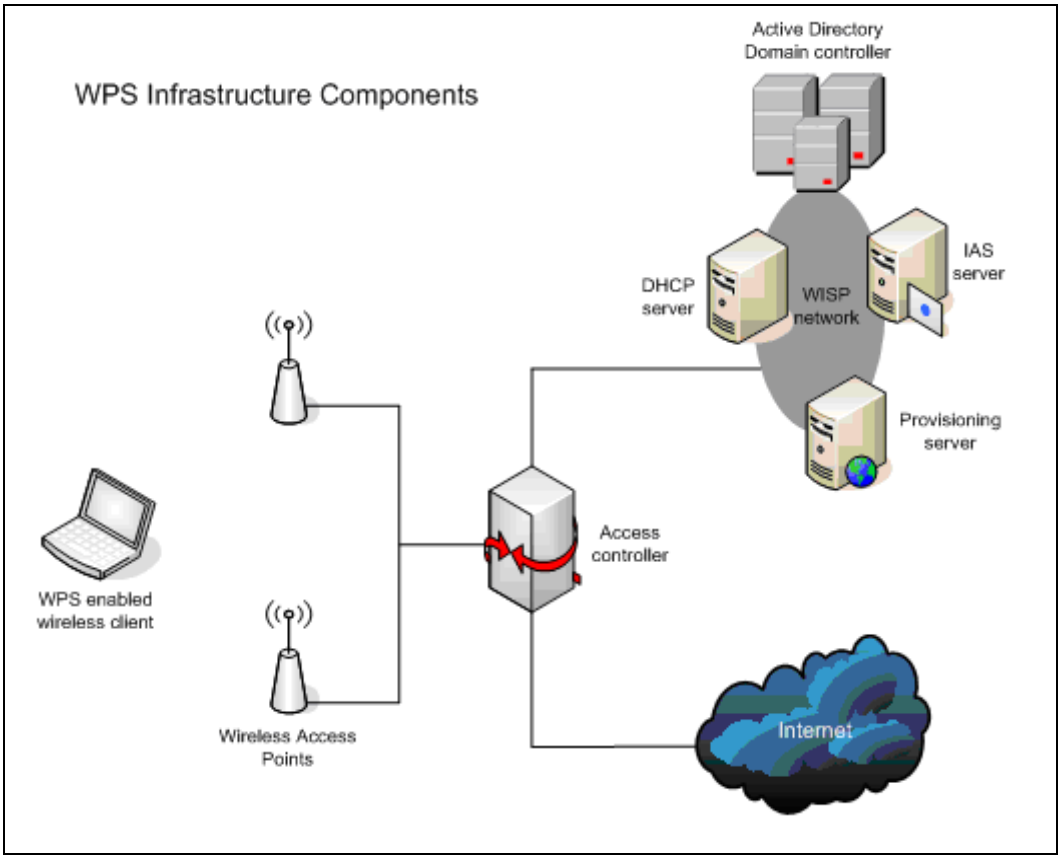
When wireless clients connect to a public WLAN, either they are already a customer of the WISP or they are not. If they are not, they must perform the following steps:

1. Configure network settings to connect to the WISP network.
2. Provide identification and payment information to the WISP.
3. Obtain credentials to connect to the network.
4. Reconnect to the WISP network after valid credentials have been obtained.

7.5.1.1 WPS Infrastructure Components

- WPS enabled wireless clients
- Wireless access points (APs) with the following required features:
  - — Support either virtual local area networks (VLANs) or Internet Protocol (IP) filtering
  - — Support for 802.1X authentication
  - — Support for Wi-Fi Protected Access (WPA) is preferred
  - — Support for RADIUS authentication and accounting
- Access controller
- Provisioning Server
- Active Directory - directory service domain controller
- Internet Authentication Service (IAS) server
- Dynamic Host Configuration Protocol (DHCP) server

Figure 14. WPS Infrastructure Components



7.5.1.2 Additional Information about Deploying WPS Technology

Additional information on WPS may be found at the Microsoft Web site: http://www.microsoft.com.

7.6 Secure Wireless Hotspot Recommendations

Below is a list of security recommendations for public hotspots. When implemented, these recommendations address many of the security issues described in this chapter. Deploying a secure hotspot requires more than simply implementing a secure wireless link. For instance, if someone can physically access an AP, they can bypass over-the-air encryption methods. Table 20 considers many aspects of making a hotspot secure:

Table 20. Recommendations to Secure Public Hotspots

Category	Recommendations
Access	Deploy an open WLAN in addition to the WLAN with security features listed below. Users can receive instructions on how to access the secure WLAN by first accessing the open WLAN.
Access	Select a secure WLAN SSID different from the SSID used by the open WLAN. The secure WLAN SSID should be easy for users to identify it as the hotspot's secure network.
Client	For ease of configuration, the hotspot should offer a client manager and/or profiles. When a user imports a hotspot profile, it makes configuration of the client managers easy.
Client	The client manager software or profile download should have all network configurations preset (e.g. SSID, certificates, EAP-type, key handling method, etc.).
Client	Provide the users with instructions on how to download and configure settings to access the secure network. These instructions can be provided through the open network.
Identification	Users and visitors of the hotspot should easily identify the security features of the hotspot. Signs displayed at the hotspot and information provided on the open network's web pages will help users know the benefits of connecting to the secure network.
Physical	Physically secure the network equipment (AP's, routers, switches, etc.) to limit access to the equipment by non-authorized persons. Consider how the network can be compromised physically including cabling and protect against those types of physical attacks.
Encryption	Use derived 128-bit minimum, or the highest allowed by law, encryption keys for over-the-air data. Pre-shared keys should not be used.
Isolation	Provide client isolation by blocking peer-to-peer communications through the hotspot network equipment. Blocking direct peer-to-peer communications prevents common ARP and route poisoning attacks. This feature should also be implemented on the open network.
Authentication	The hotspot's secure WLAN authentication system should support mutual authentication, meaning the user's client manager needs to validate the network by checking the server certificate. By checking the server certificate, the user is assured of connecting to the desired network.
Authentication	The network server certificates should be widely accepted certificates (e.g. VeriSign*) for ease of client recognition and authentication. When the network server certificate is accepted in a trusted chain, it is easier for the user to configure.

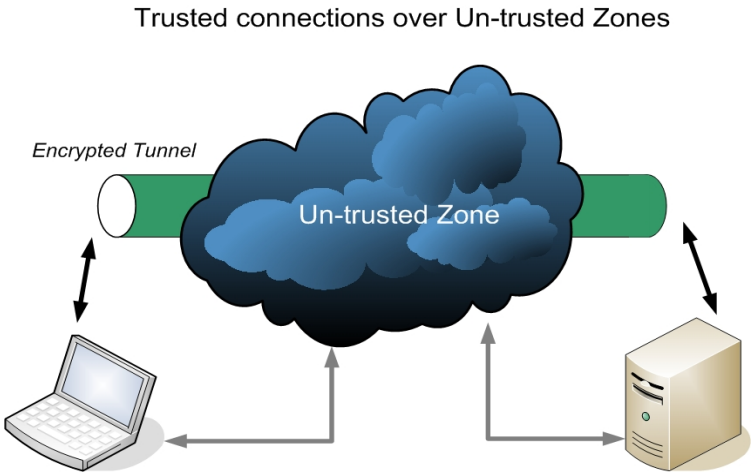
7.7 Protection Against Well-known Attacks

As wireless Internet connectivity becomes more widely available, awareness is growing of the security risks inherent with public networks. Every time you use a wireless network, you are sharing it with strangers, some with dubious intentions. This section explains trusted and un-trusted security zones and then describes some common attacks on public networks and the countermeasures to them. For each area of concern, please look for additional information online and from other resources, as security information changes constantly.

7.7.1 Trusted and Un-trusted Zones

The difference between privately managed networks and free-zone networks such as the Internet is similar to the difference between trusted and un-trusted computing zones. With public hotspots and virtual private network (VPN) connections, trusted connections are run over un-trusted networks, blurring the line between trusted and un-trusted zones. Authenticating to resources with encryption, creating VPNs, and other technologies are attempts to create trusted connections over these un-trusted zones.

Figure 15. Establishing Trusted Connections over Un-Trusted Zones



7.7.2 Attacks and Countermeasures

Network attacks can be passive or active. Passive listening in itself may not be considered an attack, however, passive listening can be used to capture and store network traffic for decryption. Check the local authority for specifics in each region. Active attacks, such as a man-in-the-middle scenario or the archiving of a user's mail transfers, are aggressive and can be presumed to be done with bad intention.

7.7.3 Snooping and Sniffing

Packet analysis is the capture and observation of network traffic. Network adapters are set in a mode that captures packets designated for other physical hardware addresses. In a public wireless network, wireless packet analyzers view each system request for information as well as the returning data. Capture devices can view outgoing and incoming email and detect Web site visitations and instant messaging programs that are not using encryption.

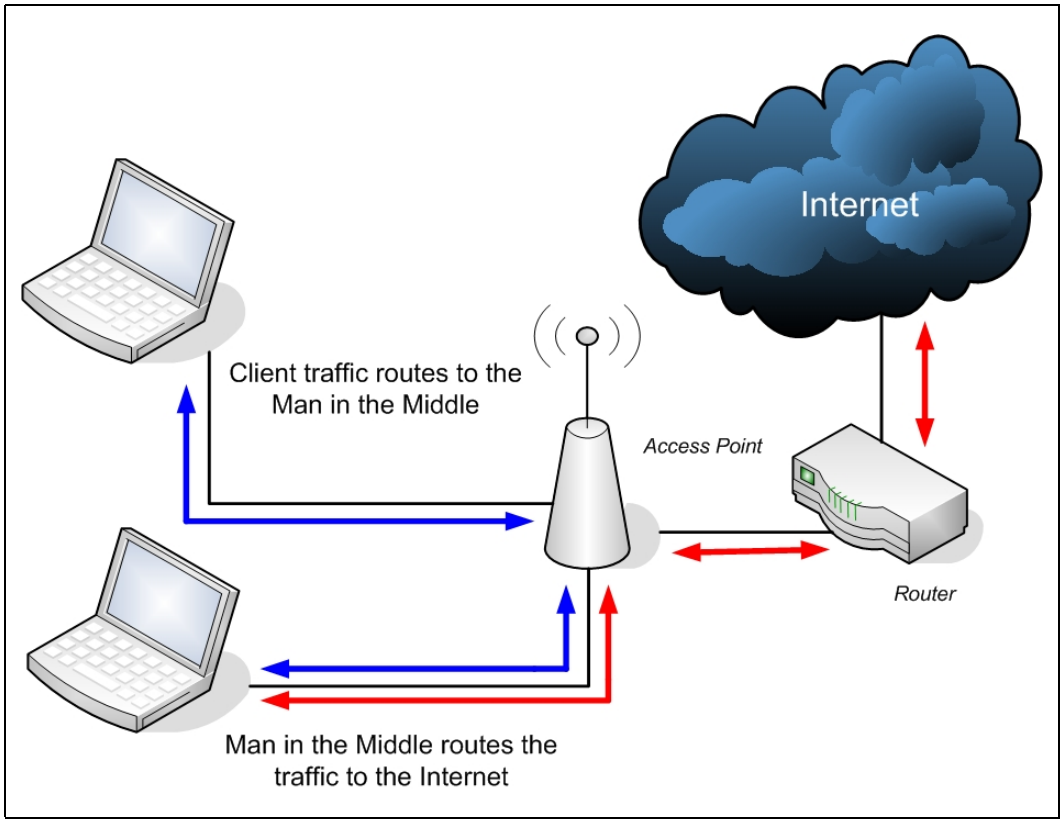
The countermeasure for snooping attacks is encryption. Using more than one encryption technology simultaneous is often easily done. Wireless link encryption techniques consist of 802.11i, WPA, WPA2 and the no longer recommended original 802.11 WEP solution. For more information on these encryption technologies, please refer to the Appendix D, “802.11i”. Higher layer security options include Internet Protocol Security (IPSec) and Secure Socket Layer (SSL). Whichever encryption is used, unique keys for every user or application pairing and key rotation techniques is required. Pre-shared key techniques are not recommended for public usage deployments.

Detecting passive capturing or archived data attacks is very difficult. It is best to implement encryption pro-actively to prevent this type of attack.

7.7.4 Man-in-Middle

In a man-in-the-middle (MiM) attack, an attacker proxies or routes an unknowing user's traffic through an attacking machine. Rogue Access Points, also know as evil twin networks, mimic the wireless name of another network, potentially causing users to switch between the two. By handling all of a user's traffic, the attacker has access to usernames, passwords and other credentials, unless the victim is using end-to-end encryption (VPN or SSL). In fact, without mutual authentication methods, even higher level protocols are potentially vulnerable to MiM attacks, including some one-way authentication VPN methods. One method is to provide DHCP serving on a public network and first hop routing. Simply changing the IP address of a system to the same as the default gateway will result in some systems updating their Address Resolution Protocol or hardware address tables to point to the MiM machine.

Figure 16. Man-in-the-Middle Attack



In the local physical network, disabling peer to peer communication between all bridged devices and out to the external routing device will eliminate MiM attacks. Some wireless and wired access devices offer this capability under various feature names. Deploying these features on access points is not enough to protect a multiple access point network however, as traffic can still be transferred between hosts if each device is connected to a separate access point connected via a layer 2 bridge such as an Ethernet switch, a requirement for proper 802.11 wireless access point roaming. In these cases, additional countermeasures are required, though such features are not available on all equipment. Some Ethernet switch hardware offers the ability to screen Address Resolutions

Protocol (ARP) packets and only allow ARP responses to certain hardware address to resolve, when static addresses are registered or a dynamic registration was previously found on another switch port. Additional research needs to be done by both standards bodies and Internet service providers into how to counteract potential MiM attacks. As in other areas of security concern, please look for the latest information available online and in other resources to address these concerns for your networks and to stay aware of new developments.

MiM attacks are detected by scanning for rogue access points, with either network-based or host-based detection tools.

7.7.5 Denial of Service

One of the simplest attacks to perform is the denial of service (DoS). DoS attacks can exist in the radio spectrum on which wireless systems operate or in higher network-protocol-based layers. Updates and patches can solve DoS attacks on software. When the wireless spectrum is attacked, the problem can only be solved by removing or shielding the noise source. Various metallic objects or paints can be used in the construction of buildings to add radio shielding and make these types of attacks more difficult. However, these attacks are often difficult to prevent. Detecting denial of service attacks may require the use of spectrum analyzers and protocol analyzers or tools with specific DoS detection capabilities. The hotspot operator can also monitor the network activity remotely and trigger alarms or notifications if the activity goes above or below certain thresholds.

7.7.6 Cryptography Attacks

Cryptography attacks generally involve finding weaknesses in security protocol implementations, which dramatically reduces the key space needed to discover the data encryption key in use for a particular session. This is done either in real time or on archived information. A well known example of this is the concerns with the original 802.11 encryption technique-WEP. The later WPA TKIP data encryption technology attempts to overcome these weaknesses. WPA2 and 802.11i embrace a newer encryption technique known as AES-CCMP, replacing WEP and TKIP entirely. These attacks can be counteracted by using the latest trusted encryption implementation, ceasing the use of implementations when they are no longer considered trusted or have been publicly broken.

Dictionary-based attacks compute lists of common passwords and compare enciphered packets of known values (commonly authentication protocol handshake packets) to determine session keys. This is done in real time or on archived data attacks. This is the basis of the cautions against using simple passwords for WPA and WPA2 pre-shared key solutions. Pick complex passwords with a minimum of 10 characters.

As with passive listening attacks, passive key-determination attacks are usually difficult to detect. The proactive use of trusted encryption is the recommended way to counter these attacks.

7.7.7 Detection Tools

Various tools are available to detect and monitor wireless networks. A network capture system is a major requirement both for troubleshooting and for detecting suspicious network activity. Linux-based operating systems usually offer the most flexibility for the lowest price, with the chance of higher configuration or development requirements. On Linux* or Windows*, a wireless access point detector and a packet capture program are recommended. The free Windows-based network discovery tool NetStumbler* is a great option to start detecting what access points are operating in a given environment, if these networks are open for association. The commercial AirMagnet* product is similar, but offers much more advanced detection of networks not broadcasting wireless

identifiers and even offers system managers the ability to detect rogue (unauthorized) access points. Hardware devices, including access points for hotspot use, sometimes also offer rogue access point detection.

System managers should configure network monitoring systems using protocols such as SNMP to detect hardware, user and security issues. System managers should also be alerted when suspect or critical events occur so they can maintain a healthy system. In addition to monitoring availability when implementing security methods, always research what options exist for monitoring security-related concerns, such as failed authentication attempts in a WPA network.

Wireless or network based intrusion detection devices are also available to detect known signatures of attacks types. These can potentially limit in real time the network resources access of suspect network hosts, either over the air or on the wired backhaul network. A popular open source tool available for network IDS is Snort*. Host-based software can provide additional IDS capabilities on the wireless clients.

7.8 Summary

Public access networks give unscrupulous individuals an opportunity to attack other users. Awareness of these types of attacks and what can be done about them is continually evolving. Continued research into the uses, strengths and weaknesses of any system in active use or considered for deployment is of the utmost importance. Wireless security has continued to improve over the life of 802.11. While WEP provides some benefits to securing the client's wireless link, WPA and WPA2 provide a much improved security model. If you are considering implementing security at a public WLAN (hotspot) then it is strongly recommend that you look at deploying WPA or WPA2. Networks utilizing advanced encryption technologies such as WPA2 offer mutual authentication methods for both the clients and the network. Once authenticated and passing traffic, additional countermeasures to disable communications between authenticated peers on a network can provide additional protection. In addition, IDS and packet analysis offer ways to detect and isolate security issues.

8.0 Managing a Hotspot

Whether your hotspot has one or a hundred APs, proper hotspot management ensures a quality end-user experience. Managing hotspots effectively requires planning and forethought in the design and the establishment of procedures for maintaining the hotspot. The operational costs of maintaining your hotspot, if the hotspot is not designed and implemented with maintenance and management controls, can be overwhelming. Ineffective hotspot management leads to poor response to issues affecting customers while non-scalable designs can limit growth, both of which impact the success of your venture.

Compounding the problem is the growing feeling among consumers that 802.11connectivity 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.

Hotspot design should include a remote management capability, regular monitoring, and direct access to equipment. In addition to performing basic management, a strategy to rollout upgrades for bug fixes and new technologies and capabilities must be established. The primary goal of any hotspot provider is to ensure that the site is up and running at all times. Its amazing how often we visit a hotspot that is not in service and the service provider is unaware.

8.1 Common Protocols

Before digging into the specific methods and tools used to manage a hotspot (or any other network element for that matter) a brief overview of the specific protocols that are commonly used is in order. While these are just a few of the protocols available, they tend to be the most prolific. As with many other application protocols, modifications can be made by the implementer to suit their own needs.

8.1.1 Internet Control Message Protocol (ICMP)

ICMP packets are one of the fundamental methods of checking to see if a network component is working or not. They also indicate that the devices you are communicating with respond at the IP layer. Two key applications built around ICMP are: Ping and TraceRoute. ICMP neither utilizes nor tests the TCP layer, commonly used by applications.

8.1.2 Simple Network Management Protocol (SNMP)

SNMP is used to provide a common management interface of devices that are on a TCP/ IP network (both UDP and TCP.) Elements of each device are defined by a database of definitions called a MIB (Management Information Base.) The MIB is used, by a management client, to determine what object classes/identifiers are what in the device (router or access point for example) that is being managed. TCP/UDP ports 161 and 162 are used for passing SNMP traffic. Port 162 is used for devices to send traps back to a central management location and are typically generated by events that occurred within the equipment.

8.1.3 Hyper Text Transport Protocol (HTTP)

HTTP commonly utilizes TCP port 80. Variants, such as HTTPS utilize port 443. While these are the most common of ports for these protocols, it is important to realize that these ports can and often do get changed to a custom setting. Network equipment management interfaces are making a

transition to web-based configuration, some of which (Linksys* for example) use port 80. However, Cisco's* default for much of their Aironet* family of access points is set to port 2002 by default.

As shown above, there are several different protocols which are utilized in network management. It is imperative the hotspot designer understand which protocols are used, which ports are used for the protocols, and what elements within the hotspot and the management site that would be affected by these decisions. For example, will your proxy Web-server pass traffic for ports other than 80 and 443? By default, most enterprise proxy / firewalls will not.

8.2 What is Manageable?

Various elements of a hotspot can be managed and others, unfortunately, cannot. These elements include the network components, the environment in which the hotspot exists, and the user experience itself. It is not sufficient to install a hotspot and think it will survive on its own without managing the specifics.

8.2.1 Environment

The hotspot environment is the most important and most difficult variable to manage, primarily due to the fact that the service provider generally doesn't control the space in which the hotspot is installed. The environment can be a hotel, a coffee shop, an airport, or an office. Typically the hotspot service provider will work an agreement with the property owner for the installation of the equipment and lines. However, the environment is checked during the pre-installation and installation visits. Hotspots can't take on the model of 'install and forget' for several important reasons:

- Things change in the environment knowingly or unknowingly.
- Addition of other wireless equipment may take place, such as: cordless phones, point-of-sale terminals, wireless microphones.
- The wireless world doesn't stop at the front door. New service providers could have installed their own hotspot just across the street, next door, or worse, in the same facility.

It is incumbent to the service provider that they keep a good dialog open with the property owner and visit the location periodically to ensure the base-line check used to design the hotspot is still accurate. Identify anything that has changed and ensure the changes don't affect your users' experience.

Unfortunately, there is no automatic method of doing this short of installing spectrum analyzers and other monitoring devices throughout the hotspot environment. Human interaction is required to control this important element.

8.2.2 Access Points - Passive with Proactive Response to Problems

Access Points can be managed in several ways, including by remote and automatic means, although there is a limit to the extent of coverage. The basic tools used for managing APs are the monitoring and configuration interfaces such as HTTP and SNMP. SNMP is the most common protocol used to monitor and trap events both critical and normal. HTTP is commonly used for upgrading and configuring the APs. Other protocols can be used (tftp, ftp, etc) to transfer configuration files.

While it is important for the service provider to have access to the Access Points for management reasons, it is more important to keep the general public from gaining access. There are several ways to make the management secure. Since the AP is primarily a bridge device, the management port for the AP can be on a separate subnet (assign it a different network from the users.) The management network would be accessible only to the service provider's service center. Proper network design will be required especially if the APs are behind a NAT router.

Monitoring of the APs, then, can be done via the maintenance network. What this may not cover, unfortunately, is the health of the radio (e.g. what is happening on the airwaves). A hotspot with little usage may look exactly the same, to the monitoring equipment, as a hotspot with a failure in the AP's radio.

8.2.3 Network Switches and Routers

Nearly all network components sold today are manageable. Managing the routers, servers, gateways, DSL modems, etc. at hotspots is essential to maintaining a reliable network. In large complex hotspots, there may be several Layer 2 switches, APs, a couple of routers plus local servers for localized content (an airport, for example.) It is important to have both passive monitoring and remote access to each of these components that will allow changes and upgrades.

8.2.4 User Performance

User performance is a manageable entity although difficult to manage if the service provider doesn't maintain and check their network. Exactly what is user performance? This can be anything from bit-rate to services used while logged in, to being able to log in. Remote monitoring of bandwidth may be done via several different means; the most common is checking round trip ICMP packet transit times to see if there are any variances. The ability to test other factors of user performance gets quite complicated. The bottom line is that a service provider either has to pro-actively check, from time to time, the performance of their hotspots or rely on a frustrated user to call and report a problem.

8.3 What is Not Manageable?

Several conditions of a hotspot are not manageable. Generally speaking, items that are not manageable (as defined above) are items or conditions that are out of the service provider control altogether. The biggest item is wireless interference.

8.3.1 Interference - Noise

Interference caused by noise is, for this discussion, interference from other non-802.11 sources, whether they are in the ISM band or outside the ISM band. Sources of this type of noise can range from a non-DSS spread spectrum radio (frequency hopped for example), wireless phones, microwave ovens, fluorescent lamps, and many other items. Since it is considered 'noise' from the 802.11 perspective, identifying the source and overcoming the source can be difficult. Whether or not the noise is random in occurrence or continuous can make the matter an order of magnitude worse.

The key to overcoming this type of interference is to have the ability to monitor the environment over a short period of time where the problem is evident. Knowing how to identify 'noise' and how it relates to the usability and/or performance of the hotspot is important. For example, does the rate

of collisions or packet retries go up? What counters and other monitoring elements of the existing equipment will provide some sort of hint that there is a problem? These are the key items that must be monitored.

Usually when there is significant interference from noise, you will see many packet retries, and possibly even CRC errors. Make sure, as a service provider, you have the ability to measure these key factors.

8.3.2 Interference - On-Channel

Since all other forms of interference are covered as noise, what's left is considered un-wanted interference from another 802.11 Wi-Fi device. This could be a rogue AP, client-to-client peer discussion, etc. More than likely, the source will be from outside the environment the service provider has covered. If the source of the interference happens to be using most of the theoretical time slices available to a channel, the user performance can degrade significantly because it is avoiding collisions. Furthermore, if you have a 802.11g environment and a single 802.11b radio enters into the equation, your performance will be reduced quite noticeably. Channel reuse becomes very important at this point. Inevitably there will be another 802.11 device sharing the channel your APs are on. Monitoring the channels will provide changes to the environment.

8.4 Management Tools Available

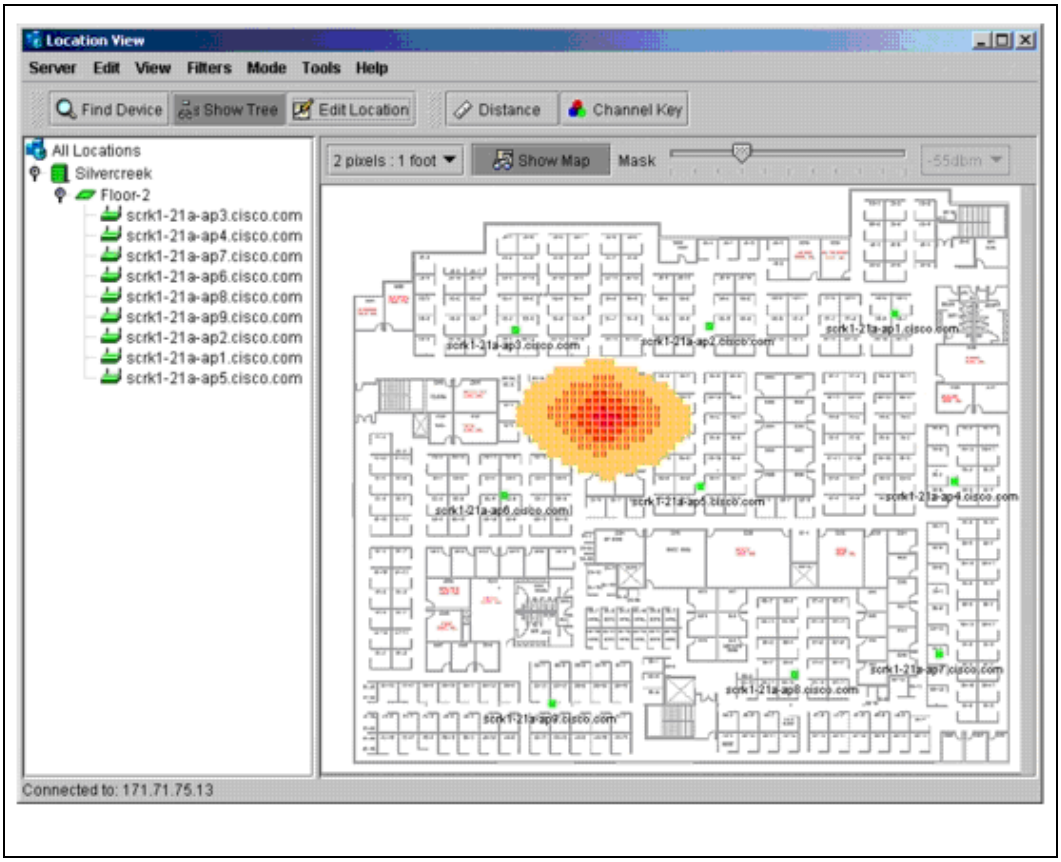
There are several management tools available to hotspot providers. These can be considered anything from a fully integrated interface showing the hotspot in map form or a simple monitoring application that consistently checks the components for the hotspot. The examples discussed are in no way a complete list of tools, but a broad range of what's available.

8.4.1 Cisco* SWAN

The Cisco* Structured Wireless-Aware Network (SWAN) is an enterprise solution for managing and monitoring wireless networks, which is quite extensive in its capabilities. Two key components of Cisco* SWAN are the CiscoWorks Wireless LAN Solution Engine (WLSE) and an IEEE 802.1X authentication server, which provides management and security functionality for wireless networks.

Using Cisco* SWAN, the characterization of the hotspot is entered into the tool. The database then builds a relationship between each of the APs so that if there is an interfering signal, it can be pin-pointed as shown in Figure 17. Furthermore, any environment changes can be captured as SNMP traps. Events within the equipment are also captured. While it was designed for large enterprise deployments, this tool would work equally well for airport hotspots.

Figure 17. Cisco* SWAN WLSE Screen Shot



8.4.2 Multi-router Traffic Grapher

Multi-Router Traffic Grapher (MRTG) is an open-source utility which utilizes SNMP to scan a network component then graph the information in a historical manner. This can be used for monitoring anything that provides data; from current throughput of an interface, number of associated clients on a access point, memory allocation in an access server, etc. It is also used to gather historical data in order to determine network requirements, such as the hotspots' back-haul connection. An example of a MRTG log is shown in Figure 18:

Figure 18. MRTG Log Example

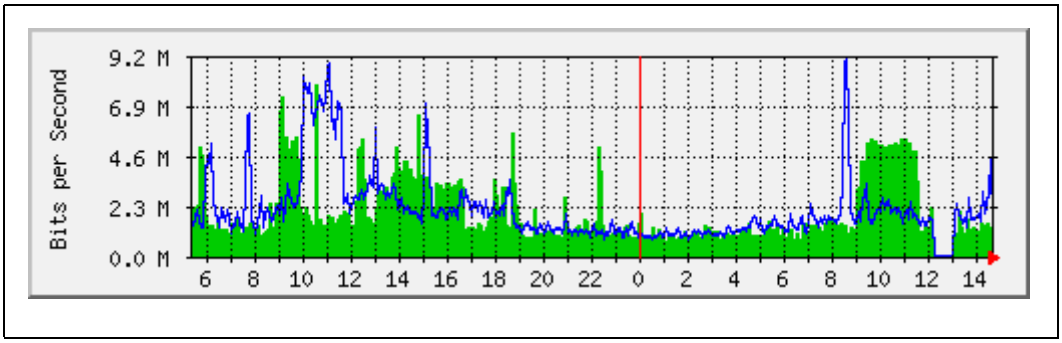
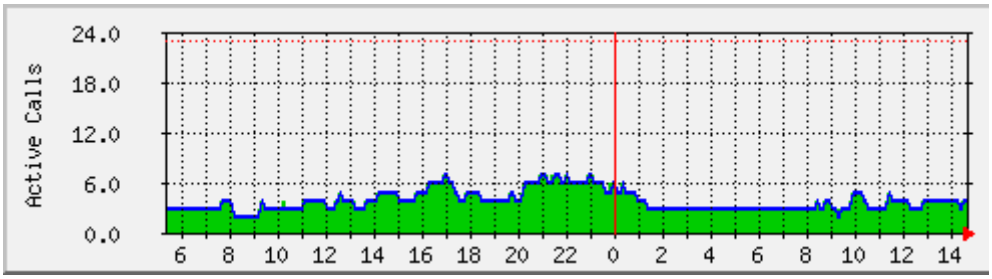


Figure 19 below shows the number of active calls over a period of time. This can easily show the number of associated clients. See http://www.mrtg.org for more details.

Figure 19. MRTG Active Calls Example



8.4.3 WhatsUp Gold* (WUG)

WhatsUp Gold* (WUG) is a product offered by Ipswitch, Inc*. This is a very capable, proactive, monitoring system that will repeatedly check your network, using selectable protocols, and report if there are problems. It also keeps a log file over time. Not only can WUG monitor the protocols, it can also monitor services. It can be programmed to look for specific responses to a Web page and act upon changes/variances. The actions include email, paging, for one or groups of people.

It also includes a toolset for testing the services in an ad-hoc manner. A nice, graphical map is easily constructed showing your network layout. Green is good, red is bad. See http://www.ipswitch.com for more details.

8.4.4 Passive 802.11 Remote Monitoring Devices

Several companies are selling passive monitoring devices for hotspots. These, in essence, are remote protocol analyzers that scan and capture all of the channels, collect the data, and report back to a central user console. This allows service providers to remotely monitor the activity, from a wireless perspective, the environment, users, and activity. A tool such as this would be crucial in problematic hotspots.

8.5 Summary

We have looked at some of the protocols which can be used for managing equipment in a hotspot as well as some tools available on the market to monitor the hotspot. There are two key decisions, regrading hotspot management that a service provider must make: what to design for and what to look for.

In designing a hotspot, there are many different variables that must be considered. To properly manage a hotspot the hotspot must be properly designed. In considering the capabilities of each component the designer needs to ensure the network will support the protocols required, through the network.

Whatever the tool is, the service provider needs to constantly monitor and manage their hotspots for key items so that problems can be identified. Network component outages are at the top of the list of concerns. Performance statistics, trends and all SNMP traps follow closely behind. Knowing 'when' and 'what' will allow you to troubleshoot and resolve problems in a timely manner.

9.0 Enterprise Applications

Enterprise business users make up a significant source of recurring revenue for hotspots. In addition, business class users are the most demanding on a wireless infrastructure due to their use of solutions 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 batch applications.

9.1 VPN and Security Applications

The VPN is the primary application for the business user, allowing them to remotely use network resources from their enterprise networks 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 Zone Labs* ZoneAlarm*, or Internet Security Systems (ISS) BlackICE*. 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 as harmless are seen as possible intrusions on 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.

9.1.1 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.

9.1.2 L2TP

Layer 2 Tunneling Protocol (L2TP) 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 in the next section.

9.1.3 IPSEC/ESP

IP Security Protocol (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).

9.1.4 Shiva* Secure Technology

Shiva Secure Technology (SST) uses a proprietary protocol. 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.

9.2 Real-time Applications

In today's business and personal computing environments, batch applications have given way to a greater 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 Protocol (RDP) has been popularized to the extent that it is now included in all new versions of Windows 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.

9.2.1 MSN* Messenger/Windows* Messenger (WM)

MSN* Messenger/Windows* Messenger is an application that utilizes many ports and functions. Windows Messenger primarily uses the Session Initiation Protocol (SIP) 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.

9.2.1.1 Reference Articles

Microsoft* TechNet articles. For details, refer to http://www.microsoft.com/technet and search for "Windows Messenger".

Internet Engineering Task Force (IETF) RFC 2543, SIP: Session Initiation Protocol. For details, refer to http://www.ietf.org/rfc.

9.2.2 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 the following:

- connecting a Web cam via TCP Port 5100
- File Transfer and File Sharing via HTTP TCP Port 80
- Voice Chat via TCP/UDP Ports 5000-5010

9.2.2.1 Reference Articles

Yahoo* Messenger Help article. For details, refer to http://help.yahoo.com and search for "Information for Network Security Administrators".

9.2.3 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.

9.2.4 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.

9.2.5 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.

9.2.6 Other Common Protocols

- 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

9.3 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.

9.4 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.

10.0 Billing

There are many billing models (including not charging for the service): it is not the intention of this guide 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.

10.1 Some Billing Models

Billing models come in many shapes and sizes. For the purpose of this guide, they are bundled into two large categories: 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.

10.1.1 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.

10.1.2 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 for 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. 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.

Note: When implementing a custom solution, ensure the connection detection algorithm uses a Layer 2 protocol, such as ARP, to avoid problems.

11.0 Common Infrastructure and Applications Issues

This section highlights some of the typical issues that can cause problems at public hotspots. In some cases, these issues can be addressed pro-actively 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.

11.1 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, how to launch the browser or network client, and describe potential problem areas such as those listed in the subsequent sections.

Note: 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.

11.2 Browser Issues

11.2.1 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.

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

11.2.2 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).

11.2.3 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."

11.3 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.

11.4 IP Addresses

11.4.1 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.

11.4.2 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.

11.4.3 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.

11.5 Ethernet Packet Problems

11.5.1 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. Not all cards with the "automatic" setting correctly set the 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, modifications in the NIC driver configuration via the operating system interface may be required. To reduce the potential for this problem, APs in public hotspots should be configured for long preamble.

11.5.2 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.

11.6 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.

11.7 Geographic Issues

While the 802.11 standard is universally 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 U.S. 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 ensure 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 U.S. and one that a U.S. 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.

Note: 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.

11.8 Non-Windows Operating Systems and the Wi-Fi Hotspot

The 802.11 wireless and TCP/IP network protocol standards function independently of platforms, operating systems and network devices. TCP packets are TCP packets, whether in a Unix*-based system, a BSD*-based system or a Windows-based system. Wireless hotspots are generally not specific to any operating system or platform. However, implementation decisions made during deployment can affect non-Windows operating system in unexpected ways, so these environments should be tested periodically for compatibility. With the great variety of operating environments now supported on mobile computers, maintaining some awareness of and testing compatibility for non-Windows operating systems is recommended, as is periodic testing of each aspect of compatibility detailed in the sections below.

11.8.1 What Hardware Aupport is available for Mobile Systems?

Most, if not all, modern operating systems support wireless network adapters to some extent, using various client managers and hardware support. For Linux, a popular Linux distribution that is entirely CD-ROM or DVD-ROM bootable is Knoppix*. For a quick look into Linux to test a hotspot's Linux compatibility, Knoppix is nearly ideal. Wireless component support has been available for many years for PC-based BSD variants.

11.8.2 Browsers and HTML

Web browsers in non-Windows operating systems vary considerably, and software distributors offer various browsers for use. One concern of hotspots is browser compatibility with authentication scripts, popup dialogs and other HTML or browser script code. While the risk of such incompatibility is low, we recommended periodic compatibility testing of browsers, font rendering, etc. Also, do not implement Windows-specific (Internet Explorer*) features that are not supported in other browsers.

11.8.3 Less Common Authentication Methods

Some providers use less common authentication protocols to access service provider networks. These include proprietary client manager applications, the Point-to-Point over Ethernet (PPPoE) protocol, Extensible Authentication Protocol with Message Digest 5 (EAP/MD5), Point to Point Tunneling Protocol (PPTP) and Virtual Private Networks (VPNs). These protocols may present problems to operating systems not based on Windows. Binary applications compiled for the Windows environment naturally do not work on non-Windows operating system environments. In these cases, an alternative standards-based option should be present to ensure compatibility. Authentication with additional methods such as PPPoE, PPTP, EAP/MD5 and others is available

on many non-Windows operating systems, although this may require a higher level of user expertise to configure and use. Validating and configuration process documentation that details such procedures for various operating system environments should be made available to customers.

11.8.4 Security Deployment Considerations

Security connection requirements present an area of concern regarding supportability and testing for non-Windows clients. For 802.1X based authentication and security methods (such as WPA), a client supplicant is required to arbitrate link authentication, and driver support must exist for the supplicant to tie into. While this support is now common in Linux, clients need installation and testing with secured hotspot configurations to support other non-Windows systems.

PPTP uses a Microsoft* protocol for Windows client VPN. This VPN can exclude some non-Windows clients. IPSec or SSL based VPN systems offer better support for non-Windows clients. In each case, non-Windows operating systems should be integrated into the design, testing and validation cycle of VPN deployments.

Dual capability hotspots, which support all clients on the unencrypted network and selected operating systems on the secured network, may offer the best support compromise.

12.0 Hotspot Blueprints

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 the purpose of illustration. See Section 2.3, “Understanding the Hotspot Environment” on page 16 for more details about 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 21 shows some of the characteristics of the hotspots:

Table 21. Hotspot Characteristics

Features	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
Special Considerations	Neighbor businesses can also implement hotspots which create RF interference. Use of microwave ovens creates RF interference. Mixture of power users and unsophisticated users	Usage bursts - from 10 to 500 users in 30 seconds or less. 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. Convention Center administration personnel should be on separate WLAN. Many users will use VPN connections to the same enterprise network. At trade shows, other WLANs might be implemented for purpose of demonstrations. Many power users

12.1 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 requirements.
   - — User Requirements
   - — Service Provider Requirements
   - — Physical Environment Requirements
   - — 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 stakeholders 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.

12.2 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 categories shown in the following sections.

12.2.1 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. These requirements include:

- 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

12.2.2 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 customers. For this reason we have grouped the location owner and the service provider requirements together. These requirements include:

- Access control
- Billing support
- Maintenance requirements
- Network performance monitoring
- Automatic software upgrade capability
- Remote management capabilities
- Availability

12.2.3 Physical Environment Requirements

These requirements are used to understand the environmental factors for which you have no control. For example, 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 of power needed. These requirements include:

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

12.2.4 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.

12.2.5 Network Requirements

- Provisioning
  - — Provided by wireless gateway
- Backhaul requirements (derive from collected requirements)
- Backbone requirements (usually CAT 5 10/100 Ethernet or consider using 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?

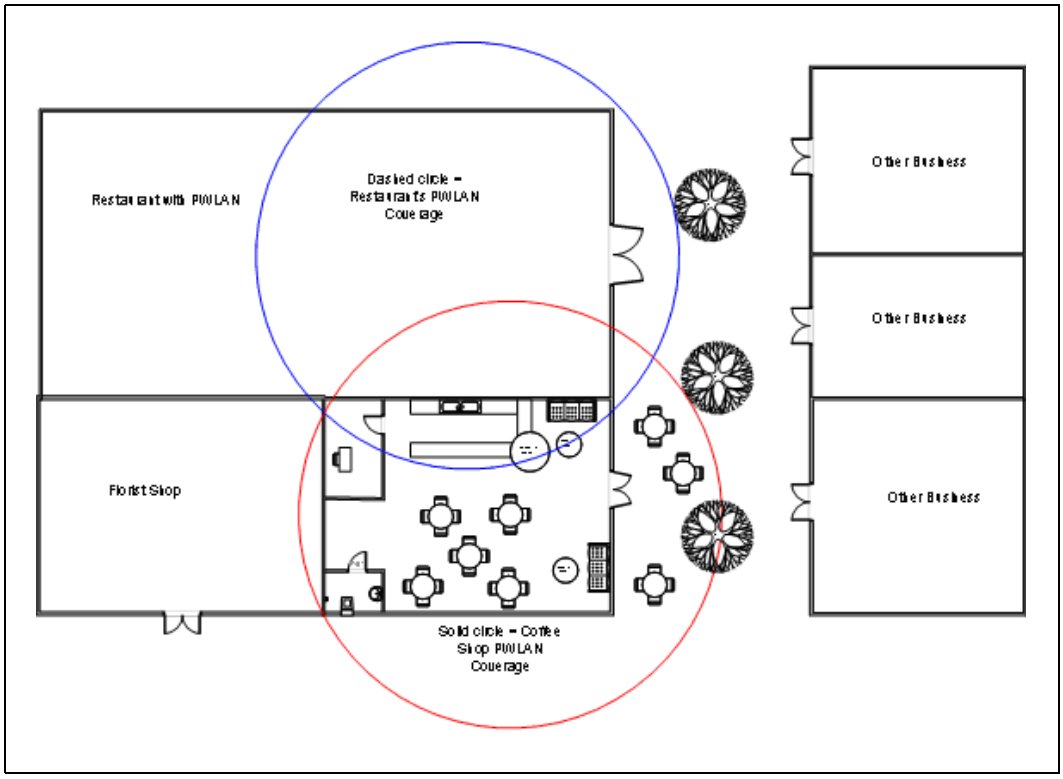
— How long to lease addresses for?

— NAT requirements

12.3 Small Hotspot - 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. (30 ft x 50 ft), 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 22. Figure 20 depicts the layout for the coffee shop hotspot.

Figure 20. Coffee Shop Layout



12.3.1 User Requirements

Table 22 shows the requirements for the user. These requirements can also be seen as requirements from the hotspot owners in terms of services they want to provide to their customers.

Table 22. User Requirements for Coffee Shop Hotspot

Requirement	Resolution
Performance	The network will provide a minimum of 200 Kbps
Maximum number of concurrent users	All network components including the AP shall support a minimum of 10 simultaneous users.
Maximum number of concurrent users per AP	The AP shall support a minimum of 10 simultaneous users.
Access to Enterprise The network must allow enterprise user access to enterprise resource through use of VPN connection	The network will provide support for multiple concurrent VPN connections to the enterprise. All currently existing VPN protocols shall be supported but only the following VPN products shall be tested: - Cisco* - CheckPoint* - Microsoft*.
Roaming/Mobility If more than one AP is used in the design, it shall be possible to roam between the APs.	Roaming is not a requirement of this hotspot with only one AP.
Security 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 must 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.

12.3.2 Location Owner/Service Provider Requirements

Table 23 shows the requirements that the hotspot owner must take into consideration in providing hotspot services:

Table 23. Location Owner/Service Provider Requirements

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 purchased 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 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.	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 wireless gateway must also keep track of the user's network usage.
Maintenance Requirements: Provide performance monitoring Support software upgrades	Network Monitoring: 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. Automatic Software Upgrades: The APs and wireless gateway shall have the ability to have software and firmware upgraded over the wire.
Remote Management Capabilities It shall be possible to perform basic management functions on the hotspot network components from a remote location (e.g., the WISP)	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.
Availability Failover is not a requirement. However, there should be a mechanism that alerts administrators that the hotspot has gone down.	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 heart beat or a polling function that will allow a central control unit to determine if the hotspot is on-line or down.

12.3.3 Physical Environment Requirements

Table 24. Physical Environment Requirements

Requirement	Resolution
Coverage Area The Coffee Shop area is 30 ft. wide by 50 ft. 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 1 Mbps at the furthest table outside.	A single AP shall be sufficient to cover the required area.
Outdoor Requirements 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 1 Mbps at the furthest table outside. There shall be no outdoor wireless equipment installed in the Coffee Shop. All outdoor patrons shall be serviced with the APs located inside the location.	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. will transmit through one outside wall to satisfy this requirement.

12.3.4 Special Requirements

Table 25. Special Requirements

Requirement	Resolution
Coexistence with administration network for the Coffee Shop. 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.	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.

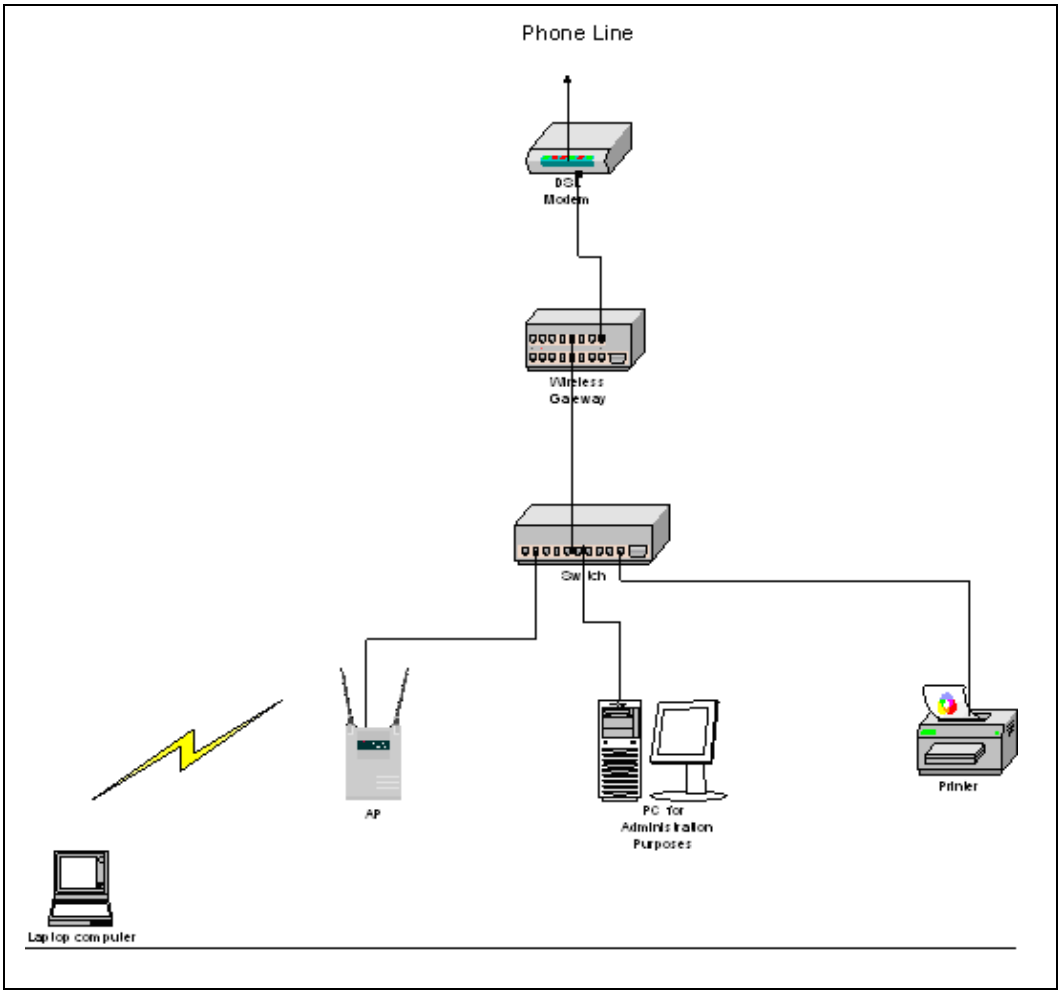
12.3.5 Network Requirements

Table 26. Network Requirements

Requirement	Resolution
Provisioning 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, 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 timeout mechanism such that the user does not have to re-login if they resume activity	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 purchase access time using a credit card. The user credentials will be checked by an AAA server that resides on the WISP network.
Backhaul Requirements The requirement to support 10 users with a sustained transfer rate of 200 Kbps requires that the backhaul connections to the Internet be at least 2 Mbps.	The backhaul shall be a 2 Mbps DSL line, at a minimum. This will allow for 200 Kpbs per user at max utilization, with increased performance with a lower number of users.
Backbone Requirements 100 Mbps	The backbone for the Coffee Shop hotspot shall be a 100 Mbps Ethernet. All equipment attached to this network must support this transfer rate.
AP Requirements 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.	The AP shall meet the stipulated requirements
IP Address Management 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	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. The wireless gateway shall implement the NAPT 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

12.3.6 Network Design

Figure 21. Network Diagram for Coffee Shop Hotspot



12.3.7 Equipment Selection

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

- AP
- Switch
- Wireless Gateway
- 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. Table 27 shows some choices. These choices are not an endorsement on these products, they are only presented as examples. Many more exist that meet the outlined requirements.

Table 27. Network Components

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

12.3.8 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.

12.4 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.

12.4.1 Site Goals and User Model

In this scenario, we are setting up a wireless network for the attendees at a conference/trade show. 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 entry way 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 1500. Each individual conference session may hold up to 50 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 400 people will be active at one time with about 12 people active in any individual conference session.

1,500 total attendees X 0.65 = 975 attendees with wireless access

975 attendees with wireless access X 0.40 = 390 attendees with access on the network

390 attendees with access on the network/1,500 total attendees = 0.26 -> 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).

12.4.2 Site Survey

Step one is to do a site survey of the location. Here we want to determine if 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 hotspot, 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 three 802.11b channels will be available for us to use. This will be critical to provide the AP density we need.

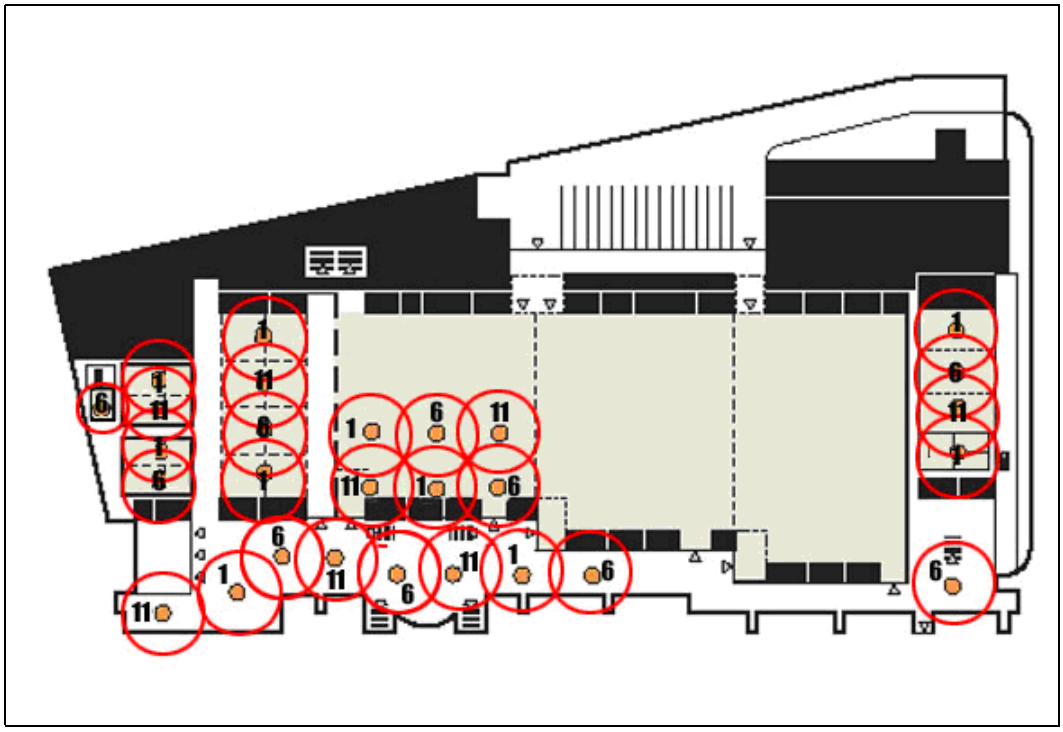
There are pillars in the main hallways where the APs can be mounted. In the session rooms, they will be hung from the ceiling. The venue provides an Ethernet drop in each of the session rooms but we'll have to string our own Ethernet cable to the APs in the main hallway. This can be a "quick and dirty"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

12.4.3 AP Layout

You can see the convention center layout in Figure 22. There is a long narrow front entry way, 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 entry way). 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 six 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 22. Convention Center Wireless Coverage



12.4.4 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.

12.4.5 Site Management

We want to be able to monitor the health of the network, bandwidth usage, and 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 analyzers, such as those from AirMagnet* or Wildpackets*.

12.4.6 Billing

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

12.4.7 Design Issues

12.4.7.1 Network Topology

The users 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.

12.4.7.2 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.

12.4.7.3 Performance

To give the users a "broadband" experience doing the types of applications we expect, roughly 200Kbps of bandwidth is desired. An AP's maximum bandwidth is roughly 5 Mbps of real throughput, which does not include TCP/IP overhead. This means about 25 users per AP can be supported. There are 28 APs in the convention center design in Figure 22. If there is a perfect distribution of users and APs (which there won't be), this means 700 simultaneous users at 200Kbps. The target is 390 users (26% of 1,500). 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 5 Mbps, then an OC-3 (155 Mbps) backhaul will be required. This assumes that all 25 users on each AP are simultaneously downloading at all times. If we assume half are actively downloading (instead of just reading content), then we'll need about 70 Mbps 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.

12.5 Conclusions

Hotspots come 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 to understand 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 your success.

13.0 Emerging Wireless Technologies

13.1 IEEE* 802.11e and Wi-Fi Multimedia* (WMM*)

The IEEE 802.11e is a standard that specifies how IEEE-compliant wireless networks implement Quality of Service (QoS) to support time-sensitive applications such as voice, video and audio.

Media streams, especially real time applications such as Voice over IP (VoIP), require a network priority scheme to allow time-critical packets to be handled differently than typical data packets for Web browsing or file transfer. QoS schemes such as 802.11e give wireless networks the capability to reliably handle time-sensitive applications and their data.

The Wi-Fi Alliance* developed the Wi-Fi Multimedia* (WMM*) profile specification from the proposed 802.11e standard. WMM is a subset of 802.11e that allows equipment vendors to implement a basic solution with interoperable QoS features that is compliant to the 802.11e standard. WMM is an optional extension to the Wi-Fi CERTIFIED* program.

This section first describes why Quality of Service is important to wireless networks. The section then examines the basic 802.11 Media Access Control functions and describe the enhancements made to support QoS (802.11e) functions. Next, the section reviews the Wi-Fi Alliance's WMM profile requirements for equipment to achieve Wi-Fi CERTIFIED for WMM. Finally, a list of some considerations for implementing QoS in public hotspots is presented.

13.1.1 The Need for Quality of Service (QOS)

There are differences between normal Web browsing data packets, buffered media streams such as CNN* broadcasts, and real-time media streams such as VoIP:

- Media streams can be buffered, all packets must arrive
- VoIP packets may have some drop-outs but must have very low latency

13.1.1.1 Traditional versus Real-Time Applications

FTP, Telnet, and Web browsing are examples of traditional applications. They do not tolerate packet loss, are not bandwidth eaters and latency and jitter are not an issue. When a user is connected to a Web site over the Internet, waiting patiently for the page to be updated is tolerated, to a certain extent.

With Internet telephony using VoIP, whether it's phone-to-phone, phone-to-PC, or PC-to-phone, voice packets can travel a myriad of different ways over the PSTN/PBXs, through telephony gateways, and over the Internet/intranet before reaching their final destination.

The problem here is latency (delay). Latency is an extremely important parameter for the user's perception of two-way communication, even in short distance calls. VoIP calls are becoming more and more popular on WLAN's and further demonstrates the need for delay management. The challenges in deploying VoIP over WLAN also include issues related to access point congestion and to those that affect the link quality.

The result is that WLANs experience significantly higher delay, with more network jitter and packet loss, than wired LANs. When several users are connected to the same access point, congestion easily occurs. The result is jitter that can be very significant, especially if large data packets are present. Also, the efficiency of the system quickly deteriorates when the number of users increases.

Real-time applications demand certain key traffic parameters to perform effectively. These applications are bandwidth intensive, but they can compensate for packet loss. For example, real-time video being sent to a client often experience packet loss, but the video encoding and decoding methods are designed to compensate and fill in the gaps.

Streaming mode is extremely sensitive to network congestion. Buffered mode loads data from the server to the client and then plays the audio/video in the client environment rather than across the network. Servers can dynamically send lower bit streams when network congestion is high followed by higher bit streams when the congestion clears.

The IETF describes the need for "Integrated Services" to provide end to end connection-oriented QoS with support for streaming and centralized scheduling. The needs of "Differentiated Services" are to provide a simple mechanism for allowing traffic priorities as part of the medium access mechanism. The QoS baseline proposal contains two different access methods and three QoS levels to accommodate both of the QoS philosophies.

QoS constantly controls and measures data rates, throughput and error rates and will improve the overall throughput of the wireless network. Network and connection management play key roles in providing a robust QoS implementation.

13.1.2 Overview of the IEEE 802.11e Standard

This section will first examine the basic 802.11 Media Access Control (MAC) layer functions that exist in all Wi-Fi Access Points and clients. We will then examine the Enhanced MAC functions and scheduling schemes developed to support 802.11e QoS, some of which are borrowed from other proven IEEE standards such as 1394. The enhanced 802.11 MAC functions determine QoS only for data sent over the wireless link.

13.1.3 Basic 802.11 Media Access Control Functions

All 802.11 wireless networks have basic MAC functions that allow data to be handled in a default method. This section will describe these functions first before introducing the enhanced (extended) functions added to support QoS.

13.1.3.1 Distributed Coordination Function (DCF)

The original 802.11 media access control protocol was designed with two modes of communication for wireless stations. The first, Distributed Coordination Function (DCF), is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), sometimes referred to as "listen before talk." A station waits for a quiet period on the network and begins to transmit data and detect collisions. DCF provides coordination, but it doesn't support any type of priority access of the wireless medium.

13.1.3.2 Point Coordination Function (PCF)

An optional second mode, Point Coordination Function (PCF), supports time-sensitive traffic flows. Wireless access points periodically send beacon frames to communicate network identification and management parameters specific to the wireless network. Between the sending of beacon frames, PCF splits the time into a contention-free period and a contention period. With PCF enabled, a station can transmit data during contention-free polling periods. However, PCF hasn't been implemented widely because the technology's transmission times such as the beacon delays and transmission durations are unpredictable or unknown.

13.1.3.3 Random Back-off

The protocol is designed to reduce collision probability at the point where collisions are most likely to occur - just after the medium becomes idle following a busy period. This is because multiple stations may have been waiting for the medium to become available again. The random back-off procedure resolves this conflict. If a station desires to transmit, but senses a busy medium, it will delay (back-off) for an additional random time. The station selecting the shortest back-off time will transmit first. Other stations will hear the transmission and defer.

When a station selects a back-off time, the value is chosen within the contention window (CW). The back-off time is computed as a random number between 0 and the current CW value.

13.1.4 Enhanced 802.11 QoS MAC Functions

The IEEE has defined enhanced MAC functions to support QoS on the wireless link. Those enhancements are described below.

13.1.4.1 Enhanced DCF (EDCF)

Because DCF and PCF do not differentiate between traffic types or sources, the IEEE has enhanced 802.11e for both coordination modes to facilitate QoS. These changes allow critical service requirements to be fulfilled while maintaining backward-compatibility with current 802.11 standards.

The enhancements to DCF, Enhanced Distribution Coordination Function (EDCF), introduce the concept of traffic categories. Each station has eight traffic categories, or priority levels. Using EDCF, stations try to send data after detecting the medium is idle and after waiting a period of time defined by the corresponding traffic category called the Arbitration Interframe Space (AIFS). A higher priority traffic category will have a shorter AIFS than a lower priority traffic category. Thus stations with lower priority traffic, must wait longer than those with high priority traffic before trying to access the medium.

13.1.4.2 Priority and Access Levels

Table 28. 802.11e Priority and Access Levels

Priority	Access Category	Designation
0	0	Best Effort
1	0	Best Effort
2	0	Best Effort
3	1	Video Probe
4	2	Video
5	2	Video
6	3	Voice
7	4	Voice

To avoid collisions within a traffic category, the station counts down an additional random number of time slots, known as a contention window (CW), before attempting to transmit data. If another station transmits before the countdown has ended, the station waits for the next idle period, after which it continues the countdown where it left off.

No guarantees of service are provided, but EDCF establishes a probabilistic priority mechanism to allocate bandwidth based on traffic categories.

13.1.4.3 Enhanced PCF (EPCF)

The Enhanced PCF provides new services and frame formats to support higher layer, end to end QoS mechanisms:

- A QoS Data service supporting Virtual Streams with specified QoS parameter values including priority, data rate, delay and jitter bounds.
- The EPCF scheduler allocates bandwidth to virtual streams and asynchronous traffic.
- An adaptive technique prevents interference among overlapping, point coordinated BSS's operating on the same channel.
- Direct station to station transfers are permitted in a QoS capable BSS (QBSS)
- A dynamic wireless repeater function can extend the spatial coverage of a QBSS.

13.1.4.4 Hybrid Coordination Function (HCF)

Another way 802.11e aims to extend the polling mechanism of PCF is with the Hybrid Coordination Function (HCF). A hybrid controller (AP) polls stations during a contention-free period. The polling grants a station a specific start time and a maximum transmit duration.

13.1.4.5 Collision Resolution Mechanisms

The IEEE 802.11e EDCA (Enhanced Distributed Channel Access) is designed to provide differentiated, distributed channel accesses for frames with 8 different user priorities by enhancing the DCF.

Each frame from the higher layer arrives at the MAC along with a specific priority value (ranging from 0 to 7). Each QoS data frame carries its priority value in the QoS Control field of the MAC frame header. An 802.11e client station implements four channel access functions, whereas channel access function is an enhanced variant of the DCF.

Each frame arriving at the MAC with a user priority is mapped into an access category (AC). A channel access function uses Arbitrary Inter-Frame Space (AIFS) and Contention Window (CW) values differently from calculating the DCF for the contention process to transmit a frame.

The values of each AC's AIFS and CW, which are referred to as the EDCA parameter set, are advertised by the AP via Beacons and Probe Response frames. The AP can adapt these parameters dynamically depending on the network conditions.

Basically, the smaller the values of AIFS and CW, the shorter the channel access delay for the corresponding priority, and hence the more capacity for a given traffic condition. However, the collision probability increases when operating with a smaller CW.

These parameters can be used in order to differentiate the channel access among different priority traffic. IEEE 802.11e EDCA also provides a new channel access method called Transmission Opportunity (TXOP), which is an interval of time when a particular client has the right to initiate frame exchange sequences onto the wireless medium. A TXOP is defined by a starting time and a maximum duration. The TXOP is either obtained by the client (STA) by successfully contending or is assigned by the AP.

It should be also noted that the AP can use the EDCA parameter values different from the announced ones for the same AC. The original 802.11 DCF was designed to provide a fair channel access to every station including the AP. However, since typically there is more downlink (i.e., AP-to-stations) traffic than uplink (i.e., stations-to-AP), AP's downlink access has been known to be the bottleneck to the entire network performance. Accordingly, EDCA, which allows the differentiation between uplink and downlink channel accesses, can be very useful to control the network performance.

13.1.5 Wi-Fi Multimedia* (WMM) Specification

The Wi-Fi Alliance's WMM prioritizes traffic demands from different applications and extends Wi-Fi's high quality end-user experience from data connectivity to voice, music, and video applications under a wide variety of environment and traffic conditions.

WMM defines four access categories (voice, video, best effort, and background) that are used to prioritize traffic so that these applications have access to the necessary network resources. Additionally, WMM-enabled Wi-Fi networks concurrently support legacy devices that lack WMM functionality. The WMM best effort access category and legacy devices transmit with the same priority.

The Wi-Fi CERTIFIED for WMM program tests interoperability with WMM and interoperability with existing Wi-Fi devices. The certification program is available to all new Wi-Fi-enabled devices. Existing Wi-Fi devices can receive a software upgrade. Wi-Fi CERTIFIED for WMM is optional, as not all clients need QoS capabilities. The Wi-Fi Alliance has worked closely with the industry and standards bodies to ensure wide adoption of WMM in new CE devices and new multimedia applications.

To take advantage of WWM functionality in a Wi-Fi network, three requirements must be met:

1. The access point is Wi-Fi CERTIFIED for WMM and has WMM enabled.
2. The client device that the application is running on must be Wi-Fi CERTIFIED for WMM.

3. The source application supports WMM.

13.1.5.1 Access Categories (AC)

WMM defines four access categories (ACs) derived from 802.1d, which correspond to priority levels (Table 29). While the four ACs were designed with specific types of traffic (voice, video, best effort, low priority data) and associated priorities in mind, WMM leaves the network owner free to choose the most appropriate network-wide policy and to decide which ACs have priority. For instance, a network owner may prefer to give priority to video streaming over voice. A customized policy for the ACs can be set through an interface in which default priority levels for ACs can be modified.

WMM specifies a protocol used by the AP to communicate the policy to QoS-enabled clients and by the clients to send transmit requests.

Table 29. WMM Access Categories

Access Category	Description	802.1d Tags
WMM Voice Priority	Highest priority. Allows multiple concurrent VoIP calls, with low latency and toll voice quality	7, 6
WMM Video Priority	Prioritize video traffic above other data traffic. One 802.11g or 802.11a channel can support 3 to 4 SDTV streams or one HDTV stream.	5, 4
WMM Best Effort Priority	Traffic from legacy devices, or traffic from applications or devices that lack QoS capabilities. Traffic less sensitive to latency, but affected by long delays, such as Internet surfing.	0, 3
WMM Background Priority	Low priority traffic (file downloads, print jobs) that does not have strict latency and throughput requirements.	2, 12, 1

The legacy 802.11 CSMA/CA-based DCF mechanism gives all devices the same priority and is based on a best effort, "listen-before-talk" algorithm. Each client waits for a random back-off time, and then it transmits only if no other device is transmitting at that time. This collision avoidance method gives all the devices the opportunity to transmit, but, under high traffic demand conditions, networks get overloaded and performance of all devices is equally affected.

WMM is an enhancement to the MAC sub-layer that adds QoS functionality to Wi-Fi networks. WMM introduces traffic prioritization capabilities based on the four ACs listed in Table 29 (the higher the AC, the higher the probability to transmit) that address Distributed Coordination Function's (DCF) inadequacy to support multimedia applications. The ACs were designed to correspond to 802.1d priorities to facilitate interoperability with QoS policy management mechanisms, such as Universal Plug and Play (UPnP).

WMM Access Points coexist with legacy devices (or devices that are not WMM-enabled) by assigning packets to the default best-effort priority if they don't have a specified AC.

The WMM baseline profile only requires Enhanced Distributed Coordination Function support. The Enhanced Point Coordination Function will be added later, known as Scheduled Access, as an optional extension to the baseline profile. Additional options will include the following:

- Direct Link Setup
- Block Acknowledgement

- Power Save

New products that support QoS must pass WMM tests to become Wi-Fi CERTIFIED.

13.1.6 Deploying QoS in Public Hotspots

Some of the key elements required for successful QoS networks (and any network) are listed below. These elements consist of more than just implementing WMM in the APs.

Network Management

- Monitoring data rates, throughput and error rates
- QoS Bandwidth Management
- Network traffic control
- Prioritize network traffic by IP or network service

Connection Management

Planning and implementing different levels of services based on connection (priority) types

Interoperability

Decide which standards to support and what certifications to look for, such as WMM.

Dynamic Adjustments for Voice (and Video) over IP

- Real-Time Transport Protocol (RTP)

  The basic role of RTP is to work as an advanced interface between real-time applications and transport layers of the existing network, not necessarily TCP. This is because RTP was developed to supply simple services independent from the transport layer with the only condition of quick transferring of packets with an expected delay and not in order. In real terms, RTP is a transport protocol that uses UDP and there is no case that guarantees the expected QoS, it just helps the inspection of the packet transport from the sender to the receiver.

- Real-Time Control Protocol (RTCP)

  RTP is a simple protocol that needs the help of RTCP to inspect and guide the RTP sessions between terminals. RTCP provides information of active session status for controlling them. There are two types of packets that are exchanged, Sender reports (SR) and Receiver Reports (RR) and they expect information for the status of every one of the RTP sessions. So, what the RTCP mainly transfer are fields which provide the capability of analyzing the percentage of data packets that have successfully arrived to their destination by giving a very clear view of the ability of the network to support QoS.

- Real-Time Streaming Protocol (RTSP)

  This is the main protocol that is used on the Internet and works at the application layer of the OSI model and is the supplement of RTP (that distributes the information packets) and of RTCP (that mentions the QoS provided). The RTSP additionally takes care of two main issues that should be fulfilled on a multimedia application, informing the network of the correct bandwidth and requesting multimedia services from the server. So there is a protocol that works over the TCP layer and manages the communication between a multimedia server and the users that will request connection and use of the application that the server provides (e.g. request for start, stop, pause to a play back server). Note that RTSP is exclusively a signaling protocol and it does nothing more than the management of streams and active multimedia

sessions. It does not, for instance, forward information packets, which is the responsibility of RTP.

13.1.7 Summary of Wireless QoS

Hotspot operators and network managers should consider deploying QoS mechanisms to support time-sensitive data such as voice, video and audio. The Wi-Fi Alliance's Wi-Fi Multimedia (WMM) certification allows hotspot operators to choose interoperable products that meet the basic requirements of the IEEE 802.11e QoS standard. While there are many other factors and elements to consider beyond the wireless link for full end-to-end QoS, 802.11e and WMM give robustness to the wireless link.

The 802.11e standard is an efficient means for QoS support in WLANs for a wide variety of applications. There is definite movement towards using voice over Wi-Fi and carriers are becoming more and more aware that corporations are becoming comfortable with the technology. The quality of service protection provided in the 802.11e standard will also be very important to the success of broadband wireless in the general marketplace.

The importance of 802.11e and WMM are difficult to overstate. For the first time, there will be classes of service for Wi-Fi. Traffic will be prioritized by type or treated as "best-effort" or "background" traffic. Voice packets or video-bearing packets are classified ahead of pure Internet access traffic, depending on how critical that traffic is to users, as well as to operators of Wi-Fi infrastructure.

However, there will still be the existing challenges to overcome in the hotspot scenario, such as channel separation and potentially increased numbers of users and client equipment types. 802.11e and WMM will only provide increased performance for delay-sensitive applications between AP and client but cannot rule out radio interference from adjacent devices if the configuration is designed poorly. There is an undoubted risk of an increased range of applications and users leading to potentially decreased performance and user frustration if all aspects of the wireless hotspot are not carefully planned and configured.

With careful design and planning combined with latest technologies, these issues should be largely overcome. Using combinations of 802.11a/b/g network devices on different frequency ranges, APs can be spread so as not to cause overlapping interference and some can be configured for higher bandwidth in specific areas. QoS architecture can create a more efficient, coordinated scheme that largely eliminates the problem of AP performance as client density rises. Rather than randomly rejecting clients when they simultaneously request access through an AP, the system can use standard 802.11 signalling mechanisms to fairly allocate resources according to each client's performance requirements. If one user is making a voice call and another is checking email, the network adjusts bandwidth for each accordingly. If one AP is too busy for a new connection, the network dynamically assigns that client to a less busy AP nearby if the APs support this optional type of functionality.

Without a standard and associated industry certification program (WMM), the risk of non-interoperable devices proliferating in the marketplace would inhibit the goals of the WLAN industry and the increased usage of hotspots for QoS-dependent applications. Users of various types of devices and applications such as VoIP will come to expect greater quality as these QoS devices proliferate.

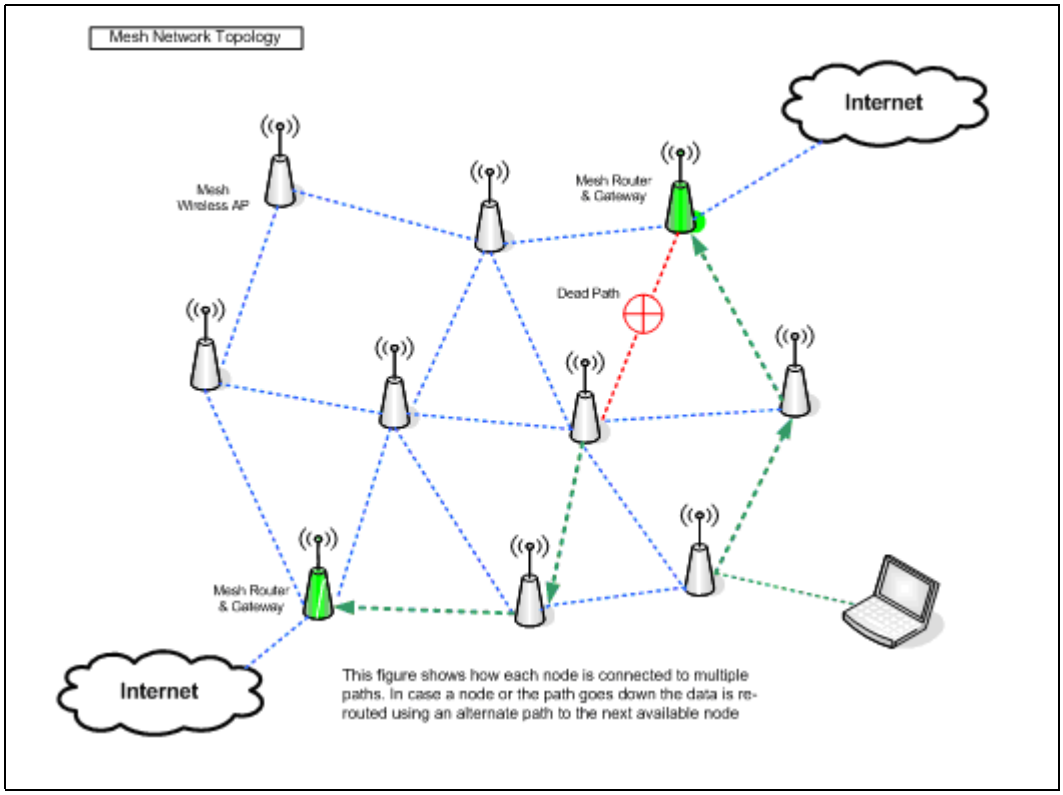
13.2 IEEE 802.11s - Mesh Technology

Mesh is a network deployment topology that extends the range of traditional LANs (Local Area Networks) and WLANs (Wireless Local Area Networks) to the client. Mesh is a type of network topology where each node is connected and communication protocols are shared across the nodes.

A Mesh infrastructure is formed when a collection of 802.11-based Access Points is interconnected by wireless 802.11 links. Mesh networks automatically learn and maintain dynamic path configurations. Wireless devices in a mesh create a seamless path for data to one another over a license-exempt spectrum at 2.4 or 5 GHz, with speeds up to 54Mbps. A WLAN user can associate with the mesh network node just as they would with an access point. In most of the mesh network deployments, the other side of backhaul node has radios that interconnect the node to other backhaul nodes that comprise the mesh network.

Current implementations of Mesh infrastructures are based on proprietary solutions. These proprietary based implementations may support Voice over IP (VoIP), Quality of Service (QoS) and increase the coverage range of standard Wi-Fi networks. However, these implementations are generally not interoperable, usually have limited scalability and may not adhere to the standard needs of most customers. The ratification of IEEE 802.11s will standardize Mesh. IEEE 802.11s is supposed to be ratified in 2007.

Figure 23. Mesh Network Topology



13.2.1 Mesh Deployment Advantages

Deployment of mesh network solutions can be advantageous in certain situations:

- Robust WLAN solution where it's not feasible to run cable to access points
- Lower installations costs due to less cabling and increased utility in difficult-to-wire areas
- The algorithm allows for multiple paths from source to destination, at the same time, smart routing allows for the data to be sent using the shortest path to destination
- If one node goes down, an alternate route can be chosen based on the routing algorithm (as shown in Figure 23)
- Ensures scalability and reliability

13.2.2 Mesh Infrastructure

- Mesh is a networking topology which extends the reach of traditional WLANs and can also be used as a last mile solution or to blanket a large area with wireless access
- IEEE standard 802.11s (Mesh networking) ratification is estimated in 2007
- Mesh Infrastructures operate in license exempt 2.4 GHz and 5 GHz bands
- Standards based WLAN solutions are designed to support distances up to 100m and speeds up to 54Mbps

13.2.3 Deploying Mesh Networks

Mesh networks can be suitable for the areas where it is not feasible to install a traditional WLAN consisting of access points. Deploying a Mesh network can be more feasible in large residential neighborhoods and city-wide municipal WLAN networks. It can be a huge task to deploy the cabled access points over a large open area, mainly because of massive amounts of cable required for installation, and the countless city permits required to complete the job. Other areas where the installation can be difficult are convention centers, stadiums, college campuses, marinas, and construction sites.

A mesh network is a viable solution when deploying a temporary wireless network because the backhaul nodes are faster to deploy and easier to take down. For example, emergency crews can quickly establish a mesh network when working at a disaster site. Other industries can also benefit from mesh networks when needing connectivity in temporary areas.

Other areas where the mesh network can add value is in older buildings and structures that do not have cabling for access points. The cost of installing cable is relatively high, especially when there are requirements to install conduits for enclosing the cable in many cases. The conduits alone can increase the access point installation costs. In this case, the deployment of mesh network can save on the overall costs of the installation.

The mesh network solutions available in the market today differ widely. Prior to considering any mesh network solution you must carefully analyze it and ensure it meets your requirements before deploying it. Since the mesh network standard (802.11s) is not ratified yet, you want to either hold off or choose the solution carefully as the current mesh network solutions may not be compatible. Given the situation, the performance, security, and management of the mesh solutions will vary considerably. Depending on the number of users, and the hops the data has to travel through the backhaul network, the latency can vary significantly.

13.3 IEEE 802.11n MIMO

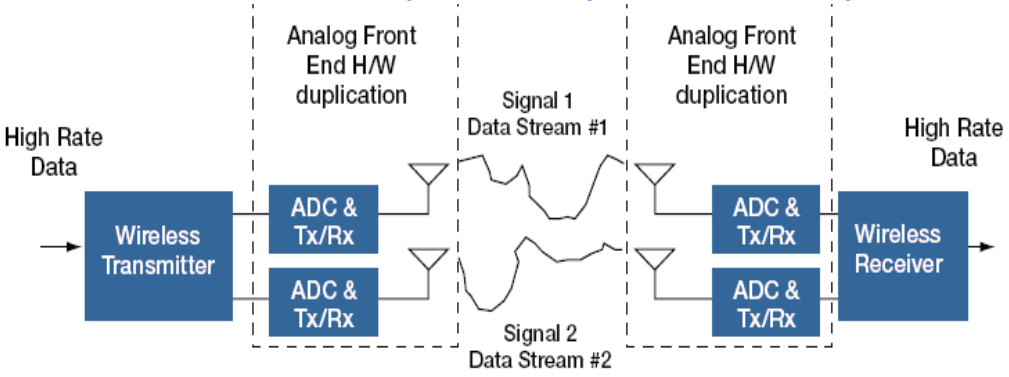
Several factors can enhance the performance of Access Point in hotspots. One that is receiving the attention of the industry as a component of the 802.11n specification is MIMO or Multiple Input, Multiple Output antenna systems. MIMO antenna technology is not new but has recently become cost effective for use in WLAN applications. Intel believes MIMO will be a fundamental component of the final 802.11n standard to increase bandwidth of WLAN to 100 Mbps and beyond. This section is intended to introduce MIMO and explain why this is of interest to public hotspots.

Before we discuss MIMO and its potential benefits, we will review some basic properties of conventional Single Input Single Output (SISO) antenna characteristics for comparison. The antenna propagates RF energy from the output of the access point (or mobile client) radio or converts incoming signals and directs to the receive circuitry of the radio. With SISO, there is one antenna available, acting as both transmit and receive antennas. This allows for a single data stream to be carried over a RF channel. Once transmitted, this stream is susceptible to typical RF interference such as multipath and fading. The effects of multipath and fading can degrade RF reception to the point that the received signal may be lost as interference.

To mitigate this phenomenon, an Access Point (or mobile client) may support temporal diversity where a second antenna is available that can be switched in based on the strength (quality) of the received signal. In a SISO system, there remains only one antenna in use during data TX/RX transfers. Diversity helps mitigate signal quality by providing the best connection but does not enhance or improve data through-put.

By comparison, a MIMO system consists of multiple transmit antennas with multiple corresponding receive antennas (see Figure 24). Note that this is more than just additional TX/RX antennas because each antenna pair is supported by its associated radio and DSP front end. Using several signal processing methods, research has shown MIMO systems can increase their overall through-put performance benefiting from the effects of multipath.

Figure 24. Basic two-antenna MIMO system showing a two stream example



MIMO accomplishes this by encoding a high-rate data stream, split into two or more separate streams (MxN). Each stream is transmitted using a unique transmitter. The data is received on two or more receiver chains. The received streams are algorithmically (mathematically) recombined, where multipath acts as a virtual stream path.

This technique is known as Spatial Division Multiplex or SDM. Since this is a fundamental change in the physical layer, SDM requires additional standardization to be compatible with legacy devices.

Another important point to highlight with MIMO is the role of diversity. In a SISO antenna system multipath and fading can degrade reception to the point the received RF is considered RF interference. MIMO provides diversity gain by using multipath through multiple separate RX antenna to capture data otherwise lost as interference and reconstruct it using appropriate algorithms in the front-end DSP.

In addition, though not specifically part of MIMO, smart antenna front ends can be used to direct the RF beam, a technique similar to methods used in cellular WWAN systems, called digital beamforming (see Figure 25.)

Figure 25. Diagram showing basic concept of digital beamforming

Digital beamforming is a technique that uses RF wave phase relationships to electronically create and steer multiple beams to/from antenna array elements based on the best connection to mobile clients.

Research has shown that MIMO in combination with digital beamforming can extend the range of existing data rates and provide less interference.

In summary, MIMO antenna systems, coupled with smart antenna front end and beam forming, promise better use of the spatial RF band, greater range and more reliable connection on the physical layer.

At this time it may be premature to consider implementing a MIMO antenna system in public hotspots. If MIMO is considered, it is important to recognize that the majority of clients are legacy 802.11 a,b or g clients. MIMO may help extend the range and provide a strong diversity but you will not see the through-put expected with a MIMO-based Access Point and MIMO based mobile client. It’s recommended therefore to keep abreast of the Tgn working group, as the development of the final 802.11n standard is anticipated in 2006.

13.4 Supporting Cellular WWAN Users

As Wi-Fi functionality proliferates to different types of devices and laptop functionality grows, the hotspot operator will need to decide how to expand services to these devices. These devices include Wi-Fi-enabled cell phones and PDA's used for voice and data. In addition, laptop users are able to purchase cellular data services using special add-in cards. As users move from the cellular wireless wide area network (WWAN) to the WLAN hotspot, the user's device will try to switch to the WLAN for data speed and cost advantages. For this to work with these devices, the hotspot will need to support authentication and roaming that is compatible with the WWAN service providers.

Large enterprise companies are evaluating and moving towards all-wireless telephone systems for their employees. Large savings are potentially possible by migrating away from fixed telephone systems to wireless voice devices that allow users to utilize the same enterprise WLAN (EWLAN) as their laptop/data devices with the added benefit of always being reachable. Wireless phones that integrate both WLAN and WWAN capabilities have wide coverage and can take advantage of cost savings when in range of a WLAN. Hotspots that support this new breed of device will have advantages over those that don't.

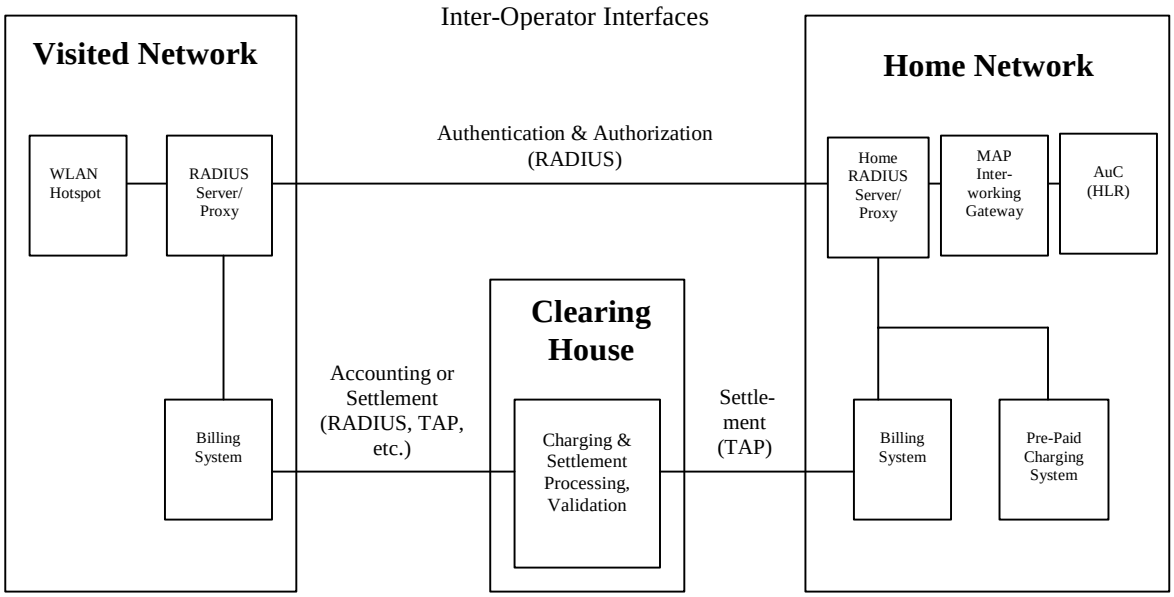
Another usage model is laptop users who are becoming accustomed to the freedom of wireless networks. They are expanding their wireless coverage by purchasing cellular 3G data services. However, when those users move to an area covered by a WLAN hotspot, they too will want to seamlessly roam to the hotspot and have the service billed to their existing cellular account. The methods described in the section below give a high-level explanation of the components and protocols used to interconnect a hotspot to another service provider, such as a cellular service.

13.4.1 Implementation Details

Hotspot operators (the Visited Network) will need to support interfaces to the cellular providers' (the Home Network) AAA services (through roaming agreements) as well as compatible interfaces to the mobile terminal devices. Protocols to the cellular providers' AAA servers will consist of the following:

- Authentication: RADIUS, EAP, EAP-SIM, 802.1X
- Accounting: RADIUS, TAP
- Authorization (if applicable): RADIUS

Figure 26. Inter-Operator Interfaces



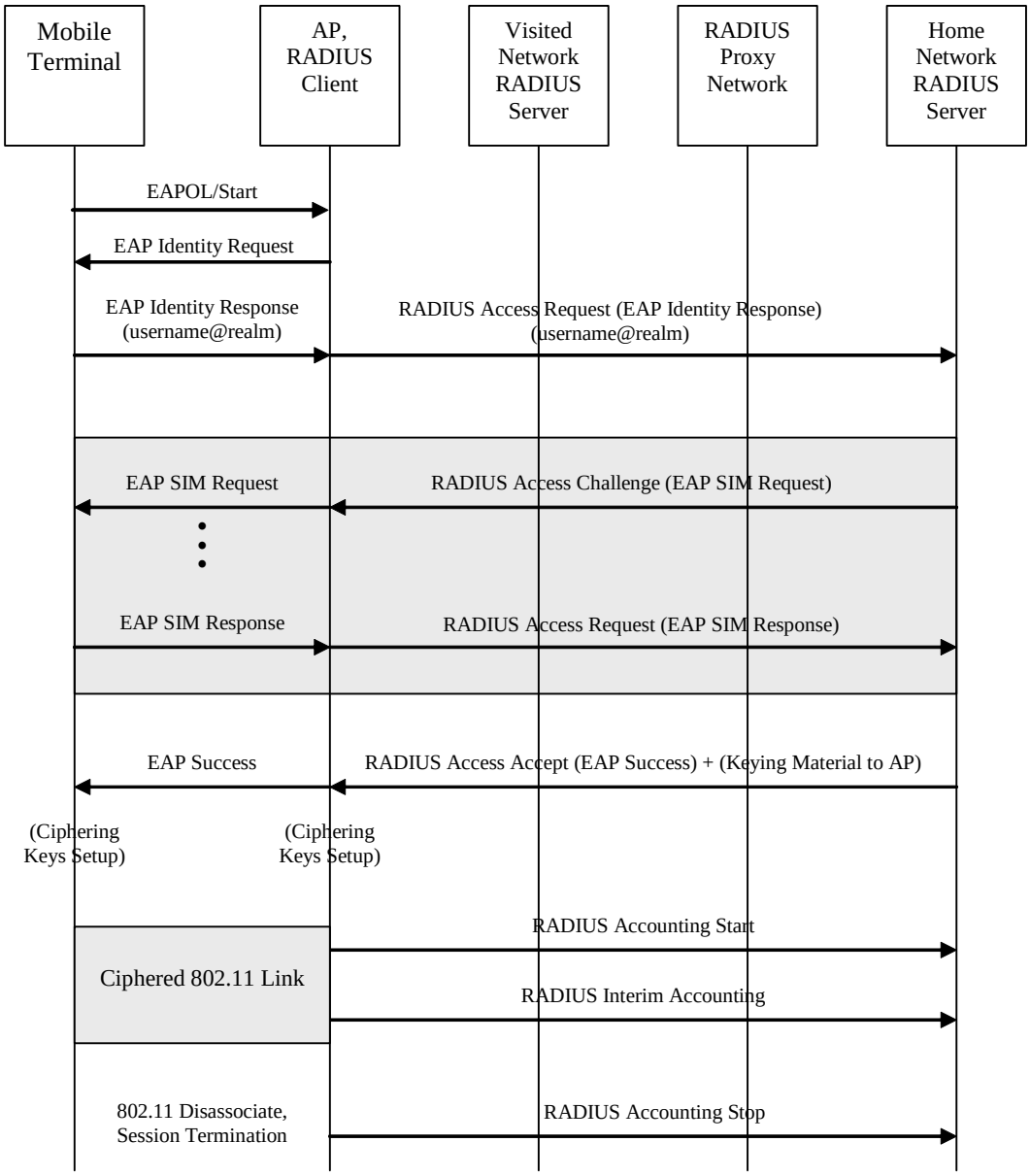
Most cell phones and WWAN devices use a secure Subscriber Information Module (SIM) for authentication to the WWAN. The EAP-SIM protocol allows SIM devices to authenticate to their home networks. The 802.1X standard is an authentication framework that uses EAPOL to carry the

EAP messaging across the wireless link. Below is a login message flow for a SIM-based device from the Visited Network to the Home Network. Note that the hotspot only needs to support the RADIUS protocol from the access network to the user's Home Network. The user is authenticated by the Home Network through tunnels established to the user's device. Once a user is authenticated, the Home Network notifies the hotspot servers through standard RADIUS messages. The hotspot is not burdened with support for the multitude of EAP protocols to allow a greater number of users to access the hotspot.

Figure 27 depicts some of the message flow from the user's device, the hotspot and the Home Network to establish a connection to the visited hotspot.

Detailed guidelines for designing WLAN to WWAN interfaces are described in the GSM Association Official Document IR.61, *WLAN Roaming Guidelines 3.1.0, August 2004*. Additional protocol and configuration specifications are contained in the International Roaming and Protocols (IRAP) specification (www.goirap.org).

Figure 27. Protocols to Support Inter-Operator Roaming



Note: Not all RADIUS Accounting Messages Shown

Appendix A IEEE 802.11 Wireless Standards

A.1 802.11a - OFDM in the 5GHz Band

802.11a is a Physical Layer (PHY) standard (IEEE Std. 802.11a-1999) that specifies operating in the 5GHz UNII band using orthogonal frequency division multiplexing (OFDM). 802.11a supports data rates ranging from 6 to 54Mbps. 802.11a-based products became available in late 2001. Because of operation in the 5GHz bands, 802.11a offers much less potential for radio frequency (RF) interference than other PHYs (e.g., 802.11b and 802.11g) that utilize 2.4GHz frequencies.

A.2 802.11b - High Rate DSSS in the 2.4GHz Band

The task group for 802.11b was responsible for enhancing the initial 802.11 DSSS PHY to include 5.5Mbps and 11Mbps data rates in addition to the 1Mbps and 2Mbps data rates of the initial standard. This was finalized as a standard (IEEE Std. 802.11b-1999) in late 1999. To provide the higher data rates, 802.11b uses CCK (Complementary Code Keying), a modulation technique that makes efficient use of the radio spectrum. In some cases, you should deploy 802.11b networks today to take advantage of the installed base of 802.11b-equipped users. For example, utilize 802.11b as the basis for public wireless LANs to maximize the number of subscribers.

A.3 802.11d - International Roaming Extensions

When 802.11 first became available, only a handful of regulatory domains (e.g., U.S., Europe, and Japan) had rules in place for the operation of 802.11 wireless LANs. In order to support a widespread adoption of 802.11, the 802.11d task group has an ongoing charter to define PHY requirements that satisfy regulatory within additional countries. This is especially important for operation in the 5GHz bands because the use of these frequencies differ widely from one country to another. The 802.11d standard mostly applies to companies developing 802.11 products.

A.4 802.11e - Supplement for MAC Enhancements for QoS

Without strong quality of service (QoS), the existing version of the 802.11 standard doesn't optimize the transmission of voice and video. There's currently no effective mechanism to prioritize traffic within 802.11. As a result, the 802.11e task group is currently refining the 802.11 MAC (Medium Access Layer) to improve QoS for better support of audio and video (such as MPEG-2) applications.

Because 802.11e falls within the MAC Layer, it will be common to all 802.11 PHYs and be backward compatible with existing 802.11 wireless LANs. As a result, the lack of 802.11e being in place today doesn't impact your decision on which PHY to use but it does impact what applications you can support in your WLAN, such as with priority media streams or VoIP. This is a draft standard as of July 2005.

A.5 802.11F - Inter-Access Point Protocol (Roaming)

The existing 802.11 standard doesn't specify the communications between access points in order to support users roaming from one access point to another. This presents a problem in that access points from different vendors may not interoperate when supporting roaming. 802.11F specifies an inter access point protocol that provides the necessary information that access points need to exchange to support the 802.11 distribution system functions (e.g., roaming). One drawback to 802.11F is that is does not address roaming in a time-efficient manner which has negative impact to applications such as VoWLAN. As a result vendors have developed their own mechanisms for fast handoff of clients creating another interoperability problem. 802.11F was ratified in 2003.

A.6 802.11g - Higher Rate Extensions in the 2.4GHz Band

The 802.11g task group developed a higher speed extension (up to 54Mbps) to the 802.11b PHY, while operating in the 2.4GHz band. 802.11g has implemented all mandatory elements of the IEEE 802.11b PHY standard. For example, an 802.11b user will be able to associate with an 802.11g access point and operate at data rates up to 11Mbps. 802.11g uses OFDM instead of DSSS as the basis for providing the higher data rate extensions.

A.7 802.11h - 5 GHz Band Regulatory Requirements

The IEEE 802.11h is a standard that addresses the requirements of the European regulatory bodies for 5 GHz band. The International Telecom-communication Union (ITU) recommended a set of rules for WLANs to share the 5-GHz spectrum with primary-use devices such as military radar systems. The 802.11h standard defines mechanisms that 802.11a WLAN devices can use to comply with the ITU recommendations. These mechanisms are dynamic frequency selection (DFS) and transmit power control (TPC). The original motivation for the DFS and TPC mechanisms defined in 802.11h ensure a standard method of operation under the regulatory requirements governing the 5-GHz band. Along with meeting regulatory requirements, DFS and TPC can be used to improve the management, deployment and operation of WLANs. DFS detects other devices using the same radio channel, and it switches WLAN operation to another channel if necessary. DFS is responsible for avoiding interference with other devices, such as radar systems and other WLAN segments, and for uniform utilization of channels.

TPC is intended to reduce interference from WLANs to satellite services by reducing the radio transmit power WLAN devices use. TPC also can be used to manage the power consumption of wireless devices and the range between access points and wireless devices.

A.8 802.11i - MAC Enhancements for Enhanced Security

802.11i is actively defining enhancements to the MAC Layer to counter the issues related to wired equivalent privacy (WEP). The existing 802.11 standard specifies the use of relatively weak, static encryption keys without any form of key distribution management. This makes it possible for hackers to access and decipher WEP-encrypted data on your WLAN. 802.11i will incorporate 802.1X and stronger encryption techniques, such as AES (Advanced Encryption Standard).

802.11i updates the MAC Layer, so you should be able to upgrade existing access points with firmware upgrades. The implementation of AES, however, may require new hardware. This was ratified in June 2004.

A.9 802.11j - Frequency Rules for Japan

The IEEE 802.11j amendments, approved in November 2004, allows for an 802.11 network to conform to frequency rules for 4.9 and 5 GHz bands in Japan.

A.10 802.11k - Radio Resource Management

The IEEE 802.11k is a standard for radio resource measurement whose aim is to provide client feedback to WLAN access points and switches. 802.11k is a defined series of measurement requests and reports that detail layer1 & 2 client statistics. In some cases client requests data from Access Point versus reporting data to Access Point. This allows for clients and Access Points to share information about the channel. With 802.11k, Access Points and WLAN switches can query all clients to get reports on their statistics. With both data sets, a WLAN system will have a more complete view of network performance.

A.11 802.11n - 100MHz + Bandwidth in Wireless Networks

The IEEE 802.11n is a proposed standard in committee scheduled to be ratified in 2007. The proposal specifies how IEEE-compliant wireless networks will take the next step in speed and develop higher bandwidth of 100Mbit + (minimum) while maintaining backward compatibility with previous 802.11 standards.

The driving business factors for increased bandwidth in wireless network are time and bandwidth sensitive applications such as voice, video and audio streams. Within enterprise networks increased bandwidth, reliability and scalability play a major role in total cost of ownership. Increased bandwidth, in addition to QoS (802.11e) standards, adds the ability to support these types of applications within enterprise networks. The digital home experience where multiple HDTV and audio streams are expected within the wireless home also require an increase in bandwidth.

It stands to reason that 802.11n holds promise for public WLAN and WISPs should monitor developments of 802.11n for future implementations.

Currently there are two major proposals in the TGn working committee, TGn Sync and Wwise. As of May 2005 neither group has managed to win majority approval of committee members for adoption as a proposal standard. Members are cooperating to find common ground for a joint proposal and expectations are they will deliver in 2006, finalizing in 2007.

A.12 P802.11r - Fast Roaming

The fast roaming project, IEEE P802.11r, will make it easier to use wireless VoIP and other real-time interactive applications. The standard will seek to foster the use of mobile, wireless VoIP phones and other time-sensitive WLAN applications by eliminating perceptible disconnections.

A.13 802.11s - Wireless Mesh Networks

The IEEE 802.11s is in a working group since September 2004. The intent of 802.11s is to describe a standard for a mesh network where each node has direct connections to many other nodes in the wireless network. This allows for many paths through the network from one node to another and implies dynamic routing within the wireless network.

Appendix B Commonly Used Terms

This section contains definitions of terms in the following categories:

- General Terminology
- Hotspot Components
- Security Terminology

B.1 General Terminology

This section lists some of the general terms used in the 802.11 specification:

802.11 - IEEE specification for wireless communication in the unregulated radio spectrum

Antenna diversity - A method of minimizing multi-path 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 effectively covered by an Access Point

Coverage - the amount of area in which the wireless network is available

Line of Sight (LOS) - the ability to see one network component from another with no 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

B.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 (AP) - a network device that interconnects a wireless radio network to a wired LAN and controls mobile station associations.

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.

Universal Access Method (UAM) - An open (non-secured) method for users (clients) to associate and authenticate to the hotspot. This method involves web-redirection and may include AAA to gain access to the Internet.

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.

B.3 Security Terminology

Following are many of the terms used when talking about 802.11 security. The terms are listed and briefly described here, with more in-depth discussion of security in Section 7.0, “Wireless Security” on page 62.

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 requirement for client certificates. In TTLS, as in PEAP, the mobile station identifies itself with username/password while the AP continues to use 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's 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.

Appendix C 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
CCM	Counter Mode with CBC-MAC
CIR	Committed Information Rate
CRC	Cyclic Redundancy Check
DCC	Direct Client Communication
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DKE	Dynamic Key Exchange
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
GHz	GigaHertz
GRE	Generic Routing Encapsulation
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
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
NAPT	Network Address Port Translator
NAT	Network Address 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
PSK	Pre-Shared Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RDP	Remote Desktop Protocol
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
SSH2	Secure Socket Shell version 2
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SST	Shiva Secure Technology
STA	(Mobile) Station
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security

TTLS	Tunneled TLS
UDP	User Datagram Protocol
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WISP	Wireless ISP
WLAN	Wireless LAN
WM	Windows Messenger
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
XOR	Exclusive OR
YM	Yahoo Messenger

Appendix D Details of Wireless Security

D.1 Wire Equivalent Privacy (WEP)

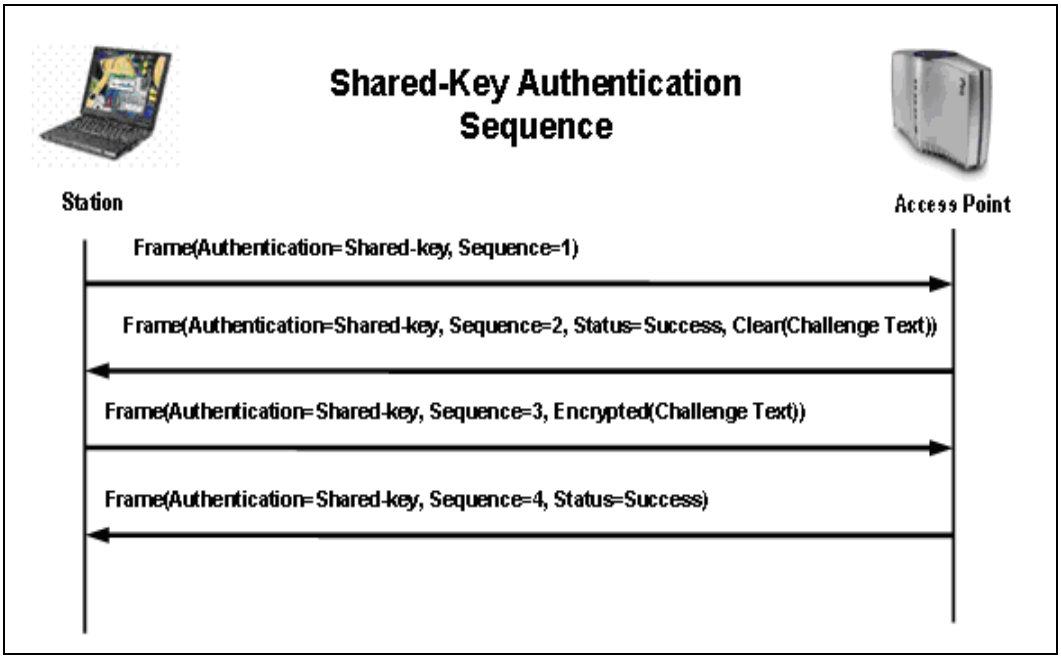
Wired Equivalent Privacy (WEP) is the original 802.11 security specification. It was designed to secure the radio link layer by protecting the data as it traverses the wireless portion of the network. WEP does not provide protection beyond the AP and applies equally to 802.11a, 802.11b and 802.11g.

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.

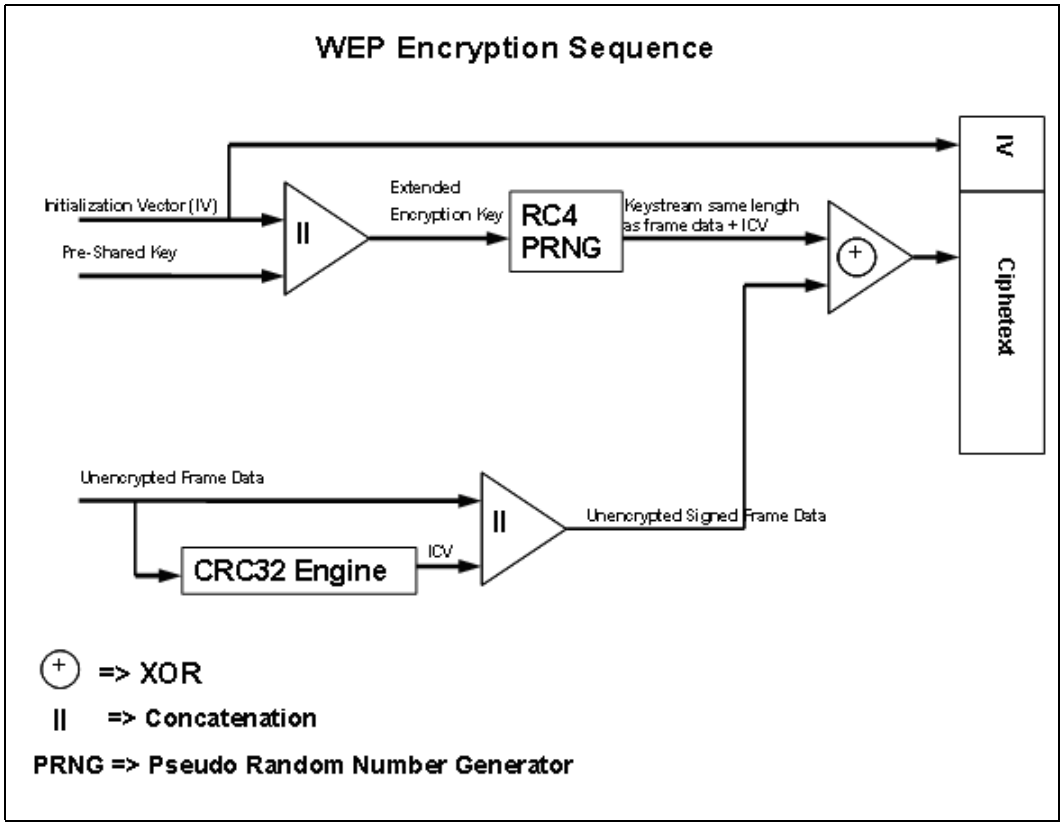
Open Authentication allows any wireless device to associate with an AP. For Shared-Key Authentication, the AP sends a text string to the MS in a challenge message. The MS is required to encrypt the string using its WEP key and to send it back to the AP. The encryption key used by the mobile station is 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 28 illustrates the Shared-Key authentication sequence.

Figure 28. Shared Key Authentication Sequence



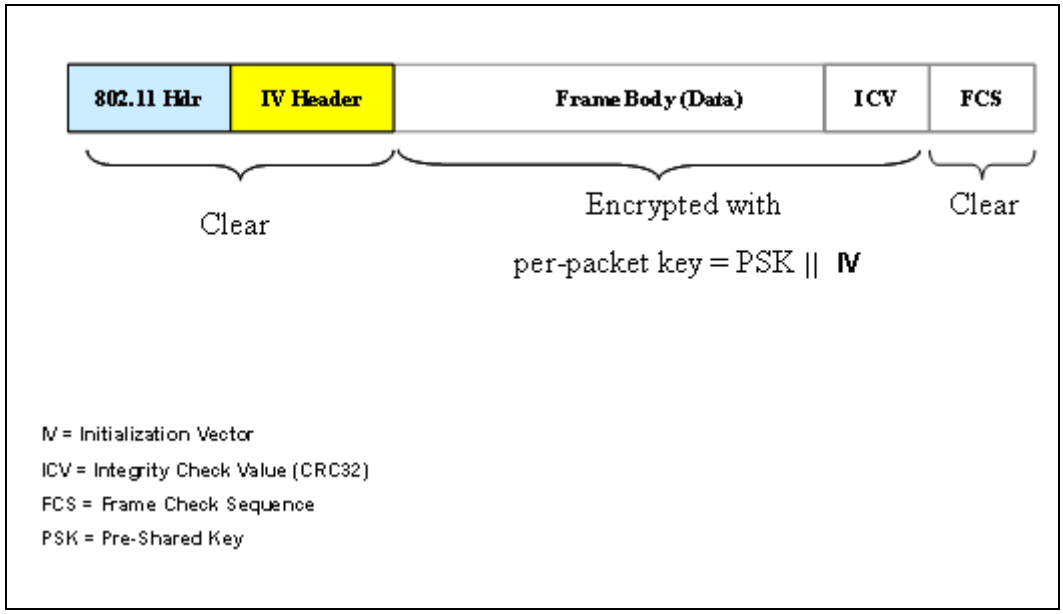
When WEP is enabled, it provides confidentiality by encrypting the messages exchanged between the mobile station and the AP over the wireless link. To encrypt the message, the sending unit first generates a 24-bit Initialization Vector (IV). The IV is used in conjunction with the 40-bit or 104-bit WEP 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 key stream 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 key stream 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 29 illustrates the encryption process. Figure 30 for frame composition details.

Figure 29. 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 with 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.

Figure 30. Clear and Encrypted Frame Areas



D.2 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 been 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.

D.2.1 Dynamic Key Exchange (DKE)

DKE is an attempt by several companies with interest in improving Wi-Fi 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.

Note: 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.

D.3 802.11i

IEEE’s solution to WEP's flaws is the 802.11i standard. 802.11i 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 crypto-analysis. 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 is discussed in Section 9.9.

D.3.1 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 crypto analysis 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.

D.3.2 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. 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:

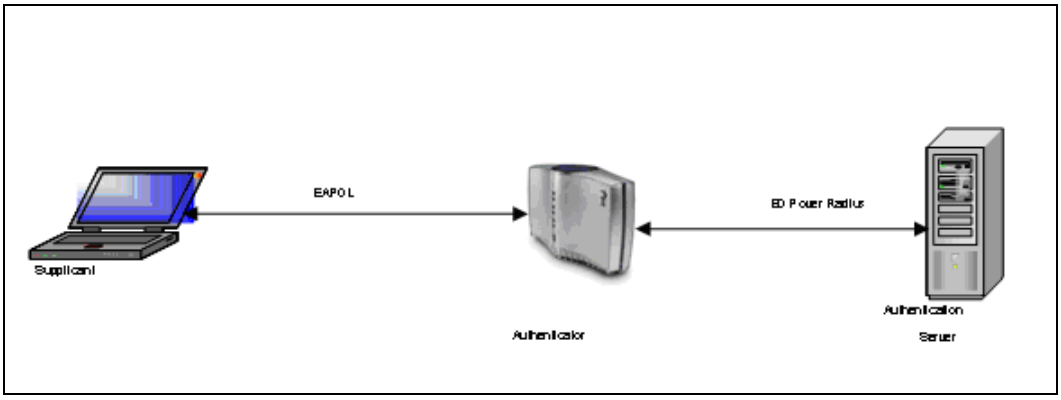
- New per-packet key mixing function
- New message integrity check (MIC) named Michael
- Longer initialization vector (from 24 bits in WEP to 48 bits in TKIP)
- New re-keying mechanism (session key renewed on a regular basis)

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.

D.3.3 Framework - 802.1X

802.1X is a specification that describes an architectural framework for an authentication and authorization mechanism 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 allows network administrators to choose from several authentication methods as appropriate for their environments. Figure 31 shows a simple 802.1X architecture diagram:

Figure 31. 802.1X Architecture



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

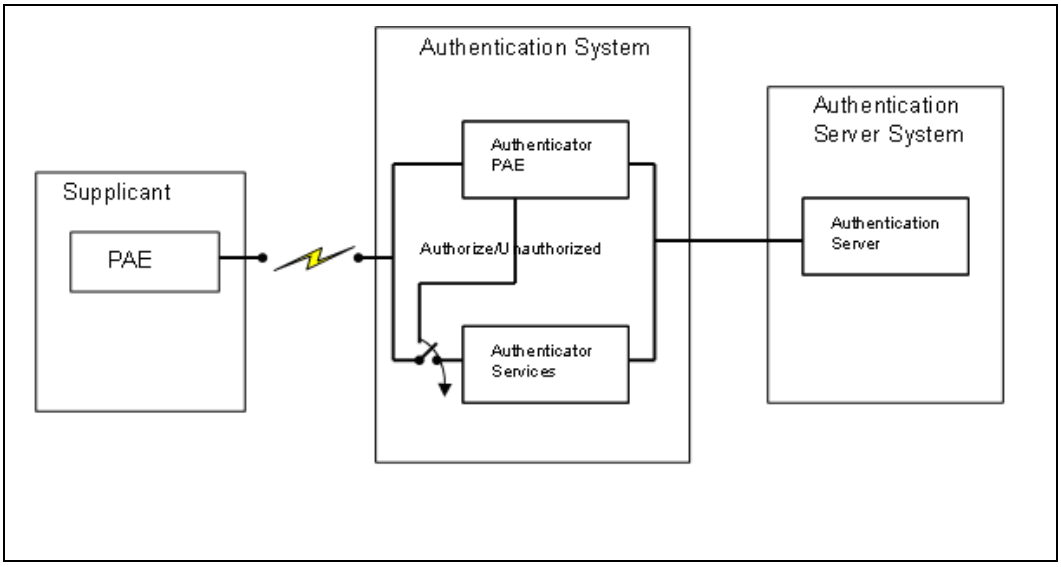
- How the access control mechanism operates
- Levels of access control supported as well as port behavior at each level

- 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.

D.3.3.1 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. Refer to Figure 32 for an illustration of port-based access:

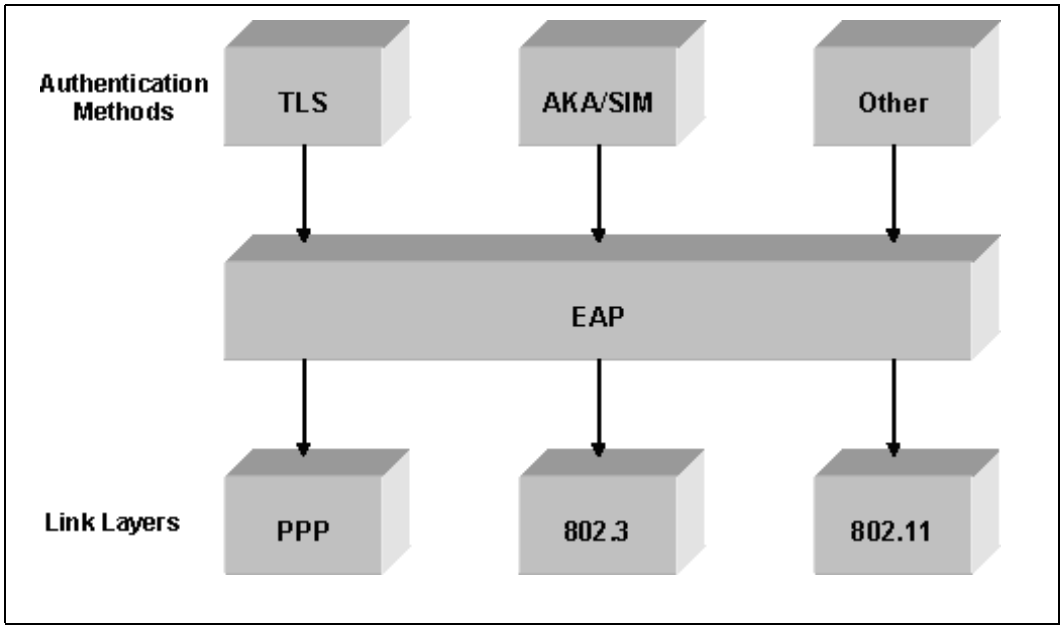
Figure 32. 802.1X Port-Based Access Control



D.3.4 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 33 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 33. EAP Framework



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

D.3.5 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.

Note: Support for authentication selection policies is implementation-dependent. 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.

D.3.5.1 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.

Note: 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.

D.3.5.2 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.

D.3.5.3 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.

D.3.5.4 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. None the less, 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.

D.3.5.5 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.

Note: 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.

NOTES

NOTES