Wi-Fi / WiMAX Primer

Utilizing Best Practices
to Build Wi-Fi Networks

A Working Draft
GUIDE
To Understanding and Building
Wireless Networks

e-NC AUTHORITY

[back of title page]

Creative Author **Albert Azzam**, co-author of "High Speed Access Technologies: ADSL, APON, Wireless, Cable Modems"

Advisory Team Jane Smith Patterson, Charles Pittman, Joanna Wright

Prepared for the 2nd Southeast Wireless Conference, December 7-8, 2004, Winston-Salem, NC.

e-NC Authority
4021 Carya Drive
Raleigh, NC 27610
http://www.e-nc.org

Overview

Abstract: This paper presents a detailed overview of the Wireless LAN (WLAN); it is widely referred to as Wi-Fi and/or IEEE 802.11. The term Wi-Fi and WLAN are interchangeable when reading this document. Wi-Fi is one of the wireless high-speed data networking technologies that is widely deployed in residential networks, enterprises, and public areas around the world. For information on all other broadband access technologies refer to "***e*-NC** Broadband briefs: Broadband technologies access overview" at www.e-nc.org.

Wi-Fi brings Internet connectivity to users equipped with a laptop, PDA, and/or cell-phone devices.

This paper intends to inform ***e*-NC** members and the public on how to build a Wi-Fi network to serve NC communities, particularly in distressed rural regions. This empowers the community with the benefits delivered through the Internet, particularly in revitalizing their depressed economic infrastructure through advertising and promotions.

For visitors with wireless devices, this will have the added value of enabling them to explore the community's resources; be it restaurants or social / economic landmarks. Widespread roaming provides a mechanism for users to roam from site-to-site, exploring local advertisements and developing awareness of the regional culture and heritage, delivering advertisements to visitors similar to other online services.

Notice: The information contained in this report is believed to be from reliable sources as of September 2004. However, the authors cannot fully guarantee either the accuracy or completeness of the published materials. It is offered for information only and is based on data available from public and private sources at the time it was prepared. Readers are urged not to fully rely on this information but to seek appropriate professionals for supplying engineering services and appropriate sources for specific and updated information.

***e*-NC** disclaims any and all liability whatsoever arising from the review, use or reliance in any way on information in this report by any person or entity.

TABLE OF CONTENTS

List of Figures

List of Tables

Wi-Fi / WiMAX Introduction

Basic Definition and Historic Perspectives

Wi-Fi: Wi-Fi stands for Wireless Fidelity. It is a high-speed wireless data network that is becoming popular among public and private network operators around the world, including the Wireless Internet Service Providers (WISP). A public location that deploys Wi-Fi service is referred to as a hot spot/hotspot. Hotspots bring to users, and particularly business road warriors, equipped with a laptop or a PDA, wireless connectivity to the Internet. Wi-Fi is a family of wireless networking protocols under development (and in commercial use since 1999) by Institute of Electrical and Electronic Engineers (IEEE) in working group 11 standard organization. The IEEE 802.11 charter is to specify the type of radio technology and its components that are needed to build a Wireless Local Area Network (WLAN).

WiMAX: WiMAX stands for Worldwide Interoperability for Microwave Access. Unlike Wi-Fi, WiMAX was conceived to address the wireless MAN (Metropolitan Area Network). Hence, WiMAX is known as one of the broadband fixed wireless access solutions for the "Last mile" IEEE 802.16 is developing the standards for WiMAX and recently approved and released a set of specifications to the industry. A WiMAX forum was hence created to certify the IEEE 802.16 standard. The WiMAX forum will work to guarantee that WiMAX devices and products conform to the standard and are interoperable.

Enabling Technologies[1]

In the last decade, major changes took place in the world of communication. Advances in technology and convergence from: Analog to digital, wire line to wireless, narrowband to broadband, circuit switching to packet switching, stand alone technology to convergent technology enabled Internet mediation that has resulted in profound change without a single "killer platform." Most consumers now embrace the Internet for a variety of social and commercial functions. Technological innovations in computing, number portability, and wireless have empowered consumers on many fronts. Competitive initiatives provided digital mobility and greater choices in laptop computer, iBook, PDA, IPOD, digital camera, camcorder, cell phones and pagers. These devices are shaping our present digital lifestyle and transforming the way we explore our world.

When examining today's technology and social trends in digital mobility, it becomes easier to prophesize the market potential of Wi-Fi /WiMAX and or other wireless broadband base technologies.

[1] Enabling Successful Services and Applications, ITU Telecom World 2003, October 2003.

Wi-Fi Market Statistics

Below are some statistics regarding Wi-Fi market deployment forecasts. Market analysts differ in their forecasts due to the assumptions they adopt. Assumptions vary from political reality to state economic forecasts in general. Below are some of those recent statistics.

Hotspot Deployment Forecast Snapshots

Analyst firm Gartner predicts that by the year 2008 there will be more than 167 thousand public WLAN hotspots around the globe. In addition, there will be over 75 million users of public WLAN hotspots worldwide. [2]

TeleAnalytics prediction of the public hotspot forecast is more optimistic and puts the global deployment to be between 100,000 and 300,000 in 2006, of which US hotspots increase from 3300 to around 100,000 in 2006. [WONS 2004 - Panel Session. January 21, 2004]
Other forecasts are as shown in figures 1, 2, and 3.

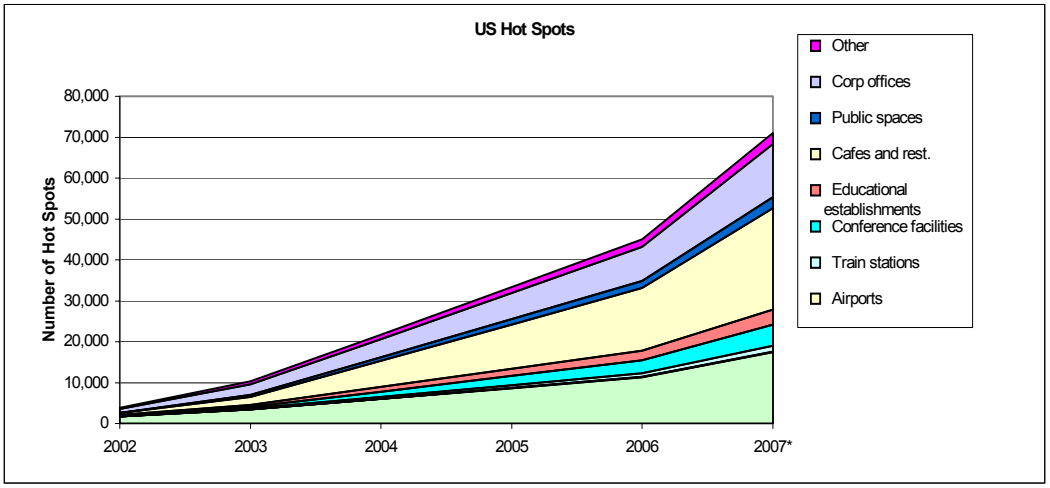


Figure 1- US Hotspot Forecast [3]

[2] Ian Keene, "Public Wireless LAN Hot Spots: Worldwide, 2002-2008" (Gartner, Inc., 2003).
[3] Kent Lundgren, "Wi-Fi Technology" Nigerian Communications Commission Wi-Fi Workshop, 2003.

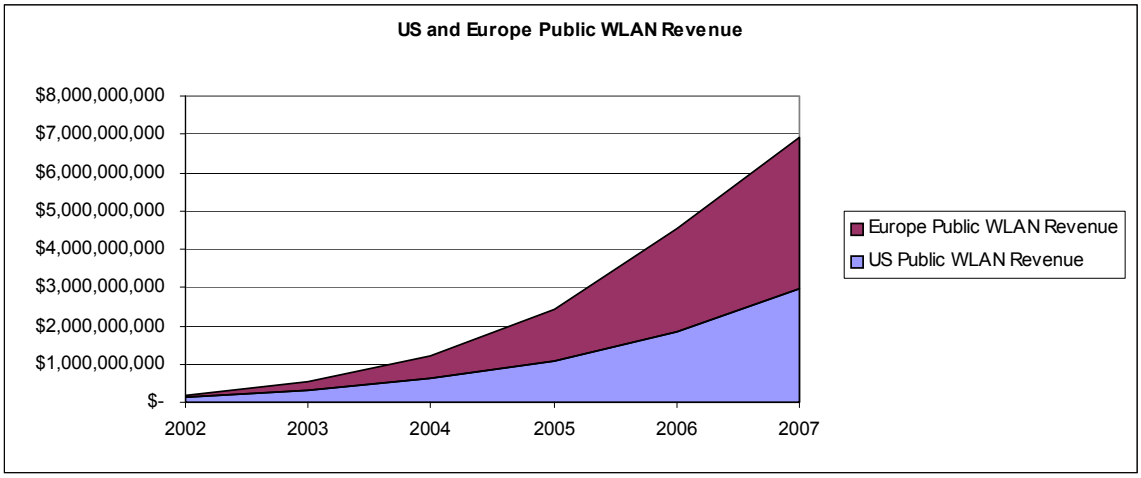


Figure 2- Wi-Fi Revenue (USA & Europe)[17]

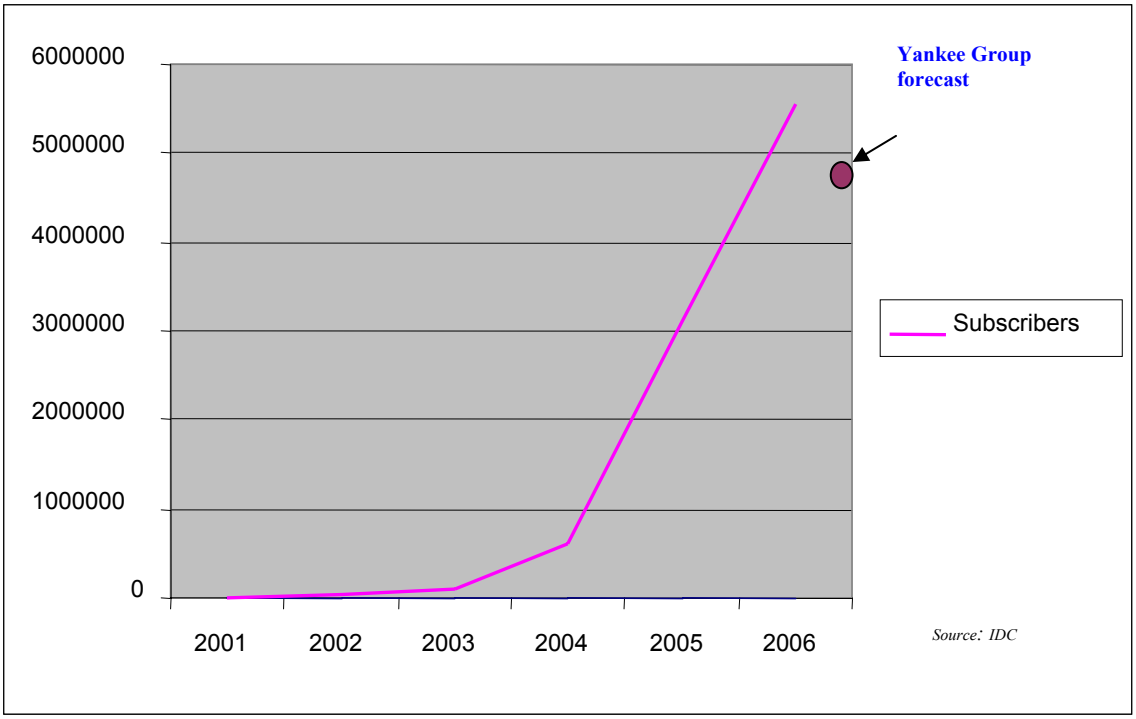


Figure 3- Wi-Fi Growth Forecast

[17] Kent Lundgren, "Wi-Fi Technology" Nigerian Communications Commission Wi-Fi Workshop, 2003.

Wi-Fi Technology Briefs

IEEE 802.11Standards Activity/Status

As previously stated, IEEE 802 standard working group is responsible for developing specifications for the Local Area Network (LAN) and the Metropolitan area Network (MAN). 802.11 is a subgroup developing specifications dealing with wireless LAN, while 802.16 subgroup is working on the wireless MAN (known as WiMAX).

Wi-Fi Foundations

Table 1 lists the 7-layer Open System Interconnect (OSI) used by all standards including IEEE 802. The details of the upper layers are beyond the scope of this manual but the basic primitives are as shown.

Wi-Fi activity is an overlay of the original LAN design and its activity falls within the Data Link Layer and the Physical Layer of the OSI reference model.

Application (Layer 7)	This layer handles the details of the applications. E.g., email, ftp, www. etc
Presentation (Layer 6)	The presentation layer works to transform data into the form that the application layer can accept
Session (Layer 5)	This layer establishes, manages and terminates connections between applications.
Transport (Layer 4)	This layer provides connection establishment and control delivery between hosts as well as flow control
Network (Layer 3)	Moves packets inside the Network., i.e., routing, congestion control etc.
Data Link (Layer 2)	This layer provides reliable transfer of data frames over a link. It is divided into two sub-layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub-layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.
Physical (Layer 1)	This layer conveys radio signals through the network at the electrical and mechanical level. It provides the means of sending and receiving data on a carrier

Table 1- 802.11 OSI Reference Model

Physical Layer and Data Link Layer (Layer 1&2)

Table 2 below lists the activities of the work done or ongoing in 802.11 (at the physical and data link layer). A brief description for each component is as shown below:

Designation	*Description*	*Range Indoor*	*Range outdoor*	*Frequency*
802.11a	54Mbps	100 feet	150 feet	5Ghz band
802.11b	11Mbps	160 feet	300-500 feet	2.4Ghz band
802.11c	Mac Bridging			
802.1d	International roaming			
802.11e	Quality of Service			
802.11f	AP protocol			
802.11g	54Mbps	150 feet	300 feet	2.4Ghz band
802.11i	Security			
802.11m	Management support			
802.11n	100++ Mbps			2.4Ghz
802.11s	Mesh networking			

Table 2- IEEE 802.11 Standards (Status & Activity)

802.11a:
802.11a is a radio transceiver, operates at the unlicensed 5 GHz range (5.15GHz to 5.35GHz). At this range, the spectrum is not crowded and hence more immune to interference than 802.11b. The theoretical bandwidth is 54Mbps and hence it enables the transfer of high-quality digital audio/video and large files across the network.

802.11b:
802.11b is currently the most popular and least expensive wireless specification. It operates in the 2.4GHz radio spectrum and can transmit data at speeds up to 11Mbps within a 160-foot range. Although it is the least expensive, the drawback is that it overlaps and shares airspace channels with cell phones, Bluetooth, security radios, baby monitors, microwave ovens, etc. Therefore, it is more vulnerable to interference.

Note: 802.11b and 802.11a use different bands within the radio spectrum and are therefore incompatible. Dual-band equipment is currently available which make it possible to connect at both 2.4GHz and 5GHz.

802.11c:
802.11c provides required information to ensure proper bridge operations between Wi-Fi networks. Product developers use this standard when developing access points.

802.11d:
802.11d is supplementary to the Media Access Control designed to promote worldwide use of Wi-Fi. The purpose of 11d is to add features and restrictions to allow Wi-Fi to operate within the regulations of these countries.

802.11e:
802.11e adds quality-of-service features and multimedia support to Wi-Fi. This will be needed to operate delay sensitive services.

802.11f:
802.11f describes wireless access-point communications between multi-vendor systems. The protocol handles the registration of APs within a network and the exchange of information when a user is roaming among coverage areas supported by different vendor's access points.

802.11g:
802.11g, released in June 2003, is 802.11b's second generation interface. 802.11g is high performance and backward compatibility with 802.11b. It offers data speeds up to 54Mbps and operates in the 2.4GHz and 5GHz range. 802.11g is likely to become more popular for Wi-Fi services and leading manufacturers released the product.

802.11i:
802.11i, released in June 2004, is a supplemental draft intended to improve security. It defines new encryption key protocols.

802.11m:
802.11m perform maintenance to Wi-Fi.

802.11n:
802.11n task group formed in September 2003, will develop a standard that will deliver bandwidth increases for 802.11 (at 2.4 and 5-GHz) of up to 108 Mbits.

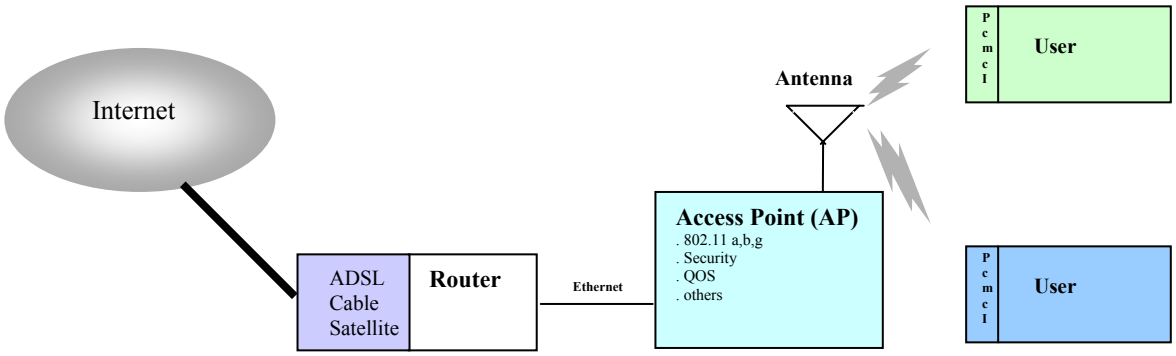
802.11s:
802.11s task group is developing the standard for mesh networking architecture.

Other Standards Organizations

Other credited standards organizations are actively drafting specifications to complement 802.11 activities. For example, The Internet Engineering Task Force (IETF) is drafting recommendations to supplement IT mobility optimizations, extensible authentication protocol, and others. The International Telecommunications Union (ITU) is working on domesticating the 802.11 to the telco world, and contributing to the draft by incorporating voice over Wi-Fi features.

Wi-Fi Building Blocks

Figure 4 shows the mapping of the above IEEE 802.11 requirements into functional Wi-Fi building blocks. Below is a brief description of each. More details, features, and options are provided in the hotspot section of this document.



PCMCI - Personal Computer Memory Card

Figure 4- Wi-Fi Functional Building Blocks

The Wi-Fi building blocks are:
1) Antenna
2) Access Point (AP)
3) Router
4) Internet access

Antenna

Basic Definition

An antenna couples Radio Frequency (RF) energy to the air medium. Access Point (AP) sends the RF signal to the antenna, which acts as a radiator and propagates the signal through the air. The antenna also captures RF signals from a user device via a Network Interface Card (NIC) and makes them available to the receiver circuitry of the AP.

Antenna Characteristics

The antennas must be able to see each other. This is known as Line Of Sight (LOS). LOS must be also tuned for either 2.4 GHz (802.11b, g) or 5 GHz (802.11a). An antenna will only work if the frequency of the antenna and radio matches.

There are two types of antennas commonly used for Wi-Fi network:

1) The more common antenna types for Wi-Fi have an omni-radiation pattern that propagates RF signals in all directions equally (spherical-like plan).
2) Another type is a directional-pattern antenna that transmits and receives RF energy more in one direction than others. Antenna manufacturers usually provide illustrations of the radiation pattern. The higher gain antenna has a narrower beam width, which limits coverage on the sides of the antennas. Directional antennas have gains much higher than omni-directional antennas.

High gain antennas work best for supporting point-to-point (PTP), and Point-to-multipoint (PTM) links to extend coverage. In some cases, a directional antenna can be used for a specific application to optimize coverage. Such typical applications would be a long loading dock of a distribution center or any facility that blends into that physical environment. Variations of directional antennas are further described in the hotspot design section of this manual.

FCC Regulations for Antennas

The Federal Communications Commission (FCC) regulates the use of antennas through FCC Part 15.247, which defines power limitations for Wi-Fi. Equivalent Isotropic Radiated Power (EIRP), represents the total effective transmit power of the radio, including gains that the antenna provides and losses from the antenna cable. For a native omni-directional-antenna, the FCC rules require EIRP to be 1 watt or less.

Access Point (AP)

AP is a transceiver that can connect a wired LAN to one or many wireless devices. AP houses functionality of the radio physical layers (802.11a, b, and g), security settings and the mechanism to provide Quality Of Service (QOS) logic.

Commercially, AP comes in various capabilities to suit particular applications. A fat/ thick AP usually contains rich features and is more suited for an enterprise network setting. A thin AP has fewer features but contains the functionalities one needs for a less sophisticated network. Some vendors provide programmable software to set the physical radio layer to 802.11a, b, g, or dual mode. AP can also be configured as repeaters whereby the RF signal is simply regenerated and relayed onto its intended destination.

Antennas are usually embedded in an AP but recently the FCC ruled that one could replace the native antenna with one that suits specific applications. More detail regarding fat/thick APs is provided in the hotspot design section of this manual.

Router

A router is a device that forwards data packets from one network to another. The packets are forwarded based on routing tables and routing protocols. Routers can also read the network address in each transmitted frame and make a decision on how to send it via the most efficient route based on traffic load, line costs, speed, hub failure, etc.

Commercial routers are available in various capabilities depending on the specific applications. Some routers contain multiple ports (acting as a switch) connecting several APs in order to provide extended coverage or more system capacity. Routers also include a Dynamic Host Control Protocol (DHCP) and Network Address Translation (NAT) modules. These modules create an individual IP address to every Wi-Fi user by sharing the original IP address provided by the Internet Service Provider (ISP). DHCP dynamically assigns an IP address when a Wi-Fi client logs onto the network. NAT takes a single IP address and creates a new one for each Wi-Fi client in order to access the Internet.

Power Over Ethernet (PoE)
The router is connected to the AP via an Ethernet connection. One should consider using Power over Ethernet (PoE) to run electricity to the access points. This avoids the costs of installing electrical outlets throughout the facility to power the APs.

Internet Connection
The router connects to the Internet using the traditional access method. The link could be a T1 connection, ADSL, a cable modem, or a satellite connection.

Note: The above describes the functionality of each building block that is needed to build a Wi-Fi network. Vendors, due to market pressure or targeting a niche market, integrated some or all of the functionalities (antenna, router, access point, and Internet connectivity) into a single box. A coin operated hotspot-in-a box-is one product marketed mainly to small restaurants or kiosks. They are limited in features but cost effective and can deliver the majority of the popular user applications.

Hotspot Design Principles

This section describes a step by step approach to constructing a hotspot zone. The goal is to design a generic hotspot network that is applicable to all without a specialized design. To that end, there are three fundamental requirements that one should look at before deploying the hotspot. The three prerequisites are:
1. Administrative
2. Technical
3. Operational

Administrative Principles
As a part of planning a hotspot deployment, one needs to define the tasks of completing the project. Administratively, the steps are simple but important. The most critical steps are:
1. Registration program
2. Free or fee
3. Broadband Internet access

Registration Program
Registering a hotspot is a very useful marketing tool. For a community operated Wi-Fi network (who offers hotspots as free community service) they can register (typically free) their hotspots in the following Websites:
- ezgoal.com/hotspots/wireless/
- Hotspot-locations.com (community partner section)
- E-nc.org

A Wireless Internet Access Provider (WISP) and others can also register hotspot availability for localities in various website directories (i.e., public hotspot database). Among the most popular are:

- Wifinder.com
- Hotspot-locations.com
- Wi-Fihotspotlist.com
- Hotspothaven.com
- E-nc.org

Free-or-Fee

The numbers of hotspots have been growing exponentially. Businesses and municipalities are recognizing the value of providing hotspots free (or at a very affordable subscription-rate) to lure customers to their premises. Municipalities and communities are also discovering that a hotspot is a great way to share the resources of their community beyond attracting new businesses to the area. Determining free-or-fee, impacts the vendor selection process when building the hotspot zone.

Broadband Internet Access

Typically, an entity has a broadband access modem in place to connect to the Internet. The types of backhaul available include ADSL, cable modem, T1, satellite, wireless radio (e.g., WiMAX), etc. In most instances, this backhaul link will be shared to service the hotspot. More often than not, a new contract should be negotiated with the broadband provider to allow the business to share that connection among its hotspot customers. To the hotspot operators who have no broadband Internet access available; they can purchase one or choose a router that has an integrated Internet access port and negotiate with their local broadband provider for installation.

Technical Principles

Below are some technical helpful hints that should assist in building a sound hotspot. They are:

1. Range vs. performance
2. AP capacity

Range vs. Performance

APs experience RF signal degradation as a user moves further away. A typical AP reduces the data rate to minimize error correction and keep the communication protocol fine-tuned. Typical association of the data rate of an AP to distance is as shown in figure 5 below.

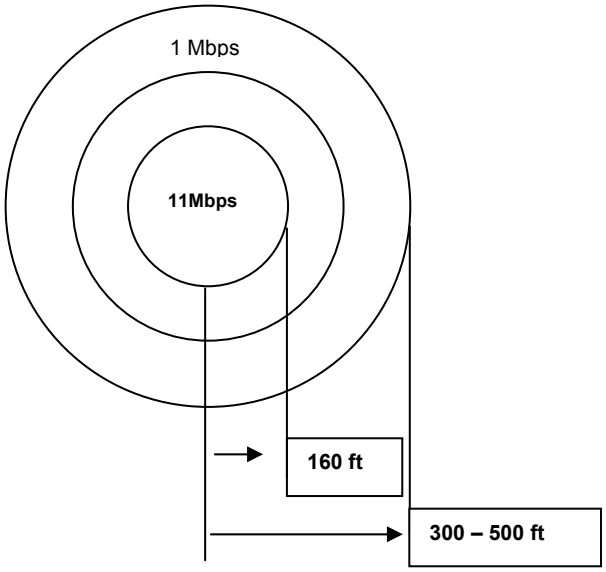


Figure 5- 802.11b Data Rate vs. Distances [5]

As shown in the figure, the data rates are highest when closest to the APs. This diagram should help when precisely computing the capacity of an AP.

AP Capacity

Determining the AP capacity of a given service area is given by the following equation[6]:

$$\#\text{ of APs} = \frac{(\text{Bandwidth}) \mathbf{X} (\text{Number of users}) \mathbf{X} (\text{Activity rate per user})}{(\%\text{ efficiency}) \mathbf{X} (\text{baseline association rate per AP})}$$

Note:

1) **% efficiency is the MAC overhead + error correction = about 50%**
2) **Activity rate per user (for enterprise user is about 25%)**
3) **For example:**
   - For 1Mbps bandwidth (average) to a single user (bi-directional)
   - 100 users
   - 25% activity rate per user
   - 50% MAC efficiency
   - 11 Mbps baseline

   = **4.5 APs or 5 APs**

Figure 6- Equation for Determining AP Capacity

[5] *The Wireless LAN Book for Enterprises* (Trapezen Networks, 2003). p 8.8
[6] *The Wireless LAN Book for Enterprises* (Trapezen Networks, 2003). p 5.15

As applications over Wi-Fi evolve, especially voice over Wi-Fi, a more complex traffic model will be required. Such a traffic model is beyond the scope of this manual. The traffic model could include crucial parameters primarily; traffic mix, percentage of local traffic (community of interest traffic), call duration, etc.

Note: An AP has a bandwidth of (11 Mbps for 802.11b or 54 Mbps for 802.11g/a). The aggregate ingress/ egress traffic (from/to the hotspot toward the Internet) cannot exceed that of the ADSL/ Cable modem speed. The ADSL cable modem typically provides a data rate of approximately .5 to 1.5 Mbps.

Operational Principles

Below are some helpful hints that will prove useful when planning deployment of a hotspot. They are:

1. Certification
2. Environmental survey pitfall
3. Turnkey solution
4. Hotspot life cycle
5. Security disclaimer
6. Maintaining your own network

Certification

When constructing a hotspot, it is highly recommended, that one should select a vendor with products that are Wi-Fi certified. Wi-Fi certified devices/ products, regardless of manufacturer, ensure interoperability e.g., it certifies that the product will work with any other. These products are stamped with the Wi-Fi logo as shown in figure 7.

Figure 7- Wi-Fi Certificate Logo

The Wi-Fi Alliance issues the certification. It is a nonprofit international association formed in 1999, and certifies that 802.11 base products are believed to meet a base standard of interoperability. For more information see vendor list in the appendix.

Environmental Survey Pitfall

When surveying the area to place the hotspot components, it is recommended to lay the antennas in early summer to account for the leaves on trees that are fully covered as opposed to winter with bare trees. Low-power microwaves will bounce off leaves, and will degrade the RF signal, and therefore network performance.

Turnkey Solution

The overall physical deployment of a hotspot is virtually a plug-n-play affair. The hotspot equipment is highly integrated, cost effective, and easy to use. Despite that, it is recommended that hotspot operators (especially those who elect to maintain their own network) should consider selecting a vendor who provides a total solution to build the Wi-Fi network. This enables an operator, in a trouble resolution cycle, to seek technical support from a single point of contact. Hotspot equipment is highly integrated and contains complex features that can best be configured using the software provided by the same vendor. Others, who are technically savvy operators, may elect to save money and shop from different vendors to build their network. Various vendors also form alliances to provide a complete network solution. They also provide a single point of contact as help desk and technical support.

Hotspot Life Cycle

The methodology of maintaining and fine tuning the hotspot network can best be described as shown in figure 8.

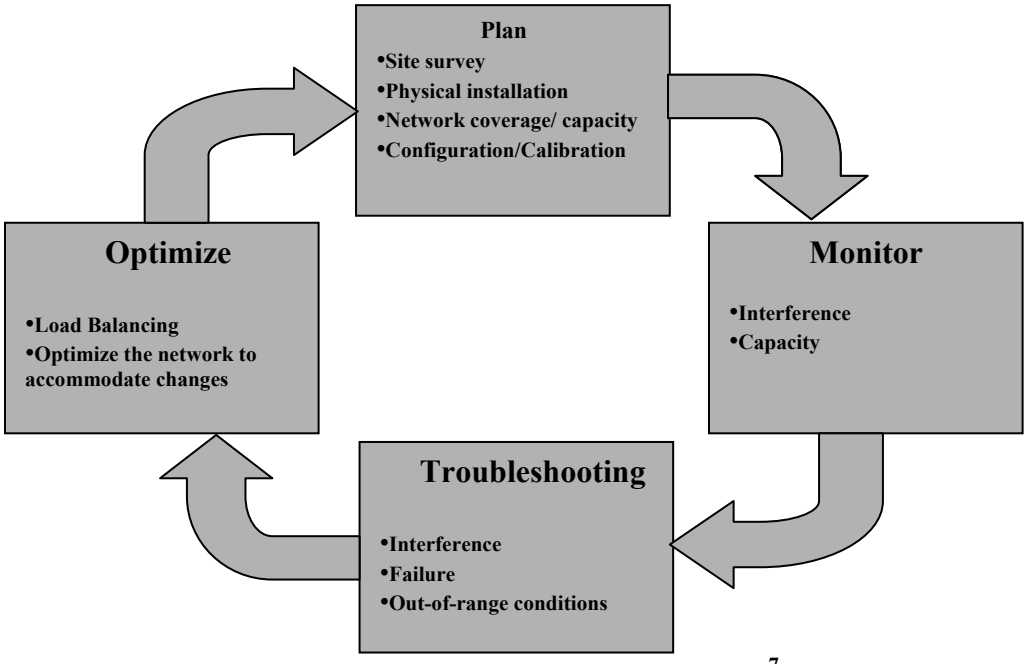


Figure 8- Hotspot Life Cycle [7]

[7] Farpoint Group, "*WLANs: The Big Issues*" NetworkWorld Seminar & Event. Atlanta, July 2004.

The figure depicts a lifecycle approach to building a Wi-Fi network, whereby the operator periodically keys or repeats processes to fine tune ongoing operations. The staff performs daily routines resulting in optimizing the hotspot design and continuously repeating/ completing the cycle while returning to the planning stage.

Security Disclaimer

Security setting plays a major role when configuring the Wi-Fi network. The details of configuring security are described in the "designing a hotspot "of this manual. For a community run Wi-Fi network, especially the ones that encourage visitors to access the community hotspot, the security setting should be set to minimum (or none) in order not to defeat its intended objective. It is therefore, recommended that operators, who are running an insecure Wi-Fi network, issue a disclaimer to users on their welcome page.

Maintaining Your Own Network

Each hotspot operator has a unique business model. The lack of regulatory barriers encourages a greater diversity of operators to enter the business. This creates a market opportunity for establishing firms who are uniquely qualified to maintain hotspot networks. A business establishment or municipality should evaluate the pros and cons of establishing and maintaining the Wi-Fi physical infrastructure, or simply outsource it.

The recurring cost of a Wi-Fi network could be significant. A case in point is the St. Cloud, FL community; its citywide Wi-Fi network, estimated that the city's yearly expense (including customer service) would be $150,000 to $200,000[8]. The network covers 30 square kilometers, deploying 300 access points and eight to 10 wireless links to the network backbone at the cost of about $1 million.

Communities are struggling on how best to pay for the ongoing cost. The two scenarios are either through user fees or as an allocation from the city's general fund. When evaluating the pros and cons of providing a free community Wi-Fi network, two factors should be included in the business model:

1. The cost of ***not*** providing broadband access to your community.
2. The recycling of funds back to the local economy. For example, in the case of the St. Cloud Wi-Fi network with 300 access points (approximately 15,000 users), $4 to $7 million (yearly) could be funneled back to the local economy assuming a user will otherwise have to pay $300 to $500 yearly subscription fee to outsiders.

[8] Debra Asbrand, "Who Pays for Wireless Cities?" *MITTechnology Review* (September 2004). http://www.technologyreview.com/articles/04/09/wo_asbrand092104.asp?p=2

Wi-Fi Deployment Best Practices

Hotspot Design

There are three steps one needs to complete the project and minimize the risk of costly modifications. The steps vary in complexity depending on the sort of hotspot zone one is building. The guidelines below address three types of Wi-Fi networks; the enterprise network, the public network, and the community operated network.

The end-result of the design procedure would enable a Wi-Fi operator to develop system architecture, identify the appropriate access point, and antennas and produce the bill of material.

The three steps are:
1. Defining the requirements
2. Site survey
3. Security

Requirement Phase

This task is critical and could have profound implications on the sort of equipment one needs to build the network that meets user expectations. For WISPs who are building a public Wi-Fi network a survey of potential customers must be completed. Communities who are entertaining the notion of "*if we build it they will come*" should consider a best case scenario because equipment costs are not likely to be the determining factor, but network redesign would be.

The list of requirements includes the following:

- End-user (your clients)
- User applications
- Project funding

End-User

Network operators should define the sort of end user devices that the client will use to access the Wi-Fi network. Most common devices used are laptop, PDAs, Pocket PC, Wi-Fi Phone, and the operating system each uses. Most devices use the 802.11b, g radio interface, but some are equipped with 802.11a (some APs can function in dual mode). Roaming is also a factor the operator needs to determine. All the above information will help determine the AP selection and will determine the class of security that must be supported by the network.

User Applications

Network operators should define the sort of applications the end-user is likely to use. Today's most popular applications are:

- Web browsing including email, file upload/ download
- Audio/ video streaming
- Telemetry (video/ audio monitoring)
- Voice over Wi-Fi
- Community of interest traffic

Listing such information determines the sort of traffic mix the Wi-Fi network must handle and therefore the AP capacity and features needed. For example, if voice over Wi-Fi is part of the traffic mix, then the AP (MAC layer) must include quality of service features.

Project Funding

Project funding plays its role in determining the scope of the overall project. Some community-run Wi-Fi network organizations that provide free Internet access to their communities were successful in securing funds from local financial institutions. Banks in particular believe in investing in community infrastructure because it will eventually revive the local economy. Securing equipment donations from Cisco, HP and other well-established companies is another avenue community developers have successfully pursued.

For example: The Tribal Digital Village of southern California was awarded a $500,000 grant. At least 75% is to be in the form of HP equipment. See http://www.sctca.net/sctdv/sctdv.html. Intel has a strong interest in supporting (in grants and programs) for K-12/higher education and community programs See: http://www.intel.com/community/grant.htm.

WISP operators and community organizations who are contemplating providing Wi-Fi Internet access and services should investigate these funding options before determining the scope of the project.

Site Survey

Site survey is a challenging part of building a Wi-Fi network. One must accurately survey the area to determine the total numbers as well as the locations of antennas and the number and classes of access points (indoor/outdoor) needed for a given coverage. Installing antennas and access points are labor intensive task and it will be worthwhile investing the needed resources to prevent costly re-engineering. Before embarking on surveying the area it is important to be familiar with the physics of the access point's RF radiation patterns, and the art of designing micro-cells for optimal coverage.

Cell Design

The 802.11b and 802.11g standard defines 11 channels for the US (14 in Europe.) that overlap. Figure 9 below shows the spectral placement of the channels as defined by IEEE

802.11b. For the 802.11a RF interfaces, all eight channels are non-overlapping. Access points are usually preset to a particular channel when shipped from the factory (normally to channel 1). The RF reach of each channel is about 160 ft indoors or 300 to 500 ft outdoors (as previously shown in figure 5). The RF dispersion is shaped in a donut-like (360-degree beam width).

There are three non-overlapping channels (channels, 1, 6, and 11). This enables a designer to install three access points (using channels 1, 6, and 11 respectively) in the same area without RF interference. This is routinely done in areas with a heavy concentration of users to provide a greater aggregate bandwidth.

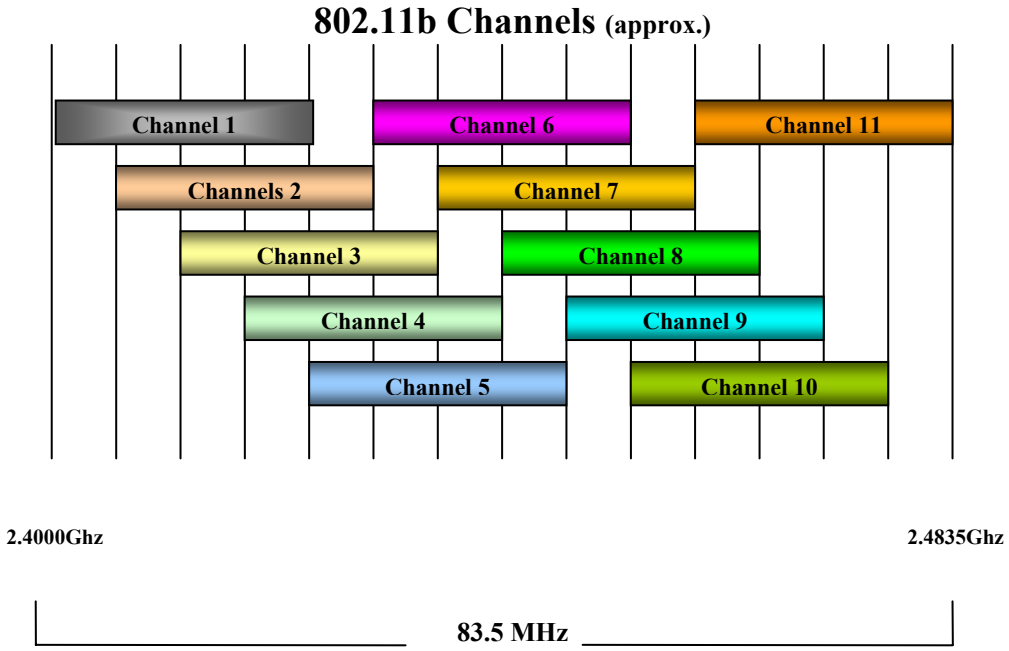


Figure 9- Spectral Distribution for 802.11b Channel

Other non-overlapping channels shown are: channels 2, 7, channels 3, 8, channels 4, 9, and channels 5, 10. Ideally, one would like to use non-overlapping channels to cover a large area without overlap. Channels 1, 6, and 11are typically used to cover a large area. Figure 10 is an example of nine access points using non-overlapping channels.

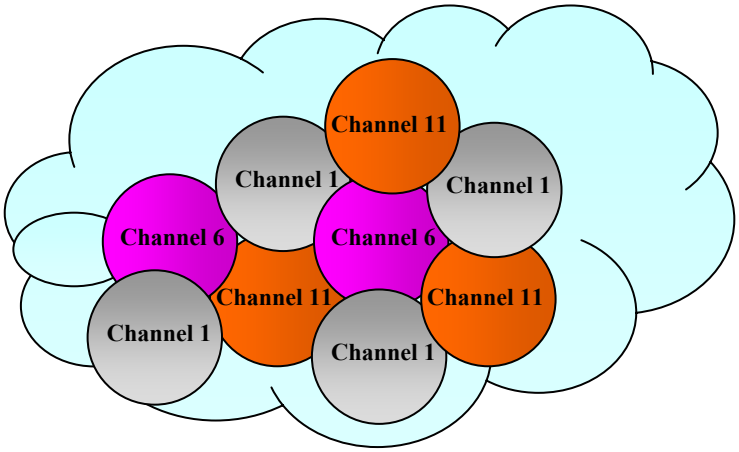


Figure 10- Example of Micro Cell Layout Using Channels 1, 6, and 11

One can also use the other sets of non-overlapping channels 2, 7, channels 3, 8, and channels 4, 9, and channels 5, 10. In either case, one must ensure that the micro-cells overlap to avoid dead spots. This design approach ensures full coverage while avoiding channel interference.

Survey Tools

Channel interference described above is self-contained, but in the real world of 802.11b, interference emanating from external sources may defeat the cell one designed. Radio interference from nearby microwave ovens, cordless telephones, or simply interference from a nearby Wi-Fi network will determine the channel selection criteria shown in figure 10. The second phase of surveying a construction site is to actually tour the area and perform RF measurement to validate the cell design and rearrange the channel numbers if needed.

RF monitoring tools are available on the market today that sniff and measure the strength of an intruding channel(s). Spectrum analyzer is a good candidate to identify all channels and noise but it is expensive. More Wi-Fi friendly RF sniffer devices (less costly) are being introduced to the market from various Wi-Fi oriented vendors.

A notebook or a Pocket PC device, with a Wi-Fi transceiver can also be used as a survey tool to detect RF signals in the underlining areas. Most Wi-Fi vendors provide site-survey software utilities (free of charge) that give a would-be operator an overview map of the channels in use emanating from a nearby network. Based on the survey findings, one can re-arrange the channel selections (shown in figure 10) to prevent interference from the intruding channels.

Survey Guidelines for the Enterprise Network

For enterprise Wi-Fi deployment, surveying a complex is simpler because one deals with more or less a controlled environment. Particular focus, however, will include the number of access points needed (per cell) to accommodate the users and their respective locations. Locating access points can be tricky in that the furnisher, type of wall paint, building

materials/structure, and personnel traffic/motions can play an obstructing role and generate ghost/ reflections of the RF signal(s) hence degrading network performance. The RF signal from a particular access point(s) can also leak to other rooms or floors and again degrade network performance. A possible solution is to place the access point (or associated antennas) at the ceiling to minimize RF interference. This ensures that a channel selected for a given cell is not in proximity to other APs operating at the same channel.

Corporate Wi-Fi network operators will more likely use the 802.11a physical layer (instead of 802.11b or g). In a corporate environment, the 802.11a has the advantages of limited wall penetration and range. Moreover, 802.11a specifies eight non-overlapping channels so, statistically, RF channel interference (with careful design) is less likely to occur.

Rouge AP is one major concern in the minds of enterprise Information Technology (IT) operators. Rouge AP is one that is not sanctioned or installed by the responsible IT staff. For example, if a RF signal leaks into a parking lot of a company, a malicious user can use a handheld device and access that network and its resources uninvited. Worst yet, the malicious user can configure an AP as a repeater or as a station (hence rouge AP) and extend coverage to others in the area. Modern security settings and firewalls are used to remedy this, but that will not prevent repeated attempts of hacking.

Survey Guidelines for Public/ Community Network

Surveying guidelines of the public/ community operated network is similar to that of the enterprise network but focuses more on the landscape, geographic area coverage and determining how much bandwidth is needed in a given area. One should assume that an AP range outdoors is typically 300 to 500 feet.

Assuming an AP capacity can handle 20 enterprise users as previously determined (per figure 6) or more (typically 50) for casual user, the rest of the exercise can then focus on:

- Physical locations of the APs
- Locations of the high gain antennas for extended coverage.

Physical Locations of the APs

Locating access points in a public area can be challenging. Trees, wet leaves (absorb/ reflect microwave energy), humidity, fences, pipes, bridges; bodies of water, and simple traffic can obstruct the originating RF signal and in some cases severely degrade network performance. APs are, usually, mounted on poles, or edges of a building for optimal performance. Placing APs indoors (to cover a public area) is preferable and should be the first choice. Indoor APs are less expensive; it will also resolve the issue of powering the units, or performing basic environmental maintenance. Outdoor APs may require lightning protection and grounding. Operators, usually negotiate with building tenants to place the APs in their dwelling's windows (clear of all obstacles) to cover the area under construction.

The cell design shown in figure 10 assumes the capability of standard APs with a native omni antenna. Depending on the survey findings, the antenna on the access point can be

exchanged with one that is better suited to meet specific area coverage that blends into a particular physical environment. See Appendix for more information regarding antennas.

Antenna Types and Variations

A summary of the type of available antennas and their characteristics are:

Omni High Gain Antenna:

Omni antenna by definition radiates RF energy in a donut-like pattern. It is a thin pole ranging in size from one to five feet. Longer poles have more gain. It is usually mounted vertically and some can replace the native AP antenna

Sector High Gain Antenna:

Sector antennas radiate the RF energy in one direction (180 degrees or 60 degrees). They come in various shapes; square, or circular. The antenna is usually mounted on ceiling or walls. Sector antennas are used for point-to-multipoint applications

Yagi Antenna:

Yagi antenna resemble a TV Arial antenna with elements crisscrossing along its pipe axis. The more elements, the higher the gain. Yagi works well in point-to-point and point-to-multipoint applications. The RF radiation pattern varies between 15 to 60 degrees.

Dish Antenna:

Dish Antennas (mesh or solid base), radiate a very narrow beam and hence ideal for a point-to-point application. The size can reach 30 feet in diameter. For a 30-mile range, the dish dimension will only be a few feet in diameter. Dish antennas are usually mounted on water towers, poles or top of buildings.

Locating High Gain Antennas for Extended Coverage

Surveying a high-gain antenna location is a demanding task and requires the establishment of a line of site (LOS). It is worth noting that one should not casually deploy a high-gain antenna (mounted on a tower) to service a high-density area. In most instances, using the cell design method described above (low power APs to saturate a hotspot zone) is much easier and less expensive to deploy. This good-citizenry approach limits interference to yours and nearby neighbor's networks.

Mapping the Topography

Surveying a facility to install a high-gain antenna for a point-to-point long-reach application is challenging. The high-gain antenna setting requires precise alignment and can be tricky. Fortunately, there are adequate online tools to simplify and minimize the risk of the planning task. The online resources available to dimension a region or a particular segment are:

- **Globexplorer.com**: provides color area photographs and high-resolution aerial photographs. One simply keys in a landmark or street address including county and state to identify an area. The service is free
- **Mapquest.com**: provides high-quality street maps and coordinates. Using a ruler, one can plot the distances between two points to get an idea about the range for the potential antenna sites. Mapquest also provides color aerial photographs.
- **Earthexplorer.usgs.gov**: Provides high-resolution photographic maps that enable a user to determine how the land lies between two points (potential antenna sites). The service is free but one can order higher quality maps for a fee.
- **Topozone.com**: Provides a topographical map of the surrounding terrain of an area. One can quickly determine the distances and observe any obstructions between any two points.
- **Esri.com**: Provides map viewer applications of the selected sites. Geographic Information Systems (GIS) tools are used to precisely determine the distances and terrain through modeling and mapping.

Most of the websites above provide longitude and latitudes measurements of the selected points.

Global Positioning System (GPS) Tool

Visiting the subject area (walking the walk) is one of the last steps one needs to survey an area after performing the paper research. A handheld GPS device or available software tools (on a PC platform) can validate the topographical map (prepared per above) and measure the precise latitude and longitude of the site(s). Once the latitude and longitude is established one can use the data online at http://www.Qsl.net/n9zia/wireless/page09.html to obtain valuable data such as: LOS path analysis, Path loss, Link analysis (power level), and others.

Installing the Antennas

Installing point-to-point antennas especially on towers, poles, on a hill, etc., should best be left to the experts. Special tools maybe needed to align the point-to-point antenna (with 30 miles or over) in order to maximize the RF signal strength. Other factors such as: Installing lightning protections, grounding, type, quality and length of the cabling; the numerous specialized types of connectors and other parts play a critical role that minimizes signal loss. Some communities are able to secure expert volunteers from their community to install and align the antennas. The task requires understanding of RF and computing technology.

Security

Security is one important concern particularly to enterprise network operators. Community-operated networks, are usually "open network" that means anyone within reach of the hotspot can access the network. Recent survey of popular community operated networks found that less than 50% have no security setting of their Wi-Fi network[9]. This is understandable since open network access encourages visitors and local residents to log on without the hassle of administrative protocols. For all other networks, enabling security features plays a vital role in protecting sensitive information stored or being transmitted over the wireless medium.

Classes of Wi-Fi Security

There are 4 classes of security mechanisms one can configure to protect the data integrity of the network and end-users. Both authentication and encryption techniques are used to secure access to the Wi-Fi network. They are:

1. Service Set ID (SSID)
2. Wired Equivalent Privacy (WEP)
3. Wi-Fi Protected Access (WPA1 and WAP2)
4. MAC Filtering

Service Set ID (SSID)

SSID is normally thought to be the first defense of authenticating an end-user to a Wi-Fi network. SSID is an association between the end-user devices and the network. An end user must know the SSID in order to access the network. It is referred to as the Wi-Fi network name. AP manufacturers normally set the SSID to the manufacturer's name. When configuring the network/ device the SSID between the end-user device and access point must match to admit a user's device to join the network. One can change the SSID (when initializing the network) to mirror your actual Wi-Fi network name.

[9] Netgear: "Wireless LAN security" technology overview. April 2003

The access point periodically broadcasts this SSID name, which makes it easy for anyone to determine it. It has been a common practice to disable this broadcasting feature when configuring the network, especially for a secure network.

Wired Equivalent Privacy (WEP)

WEP, as the name implies, provides basic security and is only intended to provide no more protection than one would have if one is physically plugged into a wired LAN. WEP encrypts the information flow based on a secret key shared among all users of that particular Wi-Fi network. It is not a perfect security key but then, it was not intended to be. A determined hacker can break the code but it is an effective deterrent to most casual users.

Enabling WEP is performed upon system configuration. One sets the key-length as well as the key itself. The key is a string of ASCII key codes that are shared among clients who subscribe to the network. The strength of the encryption is measured by the key-length. The key length determines the level of encryption used. 802.11b implementations provided 40-bit WEP; later versions strengthened WEP to use a 64-bit key, and a 152 bit.

If one uses APs from different vendors, the security setting must be set to the least common denominator. Only devices with common WEP settings will be able to communicate. Moreover, WEP enabled devices cannot communicate with devices that are not WEP enabled.

Wi-Fi Protected Access1 (WPA1)

For an enterprise grade WLAN network, using WEP encryption described above is not sufficient. The idea of a hacker in a parking lot with a directional antenna accessing the corporate LAN, understandably, does not bode well with the IT security staff. A determined malicious user with time and basic skills can crack the WEP encryption code and hence breach WLAN encryption security. The WEP encryption mechanism calls for all users to have the same key & key length in order to access the network. To periodically change encryption (in order to defeat a hacker) is an elaborate maintenance scheme, whereby all clients must change the encryption key to regain network access. Therefore, the encryption keys go unchanged for months hence providing a hacker with enough clues to crack the encryption key. Various academic studies also exposed WEP weaknesses and found that for a small business WLAN where traffic is low, a hacker can break the WEP code in a matter of hours[10]

In response to this increasing concern, Wi-Fi alliance pre-implemented IEEE 802.11i enhanced Wi-Fi Protected Access (WPA1) security features in 2003. The goal of WPA1 is to improve data encryption and introduce an authentication mechanism to the WEP approach. It is worth noting that WEP based units are software upgradeable to WPA1.

WPA1 introduced a dynamic form of WEP encryption referred to as the Temporal Key Integrity Protocol (TKIP). TKIP combines a temporal key with the client's MAC address

[10] C. Brian Grimm., "Overview Wi-Fi Protected Access" (Wi-Fi Alliance, 2002). p 1.

and then adds an initialization vector to produce the key that will encrypt the data. This procedure ensures that each station uses a different key to encrypt the data. Moreover, WPA1 automatically generates a new unique encryption key periodically for each client. This avoids the same key staying in use for months as they do with WEP. A hacker will find it more difficult to crack the encryption key since each client has a unique encryption key.

Wi-Fi Protected Access2 (WPA2)

In June 2004, IEEE 80211i was released. The new specification offers significant improvements over the old WEP standard. The Wi-Fi Alliance refers to the new 802.11i standard as WPA2.

WPA2 takes WPA1 a step further. It uses the Advanced Encryption Standard (AES); AES supports key lengths up to 256 bits and meets government security criteria and provides stronger encryption than WPA1. In addition, WPA2 encrypts the whole data frame with AES. WEP and WPA1 encrypt the data payload only. Another element of WPA2 is the Robust Security Network (RSN), which dynamically negotiates the authentication and encryption algorithms to be used for communications. This implies that as new threats are discovered, new algorithms are created and can be added.

Note: AES has its own coprocessor, which means older existing wireless hardware will have to be replaced. Current handheld devices (Pocket PCs and PDAs) do not have enough processing power to support AES. Therefore, WPA1 is the best security choice if you have users who store and transmit sensitive data via handheld devices.

Media Access Control (MAC) Filtering

This authentication method uses MAC filtering that denies access to unauthorized end-users. Every Wi-Fi communication device (for example a laptop NIC card) contains a *unique* MAC address identifying its hardware (it is affixed and clearly labeled in the hardware). Wi-Fi operators can enter a MAC address to the database of the access point as a condition to grant access. That MAC address identifies the user device as a client subscriber. Any device that is not listed in the access point database will be denied access.

The protocol of accessing the network is as follows:
The access point broadcasts its presence and grants access to any device requesting service. The access point validates the MAC address of the device requesting access in response and denies the service if that MAC address is not in its database. Note that the MAC address identifies the NIC card and not the laptop. That means one can use any laptop as long as the MAC address of the NIC card is registered and listed in the access point database.

Wi-Fi Network Architecture

Wi-Fi network topologies described below are widely deployed in residential, enterprise and public areas all around the world. Each component of a Wi-Fi requires a radio transceiver and antenna. Components are either stations (e.g., user devices) or APs.

Network Basic Service Set

A network is established when a station(s) and APs have recognized each other and established a communication link. A network can be configured in two basic ways:

1. Ad hoc (Peer-to-peer) network
2. Infrastructure network

Ad Hoc (Peer-to-Peer) Network

In this configuration, two or more stations can talk to each other without an AP. This arrangement is referred to as an Independent Basic Service Set (IBSS). Access to the wired network (Internet) is accomplished at the station that has the Internet access port.

Infrastructure Network

This configuration consists of multiple stations connected to an AP. The AP acts as a bridge to the wired network. This arrangement is referred to as a Basic Service Set (BSS)

Roaming

An Extended Service Set (ESS) is affiliated with BSS in that a sub-net is formed that contains more that one AP to serve clients. In this arrangement, the APs communicate with each other handing off authentication and IP address data hence allowing a client to roam.

Roaming between Wi-Fi networks separated by a router or roaming between Wi-Fi networks is a more complex model. Billing arrangement/ negotiation and IP address management become more complex to grant access to various types of operator's subscribers in their hotspots. Vendors offer various solutions based on a subset of 802.11f.

The basic definitions of the BSS, ESS and IBSS stated above form the various network blueprints as shown in the three figures below. They are mainly:

1. Enterprise network blueprint
2. Public/ community Wi-Fi Network: Hub and Spoke
3. Public/ community Wi-Fi Network: Mesh architecture

Enterprise Network Blueprint

Figure 11 below shows an example of a typical enterprise type network. More often than not, most literature refers to enterprise-type networks as WLAN. The figure below is one example illustrating an existing LAN overlay with wireless components to a corporate building with several floors.

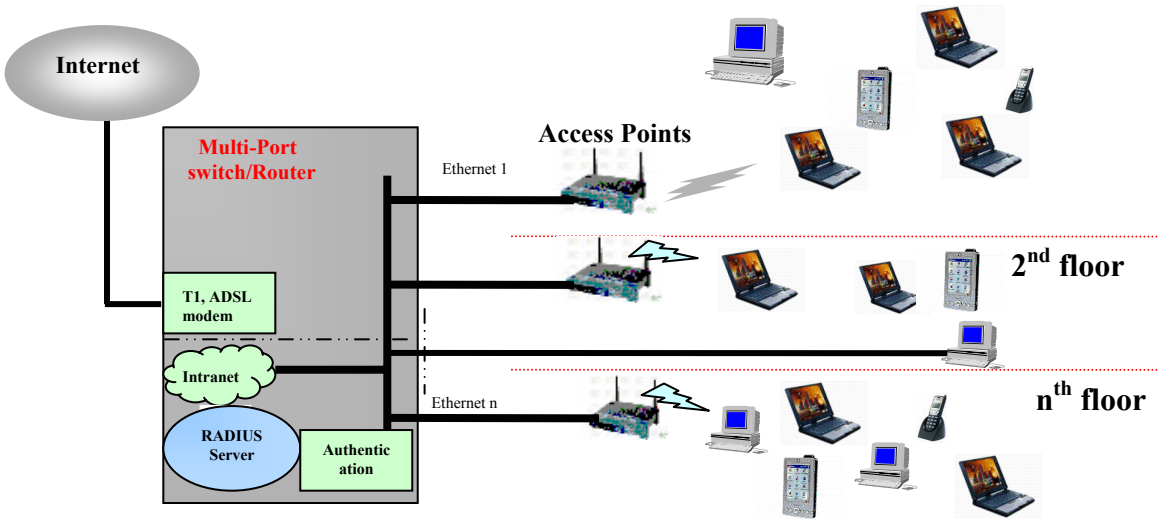


Figure 11- Typical Wi-Fi Enterprise Network Diagram

The enterprise WLAN market is fierce, green, and very profitable. WLAN vendors offer a host of AP capabilities to address the specific needs of the WLAN market. APs come in various capabilities such as Fat/thick AP, Thin AP and Intelligent AP. Fat APs are feature-rich with robust Quality Of Service (QOS) and security features. Some fat APs contain downloadable software to configure 802.11a, 802.11b/g, or dual RF interfaces. Such feature rich APs are more expensive, requiring high computing power per AP and are subject to security breach if the AP is stolen (it contains important security settings). Fat APs are easier to manage/maintain and therefore exhibit lower infrastructure cost. Thin APs contain very few features other than the radio interface. All other sensitive features are centralized in local servers. Such configurations require higher initial cost, but scale very well in price. Intelligent APs vary in capabilities addressing a specialized niche WLAN market. Firewall, up to date security features, and sniffing software (to locate rouge APs) are "must" features when addressing the WLAN market.

802.11A	802.11B	802.11G	SSID	MAC FILTERING	WEP - WPA 1, 2	CAPACITY
Usage +++	Usage +	Usage ++	Disable	Yes	WPA 1 or 2	20 users

Table 3- Enterprise AP: Suggested Selection Criteria

Public/ Community Wi-Fi Network: Hub and Spoke

Figure 12 shows a large-scale public/community Wi-Fi network diagram for the hub and spoke wireless systems. Users connect with line-of-sight antennas to a centrally located base station.

Advantages of hub & spoke deployment:

- Internet traffic (egress/ ingress) is high.
- Sparse region where long reach antennas are needed
- Interconnect nearby Wi-Fi communities
- Exhibit lower delays (latency)

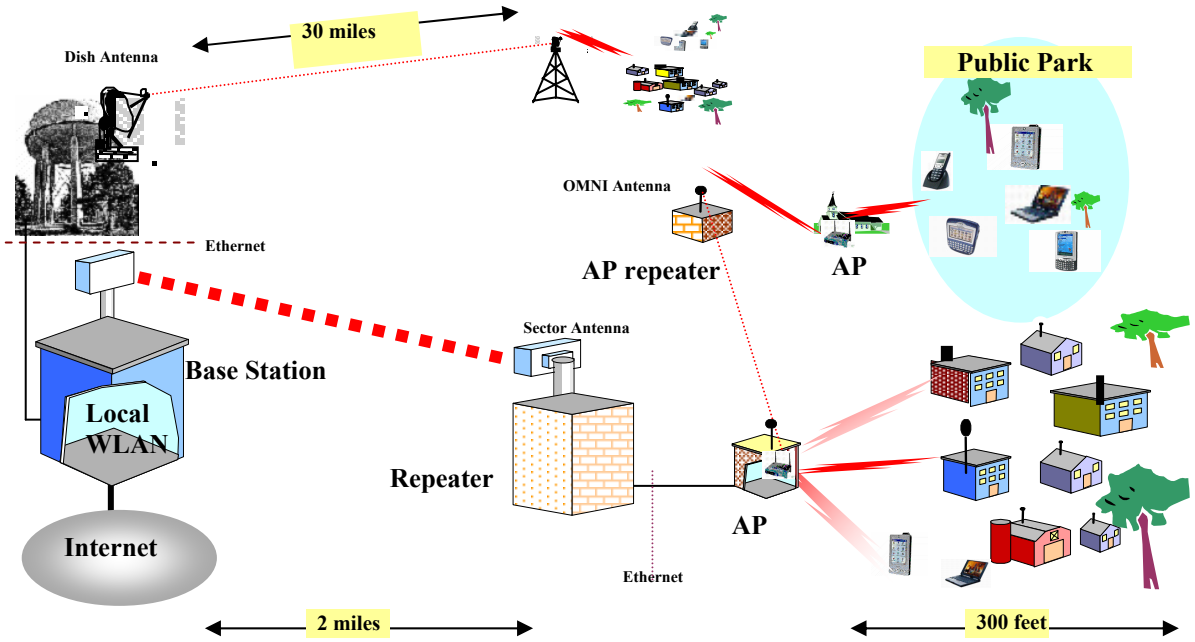


Figure 12- Typical Public/ Community Wi-Fi (Hub & Spoke) Network Diagram

802.11A	802.11B	802.11G	SSID	MAC FILTERING	WEP - WPA 1, 2	CAPACITY
Usage +	Usage +++	Usage +++	Disable	Yes	WEP, WPA 1, 2	20 to 50 users

Table 4- WISP AP: Suggested Selection Criteria

802.11A	802.11B	802.11G	SSID	MAC FILTERING	WEP - WPA 1, 2	CAPACITY
Usage +	Usage +++	Usage +++	Enable	No	Disable	20 to 50 users

Table 5- Community AP: Suggested Selection Criteria (Hub & Spoke)

Public Wi-Fi Network: Mesh Architecture

Mesh wireless system, as shown in figure 13, offers multiple points connection in that it allows large-scale deployment of wireless networks without having to physically link every access point back to the wired network. Each access point/router device (including laptop/ PDAs) hops through neighboring devices to communicate with other and or reach the wired node that has access to the Internet. Mesh users can bypass obstacles (such as hills, trees, bridges etc.) by using different path(s). Several vendors offer mesh-based software packages (pre-implementing 802.11s) Advantages of mesh systems:

- Uses less wires to connect the network
- Scalable
- Routes around congested links
- No single point of failure (self healing by using alternate route)
- Ideal applications for community/ municipality networks where community-of-interest traffic is very high. Community of interest traffic includes: police cars, fire department, command headquarter, emergency center, hospitals, Mayor's offices etc.

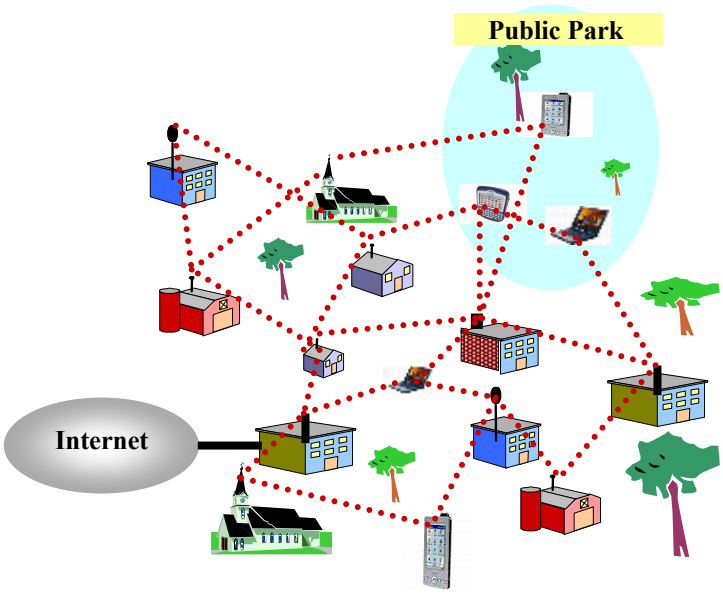


Figure 13- Typical Public/ Community Wi-Fi (Mesh) Network Diagram

802.11A	802.11B	802.11G	SSID	MAC FILTERING	WEP- WPA 1, 2	CAPACITY
Usage +	Usage +++	Usage +++	Enable	No	Disable	20 to 50 users

Table 6- Community AP: Suggested Selection Criteria (Mesh)

Putting It All Together

The information detailed thus far should have prepared an operator to determine the followings:

- Technical and policy implications
- Number and locations of access points needed to build a specific Wi-Fi network
- Access point capacity
- Access point security feature requirements to build specific Wi-Fi network
- Access point setting options to maximize performance
- Antenna selection options and installation guidelines

With this information, an operator should be able to build a specific Wi-Fi network with cost model estimates. See the appendix for the AP vendor list, and an example of a typical Wi-Fi cost model.

Equipment Selection Criteria and Configuration

Summary of AP Selection Criteria

An operator must choose the physical layer interface. The various 802.11 flavors on the market are 802.11a, b or g. 802.11b and 802.11g are the obvious choices today, because they offer high data rates and wide acceptance.

For an operator who determined that a single AP is all that is needed (based on the physical structure of the network and the anticipated traffic flow), then an AP with integrated functionality becomes an attractive choice. That means one selects an access mechanism that will handle authentication, billing and IP address translation. Hotspot-in-a-box is a typical product well suited for restaurants, coffee shops, etc.

If the Wi-Fi network design calls for multiple access points then a more cost-effective solution would be to select plain APs (referred to as a thin AP), and connect them together on the back to a router box. Similar boxes may also be needed that contain management functionality, authentication and billing functions.

Equipment Installation and Configuration

Vendors usually provide installation and configuration guidelines. An operator uses a regular PC with Windows98 or above operating system to configure the network parameters. The configuration process is routine and uses Wizard-type guidelines instructing operators to configure their network. Below are some tips that could be helpful and applied to specific implementation.

Network Parameter Setting and Configuration

In the case of a single AP deployment, the configuration is simple. One first assigns a static IP address to the access point, and then enters the IP address for the gateway. The Dynamic Host Configuration Protocol (DHCP) server is needed to route packets on the network. A Network Address Translation (NAT) server is also needed to provide a mechanism of IP address translation to all the clients connected to the Wi-Fi network. IP addresses are expensive and in high demand, therefore a WISP operator uses NAT to provide a disguise-like IP to service all Wi-Fi clients.

When configuring the network it is recommended that the operator disable WEP security. Otherwise, the operator must distribute the WEP key and key-length to every user.
For a community operated Wi-Fi network, WEP may be disabled if the operator wishes visitors to log on to the community website without the administrative protocol.

When configuring the SSID, an operator should set the name of the company/community offering the service. All access points must have the same SSID name.

Installation: Installation in most instances means cabling the equipment based on vendor instruction of APs (Ethernet cabling) or High gain antennas (when needed).

Testing: Vendors usually provide procedures and software tools to enable an operator to test that particular network configuration. It is recommended that one should periodically exercise the life cycle routines as stated as shown in figure 8 in order to keep the network fine-tuned.

WiMAX Technology Briefs

WiMAX Introduction

Fixed wireless broadband technology known as WiMAX continues to gain momentum in the industry. The WiMAX Forum was created to certify the IEEE 802.16 standard for fixed wireless broadband Metropolitan Area Networks. The WiMAX Forum certifies that a product conforms to the standard and is interoperable. The WiMAX industry consortium hopes its specification will encourage vendors to develop low-cost components for WiMAX.

WiMAX Physical Layer

WiMAX in particular focused on the "first-mile/last-mile" connection in wireless metropolitan area networks. Table 7 below shows the bandwidth interfaces between 10 and 66 GHz.

The 10 to 66 GHz standard supports varying traffic levels at many licensed frequencies (e.g., 10.5, 25, 26, 31, 38 and 39 GHz) for two-way communications. The draft amendment for the 2 to 11 GHz region will support both unlicensed and licensed bands.

Designation	*Description*	*Range/ Feature*	*Frequency band*
802.16	70 Mbps	31 miles/ LOS req.	10-66 GHz
802.16a	70 Mbps	31 miles/ NLOS/ Mesh	2 –11 GHz band
802.16b	QOS spec		
802.16c	WiMAX Profile		
802.16d	16a upgrade		
802.16e*	Cellular upgrade		

* Expected release 1Q 2005

Table 7- 802.16 (WiMAX) Standard Activities and Status

Unlike Wi-Fi, WiMAX was developed to address the Metropolitan Area Network (MAN) market. Presently, WiMAX is already deployed by educational and health-care facilities, local governments and enterprises with multiple facilities in a metropolitan area.

WiMAX has become the best way to meet the escalating business demand for rapid Internet connection and integrated data, voice and video services. Today, small businesses and residential customers typically use wired networks, such as cable modem networks and DSL. These broadband accesses may not be available in serving business subscribers because of distance limitations. Two-way satellite access is one solution, especially in rural areas, but it has limited application due to latency and high cost. One of the advantages of WiMAX is that networks can be deployed in a few weeks using a small number of base stations (on buildings or poles) to create high-capacity wireless access systems.

WiMAX MAC Layer

The released standards also defined the MAC layer that supports multiple physical layer specifications. Contention and priority schemes were also developed in the MAC layer to provide a QOS mechanism that supports the different needs of different applications. For instance, voice and video require low latency but tolerate some error rate. By contrast, data applications cannot tolerate error, but packet delay is not critical.

WiMAX architecture is optimized to operate in point-to-multipoint and mesh topologies. It is therefore scalable and affords carriers to expand the subscriber base as demand for bandwidth grows by adding channels or cells.

WiMAX Network Architecture

Figure 14 depicts a typical WiMAX architecture. Conceptually, WiMAX is similar to the cellular telephony in that a service area would be divided into cells. WiMAX is able to operate in a Line Of Sight (LOS) and near/non LOS (NLOS) access approach.

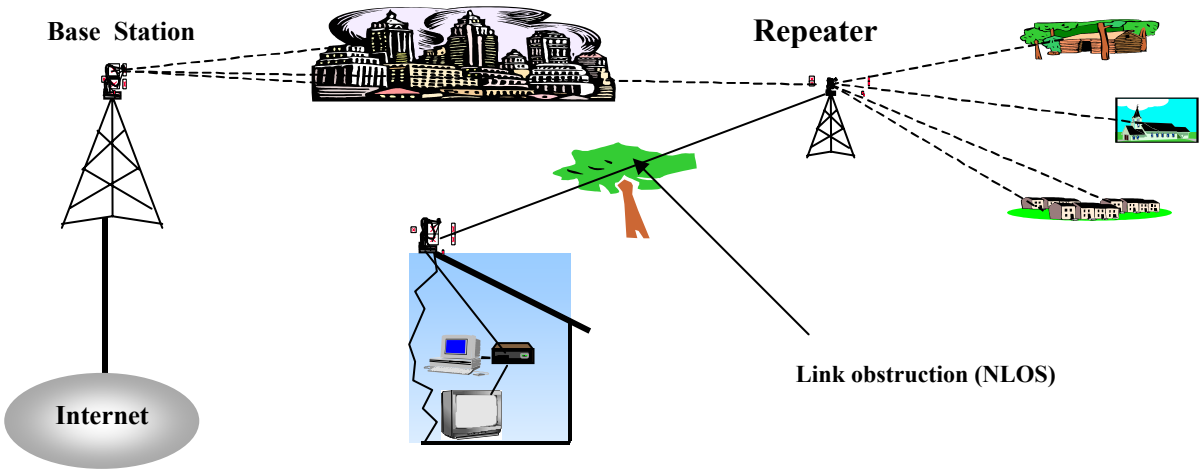


Figure 14- Typical WiMAX Network Diagram

NLOS

Unlike Wi-Fi, WiMAX (in IEEE 802.16a) standard established six channel models, from LOS to NLOS, for fixed-wireless systems operating in license-exempt frequencies from 2 GHz to 11 GHz. Orthogonal Frequency Division Multiplexing (OFDM) technique and variants of OFDM are used to penetrate foliage and walls, circumvent hills, resist radio interference, etc.

One obvious advantage of WiMAX (when compared to Wi-Fi) is the NLOS approach whereby, it is much simpler to deploy a wireless network. WISPs, also found that they can typically achieve clear LOS to only 30 to 40 percent of potential subscribers in high-rise

urban areas[11]. This low penetration rate prompted major carriers to wait until vendors developed NLOS solutions.

WiMAX System Capacity

WiMAX's base stations cover areas within a radius of ten miles. The WiMAX access bandwidth is shared among all the subscribers and in order to guarantee high speed to users, the target is to have no more than 500 subscribers per base station.

Serving Underserved Areas

WiMAX is one preferred choice for underserved rural and outlying areas with a low population density. In such areas it is important that local utilities and governments work together with a local Wireless Internet Service Provider (WISP) to deliver service. While many WISPs take advantage of the license-exempt spectrum to provide services, most deployments are in the licensed spectrum and are deployed by local exchange carriers who require voice services in addition to high-speed data. This is because in these areas the wired infrastructure either does not exist or does not offer the quality to support reliable voice, or high-speed data.

WiMAX Market Forecast

Pyramid Research forecasts that the Broadband Wireless Access (BWA) industry is growing rapidly and expects BWA connections to expand globally at a 27% Compound Annual Growth Rate between now and 2008. This is greater than today's single-digit growth of the telecom industry. With respect to subscriber line growth, Pyramid Research forecasts a growth of one million lines in 2004 to approx. 4 million lines in 2008.

WiMAX will likely succeed in most geographic markets. In emerging markets, operators are interested in using WiMAX for low-cost voice transport and delivery. In developed markets, WiMAX is about broadband Internet access. For a market without any fixed infrastructure, WiMAX could become an inexpensive means of delivering voice and high-speed data.

As the technology evolves and the distinctions between fixed and mobile services become increasingly transparent, wireless providers will more likely pursue WiMAX deployments. The local and regional wireless ISPs will turn their attention to rural areas and enterprise accounts.

[11] David Hakala, "Wireless data in the great outdoors" *VARBusine*ss (july 26, 2002).

Wi-Fi/ WiMAX Likely Evolution

When comparing Wi-Fi and WiMAX evolution, it is important to examine the wireless technology family as shown in figure 15. Each family member shown has its own unique imprint, serves a unique market and *theoretically* should not be considered as competing alternatives to each other.

The Wi-Fi success story has a lot to do with deployment simplicity, very cost effective capital investment and user demand. Market pressure, however, pushed Wi-Fi to invade the MAN space by deploying mesh network architecture and high-gain directional antennas. Wi-Fi, however, is unlikely to provide true broadband services with a bandwidth equivalent to that of WiMAX. WiMAX gives users high capacity links on both the uplink and the downlink of up to 75 Mbps on a single channel.

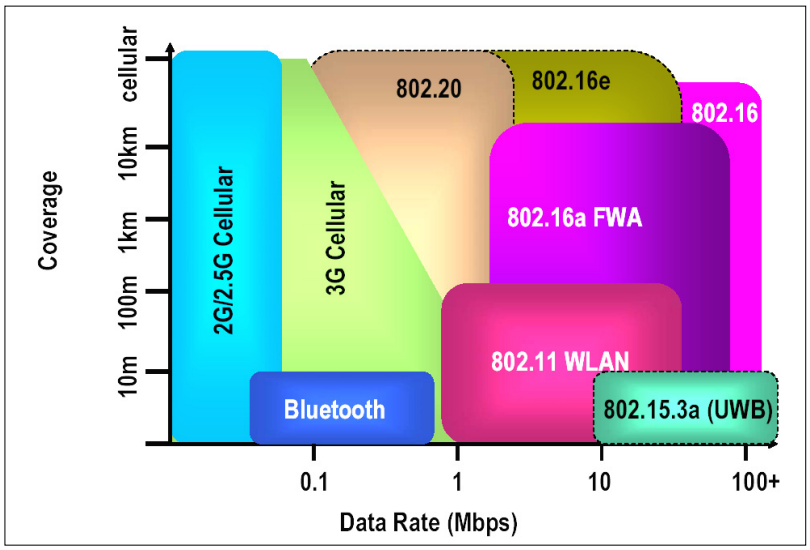


Figure 15- Wireless technology family [12]

Some in the industry believe that Wi-Fi is on its way, or already conquered the first/last mile in the high speed Internet access market. The speculation is that WiMAX is a complementary technology to Wi-Fi in the backbone portion of the network only. Although that seems evident in the short term, however, when the advanced real-time multimedia applications becomes ubiquitous and as network convergence in mobility accelerates, then complexities of Wi-Fi configurations become more pronounced and the WiMAX access solution becomes more attractive. Intel, in particular, sees this opportunity and plans to create chipsets that can handle both the 802.11 and 802.16 technologies. Laptops with these chipsets would use whichever signal was strongest in a given area.

[12] IEEE 802.11 organization website

While Wi-Fi and WiMAX may end up complementing each other in the short term, another emerging technology may provide competitions to both in the years to come.

Other Competing Alternatives

The IEEE 802.20 standard (shown in the figure 15), like 802.16 is aimed at wireless high-speed connectivity to mobile consumer devices such as cellular telephones, PDAs, and laptops. 802.20 will run in the 500 MHz to 3.5 GHz. Officially, the two standards are not considered to be competing alternatives but not everyone agrees that that is the case.

With the strong support of Intel and other industry leaders, most analysts believe that WiMAX will become successful. The real question is whether or not WiMAX be cost effective and popular in the mobility area. To that end it is too early to predict.

Unlicensed vs. Licensed Frequencies

FCC Rules of Allocating Unlicensed Spectrum

The IEEE 802.11 standards are based on wireless access using the unlicensed spectrum. Initially the FCC had allocated a total of 300 megahertz of spectrum in the 5.150-5.250 GHz, 5.250-5.350 GHz and 5.725-5.825 GHz bands.

Due to Wi-Fi market demand, the FCC, in November 3, 2003 made available an additional 255 megahertz of spectrum in the 5.470-5.725 GHz band.

Wi-Fi is deployed for inside buildings, such as offices, malls, hospitals, etc., as well as outdoor areas, such campuses, building complexes, and outdoor plants.

Advantages/ Disadvantages

Fast and inexpensive deployments are two fundamental advantages when using the unlicensed spectrum. In general, the unlicensed spectrum has several advantages over the licensed spectrum. There are applications (e.g., cordless telephone) that can best be supported (or only supported) with the unlicensed spectrum. The cost of a single license could be a significant part of a system's overall deployment cost if user penetration is low. Protection from interference is not one of those advantages; there is always a risk that too many systems will be deployed in close proximity, and hence degrade the system performance.

Licensed Vs. Unlicensed: Making the Choice

Choosing the right spectrum when deploying a network depends on the application and in understanding the limits and capabilities of each. Below are some guidelines:

The Case for the Licensed Spectrum

The attraction of the unlicensed spectrum is that it is free. While that seems like an advantage, the cost of the licensed spectrum per subscriber could be negligible if user penetration is modest.

Another attraction of the unlicensed bands is that Wi-Fi equipment is cheap. Wi-Fi proponents argue that unlicensed bands benefit from low-cost, mass-production equipment. However, similar economies of scale can also be achieved with licensed technologies for WiMAX. Hence, high-volume gear can also become cheap.

The obvious disadvantages for unlicensed deployments are:
1) Unlicensed bands today have low regulatory transmit power limits
2) Unlicensed bands are subject to uncontrolled interference.

These two factors make the unlicensed bands questionable for large-scale paying consumers and small businesses. One, therefore, could come to the following conclusions:

- **For public Wide Area Network and Business Services:** Only licensed broadband wireless can provide the high-speed and large coverage radius required to service highly distributed endpoints
- **For Converged Voice and Data Services:** When the service bundle includes data with service-level assurance and/or public switched telephone network (PSTN)-grade voice. WiMAX with high capacity licensed spectrum would be the preferred choice.

A Case for the Unlicensed Spectrum

The unlicensed spectrum has a valuable role to play. Some examples are:

- **Private WLANs in Homes and Businesses:** Wi-Fi is an ideal LAN technology and excels in the LAN environment because of the small service radius. This enables one to control interference sources. Free spectrum provides for mass-scale availability of low-cost PC-cards and other Wi-Fi equipment
- **Controlled Hotspot Service Offerings:** Wi-Fi is the preferred technology for public service offerings in isolated, high-density, privately controlled locations such as cafes, airport lounges etc.
- **WAN Services:** Unlicensed services using point-to-point or point-to-multipoint links with high-gain antennas are viable for certain applications. Another good commercial example is found in point-to-point systems that are now providing T-1 backhaul circuits over the unlicensed spectrum.

Future Trends of Allocating the Unlicensed Spectrum

The FCC holds the keys for unlocking more unlicensed spectrum and increases the power of transmitters and enhances the potential Wi-Fi distribution. Proponents and opponents, regarding unlicensed spectrum, are lobbying the FCC and Congress to rule in their favor.

Proponents (WISPs, Wi-Fi market leaders, and Media Access Project group) in particular advocated that while the FCC rules made Wi-Fi possible, they also limited what it can do. Low power level and limited number of frequency bands make it difficult to unleash the true power of Wi-Fi networking at a grand scale. They urge the FCC to change the rule by increasing the power level of the radio, and provide more frequency bands. This would ensure the continuation of ongoing efforts to promote more flexible, innovative, and market driven uses of the radio spectrum for the good of the general public.

Opponents who represent the cell phone industry, the National Association of Broadcasters and others are also lobbying the FCC to change existing rules and instead take advantage of the new technologies and throw out the old. For example, opponents favor cognitive radio technology which uses transmitters to sense when spectrum is free and allows it to transmit at that band rather than restrict unlicensed access to a particular band.

Accordingly, the FCC has several open proceedings that will address the above issues.

Wi-Fi proponents are urging the public (any one) to send their comments to the FCC. They believe that if opponents (with their vast resources) win the FCC's heart and mind it will severely limit Wi-Fi future growth.

Federal law requires the FCC to base their decision on public comments complied during a proceeding. Concerned citizens can comment to the FCC at:
http://gullfoss2.fcc.gov/prod/ecfs/upload_v2.cgi

Alternative Spectrum for Community Networks

There are other spectrum-related issues that are under discussion in educational institutions, the FCC and the Wi-Fi industry. The proposals are beneficial especially to rural communities and possible WISPs who wish to collaborate with that community. Some of these changes are being implemented today and could impact the evolutionary path of Wi-Fi and WiMAX.

The two spectrum-related areas that are finding their way toward implementations are:
1. Instructional Fixed Television Service (ITFS)
2. Cable digital channels

ITFS[13]

The FCC initially authorized ITFS (operates in the 2.5GHz to 2.7GHz frequency range) to operate using one-way, analog microwave channels through a single broadcast antenna distributed to classrooms over multi-channel closed circuit television systems. ITFS licenses were dedicated to educational organizations to provide distance learning services. The FCC web site lists the license holders for all ITFS channels in your area. In North Carolina, there are a total of 39 ITFS [14] licenses serving the counties.

The FCC recognized that many ITFS licensees lacked the technical expertise and resources to fully utilize ITFS. In late 1980's, it authorized license holders to lease their channels to commercial operators, provided they continue to dedicate a specified portion of time to educational programming or services. As technology and market dynamics evolved to digital compression and wireless mobility, so did FCC ruling. For example, in 1998, the FCC approved the use of digital compression in ITFS, which expanded the number of channels by 4 to 6 folds. Later, the FCC also authorized both cellular and two-way operations in the ITFS services and the potential for ITFS to be used for the distribution of data, as well as video.

In September 2003, The Wi-Fi community including NYCwireless.org, Seattlewireless.net, BAWUG.org, and others, with support from the New America Foundation lobbied the FCC to adopt new rules that would open the ITFS bands to unlicensed use (WT Docket No. 03-67).

[13] www.fcc.gov
[14] KPMG Consulting "Inventory and Assessment of North Carolina's ITFS Licenses". (Rural Internet Access Authority, May, 2002).

More information on ITFS present and future proceedings is available at
http://www.techlawjournal.com/alert/2004/06/04.asp
http://wireless.fcc.gov/services/itfs&mds/

Cable Digital Channels

A cable franchise renewal process generally involves the coordinated effort of experts from the cable industry, city staff, elected officials and local residents. The renewal process involves an examination of past performance of the cable service provider, and analysis of future community communication needs and negotiation. Identifying community communication cable-related needs is ascertained by conducting focus group workshops, telephone, mail survey, and public hearing(s). The negotiated agreement with cable providers usually reflects the varied demography of the region and economy development.

In the past, cable operators have devoted a single Public, Education, and Government (PEG) analog channel to serve the community. Since then, the cable industry has modernized its infrastructure into a Hybrid Fiber Coax (HFC) digital platform with an interactive capability and hence increased its capacity several fold. Experts, representing the community, are catching on and demanding new negotiating platforms for the renewal of a cable franchise [15]
The new paradigms when negotiating with cable operators are:

- Reduce the term of the franchise agreement (today - typically 10- 15 years) to make provisions for the rapid pace of advancement in technology. This ensures public interest (PEG-related) is served in kind.
- Renegotiate the PEG platform to take advantage of the new cable modem capabilities, such as broadband Internet access, digital multicasting, video on demand, and interactive data services. An example of forward PEG thinking is the Grand Rapid Community Media center at http://www.grcmc.org/
- Cable operators should make additional bandwidth available (up to 10% of their capacity) to ensure a robust community platform for Internet applications. Also, to provide video channel capacity for programmers offering city-based interactive services.
- Leverage connectivity to the Institutional Network (I-NET) to link more than municipal departments and buildings. (Use you imagination). For more information on I-Net see http://www.pgh-inet.org
- Support local economic development of the small neighborhood businesses and entrepreneurs by utilizing online services for marketing and purchasing. Cable operators should provide all neighborhoods with a network and a service model that supports the growth of community commerce.
- Create a financial support structure for PEG and PEG pipes to go beyond the traditional sources (which include up to 3 percent of gross cable revenues) for PEG equipment and facilities.

[15] Center for Digital Democracy. “Stay Tuned: Fulfilling Cable's Promise in the Franchise Renewal Process”. Symposium on the Los Angeles Cable System, University of Southern California. March 2004.

Cable operators are reluctant to relax any old PEG rules and access platforms but recent outcomes of cable franchise renewals resulted in the following examples [16] (only few cited here)

- Comcast cable with 3,500 subscribers (Healdsburg, CA) to provide the community with 20 digital PEG access channels and funding up to $250,000 for PEG equipment and facilities.
- Adelphia with 10,000 subscribers (Brunswick, OH) to provide up to 20 PEG digital access channels and PEG funding of up to $500,000 for Peg equipment and facility.
- Cox with 50,000 subscribers (Oceanside, CA) to provide up to 8 PEG digital access channels and funding of PEG access equipment and facility of up to $2.3 million

[16] The Buske group "Cable TV Franchise Renewal". The National Summit for Community Networks - University of IL at Urbana-Champaign. August 2004

Wi-Fi Applications

Broadband Applications

The technical community worldwide in cooperation with the corresponding governmental agencies evaluated the future migration of the telecommunication industry and assessed the trends of the social attitudes of the people in the industrialized nations. Based on the study's conclusion, technical experts began developing broadband applications using various network platforms.

Government Role

Governments play an important role in creating an information and technology rich society and in shaping the perception of innovation and competition on the global market. A country must have a plan to educate its citizens and provide skilled workers in order to compete in the global market. Most countries recognized this reality in that broadband applications not only secure national and international revenue streams, but also increase its workforce productivity several folds. They are therefore, aggressively funding broadband deployment in their countries and providing their citizens with broadband accesses.

From policy perspectives, the Harvard Policy Group issued a narrative to leaders of the networked world on Information Technology (IT) and its role in policy-making in the national political agenda.

The Eight Imperatives [17]

The Harvard Policy Group (at JFK School of Government) issued a comprehensive IT report outlining a road map for leaders in a Networked World to establish strategic directions in order to formulate new public policies on information technology issues. The group's members are distinguished officials and appointed executives from local, state, and federal government, identified eight imperatives designed to help leaders of the 21st century to unlock key values that are dramatically transforming our social, commercial, and political interaction. Below is a compendium of the eight imperatives:

- Imperative 1: Focuses on How IT Can Reshape Work and Public Sector Strategies.
- Imperative 2: Explores the use IT for strategic innovation, not simply technical automation
- Imperative 3: Utilize Best Practices in Implementing IT Initiatives
- Imperative 4: Improve Budgeting and Financing for Promising IT Initiatives
- Imperative 5: Protect Privacy and Security
- Imperative 6: Form IT-related partnerships to stimulate economic development
- Imperative 7: Use IT to promote equal opportunity and healthy communities
- Imperative 8: Prepare for digital democracy

Full text copy of the report is available from:
http://www.ksg.harvard.edu/exec_ed/3e/eight_imperatives.htm

[17] Jerry Mechling. "Eight Imperatives for Leaders in a Networked World" The Harvard Policy Group on Networked-Enabled Services and Government, John F. Kennedy School of Government, Harvard University, 2000.

States Role

At the state level, several states including Michigan[18] and Vermont[19] have passed legislation to promote and fund broadband deployment to their communities. In 2000 the North Carolina state legislators went a step further and created the Rural Internet Access Authority (RIAA) to serve as the coordinating organization working to promote broadband access to rural communities. The RIAA (renamed the e-NC Authority in 2003 legislation) funded several critical projects enabling rural communities to be on an even playing field in terms of the economic benefit delivered through broadband applications.

e-NC's *A 100 County Report* consistently has shown high-speed access in North Carolina is improving rapidly. By the end of 2003 – when the last report was published – 80.22 percent of the households in North Carolina had the ability to access high-speed Internet services using cable modem or DSL services. Anecdotal research indicates 2004 will herald the highest level of connectivity the state has ever seen.

The most dramatic increases occurred within 17 connectivity-challenged counties. In 2002, three of these counties were found to have no access to high-speed Internet services at all. Due to e-NC's investment and the community's response, service now is available to more than 24 percent of the households in each of these counties. By the end of 2003, there was no county with lower than 11 percent high-speed access and all areas had 100 percent dial-up access.

The number of North Carolinians who subscribe to high-speed Internet increased more than ten-fold from December 1999 to December 2002. As a result of North Carolina's jump from 57,881 to 594,039 users, the Federal Communications Commission ranked the state 11th nationally in number of subscribers to high-speed Internet.

Key Legacy Broadband Applications

A few years ago a long list of applications were developed by the industry but few survived the test of time. Today's "most wanted" list of the core features are: Video On Demand (VOD), Video conferencing, Voice over IP (VOIP), Work at home, Telemedicine, Distant learning, Home shopping, CD-ROM on demand (audio streaming), Electronic Games, and Telemetry. The industry segments that benefited most from these core features are in:

- Education
- Financial
- Government
- Manufacturing
- Medical
- Residential
- Retail

[18] Michigan Broadband Development Authority (http://www.broadbandauthority.org)
[19] Vermont, Department of Information and Innovation (http://www.dii.state.vt.us/)

Emerging Wi-Fi Broadband Applications

Below is a summary of some of the emerging Wi-Fi applications that address the needs of communities especially those in rural areas.

Challenges of Rural Communities

Rural communities are inherently disenfranchised from attaining similar socio-economic status as their urban counterparts. This is because they are geographically isolated in remote areas and therefore, are limited to local marketplaces to trade goods and services. Today however, through help from federal and state community developers, these rural communities can change their role in the economic playing field. Broadband access is one tool that can create a new type of market place with global reach.

The Benefits of Wi-Fi / WiMAX in Rural Regions

Wi-Fi deployment in rural communities offers opportunity on many fronts. Wi-Fi can cost effectively be deployed in weeks. An open wireless network allows community residents to share Internet access from stationary devices as well as from handheld devices. Visitors and residents can travel around the community and maintain Internet access through their handheld wireless devices.

One major advantage Wi-Fi has is the inherent enormous bandwidth access when compare to the legacy Internet accesses of ADSL, cable modem, or others (up to 40 times faster with 802.11g). Wi-Fi communities in NY City and Austin TX, among others are taking advantage of this vast capacity to build their own Wi-Fi broadband private virtual network serving the local needs of their communities. NYC wireless (NYCwireless.com) in particular pioneered such approach and successfully hosted several community events such as painting exhibits, arts & craft, concerts, and other programs. See http://www.spectropolis.info/ for highlights of the 3 day event held in early October 2004.

Below are some of the Wi-Fi application-specific scenarios communities should consider promoting to develop their economic potentials.

Web-Based Events

Web-based hosting events offer several possibilities for communities to merchandize their goods and services. NC rural communities, who deploy Wi-Fi, will be well positioned to host web events that portray their community's personality based on their wares and talents. For example, entrepreneurs could display pottery items, or exhibit goods and services of a particular region (e.g., Wineries, Woodworkers, Fishery, Historic landmarks etc.). Such community sites could attract new customers and potential visitors can familiarize themselves with community interests, talents, art, and business potentials.

Wi-Fi can also provide a cost effective way to remotely control equipment on farms such as irrigation systems, temperature controls, water levels and hog lagoon pumping systems. Video cameras can monitor properties 24 hours a day. If performed manually, these time-

intensive tasks can be very costly. The savings realized by utilizing a Wi-Fi network will quickly pay for the network.

In the Columbia River a free Wi-Fi network has been set up in many areas of the River valley. With seven transmission towers positioned on peaks in southeast Washington and Northeast Oregon, the wireless network of Columbia Energy cost $600,000----a fraction of what it deployment of fiber optic cable would have cost. Farmers' offices are their tractor or combine. Farmers can take connectivity with them and control or monitor equipment and applications on their farms. One lady in the area, owner of a 5,000 acre family farm noted that she had been using a dial-up connection through American Online. Now she said that she gets her email and views online photography of farming equipment from nearby auctions. Before she said, it was faster to drive to auctions …Soon she will use wireless equipment to remotely monitor irrigation systems and change water flow to the fields. Mr. Husted of Columbia Energy notes that farmers and industrial users are beginning to realize the benefits of wireless communications in their daily operations at a rate of $39.95 per month for 256 kilobits per second to $259 per month for l.5 megabits per second-speeds that are 5 times faster than dial up connections.[20]
(http://seattlepi.nwsource.com/business/189699_vivato07.html)

Video Chat

Video chat is a powerful tool for increasing interaction between users in a public setting. It encourages participants to interact in a friendly social setting. In a wireless community, town hall meetings could enjoy high 'virtual' attendance.

Wi-Fi Killer Application

Voice over Wi-Fi is an emerging application that has been referred to as the "killer application" in some reputable journals. With over 55 million lines and 15% of the voice market[21], Voice over IP (VoIP) is becoming a mature technology. Wi-Fi technology is also maturing rapidly and hence convergence of the two seems inevitable. Voice over Wi-Fi is rapidly changing with evolving standards, and some vendors today are providing a proprietary solution or implementing 802.11e (QOS) specification to meet the market demand.

In a recent ISP conference of the National Communications Cooperative Association (NCTA), the issue of voice over Wi-Fi was presented. It cited the trends of bypassing the local telephone carrier by using their unlicensed wireless networks and VoIP to support voice applications. One case study noted was the University of Arkansas. The university invested $4M in Cisco's VoIP equipment to support local voice traffic over their Wi-Fi network. The setup reduced monthly telephone service fees from $530K to $6K [22]

[20] John Cook, "Rolling wheat fields are also Wi-Fi country," Seattle Post-Intelligencer. September 4, 2004.
[21] Beth Cohen. "VoWLAN: The wireless Voice Future is Here…Almost" Wi-Fi Planet, June 14, 2002
[22] David Lowe, 2004 Spirit Telecom ISP conference. April 26, 2004

Wi-Fi phones are now also being used extensively at Dartmouth College and students are giving students software for making free long-distance calls over their wireless network. (Yahoo News)

Wireless Trends

Smart Clothing will be part of our near future. Smart fabrics such as your handbag can warn you that your wallet is being left behind or later a wall hanging in your house can glow if someone tries to use your home's wireless Internet connection.[23] (http://www.newscientist.com/news/news.jsp?id=ns99996553)

Virtual moving fences controlled from a laptop one day will herd cattle to fresh fields for grazing. "A farmer would control multiple herds from a single server at home as if they were playing a video game, said Zack Butler, of Dartmouth College in Hanover, New Hampshire. Butler and his colleagues have written software that transmits the chosen GPS co-ordinates of a virtual fence to head-collars worn by the cows in the field.

When a cow strays towards these co-ordinates, software running on the collar triggers a stimulus chosen to scare the cow away, such as a sound or a small electric shock - this is the "virtual" fence. The software also "herds" the cows when the position of the virtual fence is moved."[24] (http://www.newscientist.com/news/news.jsp?id=ns99995079)

[23] Celeste Biever, "Smart fabrics make for enhanced living," New Scientist. October 23, 2004
[24] Celeste Biever, "Virtual fences to herd Wi-Fi cattle," New Scientist. June 7, 2004.

User Devices

See CD

List of Vendors

See CD

Cost Models

See CD

Acronyms

ADSL Asynchronous Digital Subscriber Line
AES Advanced Encryption Standard
AP Access point, the 802.11 wireless transceiver providing connectivity to a wired network
BSS Basic Service Set
BWA Broadband Wireless Access
DHCP Dynamic Host Configuration Protocol
EIRP Equivalent Isotropic Radiated Power
ESS Extended Service Set
FCC Federal Communication Commission
GPS Global Positioning System
HFC Hybrid Fiber Coax
Hotspot Public location such as an airport or hotel where WLAN services have been deployed
IEEE Institute of Electrical and Electronics Engineers
IBSS Independent Basic Service Set
IP Internet Protocol
I-NET Institutional Network
ISP Internet Service Provider
IT Information Technology
ITFS Instructional Television Fixed Service
ITU International Telecommunications Union
LAN Local Area Network
LOS Line Of Sight
MAN Metropolitan Area Network
MAC Media Access Control
NAT Network Address Translation
NCTA National Communications Cooperative Association
NIC Network Interface Card
NLOS Near Line Of Sight
OSI Open System Interconnect (Interconnection)
PDA Personal Digital Assistance
PEG Public, Education and Government
PCMCI Personal Computer Memory Card International Association
PMP Point to Multipoint
POE Power Over Ethernet
PSTN Public Switched Telephone Network
PTP Point-To-Point
QOS Quality Of Service
RF Radio Frequency
RIAA Rural Internet Access Authority
SSID Service Set Identifier for 802.11 access points. The SSID is a 32-character unique
SSL Secure Sockets Layer, a popular protocol for authentication and connection-level
TKIP Temporal Key Integrity Protocol

VLAN Virtual LAN
VOIP Voice over IP
VoWIP Voice over Wireless IP
VOWLAN Voice over WLAN
VPN Virtual Private Network
WAN Wide Area Network
WEP Wired Equivalent Privacy
Wi-Fi Wireless Fidelity, refers to 802.11 standards, including 802.11b, 802.11a, and 802.11g
WiMAX Worldwide Interoperability for Microwave Access
WISP Wireless Internet service provider
WLAN Wireless local area network based on IEEE 802.11 and related standards
WAPA Wi-Fi Protected Access

References

(An electronic version of this list with 'clickable' hyperlinks is included on the CD)

Asbrand, Debra. "Who Pays for Wireless Cities?" In MIT Technology Review. September 2004. http://www.technologyreview.com/articles/04/09/wo_asbrand092104.asp?p=2

Biever, Celeste. "Smart fabrics make for enhanced living," In New Scientist. October 23, 2004. http://www.newscientist.com/news/news.jsp?id=ns99996553

Biever, Celeste. "Virtual fences to herd Wi-Fi cattle," In New Scientist. June 7, 2004. http://www.newscientist.com/news/news.jsp?id=ns99995079

Bulk, Frank. "Wireless MANs, Giving WMANs a Little Muscle." In Network Computing. Mar 18, 2004. http://www.nwc.com/showitem.jhtml?docid=1505ws1

The Buske Group (http://www.buskegroup.com) "Cable TV Franchise Renewal". Presented at Making the Connection: The 2004 National Summit for Community Wireless, University of IL at Urbana-Champaign. August 2004. http://www.communitywirelesssummit.org/

Center for Digital Democracy. "Stay Tuned: Fulfilling Cable's Promise in the Franchise Renewal Process". Presentation to a Symposium on the Los Angeles Cable System, University of Southern California. March 2004.
http://www.democraticmedia.org/ddc/DDCuschandout.php

Cohen, Beth. "VoWLAN: The Wireless Voice Future is Here ... Almost" In Wi-Fi Planet. June 14, 2004. http://www.Wi-Fiplanet.com/tutorials/article.php/3367671

Cook, John "Rolling wheat fields are also Wi-Fi country," In Seattle Post-Intelligencer. September 4, 2004. http://seattlepi.nwsource.com/business/189699_vivato07.html

Enabling Successful Services and Applications (Forum session). ITU Telecom World 2003. October 2003.
http://www.itu.int/cgi-bin/htsh/TELECOM/scripts/forum/forum.programme?event=wt2003&_sessionid=664

Farpoint Group. "*WLANs: The Big Issues.*" Presentation in NetworkWorld Seminar & Event. Atlanta. July 2004. http://www.nwfusion.com/events/index.html

Federal Communication Commission. http://www.fcc.gov

Flickenger, Rob. Building Wireless Community Networks. 1st ed. O'Reilly, 2002.

Filka, Bob. "Wireless Broadband Technologies." Michigan Broadband Initiative Authority, November 19, 2003.
http://mayor.cityoflansingmi.com/it_initiative/BandwidthSolutionsMBDA.pdf

Grimm, C. Brian. "Overview Wi-Fi Protected Access" Wi-Fi Alliance, 2002.
http://www.Wi-Fi.org/opensection/pdf/Wi-Fi_protected_access_overview.pdf

Hakala, David. "Wireless Data in the Great Outdoors" In VARBusiness, July 26, 2002.
http://www.varbusiness.com/sections/technology/tech.jhtml?articleId=18838143&printableArticle=true

IEEE Standards Association. Working Group for Wireless LANs.
http://grouper.ieee.org/groups/802/11/

Keene, Ian. "Public Wireless LAN Hot Spots: Worldwide, 2002-2008". Gartner, Inc., 2003.
http://www4.gartner.com/5_about/press_releases/pr30june2003a.jsp

Lowe, David. 2004 Spirit Telecom ISP Conference. April 26, 2004

Mathias, Craig J. (Farpoint Group) "Wireless LANs: The big issues" Networld Seminars and Events. July 2004.

Mechling, Jerry. "Eight Imperatives for Leaders in a Networked World." The Harvard Policy Group on Network-Enabled Services and Government, John F. Kennedy School of Government, Harvard University, 2000. http://www.gateway.hr/index.php?folder=130

Michigan Broadband Development Authority (http://www.broadbandauthority.org)

Rural Internet Access Authority: "Inventory and Assessment of North Carolina's ITFS Licenses" prepared by KPMG Consulting. May, 2002.
http://www.e-nc.org/pdf/ITSF_Supplement.pdf

Stone, Adam: "*Being a Hotspot*" In Wi-Fi Planet. June 4, 2004
http://www.Wi-Fiplanet.com/tutorials/article.php/3356141

Vermont, Department of Information and Innovation (http://www.dii.state.vt.us/)

Lundgren, Kent. "Wi-Fi Technology" Presented at the Nigerian Communications Commission Wi-Fi Workshop, August 2003.
http://www.ncc.gov.ng/Workshop%20Papers/Wi-Fi%20Workshop-August,%202003/ClearBusrt%20Technology.PPT

The Wireless LAN Book for Enterprises. Trapeze Networks, 2003.
http://www.trapezenetworks.com/bookPDF/

"Wireless LAN Security, Technology Overview." Netgear, April 2003.
http://www.netgear.com/pdf_docs/WLAN_Security_Concepts.pdf

Yunker, John & Bramson-Boudreau, Elizabeth. "Demystifying WiMAX." Pyramid Research, Global/Business Strategies Group. December 1, 2003.
http://www.wimaxforum.org/news/reports/pyramid_demystifying.pdf

Further Reading / Research

http://www.hms.harvard.edu/it/wireless/index.html …… (Harvard Medical School Wi-Fi)
http://www.oreillynet.com/cs/weblog/view/wlg/448 …….. (Cheap home-made antenna)
http://www.Wi-Fiplanet.com …….. (Wi-Fi tidbits)
http://www.Wi-Fi.org …….. (Wi-Fi Alliance)

Community Wireless Sites:

http://seattlewireless.net …….. (Seattle, WA)
http://www.nycwireless.net …….. (New York City)
http://www.guerrilla.net …… (Cambridge, MA)
http://www.nocat.net …….. (Sonoma County, CA.)
http://www.instantemail.net/asheville/ …….. (Asheville, NC)
http://www.cityofws.org/wifion4th/index.html ..... (Winston-Salem, NC)

If you are interested in enhancing this document or would like to add additional examples, please submit your comments on our website:
http://www.e-nc.org/wifi_primer.asp