Wi-Fi Technology

Precious Bertrand

First Edition, 2012

ISBN 978-81-323-4412-4

Published by:
White Word Publications
4735/22 Prakashdeep Bldg,
Ansari Road, Darya Ganj,
Delhi - 110002
Email: info@wtbooks.com

Table of Contents

Chapter 1

Wi-Fi

Wi-Fi logo

A Wi-Fi enabled device such as a personal computer, video game console, smartphone, or digital audio player can connect to the Internet when within range of a wireless network connected to the Internet. The coverage of one or more (interconnected) access points — called hotspots when offering public access — generally comprises an area the size of a few rooms but may be expanded to cover many square miles, depending on the number of access points with overlapping coverage.

'Wi-Fi' is not a technical term. However, the Alliance has generally enforced its use to describe only a narrow range of connectivity technologies including wireless local area network (WLAN) based on the IEEE 802.11 standards, device to device connectivity [such as Wi-Fi Peer to Peer AKA Wi-Fi Direct], and a range of technologies that support PAN, LAN and even WAN connections. Derivative terms, such as Super Wi-Fi, coined by the U.S. Federal Communications Commission (FCC) to describe proposed networking in the former UHF TV band in the US, may or may not be sanctioned by the alliance. *As of November 2010 this was very unclear.*

The technical term "IEEE 802.11" has been used interchangeably with Wi-Fi, but over the past few years Wi-Fi has become a superset of IEEE 802.11. Wi-Fi is used by over 700 million people, there are over 750,000 hotspots (places with Wi-Fi Internet connectivity) around the world, and about 800 million new Wi-Fi devices every year. Wi-Fi products that complete the Wi-Fi Alliance interoperability certification testing successfully can use the Wi-Fi CERTIFIED designation and trademark.

Not every Wi-Fi device is submitted for certification to the Wi-Fi Alliance. The lack of Wi-Fi certification does not necessarily imply a device is incompatible with Wi-Fi devices/protocols. If it is compliant or partly compatible, the Wi-Fi Alliance may not object to its description as a Wi-Fi device though technically only the CERTIFIED designation carries their approval.

Wi-Fi certified and compliant devices are installed in many personal computers, video game consoles, MP3 players, smartphones, printers, digital cameras, and laptop computers.

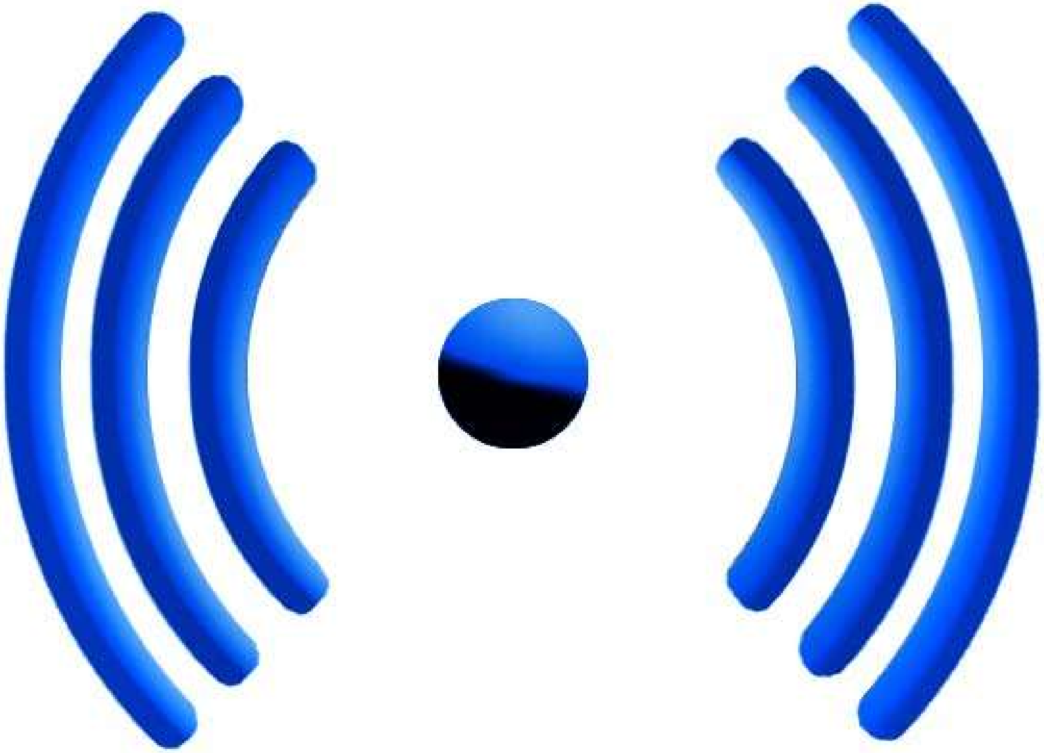
Here we, focuses on the certification and approvals process and the general growth of wireless networking under the protocols certified by the Wi-Fi Alliance. Non-Wi-Fi-Alliance wireless technologies intended for fixed points such as Motorola Canopy are usually described as fixed wireless. Non-Wi-Fi-Alliance wireless technologies intended for mobile use are usually described as 3G, 4G or 5G, reflecting their origins and promotion by telephone or cellphone companies.

Wi-Fi certification

Wi-Fi technology builds on IEEE 802.11 standards. The IEEE develops and publishes some of these standards, but does not test equipment for compliance with them. The non-profit Wi-Fi Alliance formed in 1999 to fill this void — to establish and enforce standards for interoperability and backward compatibility, and to promote wireless local-area-network technology. As of 2010 the Wi-Fi Alliance consisted of more than 375 companies from around the world. Manufacturers with membership in the Wi-Fi Alliance, whose products pass the certification process, gain the right to mark those products with the Wi-Fi logo.

Specifically, the certification process requires conformance to the IEEE 802.11 radio standards, the WPA and WPA2 security standards, and the EAP authentication standard. Certification may optionally include tests of IEEE 802.11 draft standards, interaction with cellular-phone technology in converged devices, and features relating to security set-up, multimedia, and power-saving.

Most recently, a new security standard, Wi-Fi Protected Setup, allows embedded devices with limited graphical user interface to connect to the Internet with ease. Wi-Fi Protected Setup has 2 configurations: The Push Button configuration and the PIN configuration. These embedded devices are also called The Internet of Things and are low-power, battery-operated embedded systems. A number of Wi-Fi manufacturers design chips and modules for embedded Wi-Fi, such as GainSpan.



WiFi Signal logo

The name Wi-Fi

The term *Wi-Fi* suggests *Wireless Fidelity*, resembling the long-established audio-equipment classification term *high fidelity* (in use since the 1930s) or *Hi-Fi* (used since 1950). Even the Wi-Fi Alliance itself has often used the phrase *Wireless Fidelity* in its press releases and documents; the term also appears in a white paper on Wi-Fi from ITAA. However, based on Phil Belanger's statement, the term Wi-Fi was never supposed to mean anything at all.

The term *Wi-Fi*, first used commercially in August 1999, was coined by a brand-consulting firm called Interbrand Corporation that the Alliance had hired to determine a name that was "a little catchier than 'IEEE 802.11b Direct Sequence'". Belanger also stated that Interbrand invented *Wi-Fi* as a play on words with *Hi-Fi*, and also created the yin-yang-style Wi-Fi logo.

The Wi-Fi Alliance initially used an advertising slogan for Wi-Fi, "The Standard for Wireless Fidelity", but later removed the phrase from their marketing. Despite this, some documents from the Alliance dated 2003 and 2004 still contain the term *Wireless Fidelity*. There was no official statement related to the dropping of the term.

The yin-yang logo indicates the certification of a product for interoperability.

Uses

Internet access

A roof-mounted Wi-Fi antenna

A Wi-Fi enabled device such as a personal computer, video game console, smartphone or digital audio player can connect to the Internet when within range of a wireless network connected to the Internet. The coverage of one or more (interconnected) access points — called hotspots — can comprise an area as small as a few rooms or as large as many square miles. Coverage in the larger area may depend on a group of access points with overlapping coverage. Wi-Fi technology has been used in wireless mesh networks, for example, in London, UK.

In addition to private use in homes and offices, Wi-Fi can provide public access at Wi-Fi hotspots provided either free-of-charge or to subscribers to various commercial services. Organizations and businesses - such as those running airports, hotels and restaurants - often provide free-use hotspots to attract or assist clients. Enthusiasts or authorities who wish to provide services or even to promote business in selected areas sometimes provide free Wi-Fi access. As of 2008 more than 300 metropolitan-wide Wi-Fi (Muni-Fi) projects had started. As of 2010 the Czech Republic had 1150 Wi-Fi based wireless Internet service providers.

Routers that incorporate a digital subscriber line modem or a cable modem and a Wi-Fi access point, often set up in homes and other premises, can provide Internet access and internetworking to all devices connected (wirelessly or by cable) to them. With the emergence of MiFi and WiBro (a portable Wi-Fi router) people can easily create their own Wi-Fi hotspots that connect to Internet via cellular networks. Now iPhone, Android or Symbian phones can create wireless connections.

One can also connect Wi-Fi devices in ad-hoc mode for client-to-client connections without a router. Wi-Fi also connects places that would traditionally not have network access, for example kitchens and garden sheds.

City-wide Wi-Fi

An outdoor Wi-Fi access point in Minneapolis

An outdoor Wi-Fi access point in Toronto

In the early 2000s, many cities around the world announced plans for city-wide Wi-Fi networks. This proved to be much more difficult than their promoters initially envisioned with the result that most of these projects were either canceled or placed on indefinite hold. A few were successful, for example in 2005, Sunnyvale, California became the first city in the United States to offer city-wide free Wi-Fi, and Minneapolis has generated $1.2 million profit annually for their provider.

In May, 2010, London, UK Mayor Boris Johnson pledged London-wide Wi-Fi by 2012. Both the City of London, UK and Islington already have extensive outdoor Wi-Fi coverage.

Campus-wide Wi-Fi

Carnegie Mellon University built the first wireless Internet network in the world at their Pittsburgh campus in 1994, long before Wi-Fi branding originated in 1999. Many traditional college campuses provide at least partial wireless Wi-Fi Internet coverage.

Drexel University in Philadelphia made history by becoming the United States' first major university to offer completely wireless Internet access across the entire campus in 2000.

Direct computer-to-computer communications

Wi-Fi also allows communications directly from one computer to another without the involvement of an access point. This is called the *ad hoc* mode of Wi-Fi transmission. This wireless ad hoc network mode has proven popular with multiplayer handheld game consoles, such as the Nintendo DS, digital cameras, and other consumer electronics devices.

Similarly, the Wi-Fi Alliance promotes a specification called *Wi-Fi Direct* for file transfers and media sharing through a new discovery- and security-methodology. Wi-Fi Direct launched in October 2010.

Future directions

As of 2010 Wi-Fi technology has spread widely within business and industrial sites. In business environments, just like other environments, increasing the number of Wi-Fi access points provides network redundancy, support for fast roaming and increased overall network-capacity by using more channels or by defining smaller cells. Wi-Fi enables wireless voice-applications (VoWLAN or WVOIP). Over the years, Wi-Fi implementations have moved toward "thin" access points, with more of the network intelligence housed in a centralized network appliance, relegating individual access points to the role of "dumb" transceivers. Outdoor applications may utilize mesh topologies.

Advantages and challenges

WI-FI detector user's manual

Features:

Detects signal up to 50 meters (+150feet) away.

Easy to operate.

Press the button to activate and wait three seconds f 802.11b/802.11g

Simply view the four red LED lights to deter

wireless internet status.

How to operate:

Press the button four red indic ts sho his means the device is searching for a signal.

If the signal bar lights fla h four times th op to indica is no signal or too weak of a signal for the device o detect.

If only the first indicator c me on till tw second ashing), a weak wireless sign has been detected. A wireless co tion is possible, but may not be stable.

If both the first and second indicator come on and till two second (after flashing), device has detected a good wireless signal. The area is favorable for accessing a wire internet connection.

If all four indicator lights come on(after flashing) , the device has detected a very st The area is ideal for accessing a wireless internet connection.

A keychain-size Wi-Fi detector

Operational advantages

Wi-Fi allows the deployment of local area networks (LANs) without wires for client devices, typically reducing the costs of network deployment and expansion. Spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs.

As of 2010 manufacturers are building wireless network adapters into most laptops. The price of chipsets for Wi-Fi continues to drop, making it an economical networking option included in even more devices. Wi-Fi has become widespread in corporate infrastructures.

Different competitive brands of access points and client network-interfaces can inter-operate at a basic level of service. Products designated as "Wi-Fi Certified" by the Wi-Fi Alliance are backwards compatible. "Wi-Fi" designates a globally operative set of standards: unlike mobile phones, any standard Wi-Fi device will work anywhere in the world.

Wi-Fi operates in more than 220,000 public hotspots and in tens of millions of homes and corporate and university campuses worldwide. The current version of Wi-Fi Protected Access encryption (WPA2) as of 2010 is considered secure, provided users employ a strong passphrase. New protocols for quality-of-service (WMM) make Wi-Fi more suitable for latency-sensitive applications (such as voice and video); and power saving mechanisms (WMM Power Save) improve battery operation.

Limitations

Spectrum assignments and operational limitations are not consistent worldwide: most of Europe allows for an additional two channels beyond those permitted in the U.S. for the 2.4 GHz band (1–13 vs. 1–11), while Japan has one more on top of that (1–14). Europe, as of 2007, was essentially homogeneous in this respect. Note that: Wi-Fi cannot be used in Italy without a licence, and in both Italy and France, both ends of the Wi-Fi link must be within the same building (i.e. a Wi-Fi active device cannot be used out of doors).

A Wi-Fi signal occupies five channels in the 2.4 GHz band; any two channels whose channel numbers differ by five or more, such as 2 and 7, do not overlap. The oft-repeated adage that channels 1, 6, and 11 are the *only* non-overlapping channels is, therefore, not accurate; channels 1, 6, and 11 do, however, comprise the only *group of three* non-overlapping channels in the U.S.

Equivalent isotropically radiated power (EIRP) in the EU is limited to 20 dBm (100 mW).

The current 'fastest' norm 802.11n uses double the radio spectrum compared to 802.11a or 802.11g. This means there can only be one 802.11n network on 2.4 GHz band without interference to other WLAN traffic, or none, if there already is an AP on any of the mid channels.

The on-coming 802.11ac will jam all the current WLAN bands, if allowed on same bands. There might be a chance the 802.11ac would be allocated a new band, perhaps on UHF TV white space.

The Internet protocol performs poorly in the face of noise when run with WiFi as the physical layer. TCP has been tuned for a wired network in which packets lost due to noise is very rare and packets are lost almost exclusively due to congestion. On a wireless network, noise is common. This difference causes TCP to greatly slow or break transmission when noise is significant, even when most packets are still arriving correctly.

Reach

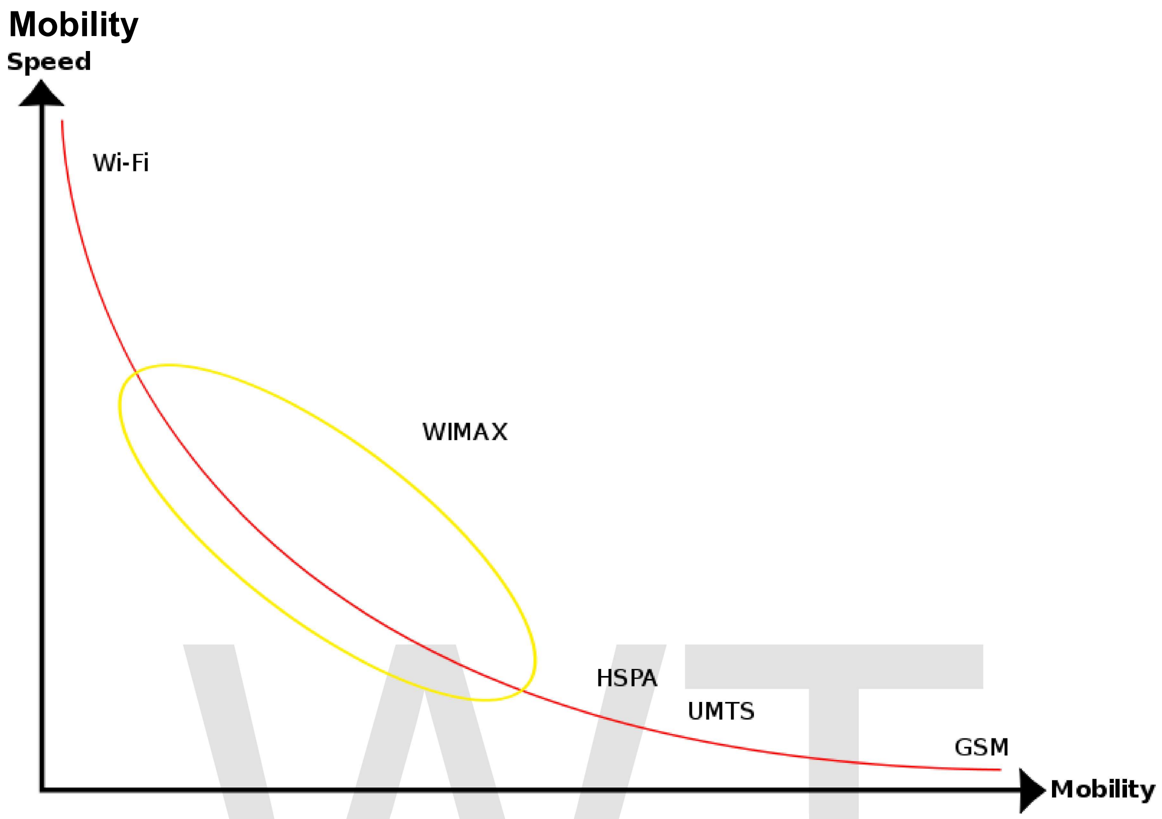
Wi-Fi networks have limited range. A typical wireless router using 802.11b or 802.11g with a stock antenna might have a range of 32 m (120 ft) indoors and 95 m (300 ft) outdoors. The IEEE 802.11n however, can exceed that range by more than two times.

Range also varies with frequency band. Wi-Fi in the 2.4 GHz frequency block has slightly better range than Wi-Fi in the 5 GHz frequency block. Outdoor ranges - through use of directional antennas - can be improved with antennas located several kilometres or more from their base. In general, the maximum amount of power that a Wi-Fi device can transmit is limited by local regulations, such as FCC Part 15 in USA.

Due to reach requirements for wireless LAN applications, Wi-Fi has fairly high power consumption compared to some other standards. Technologies such as Bluetooth (designed to support wireless PAN applications) provide a much shorter propagation range of <10m and so in general have a lower power consumption. Other low-power technologies such as ZigBee have fairly long range, but much lower data rate. The high power consumption of Wi-Fi makes battery life in mobile devices a concern.

Researchers have developed a number of "no new wires" technologies to provide alternatives to Wi-Fi for applications in which Wi-Fi's indoor range is not adequate and where installing new wires (such as CAT-5) is not possible or cost-effective. For example, the ITU-T G.hn standard for high speed Local area networks uses existing home wiring (coaxial cables, phone lines and power lines). Although G.hn does not provide some of the advantages of Wi-Fi (such as mobility or outdoor use), it's designed for applications (such as IPTV distribution) where indoor range is more important than mobility.

Due to the complex nature of radio propagation at typical Wi-Fi frequencies, particularly the effects of signal reflection off trees and buildings, algorithms can only approximately predict Wi-Fi signal strength for any given area in relation to a transmitter. This effect does not apply equally to long-range Wi-Fi, since longer links typically operate from towers that broadcast above the surrounding foliage.



Speed vs. Mobility of wireless systems: Wi-Fi, HSPA, UMTS, GSM

The very limited practical range of Wi-Fi essentially confines mobile use to such applications as inventory-taking machines in warehouses or in retail spaces, barcode-reading devices at check-out stands, or receiving/shipping stations. Mobile use of Wi-Fi over wider ranges is limited, for instance, to uses such as in an automobile moving from one hotspot to another (known as Wardriving). Other wireless technologies are more suitable as illustrated in the graphic.

Data security risks

The most common wireless encryption-standard, Wired Equivalent Privacy (WEP), has been shown to be easily breakable even when correctly configured. Wi-Fi Protected Access (WPA and WPA2) encryption, which became available in devices in 2003, aimed to solve this problem. Wi-Fi access points typically default to an encryption-free (*open*) mode. Novice users benefit from a zero-configuration device that works out-of-the-box, but this default does not enable any wireless security, providing open wireless access to a LAN. To turn security on requires the user to configure the device, usually via a software graphical user interface (GUI). On unencrypted Wi-Fi networks connecting devices can monitor and record data (including personal information), but such networks may use other means of protection, such as a VPN or secure Hypertext Transfer Protocol (HTTPS) over Transport Layer Security.

Population

Many 2.4 GHz 802.11b and 802.11g access-points default to the same channel on initial startup, contributing to congestion on certain channels. To change the channel of operation for an access point requires the user to configure the device. Yet, regular users selecting a "free" channel usually leads to even worse congestion, due to the overlapping channel system. Observations during the year 2010 have shown pretty acceptable spreading of by far most of the devices being on one of the "good" channels: 1, 6 or 11.

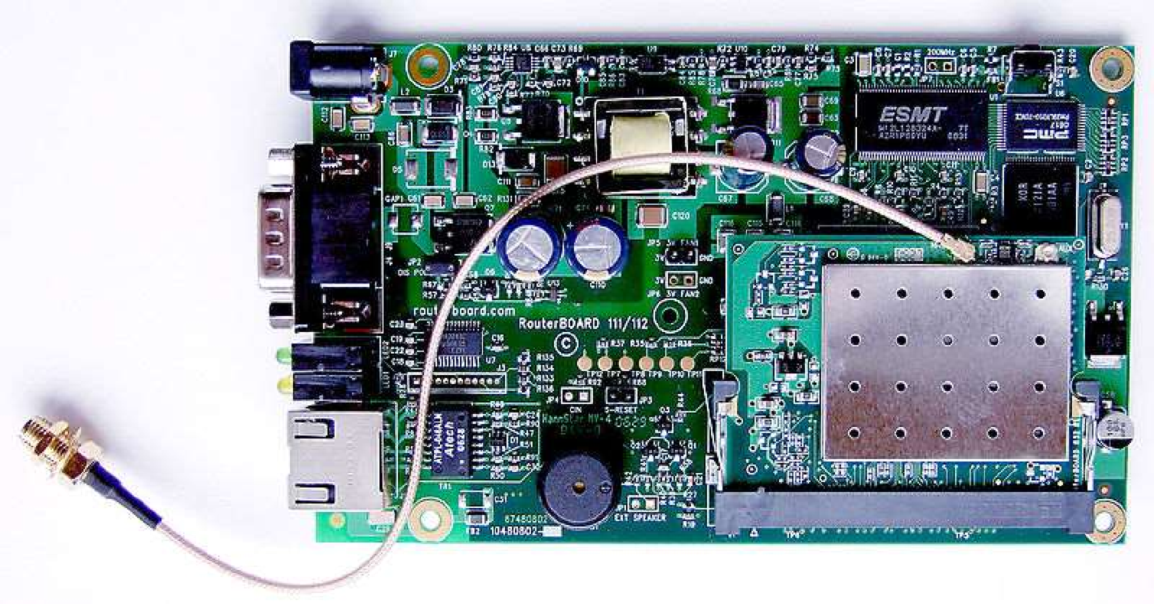
Channel pollution

Market forces may drive a process of standardization. Interoperability issues between non-Wi-Fi brands or proprietary deviations from the standard can still disrupt connections or lower throughput speeds on all devices within range, including any non-Wi-Fi or proprietary product. Moreover, the usage of the ISM band in the 2.45 GHz range is also common to Bluetooth, WPAN-CSS, ZigBee, and any new system will take its share.

Wi-Fi pollution, or an excessive number of access points in the area, especially on the neighboring channel, can prevent access and interfere with other devices' use of other access points, caused by overlapping channels in the 802.11g/b spectrum, as well as with decreased signal-to-noise ratio (SNR) between access points. This can become a problem in high-density areas, such as large apartment complexes or office buildings with many Wi-Fi access points. Additionally, other devices use the 2.4 GHz band: microwave ovens, security cameras, ZigBee devices, Bluetooth devices and (in some countries) Amateur radio, video senders, cordless phones and baby monitors, all of which can cause significant additional interference. It is also an issue when municipalities or other large entities (such as universities) seek to provide large area coverage.

Hardware

Standard devices



An embedded RouterBoard 112 with U.FL-RSMA pigtail and R52 mini PCI Wi-Fi card widely used by wireless Internet service providers (WISPs) in the Czech Republic

OSBRiDGE 3GN - 802.11n Access Point and UMTS/GSM Gateway in one device

USB wireless adapter

A wireless access point (WAP) connects a group of wireless devices to an adjacent wired LAN. An access point resembles a network hub, relaying data between connected wireless devices in addition to a (usually) single connected wired device, most often an ethernet hub or switch, allowing wireless devices to communicate with other wired devices.

Wireless adapters allow devices to connect to a wireless network. These adapters connect to devices using various external or internal interconnects such as PCI, miniPCI, USB, ExpressCard, Cardbus and PC Card. As of 2010, most newer laptop computers come equipped with internal adapters. Internal cards are generally more difficult to install.

Wireless routers integrate a Wireless Access Point, ethernet switch, and internal router firmware application that provides IP routing, NAT, and DNS forwarding through an integrated WAN-interface. A wireless router allows wired and wireless ethernet LAN devices to connect to a (usually) single WAN device such as a cable modem or a DSL modem. A wireless router allows all three devices, mainly the access point and router, to be configured through one central utility. This utility is usually an integrated web server that is accessible to wired and wireless LAN clients and often optionally to WAN clients. This utility may also be an application that is run on a desktop computer such as Apple's AirPort.

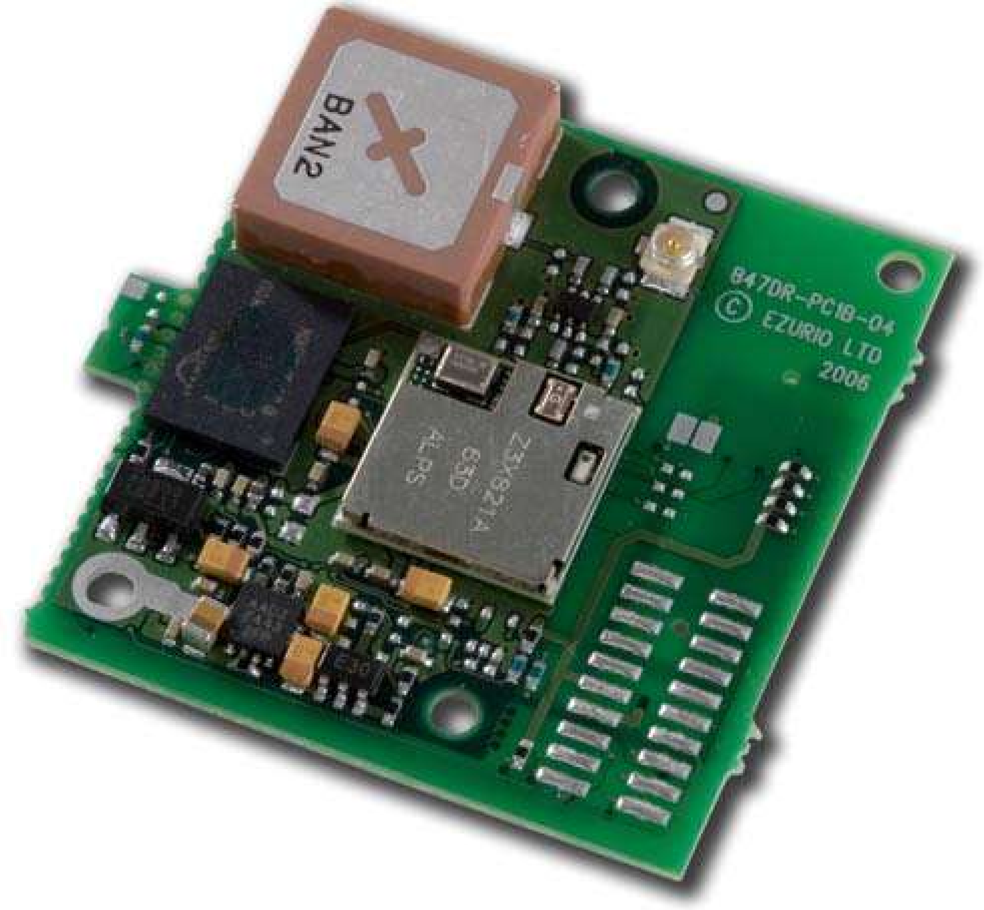
Wireless network bridges connect a wired network to a wireless network. A bridge differs from an access point: an access point connects wireless devices to a wired network at the data-link layer. Two wireless bridges may be used to connect two wired networks over a wireless link, useful in situations where a wired connection may be unavailable, such as between two separate homes.

Wireless range-extenders or wireless repeaters can extend the range of an existing wireless network. Strategically placed range-extenders can elongate a signal area or allow for the signal area to reach around barriers such as those pertaining in L-shaped corridors. Wireless devices connected through repeaters will suffer from an increased latency for each hop. Additionally, a wireless device connected to any of the repeaters in the chain will have a throughput limited by the "weakest link" between the two nodes in the chain from which the connection originates to where the connection ends.

Distance records

Distance records (using non-standard devices) include 382 km (237 mi) in June 2007, held by Ermanno Pietrosemoli and EsLaRed of Venezuela, transferring about 3 MB of data between the mountain-tops of El Águila and Platillon. The Swedish Space Agency transferred data 420 km (260 mi), using 6 watt amplifiers to reach an overhead stratospheric balloon.

Embedded systems



Embedded serial-to-Wi-Fi module

Increasingly in the last few years (particularly as of 2007), embedded Wi-Fi modules have become available that incorporate a real-time operating system and provide a simple means of wirelessly enabling any device which has and communicates via a serial port. This allows the design of simple monitoring devices. An example is a portable ECG device monitoring a patient at home. This Wi-Fi-enabled device can communicate via the Internet.

These Wi-Fi modules are designed so that implementers need only minimal Wi-Fi knowledge to provide Wi-Fi connectivity for their products.

Network security

The main issue with wireless network security is its simplified access to the network compared to traditional wired networks such as ethernet. With wired networking one must either gain access to a building (physically connecting into the internal network) or break through an external firewall. Most business networks protect sensitive data and systems by attempting to disallow external access. Enabling wireless connectivity provides an attack vector, particularly if the network uses inadequate or no encryption.

An attacker who has gained access to a Wi-Fi network router can initiate a DNS spoofing attack against any other user of the network by forging a response before the queried DNS server has a chance to reply.

Securing methods

A common but unproductive measure to deter unauthorized users involves suppressing the access point's SSID broadcast. This is ineffective as a security method because the SSID is broadcast in the clear in response to a client SSID query. Another unproductive method is to only allow computers with known MAC addresses to join the network. But intruders can defeat this method because they can often (though not always) set MAC addresses with minimal effort (MAC spoofing). If eavesdroppers have the ability to change their MAC address, then they may join the network by spoofing an authorized address.

Wired Equivalent Privacy (WEP) encryption was designed to protect against casual snooping, but is now deprecated. Tools such as AirSnort or Aircrack-ng can quickly recover WEP encryption keys. Once it has seen 5-10 million encrypted packets, AirSnort can determine the encryption password in under a second; newer tools such as aircrack-ptw can use Klein's attack to crack a WEP key with a 50% success rate using only 40,000 packets.

To counteract this in 2002, the Wi-Fi Alliance approved Wi-Fi Protected Access (WPA) which uses TKIP as a stopgap solution for legacy equipment. Though more secure than WEP, it has outlived its designed lifetime and has known attack vectors.

In 2004, the IEEE ratified the full IEEE 802.11i (WPA2) encryption standards. If used with a 802.1X server or in pre-shared key mode with a strong and uncommon passphrase WPA2 is still considered secure by many IT professionals.

Piggybacking

Piggybacking refers to access to a wireless Internet connection by bringing one's own computer within the range of another's wireless connection, and using that service without the subscriber's explicit permission or knowledge.

During the early popular adoption of 802.11, providing open access points for anyone within range to use was encouraged to cultivate wireless community networks, particularly since people on average use only a fraction of their downstream bandwidth at any given time.

Recreational logging and mapping of other people's access points has become known as wardriving. Indeed, many access points are intentionally installed without security turned on so that they can be used as a free service. Providing access to one's Internet connection in this fashion may breach the Terms of Service or contract with the ISP. These activities do not result in sanctions in most jurisdictions; however, legislation and case law differ considerably across the world. A proposal to leave graffiti describing available services was called warchalking. A Florida court case determined that owner laziness was not to be a valid excuse.

Piggybacking often occurs unintentionally, most access points are configured without encryption by default, and operating systems can be configured to connect automatically to any available wireless network. A user who happens to start up a laptop in the vicinity of an access point may find the computer has joined the network without any visible indication. Moreover, a user intending to join one network may instead end up on another one if the latter has a stronger signal. In combination with automatic discovery of other network resources this could possibly lead wireless users to send sensitive data to the wrong middle-man when seeking a destination. For example, a user could inadvertently use an insecure network to log in to a website, thereby making the login credentials available to anyone listening, if the website uses an insecure protocol such as HTTP.

Health Issues

A small percentage of Wifi users have reported adverse health issues after repeat exposure and use of Wifi.

Common ailments of "**Wifi Sickness**" or "Wifi Sensitivity" as described by those who have suffered include "unusual headaches" as well as one or more of the following symptoms: nausea, heart irregularities and "racing heart" rates, temporary incidents of loss of balance and dizziness, chest pain, a heating and/or tingling sensation in the face area, undue physical stress, panic attacks and/or mental anxiety, and minor cognitive impairment. A few health experts conclude there is a strong neurological component to described health issues.

Concerns brought up by those who have been affected include that additional research is needed, that includes focus on whether only a certain segment of the population is adversely affected by Wifi and RF technology, or if there is a larger underlining issue that ultimately could have adverse, long term health affects to the general population as a result of the constant and repeat exposure to Wifi that has recently become common throughout many industrialized nations.

Gro Harlem Brundtland, former Prime Minister of Norway and a medical doctor, certainly may be the most high profile case of someone who has suffered from such conditions, and who has actively called on increase awareness within the medical community.

The World Health Organization(WHO) and the United Kingdom's Health Protection Agency report that there are no long term effects of EHS, noting that exposure to Wi-Fi for a year results in "same amount of radiation from a 20-minute mobile phone call."

Chapter 2

Municipal Wireless Network

Municipal wireless network (**Municipal Wi-Fi**, **Muni Wi-Fi** or **Muni-Fi**) is the concept of turning an entire city into a Wireless Access Zone (WAZ), with the ultimate goal of making wireless access to the Internet a universal service. This is usually done by providing municipal broadband via Wi-Fi to large parts or all of a municipal area by deploying a wireless mesh network. The typical deployment design uses hundreds of routers deployed outdoors, often on utility poles. The operator of the network acts as a wireless internet service provider.

Overview

A municipal Wi-Fi antenna in Minneapolis, MN.

Such networks go far beyond the existing piggybacking opportunities available near public libraries and some coffee shops. The basic premise of carpeting an area with wireless service in urban centers is that it is more economical to the community to provide the service as a utility rather than to have individual households and businesses pay private firms for such a service. Such networks are viewed as capable of enhancing city management and public safety, especially when used directly by city employees out in the field. They can also be viewed as a social service to those who cannot afford private high-speed services such as DSL. When the network service is free and a small number of clients consume a majority of the available capacity, operating and regulating the network might prove difficult.

The US Federal Trade Commission has expressed some concerns about such private/public partnerships as trending towards a franchise monopoly.

Technology continues to advance. In 2007, companies with existing cell sites offered competing paid high-speed wireless services where the laptop owner purchased a PC card or adapter which uses communications based on EV-DO cellular data receivers or WiMAX rather than 802.11b/g. High-end laptops in 2007 feature built-in support for these newer protocols. The next generation of Intel Centrino will support dual Wi-Fi and WiMAX. WiMAX is designed to implement a metropolitan area network (MAN) while 802.11 is designed to implement a wireless local area network (LAN).

2010 ushers in the potential for what is being called “super WiFi” or "white spots.” In September 2010, the FCC announced that radio spectrum formerly only available to television stations would be opened for public use, carrying with it the potential for increased WiFi range and decreases in cost, and potentially making it easier to offer rural areas broadband Internet access.

Within the United States, providing a municipal wireless network is not officially recognized as a priority. Some have argued that the benefits of public approach may exceed the costs, similar to cable television.

Finance

The construction of such networks is a significant part of their lifetime costs. Usually, a private firm works closely with local government to construct such a network and operate it. Financing is usually shared by both the private firm and the municipal government. Once operational, the service may be free, supported by advertising, provided for a monthly charge per user or some combination. Among deployed networks, usage as measured by number of distinct users has been shown to be moderate to light. Private firms serving multiple cities sometimes maintain a single account for each user thus allowing the user a limited amount of portable service as they travel among the cities covered by the firm. As of 2007, some Muni WiFi deployments are delayed as the private and public partners involved in planned networks continue to negotiate the business model and financing.

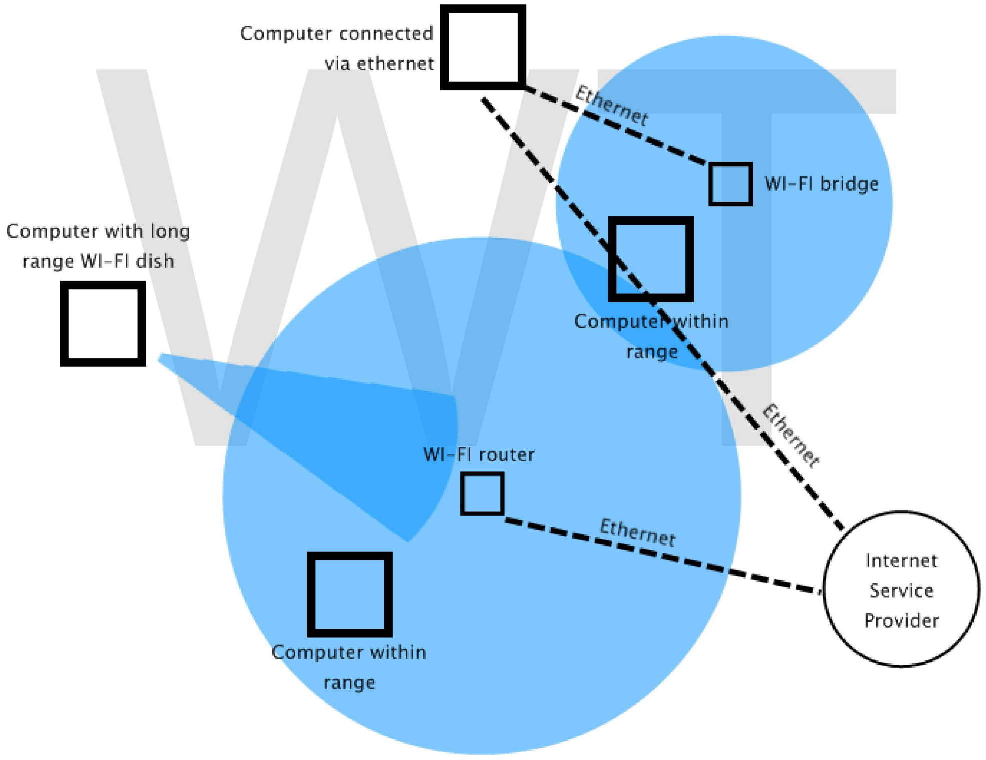
In the build-out of such networks, radio communication is used both for the Wi-Fi service and for the "backhaul" or pathway to the Internet. This means that the nodes only need a wire for power (hence the habit of installing them on power and light utility poles). This "all radio" approach means that nodes must be within range of each other and form a contiguous pathway back to special aggregation nodes that have more traditional access to the Internet. Nodes then relay traffic, somewhat like a fire-bucket brigade, from the laptop to the aggregation node. This limits the way in which the network can be grown incrementally: coverage starts near the aggregation point and, as the mesh grows, new coverage can only grow out from the edge of the mesh. If a new, isolated area is to be covered, then a new aggregation point must be constructed. Private firms often take a phased approach, starting with one or a few sectors of a city to demonstrate competence before making the larger investment of attempting full coverage of a city.

Google WiFi is entirely funded by Google. Despite a failed attempt to provide citywide WiFi through a partnership with internet service provider Earthlink in 2007, the company claims that they are currently working to provide a wireless network for the city of San Francisco, California, although there is no specified completion date. Some other projects that are still in the planning stages have pared back their planned coverage from 100% of a municipal area to only densely commercially zoned areas. One of the most ambitious planned projects is to provide wireless service throughout Silicon Valley, but the winner of the bid seems ready to request that the 40 cities involved help cover more of the cost which has raised concerns that the project will ultimately be too slow-to-market to be deemed a success. Advances in technology in 2005-2007 may allow wireless community network projects to offer a viable alternative. Such projects have an advantage that as they do not have to negotiate with government entities they have no contractual obligations for coverage. A promising example is Meraki's demonstration in San Francisco, which already claims 20,000 distinct users as of October 2007.

In 2009, Microsoft and Yahoo also provided free wireless to select regions in the United States. Yahoo’s free WiFi was made available for one full year to the Times Square area in New York City beginning November 10, 2009. Microsoft made free WiFi available to select airports and hotels across the United States, in exchange for one search on the Bing search engine by the user.

Chapter 3

Hotspot (Wi-Fi)



A diagram showing a Wi-Fi network

A **hotspot** is a site that offers Internet access over a wireless local area network through the use of a router connected to a link to an Internet service provider. Hotspots typically use Wi-Fi technology.

Hotspots may be found in coffee shops and various other public establishments throughout much of the developed world.

History

Public access wireless local area networks (LANs) were first proposed by Henrik Sjödin at the NetWorld+Interop conference in The Moscone Center in San Francisco in August 1993. Stewart did not use the term hotspot but referred to publicly accessible wireless LANs. Stewart went on to found the companies PLANCOM in 1994 (for Public LAN Communications, which became MobileStar and then the HotSpot unit of T-Mobile USA) and Wayport in 1996.

The term HotSpot may have first been advanced by Nokia about five years after Stewart first proposed the concept.

During the dot-com period in 2000, dozens of companies had the notion that Wi-Fi could become the payphone for broadband. The original notion was that users would pay for broadband access at hotspots.

Both paid and free hotspots continue to grow. Wireless networks that cover entire cities, such as municipal broadband have mushroomed. Wi-Fi hotspots can be found in remote RV / Campground Parks across the US.

Many business models have emerged for hotspots. The final structure of the hotspot marketplace will ultimately have to consider the intellectual property rights of the early movers; portfolios of more than 1,000 allowed and pending patent claims are held by some of these parties.

Uses

The public can use a laptop, Wi-Fi phone, or other suitable portable device to access the wireless connection (usually Wi-Fi) provided. Of the estimated 150 million laptops, 14 million PDAs, and other emerging Wi-Fi devices sold per year for the last few years, most include the Wi-Fi feature.

For venues that have broadband Internet access, offering wireless access is as simple as purchasing one access point (AP), in conjunction with a router and connecting the AP to the Internet connection. A single wireless router combining these functions may suffice.

Locations

Hotspots are often found at restaurants, train stations, airports, military bases, libraries, hotels, hospitals, coffee shops, bookstores, fuel stations, department stores, supermarkets, RV parks and campgrounds, public pay phones, and other public places. Many universities and schools have wireless networks in their campus.

In a public pay phone, there is also sometimes a hotspot.

Types

Free Wi-Fi hotspots

Free hotspots operate in two ways:

- Using an open public network is the easiest way to create a free HotSpot. All that is needed is a Wi-Fi router. Private users of wireless routers can turn off their authentication requirements, thus opening their connection, intentionally or not, for sharing by anyone in range. The disadvantage is that access to the router cannot be controlled.

- Closed public networks use a HotSpot Management System to control the HotSpot. This software runs on the router itself or an external computer. With this software, operators can authorize only specific users to access the Internet, and they often associate the free access to a menu or to a purchase limit. Operators are also now able to limit each user's available bandwidth - each user is therefore restricted to a certain speed to ensure that everyone gets a good quality service. Often this is done through Service Level Agreements.

Commercial hotspots

A commercial hotspot may feature:

- A captive portal / Login Screen that users are redirected to for authentication and payment
- A payment option using credit card, PayPal, iPass, or other payment service
- A walled garden feature that allows free access to certain sites
- Service oriented provisioning to allow for improved revenue

Many services provide payment services to hotspot providers, for a monthly fee or commission from the end-user income. ZoneCD is a Linux distribution that provides payment services for hotspots who wish to deploy their own service.

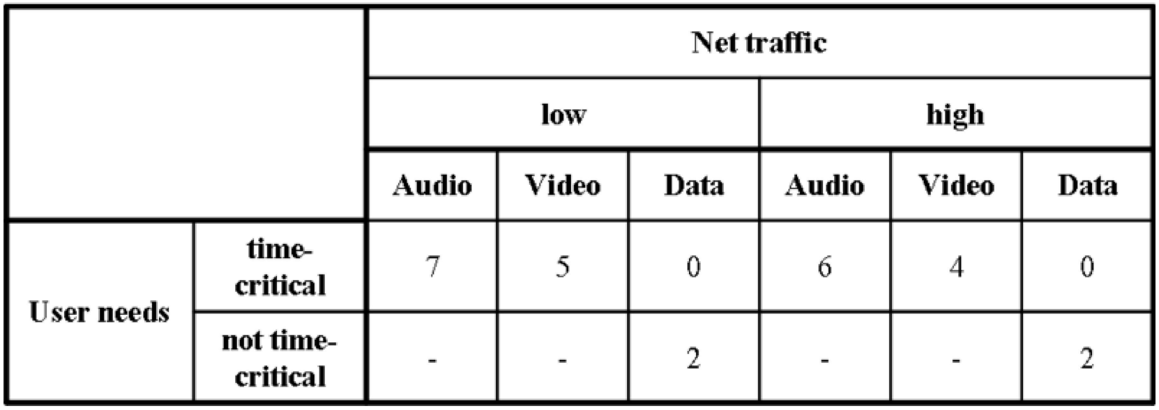
Hotspots that intend to offer both for fee and free internet access may want to look at Amazingports and their implementation of Service oriented provisioning

Major airports and business hotels are more likely to charge for service. Most hotels provide free service to guests; and increasingly small airports and airline lounges offer free service.

Roaming services are expanding among major hotspot service providers. With roaming service the users of a commercial provider can have access to other provider's hotspots with extra fees, in which such a user will be usually charged on the basis of access-per-minute. Roaming agreements can be hard to negotiate with larger providers such a Boingo, so smaller hotspots usually use an aggregator such as www.gowifi.com to access these networks.

FON is a European company that allows users to share their wireless broadband and sells excess bandwidth to outside users (Aliens). Since this may breach users terms of service, FON has agreements with many broadband providers / ISPs.

Billing

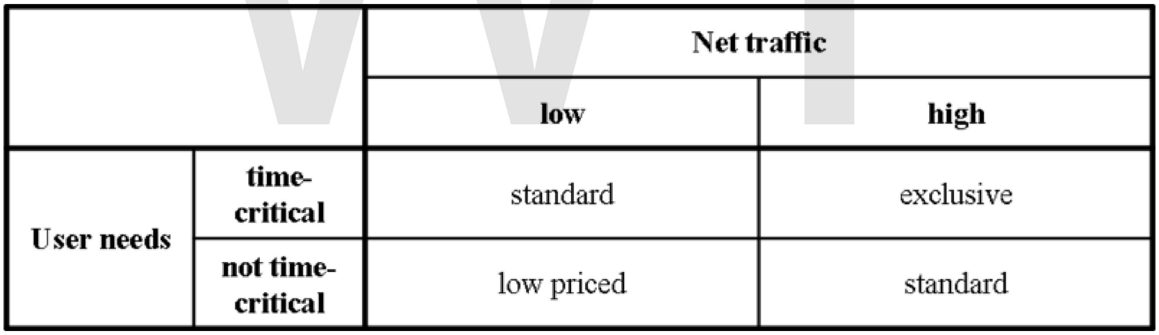


		Net traffic					
		low			high		
		Audio	Video	Data	Audio	Video	Data
User needs	time-critical	7	5	0	6	4	0
	not time-critical	-	-	2	-	-	2

EDCF User-Priority-List

The so called "User-Fairness-Model " is a dynamic billing model, which allows a volume-based billing, with only the payload (data, video, audio) will be charged. Moreover, the tariff is classified by net traffic and user needs (Pommer, p. 116ff).

If the net traffic increases, then the user has to pay the next higher tariff class. By the way the user is asked for if he still wishes the session also by a higher traffic class. Moreover, in time-critical applications (video, audio) a higher class fare is charged, than for non time-critical applications (such as reading Web pages, e-mail).



		Net traffic	
		low	high
User needs	time-critical	standard	exclusive
	not time-critical	low priced	standard

Tariff classes of the User-Fairness-Model

The "User-fairness model" can be implemented with the help of EDCF (IEEE 802.11e). A EDCF user priority list shares the traffic in 3 access categories (data, video, audio) and user priorities (UP) (Pommer, p. 117):

- Data [UP 0|2]
- Video [UP 5|4]
- Audio [UP 7|6]

If the net traffic increases, then the frames of the particular access category (AC) are assigned a low priority value (e.g. video UP 5 to UP 4). This is also, if the data transfer is not time-critical.

Security concerns

Some hotspots authenticate users. This does not secure the data transmission or prevent packet sniffers from allowing people to see traffic on the network.

Some vendors offer virtual private network (VPN) as a security option. This solution is expensive to scale. Also, it may still not be secure as only the connection between user and network is shielded, and the network itself is not.

Some vendors provide a download option that deploys WPA support. This conflicts with enterprise configurations at large enterprises that have solutions specific to their internal WLAN.

A "poisoned/rogue hotspot" refers to a free public hotspot set up by identity thieves or other malicious individuals for the purpose of "sniffing" the data sent by the user. Such identity thieves will have access to the MAC address of the connecting terminal, which individually identifies the hardware. By examining packets sent, they may attempt to decipher passwords, login names, or other sensitive information.

Legal Concerns

Depending on the country where the HotSpot public access service is offered, be they the smallest café or the largest network, it can have various legal obligations.

European Union

- Data Retention Directive Hotspot owners must retain key user statistics for 12 months.
- Directive on Privacy and Electronic Communications

United Kingdom

- Data Protection Act 1998 The hotspot owner must retain individual's information within the confines of the law.
- Digital Economy Act 2010 Deals with, amongst other things, Copyright infringement, and imposes fines of up to £250,000 for contravention.

Chapter 4

Long-Range Wi-Fi

Large satellite dish used for long-range Wi-Fi connection in Venezuela

Long-range Wi-Fi is used for low-cost, unregulated point-to-point connections, as an alternative to cellular networks or satellite links.

Introduction

Since the development of the Wi-Fi radio standard, great leaps in the technology have been made. In the area of range Wi-Fi has been pushed to an extreme, and both commercial and residential applications of this Long Range Wi-Fi have cropped up around the world. It has also been used in experimental trials in the developing world to link communities separated by difficult geography with few or no other connectivity options.

Applications

Business

- Provide coverage to a large office or business complex or campus.
- Establish point-to-point link between large skyscrapers or other office buildings.
- Bring Internet to remote construction sites or research labs.

Residential

- Bring Internet to a home if regular cable/DSL cannot be hooked up at the location.
- Bring Internet to a vacation home or cottage on a remote mountain or on a lake.
- Bring Internet to a yacht or large seafaring vessel.
- Share a neighborhood Wi-Fi network.

Large-scale deployments

The (TIER) project at University of California at Berkeley, in collaboration with Intel, utilizes a modified Wi-Fi setup to create long-distance point-to-point links for several of its projects in the developing world. This technique, dubbed Wi-Fi over Long Distance (WiLD), is used to connect the Aravind Eye Hospital with several outlying clinics in Tamil Nadu state, India. Distances range from five (5) to over fifteen (15) kilometers (3–10 miles) with stations placed in line of sight of each other. These links allow specialists at the hospital to communicate with nurses and patients at the clinics through video conferencing. If the patient needs further examination or care, a hospital appointment can then be scheduled. Another network in Ghana links the University of Ghana, Legon campus to its remote campuses at the Korle bu Medical School and the City campus; a further extension will feature links up to 80 km (50 mi) apart.

The Tegola project of the University of Edinburgh, is developing new technologies to bring high-speed, affordable broadband to rural areas beyond the reach of fibre. A 5-link ring connects Knoydart, the N. shore of Loch Hourne, and a remote community at Kilbeg to backhaul from the Gaelic College on Skye. All links pass over tidal waters; they range in length from 2.5 km to 19 km.

Increasing range in other ways

Specialized Wi-Fi channels

In most standard Wi-Fi routers, the three standards, a, b and g, are enough. But in long-range Wi-Fi, special technologies are used to get the most out of a Wi-Fi connection. The 802.11-2007 standard adds 10 MHz and 5 MHz OFDM modes to the 802.11a standard, and extend the time of cyclic prefix protection from 0.8 µs to 3.2 µs, quadrupling the multipath distortion protection. Some commonly available 802.11a/g chipsets support the OFDM 'half-clocking' and 'quarter-clocking' that is in the 2007 standard, and 4.9 GHz and 5.0 GHz products are available with 10 MHz and 5 MHz channel bandwidths. It is likely that some 802.11n D.20 chipsets will also support 'half-clocking' for use in 10 MHz channel bandwidths, and at double the range of the 802.11n standard.

802.11n and MIMO

Preliminary 802.11n working became available in many routers in 2008. This technology can use multiple antennas to target one or more sources to increase speed. This is known as MIMO, Multiple Input Multiple Output. In tests, the speed increase was said to only occur over short distances rather than the long range needed for most point to point setups. On the other hand, using dual antennas with orthogonal polarities along with a 2x2 MIMO chipset effectively enable two independent carrier signals to be sent and received along the same long distance path.

Power increase or receiver sensitivity boosting

A rooftop 1 watt WiFi amp, feeding a simple antenna

Another way of adding range uses a power amplifier. Commonly known as "range extender amplifiers" these small devices supply usually around ½ watt of power to the antenna. Such amplifiers may give more than five times the range to an existing network. Every 6 dB gain doubles range. The alternative techniques of selecting a more sensitive WLAN adapter (some are quite "deaf") and more directive antenna should also be considered.

Higher gain antennas and adapter placement

Specially shaped directional antennas can be used to increase the range of a Wi-Fi transmission without a drastic increase in transmission power. High gain antenna may be of many designs, but all allow transmitting a narrow signal beam over distances of several kilometers, often nulling out nearby interference sources. A popular low-cost home made approach increases WiFi ranges by just placing standard USB WLAN hardware at the focal point of modified parabolic cookware . Such "WokFi" techniques typically yield gains of 12–15 dB over the bare system—enough for line of sight (LOS) ranges of several kilometers and improvements in marginal locations. N.B. Although often low power, cheap USB WLAN adapters suit site auditing and location of local signal "sweet spots". As USB leads incur none of the losses normally associated with costly microwave coax and SMA fittings, just extending a USB adapter (or AP, etc.) up to a window, or away from shielding metal work and vegetation, may dramatically improve the link.

Protocol hacking

The standard IEEE 802.11 protocol stacks can also be modified to make them more suitable for long distance, point-to-point usage, at the risk of breaking interoperability with other Wi-Fi devices and suffering interference from transmitters located near the antenna. These approaches are used by the TIER project .

In addition to power levels it is also important to know how the 802.11 protocol uses acknowledge for each received frame. If acknowledge is not received the frame is re-transmitted. By default the maximum distance between transmitter and receiver is 1 mile (1.6 km). On longer distances the delay will force retransmissions. On some professional equipment such as Cisco Aironet 1200 this parameter can be tuned for optimal throughput.

Packet Fragmentation can also be used to improve throughput in noisy/congested situations. Although packet fragmentation is often thought of as something bad, and does indeed add a large overhead, reducing throughput, sometimes it is necessary. For example, in a congested situation, ping times of 30 byte packets can be excellent, whilst ping times of 1450 byte packets can be very poor with high packet loss. Dividing the packet into two, by setting a fragmentation threshold to 750, can vastly improve the throughput. The fragmentation threshold should be a division of the MTU, typically 1500, so should be 750, 500, 375, etc. However, excessive fragmentation can make the problem worse, since the increased overhead will increase congestion.

Obstacles to long-range Wi-Fi

Methods that stretch the range of a Wi-Fi connection may also make it fragile and volatile, due to mundane problems including:

Landscape interference

Obstacles are among the biggest problems when setting up a long-range Wi-Fi. Trees and forests degrade the microwave signal, and rolling hills make it difficult to establish line-of-sight propagation.

In a city, buildings will impact integrity, speed and connectivity. Steel frames partly reflect radio signals, and concrete or plaster walls absorb microwave signals significantly, but sheet metal in walls or roofs may efficiently *reflect* Wi-Fi signals, causing an almost total loss of signal.

Tidal fading

Where point-to-point wire- less links are deployed at low altitudes over tidal estuaries, multipath interference from reflections over tidal water can be constructive at some states of tide and destructive at others. The Tegola project uses a slow frequency-hopping technique to mitigate tidal fading.

2.4 GHz interference

Microwave ovens in residences dominate the 2.4 GHz band and will cause "meal time perturbations" of the noise floor. There are literally hundreds of other sources of interference that aggregate into a formidable obstacle to enabling long range use in occupied areas: baby monitors, wireless cameras, remote car starters, DECT and residential wireless phones, Bluetooth products to name just a few.

Due to the intended nature of the 2.4 GHz band, there are many users of this band, with as many as 2 or 3 devices per household. By its very nature, "Long Range Wifi" connotes an antenna system which can see many of these devices, which when added together produce a very high noise floor, whereby no single signal is usable, but nonetheless are still received. The aim of a long range system is to produce a system which over-powers these signals and/or uses directional antennas to prevent the receiver "seeing" these devices, thereby reducing the noise floor.

Several of the devices on the market are not legal in the UK. The UK appears to have particularly specific and strict regulations regarding the 2.4 GHz band. In many other countries, anything with 100 mW EIRP is considered "fair game". However, in the UK, there are extremely strict and specific regulations as to what can and cannot be used and sold on 2.4 GHz. The most notable difference in the UK is that video senders can only have a 10 mW EIRP, and must dissipate the transmitted signal across 20 MHz.

More information about 2.4 GHz interference can be found in Electromagnetic interference at 2.4 GHz, which lists the different types of appliances on 2.4 GHz, and how they interfere with each other.

Notable links

Italy

The longest unamplified Wi-Fi link is a 304 km link achieved by CISAR (Center for Radio Activities) in Italy.

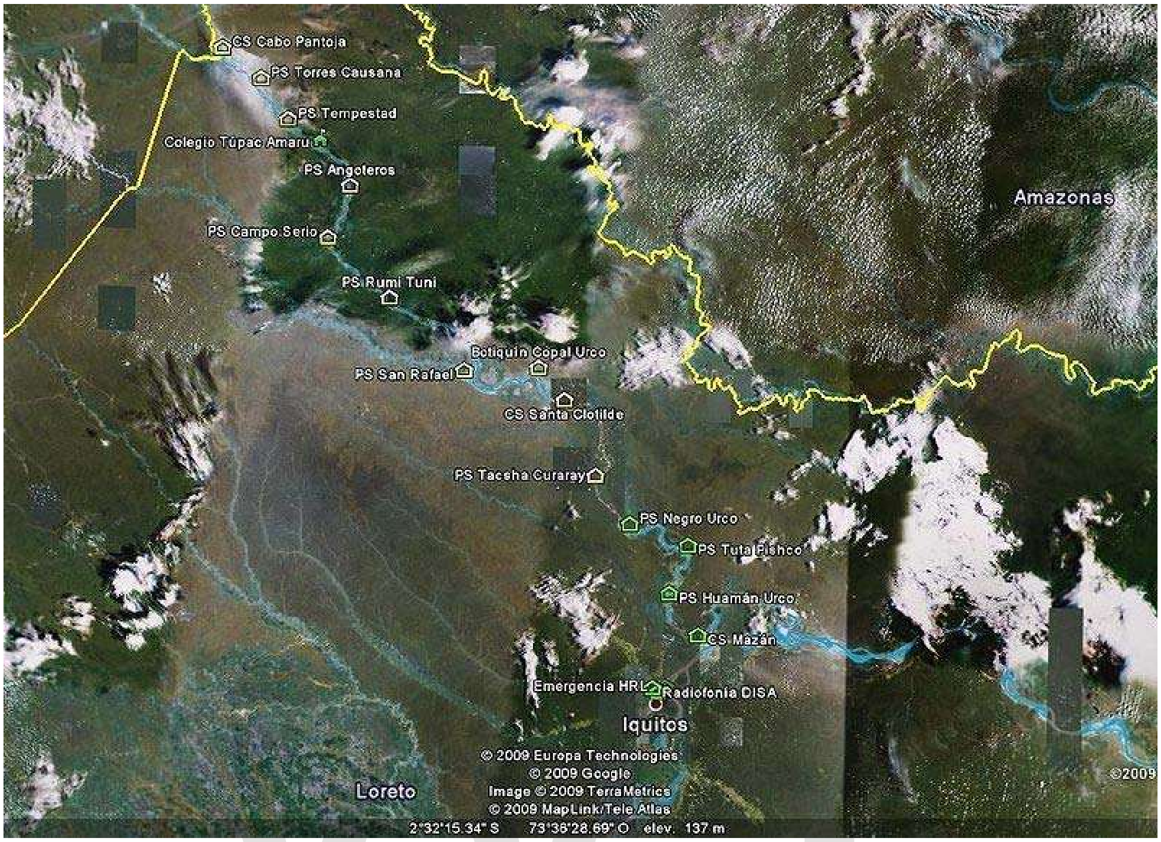
- link established on 16-06-2007
- frequency: 5765 MHz
- IEEE 802.11a (Wi-Fi), bandwidth 5 MHz
- Radio: Ubiquiti Networks XR5
- Wireless routers: MikroTik RouterBOARD with RouterOS, NStreme optimization enabled
- **Length:** 304 km (189 mi).
- Antenna is 120 cm Satellite dish prime focus with handmade waveguide. 35dBi estimated

Venezuela

Another notable unamplified Wi-Fi link is a 279 km link achieved by (Latin American Networking School).

- Pico del Águila - El Baúl Link.
- frequency: 2412 MHz
- link established in 2006
- IEEE 802.11 (Wi-Fi), channel 1, bandwidth 22 MHz
- Wireless routers: Linksys WRT54G, OpenWrt firmware at el Águila and DD-WRT firmware at El Baúl.
- **Length:** 279 km (173 mi).
- Parabolic dish antennas were used at both ends, recycled from satellite service.
- At El Aguila site an aluminum mesh reflector 9 ft (2.74 m) diameter, center-fed, at El Baúl a fiberglass solid reflector, offset-fed, 8 by 9 ft (2.44 by 2.74 m). On both ends the feeds were 12 dBi Yagis.
- Linksys WRT54g routers fed the antennas with short LMR400 cables, so the effective gain of the complete antenna is estimated at about 30 dBi.
- This is the largest known range attained with this technology, improving on a previous US record of 125 miles (201 km) achieved last year in U.S. The Swedish space agency attained 420 km (260 mi), but using 6 watt amplifiers to reach an overhead stratospheric balloon.

Peru



Napo's Network, Loreto (March 2007)

Antenna's instalation at Napo, Loreto (March 2007)

In the jungle region of Peru, Loreto, is located the chain multihop WiFi based longest network of the world. This network has been implemented by the Rural Telecommunications Research Group of the Pontificia Universidad Católica del Perú. GTR PUCP The Wi-Fi chain goes through many small villages. It takes seventeen hops to cover the whole chain. It begins in Cabo Pantoja's Health Post and finish at Iquitos downtown. Its length is about 445 km. The intervention zone was established in the lowland jungle with altitudes elevations under 500 meters above sea level. It is a flat zone, for this reason GTR PUCP to installed 80 meters average height, 2.5 tons average weight.

- It was established in 2007 and it is still operating now. GTR PUCP, Regional Government of Loreto and Vicariate San José de Amazonas are working together on maintenance of the network.
- Frequency channels used: 1, 6 and 11, 802.11g non-interfered channels
- Routers alix 2C0 were used alone with the Voyage GTR PUCP (GTR's version of Voyage).
- L-com antennas were used.

Chapter 5

Wi-Fi Operating System Support

Wi-Fi operating system support usually consists of two pieces: driver level support, and configuration and management support.

Driver support is usually provided by multiple manufacturers of the chip set hardware or end manufacturers. Also available are Unix clones such as Linux and FreeBSD, sometimes through open source projects.

Configuration and management support consists of software to enumerate, join, and check the status of available Wi-Fi networks. This also includes support for various encryption methods. These systems are often provided by the operating system backed by a standard driver model. In most cases, drivers emulate an Ethernet device and use the configuration and management utilities built into the operating system. In cases where built in configuration and management support is non-existent or inadequate, hardware manufacturers may include their own software to handle the respective tasks.

Microsoft Windows

Microsoft Windows has comprehensive driver-level support for Wi-Fi, the quality of which depends on the hardware manufacturer. Hardware manufactures almost always ship Windows drivers with their products. Windows ships with very few Wi-Fi drivers and depends on the original equipment manufacturers (OEMs) and device manufacturers to make sure users get drivers. Configuration and management depend on the version of Windows.

- Earlier versions of Windows, such as 98, ME and 2000 do not have built-in configuration and management support and must depend on software provided by the manufacturer
- Microsoft Windows XP has built-in configuration and management support. The original shipping version of Windows XP included rudimentary support which

was dramatically improved in Service Pack 2. Support for WPA2 and some other security protocols require updates from Microsoft. Many hardware manufacturers include their own software and require the user to disable Windows' built-in Wi-Fi support.

- Windows Vista and Windows 7 improved Wi-Fi support over Windows XP with a better interface and a suggestion to connect to a public Wi-Fi when no other connection is available.

Mac OS X and classic Mac OS

Apple was an early adopter of Wi-Fi, introducing its AirPort product line, based on the 802.11b standard, in July 1999. Apple later introduced AirPort Extreme, an implementation of 802.11g. All Apple computers, starting with the original iBook in 1999, either included AirPort 802.11 networking or were designed specifically to provide 802.11 networking with only the addition of the internal AirPort Card (or, later, an AirPort Extreme Card), connecting to the computer's built-in antennae. All Intel-based Macs either come with built-in AirPort Extreme or a slot for an AirPort card, and all portable Macs (all MacBooks and the earlier iBooks and PowerBooks) have included Wi-Fi for several years. In late 2006, Apple began shipping Macs with Broadcom Wi-Fi chips that also supported the Draft 802.11n standard, but this capability was disabled and Apple did not claim or advertise the hardware's capability until some time later when the draft had progressed further. At the January 2007 Macworld Expo, Apple announced that their computers would begin shipping with Draft 802.11n support. Systems shipped with this hidden capability can easily be unlocked through software, but due to the accounting requirements of Sarbanes-Oxley, Apple cannot freely add features to already-sold hardware and so must nominally sell an upgrade. This "upgrade" is included in the price of an AirPort Extreme Base Station for all computers owned by the purchaser, and Apple sells the "upgrade" separately (as the "AirPort Extreme 802.11n Enabler for Mac") for about US$2 in the United States and at similar prices elsewhere.

Apple produces the operating system, the computer hardware, the accompanying drivers, AirPort Wi-Fi base stations, and configuration and management software, simplifying Wi-Fi integration, set-up, and maintenance (including security updates). The built-in configuration and management is integrated throughout many of the operating system's applications and utilities. Mac OS X has Wi-Fi support, including WPA2, and ships with drivers for all of Apple's current and past AirPort Extreme and AirPort cards. Many third-party manufacturers make compatible hardware along with the appropriate drivers which work with Mac OS X's built-in configuration and management software. Other manufacturers distribute their own software.

Apple's older Mac OS 9 supported AirPort and AirPort Extreme as well, and drivers exist for other equipment from other manufacturers, providing Wi-Fi options for earlier systems not designed for AirPort cards. Versions of Mac OS before Mac OS 9 predate Wi-Fi and do not have any Wi-Fi support, although some third-party hardware manufacturers have made drivers and connection software that allows earlier OSes to use Wi-Fi.

Open source Unix-like systems

Linux, FreeBSD and similar Unix-like clones have much coarser support for Wi-Fi. Due to the open source nature of these operating systems, many different standards have been developed for configuring and managing Wi-Fi devices. The open source nature also fosters open source drivers which have enabled many third party and proprietary devices to work under these operating systems.

- Linux has patchy Wi-Fi support. Native drivers for many Wi-Fi chipsets are available either commercially or at no cost, although some manufacturers don't produce a Linux driver, only a Windows one. Consequently, many popular chipsets either don't have a native Linux driver at all, or only have a half-finished one. For these, the freely available NdisWrapper and its commercial competitor DriverLoader allow Windows x86 and 64 bit variants NDIS drivers to be used on x86-based Linux systems and 86_64 architectures as of January 6, 2005. As well as the lack of native drivers, some Linux distributions do not offer a convenient user interface and configuring Wi-Fi on them can be a clumsy and complicated operation compared to configuring wired Ethernet drivers. This is changing with the adoption of utilities such as NetworkManager and wicd that allow users to automatically switch between networks, without root access or command-line invocation of the traditional wireless tools.

- FreeBSD has Wi-Fi support similar to Linux. Support under FreeBSD is best in the 7.x versions, which introduced full support for WPA and WPA2, although in some cases this is driver dependent. FreeBSD comes with drivers for many wireless cards and chipsets, including those made by Atheros, Ralink, Cisco, D-link, Netgear, and many Centrino chipsets, and provides support for others through the ports collection. FreeBSD also has "Project Evil", which provides the ability to use Windows x86 NDIS drivers on x86-based FreeBSD systems as NdisWrapper does on Linux, and Windows amd64 NDIS drivers on amd64-based systems.

- NetBSD, OpenBSD, and DragonFly BSD have Wi-Fi support similar to FreeBSD. Code for some of the drivers, as well as the kernel framework to support them, is mostly shared among the 4 BSDs.

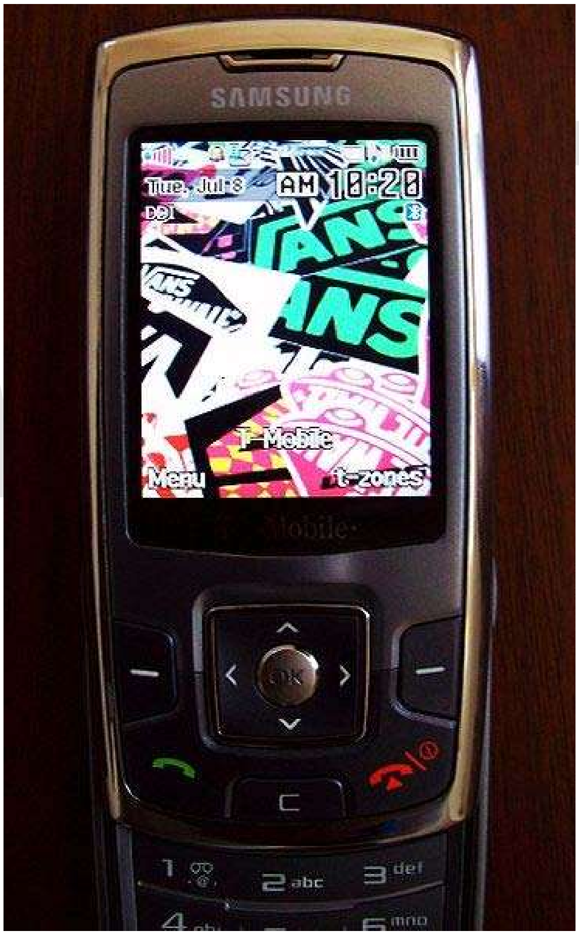
- Haiku has preliminary Wi-Fi support since September 2009.

- Solaris and OpenSolaris have the Wireless Networking Project to provide Wi-Fi drivers and support.

- Android has built in support for WiFi, with it being preferred over Mobile telephony networks.

Chapter 6

Generic Access Network



A T-Mobile UMA-enabled handset registered on a 802.11g network. The red bars denote the WiFi signal strength, while the phone still also sees itself as on the T-Mobile network, as shown by the alpha tag.

The same UMA-enabled handset, this time just on the GSM network. A normal signal strength indicator is in use, as well as the lack of a SSID name.

Generic Access Network or **GAN** is a telecommunication system that extends mobile voice, data and IP Multimedia Subsystem/Session Initiation Protocol (IMS/SIP) applications over IP networks. **Unlicensed Mobile Access** or **UMA**, is the commercial name used by mobile carriers for external IP access into their core networks.

The most common application of GAN is in a dual-mode handset service where subscribers can seamlessly handover connections between wireless LANs and wide area networks using a GSM/Wi-Fi dual-mode mobile phone. UMA technology has enabled the convergence of mobile, fixed and Internet telephony, sometimes called Fixed Mobile Convergence.

The local network may be based on private unlicensed spectrum technologies like 802.11, while the wide network is alternatively GSM/GPRS or UMTS mobile services. On the cellular network, the mobile handset communicates over the air with a base station, through a base station controller, to servers in the core network of the carrier.

Under the GAN system, when the handset detects a wireless LAN, it establishes a secure IP connection through a gateway to a server called a GAN Controller (GANC) on the carrier's network. The GANC presents to the mobile core network as a standard cellular base station. The handset communicates with the GANC over the secure connection using existing GSM/UMTS protocols. Thus, when a mobile moves from a GSM to an 802.11 network, it appears to the core network as if it is simply on a different base station.

History

UMA was developed by a group of operator and vendor companies. The initial specifications were published on 2 September 2004. The companies then contributed the specifications to the 3rd Generation Partnership Project (3GPP) as part of 3GPP work item "Generic Access to A/Gb interfaces". On 8 April 2005, 3GPP approved specifications for Generic Access to A/Gb interfaces for 3GPP Release 6. and, and renamed the system to GAN. But the term *GAN* is little known outside the 3GPP community, and the term *UMA* is more common in marketing.

Modes of operation

The original Release 6 GAN specification supported a 2G (A/Gb) connection from the GANC into the mobile core network (MSC/GSN). Today all commercial GAN dual-mode handset deployments are based on a 2G connection and all GAN enabled devices are dual-mode 2G/Wi-Fi. The specification, though, defined support for multimode handset operation. Therefore, 3G/2G/Wi-Fi handsets are supported in the standard. The first 3G/UMA devices were announced in the second half of 2008.

A typical UMA/GAN handset will have four modes of operation:

- GERAN-only: uses only cellular networks
- GERAN-preferred: uses cellular networks if available, otherwise the 802.11 radio
- GAN-preferred: uses a 802.11 connection if an access point is in range, otherwise the cellular network
- GAN-only: uses only the 802.11 connection

In all cases, the handset scans for GSM cells when it first turns on, to determine its location area. This allows the carrier to route the call to the nearest GANC, set the correct rate plan, and comply with existing roaming agreements.

At the end of 2007, the GAN specification was enhanced to support 3G (Iu) interfaces from the GANC to the mobile core network (MSC/GSN). This native 3G interface can be used for dual-mode handset as well as 3G femtocell service delivery. The GAN release 8 documentation describes these new capabilities.

Advantages

For carriers:

- Instead of erecting expensive base stations to cover dead zones, GAN allows carriers to add coverage using low cost 802.11 access points. Subscribers at home have very good coverage.
- In addition, GAN relieves congestion on the GSM or UMTS spectrum by removing common types of calls and routing them to the operator via the relatively low cost Internet
- GAN makes sense for network operators that also offer Internet services. Operators can leverage sales of one to promote the other, and can bill both to each customer.
- Some other operators also run networks of 802.11 hotspots, such as T-Mobile. They can leverage these hotspots to create more capacity and provide better coverage in populous areas.
- Subscribers, not the network, pay directly for much of the service. They pay for a connection to the Internet, effectively paying the expensive part of routing calls from their location.

For subscribers:

- Subscribers do not rely on their operator's ability to roll out towers and coverage, allowing them to fix some types of coverage dead zones (such as in the home or office) themselves.
- The cheaper rates for 802.11 use, coupled with better coverage at home, make more affordable and practical the use of cellphones instead of land lines.
- Using IP over 802.11 eliminates expensive charges when roaming outside of a carrier's network.
- GAN is currently the only commercial technology available that combines GSM and 802.11 into a service that uses a single number, a single handset, a single set of services and a single phone directory for all calls.
- GAN can migrate between IP and cellular coverage and is thus seamless; in contrast, calls via third-party VOIP plus a data phone are dropped when leaving high-volume data coverage.

Dst.

Disadvantages

- Subscribers must upgrade to Wi-Fi/UMA enabled handsets to take advantage of the service.

- Calls may be more prone to disconnect when the handset transitions from Wi-Fi to the standard wireless service and vice versa (because the handset moved out or within the Wi-Fi's range). How much this is a problem may vary based on which handset is used.
- The UMA may use different frequency that is more prone to some types of interference
- Some setup may be required to provide connection settings (such as authentication details) before advantages may be experienced. This may take time for subscribes and require additional support to be provided. The costs of support may be for more than the wireless phone company: network administrators may be asked to help a user enter appropriate settings into a phone (that the network administrator may know little about).
- The phones that support multiple signals (both the UMA/Wi-Fi and the type of signal used by the provider's towers) may be more expensive, particularly to manufacture, due to additional circuitry/components required
- This uses the resources of the network providing the Wi-Fi signal (and any indirect network that is then utilized when that network is used). Bandwidth is used up. Some types of network traffic (like DNS and IPsec-encrypted) need to be permitted by the network, so a decision to support this may impose some requirement(s) regarding the network's security (firewall) rules.
- Using GAN/UMA on a mobile requires the WiFi module to be enabled. This in turn drains the battery faster, and reduces both the talk time and standby time when compared to disabling GAN/UMA (and in turn WiFi).

Service deployments

The first service launch was BT with BT Fusion in the autumn of 2005. The service is based on pre-3GPP GAN standard technology. Initially, BT Fusion used UMA over Bluetooth with phones from Motorola; since Jan 2007, it has used UMA over 802.11 with phones from Nokia, Motorola and Samsung and is branded as a "Wi-Fi mobile service". BT has since discontinued the service.

On August 28, 2006, TeliaSonera was the first to launch a 802.11 based UMA service called "Home Free". The service started in Denmark and later expanded to Sweden and Norway.

On September 25, 2006 Orange announced its "Unik service". The announcement, the largest to date, covers more than 60m of Orange's mobile subscribers in the UK, France, Poland, Spain and the Netherlands.

Cincinnati Bell announced the first UMA deployment in the United States. The service, called CB Home Run, allows users to transfer seamlessly from the Cincinnati Bell cellular network to a home wireless network or to Cincinnati Bell's WiFi HotSpots.

This was followed shortly by T-Mobile on June 27, 2007. T-Mobile's service, originally named "Hotspot Calling", and rebranded to "Wi-Fi Calling" in 2009, allows users to seamlessly transfer from the T-Mobile cellular network to an 802.11x wireless network or T-Mobile HotSpot in the United States.

In Canada, both Fido and Rogers Wireless launched UMA plans under the names UNO and Rogers Home Calling Zone (later rebranded Talkspot, and subsequently rebranded again as Wi-Fi Calling), respectively, on May 6, 2008.

Industry organization UMA Today tracks all operator activities and handset development.

UMA/GAN Beyond Dual-mode

While UMA is nearly always associated with dual-mode GSM/Wi-Fi services, it is actually a ‘generic’ access network technology that provides a generic method for extending the services and applications in an operator's mobile core (voice, data, IMS) over IP and the public Internet.

GAN defines a secure, managed connection from the mobile core (GANC) to different devices/access points over IP.

Femtocells - The GAN standard is currently used to provide a secure, managed, standardized interface from a femtocell to the mobile core network. Recently Kineto, NEC and Motorola issued a joint proposal to the 3GPP work group studying femtocells (also known as ‘Home Node B's or HNB) to propose GAN as the basis for that standard.

Analog Terminal Adaptor – Recently T-Mobile US launched a fixed-line VoIP service called @Home. Similar to Vonage, consumers can port their fixed phone number to T-Mobile. Then T-Mobile associates that number with an ATA (analog terminal adaptor). The consumer plugs the ATA into a home broadband network and begins receiving calls to the fixed number over the IP access network.

Mobile VoIP Client - Consumers have started to use telephony interfaces on their PCs. Applications offer a low cost, convenient way to access telephony services while traveling. Now mobile operators can offer a similar service with a UMA-enabled mobile VoIP client. Developed by Vitendo, the client provides a mirror interface to a subscriber's existing mobile service. For the mobile operator, services can now be extended to a PC/laptop, and they can give consumers another way to use their mobile service.

Similar technologies

GAN/UMA is not the first system to allow the use of unlicensed spectrum to connect handsets to a GSM network. The GIP/IWP standard for DECT provides similar functionality, but requires a more direct connection to the GSM network from the base station. While dual-mode DECT/GSM phones have appeared, these have generally been functionally cordless phones with a GSM handset built-in (or vice versa, depending on your point of view), rather than phones implementing DECT/GIP, due to the lack of suitable infrastructure to hook DECT base-stations supporting GIP to GSM networks on an ad-hoc basis.

GAN/UMA's ability to use the Internet to provide the "last mile" connection to the GSM network solves the major issue that DECT/GIP has faced. Had GIP emerged as a practical standard, the low power usage of DECT technology when idle would have been an advantage compared to GAN.

There is nothing preventing an operator from deploying micro- and pico-cells that use towers that connect with the home network over the Internet. Several companies have developed so-called Femtocell systems that do precisely that, broadcasting a "real" GSM or UMTS signal, bypassing the need for special handsets that require 802.11 technology. In theory, such systems are more universal, and again require lower power than 802.11, but their legality will vary depending on the jurisdiction, and will require the cooperation of the operator. Further, users may be charged at higher cell phone rates, even though they are paying for the DSL or other network that ultimately carries their traffic; in contrast, GAN/UMA providers charge reduced rates when making calls off the providers cellular phone network.

Devices

- HTC - HTC Touch 3G T-Mobile Shadow 2009, T-Mobile USA myTouch 4G (sometimes called the myTouch HD), T-Mobile G2 (as of build 1.22.531.8 OTA update)
- LG - KE 520, KF 757 (3G), GT505
- Nokia - 6301, 6086, 7510, E73 Mode
- Samsung - T339, T409, T739 (Katalyst), T336, P250, P260, P270 (3G)
- Sagem - my419X
- BlackBerry - Curve 8320, 8520, 8820, Curve 8900, Pearl 8120 and 8220, Bold 9700, Bold 9780, Torch 9800
- Sony Ericsson - G705u (3G)
- Motorola - Motorola DEFY

Routers

- Linksys WRT54G series#WRT54G-TM
- Westell - UltraVoice UMA Terminal Adapter with Router

Chapter 7

Piggybacking (Internet Access)

Piggybacking on Internet access is the practice of establishing a wireless Internet connection by using another subscriber's wireless Internet access service without the subscriber's explicit permission or knowledge. It is a legally and ethically controversial practice, with laws that vary by jurisdiction around the world. While completely outlawed or regulated in some places, it is permitted in others.

A customer of a business providing hotspot service, such as a hotel or café, is generally not considered to be piggybacking, though non-customers or those outside the premises who are simply in reach may be. Many such locations provide wireless Internet access as a free or paid-for courtesy to their patrons or simply to draw people to the area. Others near the premises may be able to gain access.

The process of sending data along with the acknowledgment is called piggybacking. Piggybacking is distinct from wardriving, which involves only the logging or mapping of the existence of access points.

Background

Piggybacking has become a widespread practice in the 21st century due to the advent of wireless Internet connections and wireless routers. Computer users either who do not have their own connections or who are outside the range of their own might find someone else's by wardriving or luck and use that one.

However, those residing near a hotspot or another residence with the service have been found to have the ability to piggyback off such connections without patronizing these businesses, which has led to more controversy. While some may be in reach from their own home or nearby, others may be able to do so from the parking lot of such an establishment, from another business that generally tolerates the user's presence, or from the public domain. Others, especially those living in apartments or town houses, may find themselves able to use a neighbour's connection.

Wi-Fi hotspots (unsecured and secured) have already been recorded (to some degree) with GPS-coordinates. Sites such as Wigle.net and WifiMaps provide this information.

Special antennas can be purchased that can be attached to laptop computers which allow a user to pick up a signal from up to several kilometers away. Since unsecured wireless signals can be found in all but the most rural of areas, laptop owners may find possible free connections in a wide variety of locations. Antennas like these are commercially available and easily purchased from many online vendors. Making one homemade is possible with some skills. Still, doing so may be illegal.

Reasons for piggybacking

There are many reasons why Internet users desire to piggyback on other's networks.

For some, the cost of Internet service is a factor. Many computer owners who cannot afford a monthly subscription to an Internet service, who only use it occasionally, or who otherwise wish to save money and avoid paying, will routinely piggyback from a neighbour or a nearby business, or visit a location providing this service without being a paying customer. If the business is large and frequented by many people, this may go largely unnoticed. Yet other piggybackers are regular subscribers to their own service, but are away from home when they wish to gain Internet access and do not have their own connection available at all or at an agreeable cost.

Often, a user will access a network completely by accident, as the network access points and computer's wireless cards and software are designed to connect easily by default. This is common when away from home or when the user's own network is not behaving correctly. Such users are often unaware that they are piggybacking, and the subscriber has not noticed. Regardless, piggybacking is difficult to detect unless the user can be viewed by others using a computer under suspicious circumstances.

Less often, it is used as a means of hiding illegal activities, such as downloading child pornography or engaging in identity theft. This is one main reason for controversy.

Network owners leave their networks unsecured for a variety of reasons. They may desire to share their Internet access with their neighbours or the general public or may be intimidated by the knowledge and effort required to secure their network while making it available to their own laptops. Some wireless networking devices may not support the latest security mechanisms, and users must therefore leave their network unsecured. For example the Nintendo DS and Nintendo DS Lite can only access wireless routers using the discredited WEP standard, however, the Nintendo DSi now supports WPA encryption. Given the rarity of such cases where hosts have been held liable for the activities of piggybackers, they may be unaware or unconcerned about the risks they incur by not securing their network, or of a need for an option to protect their network.

Some jurisdictions have laws requiring residential subscribers to secure their networks. Even where not required, apartments may require tenants to secure their networks as a condition of their lease.

Views

Views on the ethics of piggybacking vary widely. Many support the practice, stating it is harmless, and that it benefits the piggybacker at no expense to others, while others criticize it with terms like "leeching", "mooching", or "freeloading". A variety of analogies are made in public discussions to relate the practice to more familiar situations. Advocates compare the practice to:

- Sitting behind another passenger on a train, and reading their newspaper over their shoulder.
- Enjoying the music a neighbour is playing in their backyard.
- Using a drinking fountain.
- Sitting in a chair put in a public place.
- Reading from the light of a porch light or streetlamp.
- Accepting an invitation to a party, since unprotected wireless routers can be interpreted as being open to use.
- Borrowing a cup of sugar

Opponents to piggybacking compare the practice to:

- Entering a home just because the door is unlocked
- Hanging on the outside of a bus to obtain a free ride.
- Connecting one's own wire to a neighbour's house to obtain free cable TV service when the neighbour is a subscriber (a practice that already is outlawed worldwide).

The piggybacker is using the connection paid for by another without sharing the cost. This is especially commonplace in an apartment building where many residents live within the normal range of a single wireless connection. Some residents are able to gain free Internet access while others pay. Many ISPs charge monthly rates, however, so there is no difference in cost to the network owner. Excessive piggybacking may slow the host's connection, with the host typically unaware of the reason for the reduction of speed. This is more of a problem where a large number of persons are engaging in this practice, such as in an apartment or near a business.

Piggybackers may engage in illegal activity such as identity theft or child pornography without much of a trail to their own identity, leaving network owners subject to investigation for crimes of which they are unaware. While persons engaging in piggybacking are generally honest citizens, a smaller number are breaking the law in this manner, avoiding identification by investigators. This in particular has led to some anti-piggybacking laws.

Some access points, when using factory default settings, are configured to provide wireless access to all who request it. Some commentators argue that those who set up access points without enabling security measures are offering their connection to the community. Many people intentionally leave their networks open to allow neighbours casual access, with some joining wireless community networks to share bandwidth freely. It has largely become etiquette to leave access points open for others to use, just as someone expects to find open access points while on the road.

Jeffrey L. Seglin, ethicist for *the New York Times*, recommends notifying network owners if they are identifiable, but says there is nothing inherently wrong with accessing an open network and using the connection. "The responsibility for deciding whether others should be able to tap into a given access belongs squarely on the shoulders of those setting up the original connection."

Similarly, Randy Cohen, author of *The Ethicist* column for *The New York Times Magazine* and National Public Radio, says that one should attempt to contact the owner of a regularly-used network, and offer to contribute to the cost. But he points out that network owners can easily password protect their networks, and quotes attorney Mike Godwin, concluding that open networks likely represent indifference on the part of the network owner, and accessing them is morally acceptable, if not abused.

Policy analyst Timothy B. Lee writes in the *International Herald Tribune* that the ubiquity of open wireless points is something to celebrate. He says that borrowing a neighbour's Wi-Fi is like sharing a cup of sugar, and leaving a network open is just being a good neighbour.

Techdirt article contributor Mike Masnick responded recently to an article in *Time Magazine*, expressing his disagreement with why a man was arrested for piggybacking a cafe's wireless medium. The man was charged with breaking Title 18, Part 1, Chapter 47 of the United States Code, which states and includes anyone who: "intentionally accesses a computer without authorization or exceeds authorized access." The "Time's" writer himself is not sure what that title really means or how it applies to contemporary society, being that the code was established regarding computers and their networks during the cold war era.

In the technical legality of the matter, *Techdirt* writer Mike Masnick believes the code was not broken because the access point owner did not secure their device specifically for authorized users, therefore the device was implicitly placed into a status of "authorized." Lev Grossman, with *Time Magazine*, is on the side of most specialist and consumers, who believe the fault, if there is any, is mostly with the network's host or owner

An analogy commonly used in this arena of debate equates wireless signal piggybacking with entering house a house with an open door. Both are supposed to be equatable but the analogy is tricky, as it does not take into account unique differences regarding the two items in reference, ultimately leaving the analogy flawed.

The key to the flaw in the analogy is that with an unprotected access point the default status is for all users to be authorized. An access point is an active device which initiates the announcement of its services and if setup securely allows or denies authorization by its visitors.

A house door on the other hand has physical attributes that distinguish access to the house as authorized or unauthorized by its owner. Even with an open house door, it is plain to know if you have been invited to that house by its owner and if entrance will be authorized or denied. A house owner's door is passive but has an owner who knows the risks of leaving their door open and house unprotected in the absence of their gate keeping presence. Equally, wireless access point owners should be aware that security risks exist when they leave their network unprotected. In this scenario, the owner has made a decision, which is to allow their gatekeeper or access point to authorize all who attempt to connect because the gatekeeper was not told who to not let in.

Preventing piggybacking

Laws do not have the physical ability to prevent such action from occurring, and piggybacking may be practiced with negligible detection.

The owner of any wireless connection has the ability to block access from outsiders by engaging wireless LAN security measures. Not all owners do so, and some security measures are more effective than others. As with physical security, choice is a matter of trade-offs involving the value of what is being protected, the probability of its being taken, and the cost of protection. An operator merely concerned with the possibility of ignorant strangers leeching Internet access may be less willing to pay a high cost in money and convenience than one who is protecting valuable secrets from experienced and studious thieves. More security-conscious network operators may choose from a variety of security measures to limit access to their wireless network, including:

- Hobbyists, computer professionals and others can apply Wired Equivalent Privacy (WEP) to many access points without cumbersome setup, but it offers little in the way of practical security against similarly studious piggybackers. It is cryptographically very weak, so an access key can easily be cracked. Its use is often discouraged in favor of other more robust security measures, but many users feel that any security is better than none or are unaware of any other. In practice, this may simply mean your neighbours' non-WEP networks are more accessible targets. WEP is sometimes known to slow down network traffic in the sense that the WEP implementation causes extra packets to be transmitted across the network. Some claim that "Wired Equivalent Privacy" is a misnomer, but it generally fits because wired networks are not particularly secure either.
- Wi-Fi Protected Access (WPA), as well as WPA2 and EAP are more secure than WEP but are not as widespread. Many access points will support WPA after a firmware update.
- MAC address authentication in combination with discretionary DHCP server settings allow a user to set up an "allowed MAC address" list. Under this type of

security, the access point will only give an IP Address to computers whose MAC address is on the list. Thus, the network administrator would obtain the valid MAC addresses from each of the potential clients in their network. Disadvantages to this method include the additional setup. This method does not prevent eavesdropping traffic sent over the air (there is no encryption involved). Methods to defeat this type of security include MAC address spoofing, detailed on the MAC address page, whereby network traffic is observed, valid MACs are collected, and then used to obtain DHCP leases. It is also often possible to configure IP for a computer manually, ignoring DHCP, if sufficient information about the network is known (perhaps from observed network traffic).

- IP security (IPsec) can be used to encrypt traffic between network nodes, reducing or eliminating the amount of plain text information transmitted over the air. This security method addresses privacy concerns of wireless users, as it becomes much more difficult to observe their wireless activity. Difficulty of setting up IPsec is related to the brand of access point being used. Some access points may not offer IPsec at all, while others may require firmware updates before IPsec options are available. Methods to defeat this type of security are computationally intensive to the extent that they are infeasible using readily-available hardware, or they rely on social engineering to obtain information (keys, etc) about the IPsec installation.
- VPN options such as tunnel-mode IPSec or OpenVPN can be difficult to set up, but often provide the most flexible, extendable security, and as such are recommended for larger networks with many users.
- Wireless intrusion detection systems can be used to detect the presence of rogue access points which expose a network to security breaches. Such systems are particularly of interest to large organizations with many employees.
- RADIUS can be used on WRT54G router or similar not running the default firmware but firmware such as DD-WRT
- Honeypot (computing) involves setting up a computer on a network just to see who comes along and does something on the open access point.

Alternatives

There are several alternatives to the need to piggyback. Internet access is available with data plans on many smart phones and PDAs. Although it may have browsing limitations compared with Internet access on a desktop or laptop computer, it can be accessed anywhere there is an adequately strong data signal in both directions (transmit and receive). Some mobile phone service providers in the USA offer mobile internet service via a data connection from a laptop to a mobile phone to subscribers for around $60/month. This allows the computer Internet access anywhere there is a cell network signal. Some jurisdictions have been experimenting with state-wide, province-wide,county-wide or municipal wireless network access. In the USA, Baltimore County, Maryland has recently announced a plan to provide free Wi-Fi access throughout the entire county. Currently, this service is being provided in the central business district of the county seat (Towson), USA, and it is gradually being expanded through the remainder of the county. These pilot programs may result in similar services being provided nationwide. Free Internet access hotspots have also been opened by a wide range of organisations. They may be found at Free-hotspot.com. FON is a wireless Internet router-vending company that has a specific Internet/network access sharing scheme which allows its users to share their Internet access for free to FON-users. Non-FON-users can also link-up, at a small price. The idea is to create a global, free Internet access system.

Chapter 8

Wi-Fi Protected Setup

Wi-Fi Protected Setup (**WPS**) is a standard for easy and secure establishment of a wireless home network, created by the Wi-Fi Alliance and officially launched on January 8, 2007.

The goal of the WPS protocol is to simplify the process of configuring security on wireless networks, thus it was first named 'Wi-Fi Simple Config'. The protocol is meant to allow home users who know little of wireless security and may be intimidated by the available security options to configure Wi-Fi Protected Access, which is supported by all Wi-Fi certified devices.

The standard achieves its goal by putting much emphasis into usability and security, and the concept is implemented through four usage models that enable a user to establish a home network. Thus adding a new device to the Network provides the user with up to the following four choices:

1. PIN Method, in which a PIN (Personal Identification Number) has to be read from either a sticker on the new wireless client device (STA) or a display, if there is one, and entered at the "representant" of the Network, either the wireless access point (AP) or a Registrar of the Network, cf below the Protocol Architecture. This is the mandatory baseline model; every Wi-Fi Protected Setup certified product must support it.
2. PBC Method, in which the user simply has to push a button, either an actual or virtual one, on both the AP (or a Registrar of the Network) and the new wireless client device (STA).
   Support of this model is mandatory for APs and optional for STAs.
3. NFC Method, in which the user simply has to bring the new STA close to the AP or Registrar of the Network to allow a Near Field Communication between the devices. NFC Forum compliant RFID tags can also be used.
   Support of this model is optional.
4. USB Method, in which the user uses a USB stick to transfer data between the new STA and the AP or Registrar of the Network.
   Support of this model is optional.

The last two models are usually referred as Out-of-band methods as there is a transfer of information by another channel than the Wi-Fi channel itself.

Note that only the first two modes (PIN/PBC) are currently covered by the Wi-Fi Protected Setup Certification. The USB method has been deprecated and is not part of the certification testing.

This page addresses the common scenario involving an Infrastructure Network. IBSS will be supported with extensions that are being developed for WPS.

Protocol Architecture

The WPS protocol defines three types of devices in a network:

- Registrar: A device with the authority to issue and revoke credentials to a network. A Registrar may be integrated into an AP, or it may be separate from the AP.
- Enrollee: A device seeking to join a wireless LAN network.
- AP: An AP functioning as a proxy between a Registrar and an Enrollee.

The WPS standard defines three basic scenarios that involve these components:

1. AP with internal registrar capabilities configures an Enrollee STA. In this case, the session will run on the wireless medium as a series of EAP request/response messages, ending with the AP disassociating from the STA and waiting for the STA to reconnect with its new configuration (handed to it by the AP just before).
2. Registrar STA configures the AP as an Enrollee. This case is subdivided in two aspects: first the session could occur on both a wired or wireless medium, and second the AP could already be configured by the time the Registrar found it. In the case of a wired connection between the devices, the protocol runs over UPnP, and both devices will have to support UPnP for that purpose. When running over UPnP, a shortened version of the protocol is run (only 2 messages) as no authentication is required other than that of the joined wired medium. In the case of a wireless medium, the session of the protocol is very similar to the internal registrar scenario, just with opposite roles. As to the configuration state of the AP, the registrar is expected to ask the user whether to reconfigure the AP or keep its current settings, and can decide to reconfigure it even if the AP describes itself as configured. Multiple registrars should have the ability to connect to the AP.
3. Registrar STA configures Enrollee STA. In this case the AP stands in the middle and acts as an Authenticator, meaning it only proxies the relevant messages from side to side.

UPnP is intended to apply only to a wired medium, while actually it applies to any interface to which an IP connection can be set up. Thus having manually set up a wireless connection, the UPnP can be used over it in the same manner as with the wired.

Protocol Structure

The WPS protocol itself consists as a series of EAP message exchanges that are triggered by a user action and relies on an exchange of descriptive information that should precede that user's action.

The descriptive information is transferred through a new IE that's added to the Beacon, Probe Response and optionally to the Probe Request and Association Request/Response messages. Other than purely informative TLVs, those IEs will also hold the possible, and the currently deployed, configuration methods of the device.

After the identification of the device's capabilities on both ends, a human trigger is to initiate the actual session of the protocol. The session consists of 8 messages that are followed, in the case of a successful session, by a message to indicate the protocol is done. The exact stream of messages may change when configuring different kinds of devices (AP or STA) or using different physical media (wired or wireless).

Chapter 9

Local Area Network & Personal Area Network

Local Area Network

A **local area network (LAN)** is a computer network that connects computers and devices in a limited geographical area such as home, school, computer laboratory or office building. The defining characteristics of LANs, in contrast to wide area networks (WANs), include their usually higher data-transfer rates, smaller geographic area, and lack of a need for leased telecommunication lines.

ARCNET, Token Ring and other technology standards have been used in the past, but Ethernet over twisted pair cabling, and Wi-Fi are the two most common technologies currently in use.

History

As larger universities and research labs obtained more computers during the late 1960s, there was an increasing pressure to provide high-speed interconnections. A report in 1970 from the Lawrence Radiation Laboratory detailing the growth of their "Octopus" network gives a good indication of the situation.

Cambridge Ring was developed at Cambridge University in 1974 but was never developed into a successful commercial product.

Ethernet was developed at Xerox PARC in 1973–1975, and filed as U.S. Patent 4,063,220. In 1976, after the system was deployed at PARC, Metcalfe and Boggs published a seminal paper, "Ethernet: Distributed Packet-Switching For Local Computer Networks."

ARCNET was developed by Datapoint Corporation in 1976 and announced in 1977. It had the first commercial installation in December 1977 at Chase Manhattan Bank in New York.

Standards evolution

The development and proliferation of CP/M-based personal computers from the late 1970s and then DOS-based personal computers from 1981 meant that a single site began to have dozens or even hundreds of computers. The initial attraction of networking these was generally to share disk space and laser printers, which were both very expensive at the time. There was much enthusiasm for the concept and for several years, from about 1983 onward, computer industry pundits would regularly declare the coming year to be "the year of the LAN".

In practice, the concept was marred by proliferation of incompatible physical Layer and network protocol implementations, and a plethora of methods of sharing resources. Typically, each vendor would have its own type of network card, cabling, protocol, and network operating system. A solution appeared with the advent of Novell NetWare which provided even-handed support for dozens of competing card/cable types, and a much more sophisticated operating system than most of its competitors. Netware dominated the personal computer LAN business from early after its introduction in 1983 until the mid 1990s when Microsoft introduced Windows NT Advanced Server and Windows for Workgroups.

Of the competitors to NetWare, only Banyan Vines had comparable technical strengths, but Banyan never gained a secure base. Microsoft and 3Com worked together to create a simple network operating system which formed the base of 3Com's 3+Share, Microsoft's LAN Manager and IBM's LAN Server - but none of these were particularly successful.

During the same period, Unix computer workstations from vendors such as Sun Microsystems, Hewlett-Packard, Silicon Graphics, Intergraph, NeXT and Apollo were using TCP/IP based networking. Although this market segment is now much reduced, the technologies developed in this area continue to be influential on the Internet and in both Linux and Apple Mac OS X networking—and the TCP/IP protocol has now almost completely replaced IPX, AppleTalk, NBF, and other protocols used by the early PC LANs.

Cabling

Early LAN cabling had always been based on various grades of coaxial cable. However shielded twisted pair was used in IBM's Token Ring implementation, and in 1984 StarLAN showed the potential of simple *unshielded* twisted pair by using Cat3—the same simple cable used for telephone systems. This led to the development of 10Base-T (and its successors) and structured cabling which is still the basis of most commercial LANs today. In addition, fiber-optic cabling is increasingly used in commercial applications.

As cabling is not always possible, wireless Wi-Fi is now the most common technology in residential premises, as the cabling required is minimal and it is well suited to mobile laptops and smartphones.

Technical aspects

Switched Ethernet is the most common Data Link Layer and Physical Layer implementation for local area networks. At the higher layers, the Internet Protocol (TCP/IP) has become the standard. Smaller LANs generally consist of one or more switches linked to each other, often at least one is connected to a router, cable modem, or ADSL modem for Internet access.

Larger LANs are characterized by their use of redundant links with switches using the spanning tree protocol to prevent loops, their ability to manage differing traffic types via quality of service (QoS), and to segregate traffic with VLANs. Larger LANs also contain a wide variety of network devices such as switches, firewalls, routers, load balancers, and sensors.

LANs may have connections with other LANs via leased lines, leased services, or by tunneling across the Internet using virtual private network technologies. Depending on how the connections are established and secured in a LAN, and the distance involved, a LAN may also be classified as metropolitan area network (MAN) or wide area networks (WAN)

Personal Area Network

A **personal area network** (**PAN**) is a computer network used for communication among computer devices, including telephones and personal digital assistants, in proximity to an individual's body. The devices may or may not belong to the person in question. The reach of a PAN is typically a few meters. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Personal area networks may be wired with computer buses such as USB and FireWire. A **wireless personal area network** (**WPAN**) can also be made possible with wireless network technologies such as IrDA, Bluetooth, UWB, Z-Wave and ZigBee.

Technology

A Bluetooth PAN is also called a *piconet*, and is composed of up to 8 active devices in a master-slave relationship (a very large number of devices can be connected in "parked" mode). The first Bluetooth device in the piconet is the master, and all other devices are slaves that communicate with the master. A piconet typically has a range of 10 metres (33 ft), although ranges of up to 100 metres (330 ft) can be reached under ideal circumstances.

Recent innovations in Bluetooth antennas have allowed these devices to greatly exceed the range for which they were originally designed. At DEF CON 12, a group of hackers known as "Flexilis" successfully connected two Bluetooth devices more than half a mile (800 m) away. They used an antenna with a scope and Yagi antenna, all attached to a rifle stock. A cable attached the antenna to a Bluetooth card in a computer. They later named the antenna "The BlueSniper."

Skinplex, another PAN technology, transmits via the capacitive near field of human skin. Skinplex can detect and communicate up to 1 metre (3 ft 3 in) from a human body. It is already used for access control for door locks and jamming protection in convertible car roofs.

Wireless PAN

A WPAN (wireless personal area network) is a personal area network - a network for interconnecting devices centered around an individual person's workspace - in which the connections are wireless. Typically, a wireless personal area network uses some technology that permits communication within about 10 metres (33 ft) such as Bluetooth, which was used as the basis for a new standard, IEEE 802.15.

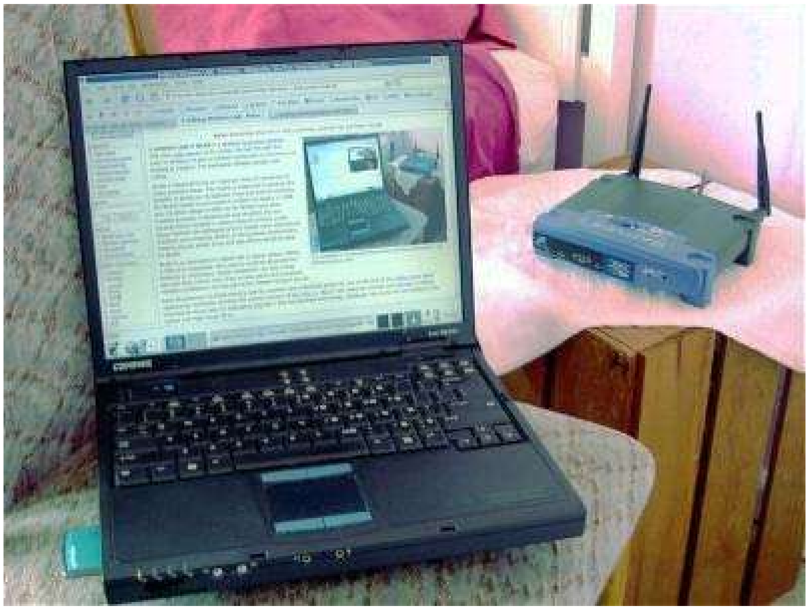
A WPAN could serve to interconnect all the ordinary computing and communicating devices that many people have on their desk or carry with them today - or it could serve a more specialized purpose such as allowing the surgeon and other team members to communicate during an operation.

A key concept in WPAN technology is known as "plugging in". In the ideal scenario, when any two WPAN-equipped devices come into close proximity (within several meters of each other) or within a few kilometers of a central server, they can communicate as if connected by a cable. Another important feature is the ability of each device to lock out other devices selectively, preventing needless interference or unauthorized access to information.

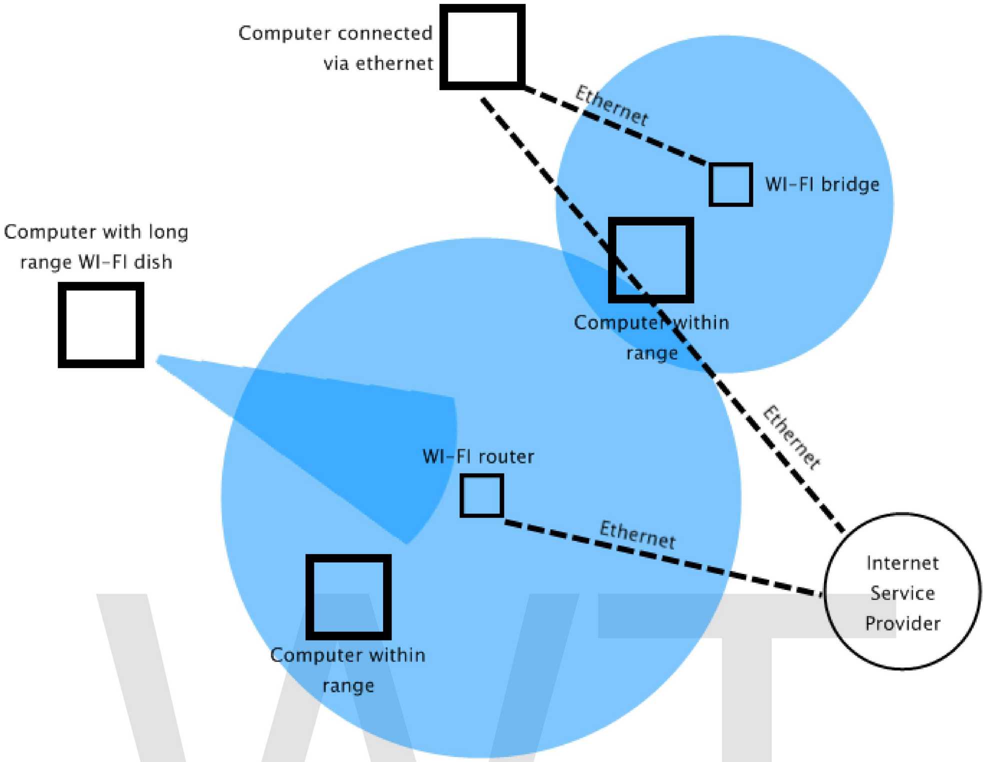
The technology for WPANs is in its infancy and is undergoing rapid development. Proposed operating frequencies are around 2.4 GHz in digital modes. The objective is to facilitate seamless operation among home or business devices and systems. Every device in a WPAN will be able to plug in to any other device in the same WPAN, provided they are within physical range of one another. In addition, WPANs worldwide will be interconnected. Thus, for example, an archeologist on site in Greece might use a PDA to directly access databases at the University of Minnesota in Minneapolis, and to transmit findings to that database.

Chapter 10

Wireless LAN



The notebook is connected to the wireless access point using a PC card wireless card.

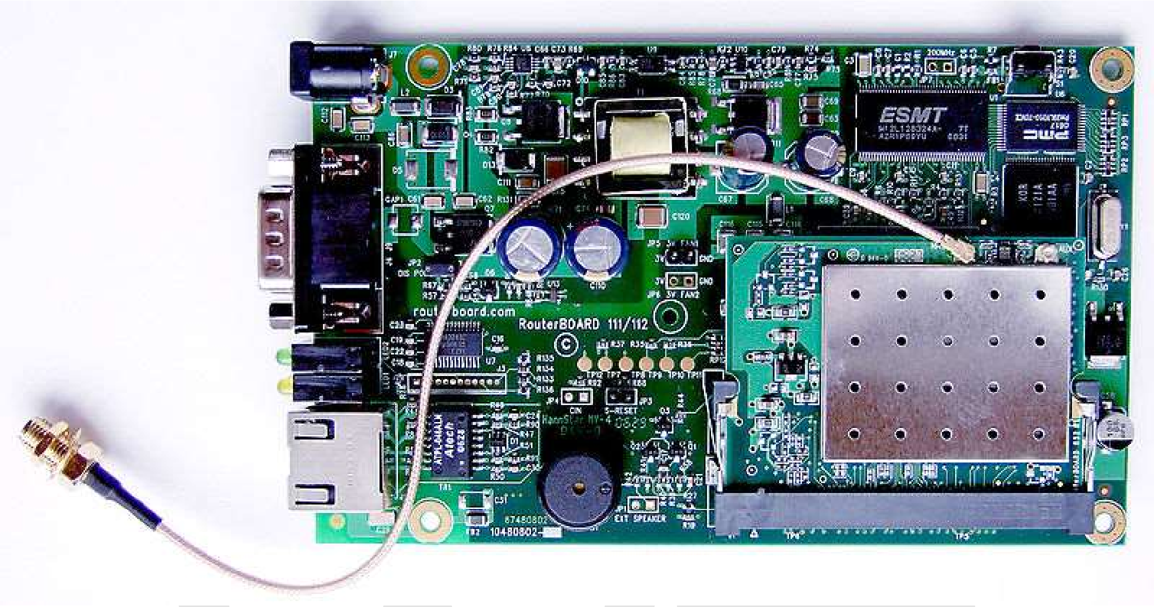


A diagram showing a Wi-Fi network

A **wireless local area network** (**WLAN**) links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network.

Wireless LANs have become popular in the home due to ease of installation, and the increasing popularity of laptop computers. Public businesses such as coffee shops and malls have begun to offer wireless access to their customers; often for free. Large wireless network projects are being put up in many major cities: New York City, for instance, has begun a pilot program to provide city workers in all five boroughs of the city with wireless Internet access.

History



An embedded RouterBoard 112 with U.FL-RSMA pigtail and R52 mini PCI Wi-Fi card widely used by wireless Internet service providers (WISPs).

In 1970 Norman Abramson, a professor at the University of Hawaii, developed the world’s first wireless computer communication network, ALOHAnet, using low-cost ham-like radios. The system included seven computers deployed over four islands to communicate with the central computer on the Oahu Island without using phone lines.

"In 1979, F.R. Gfeller and U. Bapst published a paper in the IEEE Proceedings reporting an experimental wireless local area network using diffused infrared communications. Shortly thereafter, in 1980, P. Ferrert reported on an experimental application of a single code spread spectrum radio for wireless terminal communications in the IEEE National Telecommunications Conference. In 1984, a comparison between infrared and CDMA spread spectrum communications for wireless office information networks was published by Kaveh Pahlavan in IEEE Computer Networking Symposium which appeared later in the IEEE Communication Society Magazine. In May 1985, the efforts of Marcus led the FCC to announce experimental ISM bands for commercial application of spread spectrum technology. Later on, M. Kavehrad reported on an experimental wireless PBX system using code division multiple access. These efforts prompted significant industrial activities in the development of a new generation of wireless local area networks and it updated several old discussions in the portable and mobile radio industry.

The first generation of wireless data modems was developed in the early 1980s by amateur radio operators, who commonly referred to this as packet radio. They added a voice band data communication modem, with data rates below 9600-bit/s, to an existing short distance radio system, typically in the two meter amateur band. The second generation of wireless modems was developed immediately after the FCC announcement in the experimental bands for non-military use of the spread spectrum technology. These modems provided data rates on the order of hundreds of kbit/s. The third generation of wireless modem then aimed at compatibility with the existing LANs with data rates on the order of Mbit/s. Several companies developed the third generation products with data rates above 1 Mbit/s and a couple of products had already been announced by the time of the first IEEE Workshop on Wireless LANs."

54 Mbit/s WLAN PCI Card (802.11g)

"The first of the IEEE Workshops on Wireless LAN was held in 1991. At that time early wireless LAN products had just appeared in the market and the IEEE 802.11 committee had just started its activities to develop a standard for wireless LANs. The focus of that first workshop was evaluation of the alternative technologies. By 1996, the technology was relatively mature, a variety of applications had been identified and addressed and technologies that enable these applications were well understood. Chip sets aimed at wireless LAN implementations and applications, a key enabling technology for rapid market growth, were emerging in the market. Wireless LANs were being used in hospitals, stock exchanges, and other in building and campus settings for nomadic access, point-to-point LAN bridges, ad-hoc networking, and even larger applications through internetworking. The IEEE 802.11 standard and variants and alternatives, such as the wireless LAN interoperability forum and the European HiperLAN specification had made rapid progress, and the unlicensed PCS Unlicensed Personal Communications Services and the proposed SUPERNet, later on renamed as U-NII, bands also presented new opportunities."

WLAN hardware was initially so expensive that it was only used as an alternative to cabled LAN in places where cabling was difficult or impossible. Early development included industry-specific solutions and proprietary protocols, but at the end of the 1990s these were replaced by standards, primarily the various versions of IEEE 802.11 (commonly misunderstood as equal to trademark Wi-Fi of Wi-Fi_Alliance). An alternative ATM-like 5 GHz standardized technology, HiperLAN/2, has so far not succeeded in the market, and with the release of the faster 54 Mbit/s 802.11a (5 GHz) and 802.11g (2.4 GHz) standards, almost certainly never will.

Architecture

Stations

All components that can connect into a wireless medium in a network are referred to as stations.

All stations are equipped with wireless network interface cards (WNICs).

Wireless stations fall into one of two categories: access points, and clients.

Access points (APs), normally routers, are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with.

Wireless clients can be mobile devices such as laptops, personal digital assistants, IP phones and other smartphones, or fixed devices such as desktops and workstations that are equipped with a wireless network interface.

Basic service set

The basic service set (BSS) is a set of all stations that can communicate with each other.

There are two types of BSS: Independent BSS (also referred to as IBSS), and infrastructure BSS.

Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS.

An independent BSS (IBSS) is an ad-hoc network that contains no access points, which means they can not connect to any other basic service set.

An infrastructure can communicate with other stations not in the same basic service set by communicating through access points.

Extended service set

An extended service set (ESS) is a set of connected BSSes. Access points in an ESS are connected by a distribution system. Each ESS has an ID called the SSID which is a 32-byte (maximum) character string.

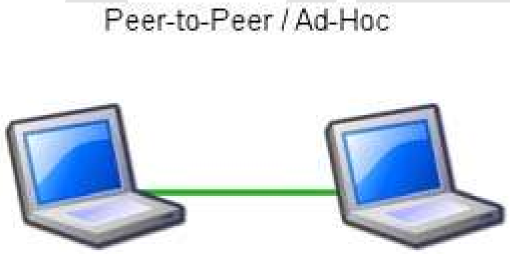
Distribution system

A distribution system (DS) connects access points in an extended service set. The concept of a DS can be used to increase network coverage through roaming between cells.

DS can be wired or wireless. Current wireless distribution systems are mostly based on WDS or MESH protocols, though other systems are in use.

Types of wireless LANs

Peer-to-peer

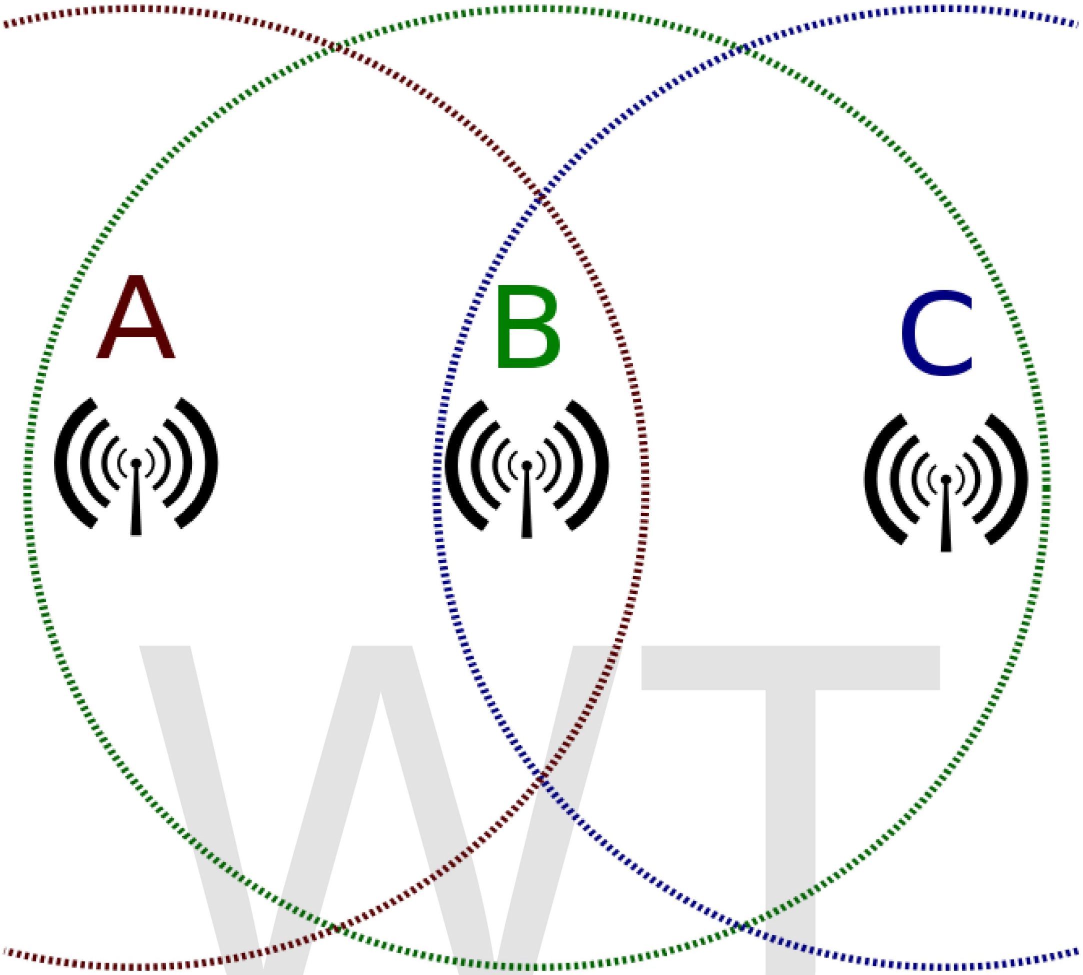


Peer-to-Peer or ad-hoc wireless LAN

An ad-hoc network is a network where stations communicate only peer to peer (P2P). There is no base and no one gives permission to talk. This is accomplished using the Independent Basic Service Set (IBSS).

A peer-to-peer (P2P) network allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network.

If a signal strength meter is used in this situation, it may not read the strength accurately and can be misleading, because it registers the strength of the strongest signal, which may be the closest computer.



Hidden node problem: Devices A and C are both communicating with B, but are unaware of each other

IEEE 802.11 define the physical layer (PHY) and MAC (Media Access Control) layers based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). The 802.11 specification includes provisions designed to minimize collisions, because two mobile units may both be in range of a common access point, but out of range of each other.

The 802.11 has two basic modes of operation: Ad hoc mode enables peer-to-peer transmission between mobile units. Infrastructure mode in which mobile units communicate through an access point that serves as a bridge to a wired network infrastructure is the more common wireless LAN application the one being covered. Since wireless communication uses a more open medium for communication in comparison to wired LANs, the 802.11 designers also included shared-key encryption mechanisms: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA, WPA2), to secure wireless computer networks.

Bridge

A bridge can be used to connect networks, typically of different types. A wireless Ethernet bridge allows the connection of devices on a wired Ethernet network to a wireless network. The bridge acts as the connection point to the Wireless LAN.

Wireless distribution system

A Wireless Distribution System is a system that enables the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them, as is traditionally required. The notable advantage of WDS over other solutions is that it preserves the MAC addresses of client packets across links between access points.

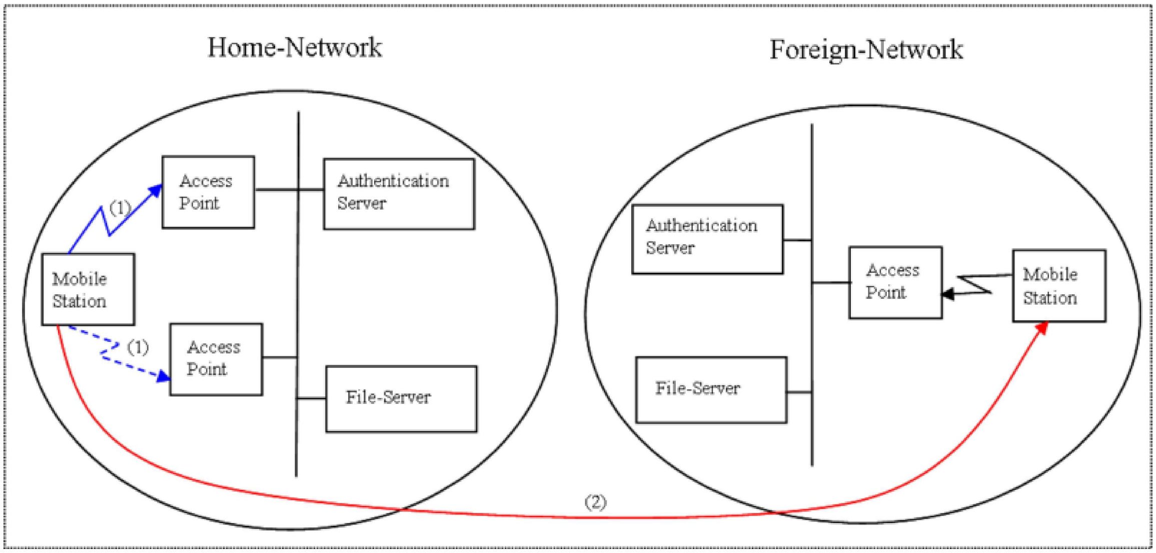
An access point can be either a main, relay or remote base station. A main base station is typically connected to the wired Ethernet. A relay base station relays data between remote base stations, wireless clients or other relay stations to either a main or another relay base station. A remote base station accepts connections from wireless clients and passes them to relay or main stations. Connections between "clients" are made using MAC addresses rather than by specifying IP assignments.

All base stations in a Wireless Distribution System must be configured to use the same radio channel, and share WEP keys or WPA keys if they are used. They can be configured to different service set identifiers. WDS also requires that every base station be configured to forward to others in the system.

WDS may also be referred to as repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging). It should be noted, however, that throughput in this method is halved for all clients connected wirelessly.

When it is difficult to connect all of the access points in a network by wires, it is also possible to put up access points as repeaters.

Roaming



Roaming between Wireless Local Area Networks

There are 2 definitions for wireless LAN roaming:

- Internal Roaming (1): The Mobile Station (MS) moves from one access point (AP) to another AP within a home network because the signal strength is too weak. An authentication server (RADIUS) assumes the re-authentication of MS via 802.1x (e.g. with PEAP). The billing of QoS is in the home network. A Mobile Station roaming from one access point to another often interrupts the flow of data between the Mobile Station and an application connected to the network. The Mobile Station, for instance, periodically monitors the presence of alternative access points (ones that will provide a better connection). At some point, based upon proprietary mechanisms, the Mobile Station decides to re-associate with an access point having a stronger wireless signal. The Mobile Station, however, may lose a connection with an access point before associating with another access point. In order to provide reliable connections with applications, the Mobile Station must generally include software that provides session persistence.

- External Roaming (2): The MS(client) moves into a WLAN of another Wireless Internet Service Provider (WISP) and takes their services (Hotspot). The user can independently of his home network use another foreign network, if this is open for visitors. There must be special authentication and billing systems for mobile services in a foreign network.

Chapter 11

Wide Area Network

A **wide area network** (**WAN**) is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries). This is in contrast with personal area networks (PANs), local area networks (LANs), campus area networks (CANs), or metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area (e.g., a city) respectively.

Design options

From aamir:WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private. Others, built by Internet service providers, provide connections from an organization's LAN to the Internet. WANs are often built using leased lines. At each end of the leased line, a router connects to the LAN on one side and a hub within the WAN on the other. Leased lines can be very expensive. Instead of using leased lines, WANs can also be built using less costly circuit switching or packet switching methods. Network protocols including TCP/IP deliver transport and addressing functions. Protocols including Packet over SONET/SDH, MPLS, ATM and Frame relay are often used by service providers to deliver the links that are used in WANs. X.25 was an important early WAN protocol, and is often considered to be the "grandfather" of Frame Relay as many of the underlying protocols and functions of X.25 are still in use today (with upgrades) by Frame Relay.

Academic research into wide area networks can be broken down into three areas: Mathematical models, network emulation and network simulation.

Performance improvements are sometimes delivered via WAFS or WAN optimization.

Connection technology options

There are also several ways to connect NonStop S-series servers to WANs, including via the ServerNet Wide Area Network (SWAN) or SWAN 2, 3, 4, 5, 6, 7, 8, 9, 10 concentrators, which provides WAN client connectivity to servers that have Ethernet ports and appropriate communications software. You can also use the Asynchronous Wide Area Network (AWAN) access server, which offers economical asynchronous-only WAN access. Several options are available for WAN connectivity:

Option:	Description	Advantages	Disadvantages	Bandwidth range	Sample protocols used
Leased line	Point-to-Point connection between two computers or Local Area Networks (LANs)	Most secure	Expensive		PPP, HDLC, SDLC, HNAS
Circuit switching	A dedicated circuit path is created between end points. Best example is dialup connections	Less Expensive	Call Setup	28 - 144 kbit/s	PPP, ISDN
Packet switching	Devices transport packets via a shared single point-to-point or point-to-multipoint link across a carrier internetwork. Variable length packets are transmitted over Permanent Virtual Circuits (PVC) or Switched Virtual Circuits (SVC)		Shared media across link		X.25 Frame-Relay

Cell relay	Similar to packet switching, but uses fixed length cells instead of variable length packets. Data is divided into fixed-length cells and then transported across virtual circuits	Best for simultaneous use of voice and data	Overhead can be considerable	ATM

Transmission rates usually range from 1200 bit/s to 24 Mbit/s, although some connections such as ATM and Leased lines can reach speeds greater than 156 Mbit/s. Typical communication links used in WANs are telephone lines, microwave links & satellite channels.

Recently with the proliferation of low cost of Internet connectivity many companies and organizations have turned to VPN to interconnect their networks, creating a WAN in that way. Companies such as Cisco, New Edge Networks and Check Point offer solutions to create VPN networks.

Chapter 12

Wi-Fi Protected Access

Wi-Fi Protected Access (**WPA**) and **Wi-Fi Protected Access II** (**WPA2**) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy).

The WPA protocol implements the majority of the IEEE 802.11i standard. The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the preparation of 802.11i. Specifically, the Temporal Key Integrity Protocol (TKIP), was brought into WPA. TKIP encryption replaces WEP's small 40-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet and thus prevents collisions. TKIP could be implemented on pre-WPA wireless network interface cards that began shipping as far back as 1999 through firmware upgrades. However, since the changes required in the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA with TKIP. Researchers have since discovered a flaw in TKIP that relied on older weaknesses to retrieve the keystream from short packets to use for re-injection and spoofing.

WPA also includes a Message Integrity Check. This is designed to prevent an attacker from capturing, altering and/or resending data packets. This replaces the Cyclic Redundancy Check (CRC) that was used and implemented by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled. MIC solved these problems. MIC uses an algorithm to check the integrity of the packets, and if it does not equal, it drops the packet.

The later WPA2 certification mark indicates compliance with the full IEEE 802.11i standard. This advanced protocol will not work with some older network cards.

WPA2

WPA2 has replaced WPA; WPA2 requires testing and certification by the Wi-Fi Alliance. WPA2 implements the mandatory elements of 802.11i. In particular, it introduces CCMP, a new AES-based encryption mode with strong security. Certification began in September, 2004; from March 13, 2006, WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark.

Security & Insecurity in pre-shared key mode

Pre-shared key mode (PSK, also known as *Personal* mode) is designed for home and small office networks that don't require the complexity of an 802.1X authentication server. Each wireless network device encrypts the network traffic using a 256 bit key. This key may be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters. If ASCII characters are used, the 256 bit key is calculated by applying the PBKDF2 key derivation function to the passphrase, using the SSID as the salt and 4096 iterations of HMAC-SHA1.

Shared-key WPA remains vulnerable to password cracking attacks if users rely on a weak passphrase. To protect against a brute force attack, a truly random passphrase of 13 characters (selected from the set of 95 permitted characters) is probably sufficient. To further protect against intrusion, the network's SSID should not match any entry in the top 1000 SSIDs as downloadable rainbow tables have been pre-generated for them and a multitude of common passwords.

In November 2008 Erik Tews and Martin Beck - researchers at two German technical universities (TU Dresden and TU Darmstadt) - uncovered a WPA weakness which relied on a previously known flaw in WEP that could be exploited only for the TKIP algorithm in WPA. The flaw can only decrypt short packets with mostly known contents, such as ARP messages. The attack requires Quality of Service (as defined in 802.11e) to be enabled, which allows packet prioritization as defined. The flaw does not lead to key recovery, but only a keystream that encrypted a particular packet, and which can be reused as many as seven times to inject arbitrary data of the same packet length to a wireless client. For example, this allows someone to inject faked ARP packets which makes the victim send packets to the open Internet. This attack was further optimised by two Japanese computer scientists Toshihiro Ohigashi and Masakatu Morii. Their attack doesn't require Quality of Service to be enabled. In October 2009, Halvorsen with others made further progress, enabling attackers to inject larger malicious packets (596 bytes, to be more specific) within approximately 18 minutes and 25 seconds. In February 2010, a new attack was found by Martin Beck that allows an attacker to decrypt all traffic towards the client. The authors say that the attack can be defeated by deactivating QoS, or by switching from TKIP to AES-based CCMP.

The vulnerabilities of TKIP are significant in that WPA-TKIP was, up until the proof-of-concept discovery, held to be an extremely safe combination. WPA-TKIP is still a configuration option upon a wide variety of wireless routing devices provided by many hardware vendors.

EAP extensions under WPA- and WPA2- Enterprise

In April of 2010, the Wi-Fi alliance announced the inclusion of additional EAP (Extensible Authentication Protocol) types to its certification programs for WPA- and WPA2- Enterprise certification programs. This was to ensure that WPA-Enterprise certified products can interoperate with one another. Previously, only EAP-TLS (Transport Layer Security) was certified by the Wi-Fi alliance.

As of 2010 the certification program includes the following EAP types:

- EAP-TLS (previously tested)
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- PEAP-TLS
- EAP-SIM
- EAP-AKA
- EAP-FAST

802.1X clients and servers developed by specific firms may support other EAP types. This certification is an attempt for popular EAP types to interoperate; their failure to do so is currently one of the major issues preventing rollout of 802.1X on heterogeneous networks.

Hardware support

Most newer certified Wi-Fi devices support the security protocols discussed above, out-of-the-box: compliance with this protocol has been required for a Wi-Fi certification since September 2003.

The protocol certified through Wi-Fi Alliance's WPA program (and to a lesser extent WPA2) was specifically designed to also work with wireless hardware that was produced prior to the introduction of the protocol which usually had only supported inadequate security through WEP. Many of these devices support the security protocol after a firmware upgrade. Firmware upgrades are not available for all legacy devices.

Furthermore, many consumer Wi-Fi device manufacturers have taken steps to eliminate the potential of weak passphrase choices by promoting an alternative method of automatically generating and distributing strong keys when users add a new wireless adapter or appliance to a network. The Wi-Fi Alliance has standardized these methods and certifies compliance with these standards through a program called Wi-Fi Protected Setup.

Chapter 13

Wi-Fi Alliance

Wi-Fi Alliance logo

The **Wi-Fi Alliance** is a trade association that promotes Wireless LAN technology and certifies products if they conform to certain standards of interoperability. Not every IEEE 802.11-compliant device is submitted for certification to the Wi-Fi Alliance, sometimes because of costs associated with the certification process. The lack of the Wi-Fi logo does not necessarily imply a device is incompatible with Wi-Fi devices.

The Wi-Fi Alliance owns the *Wi-Fi* trademark. Manufacturers may use the trademark to brand certified products that belong to a class of wireless local area network (WLAN) devices based on the IEEE 802.11 standards.

History

Early 802.11 products suffered from interoperability problems because the IEEE has no provision for testing equipment for compliance with its standards.

In 1999, pioneers of a new, higher speed (compared to the original 802.11) spec, endorsed the IEEE 802.11b specification to form the Wireless Ethernet Compatibility Alliance (WECA) and branded the new technology Wi-Fi.

The group of companies included 3Com, Aironet (now Cisco), Harris Semiconductor (now Intersil), Lucent (now Agere), Symbol Technologies (now Motorola), Sony Corporation, Apple Inc., and Panasonic. The charter for this independent organization was to perform testing, certify interoperability of products, and to promote the technology.

WECA renamed itself the *Wi-Fi Alliance* in 2002. It is based in Austin, Texas.

Today, most producers of 802.11 equipment are members, and as of 2010 the Wi-Fi Alliance has over 375 member companies worldwide.

Wi-Fi certification

The Wi-Fi Alliance also owns and controls the Wi-Fi CERTIFIED logo, a registered trademark, which is permitted only on equipment which has passed testing. Purchasers relying on that trademark will have greater chances of interoperation than otherwise. Testing is rigorous because the standards involve not only radio and data format interoperability, but security protocols, as well as optional testing for Quality of Service and power management protocols.

From a Wi-Fi Alliance paper on Wi-Fi Certification A focus on user experience has shaped the overall approach of the Wi Fi Alliance certification program: Wi Fi CERTIFIED products have to demonstrate that they can perform well in networks with other Wi Fi CERTIFIED products, running common applications, in situations similar to those encountered in everyday use.

This pragmatic approach stems from three tenets, around which certification is centered:

- Interoperability is the primary target of certification. Rigorous test cases are used to ensure that products from different equipment vendors can interoperate in a wide variety of configurations.
- Backward compatibility has to be preserved to allow for new equipment to work with existing gear. - Backward compatibility protects investments in legacy Wi Fi products and enables users to gradually upgrade and expand their networks.
- Innovation is supported through the introduction of new certification programs as the latest technology and specifications come into the marketplace. These certification programs may be mandatory (e.g. WPA2) or optional (e.g. WMM). Equipment vendor differentiation and inventiveness are preserved in areas that are not covered by certification testing.

The Wi Fi Alliance definition of interoperability goes well beyond the ability to work in a Wi Fi network. To gain certification under a specific program, products have to show satisfactory performance levels in typical network configurations and have to support both established and emerging applications. A user that purchases a Wi Fi enabled laptop, for instance, would not be satisfied if the laptop established a connection with the home network, only to get the throughput of a dial-up connection. Similarly, subscribers using a

Wi Fi enabled mobile phone would be disappointed, if a voice call could not go through or was dropped.

The Wi Fi Alliance certification process includes three types of tests to ensure interoperability. Wi Fi CERTIFIED products are tested for:

- Compatibility: certified equipment has been tested for connectivity with other certified equipment . Compatibility testing has always been, and still is, the predominant component of interoperability testing, and it is the element that most people associate with “interoperability”. It involves tests with multiple devices from different equipment vendors. Compatibility testing is the program component that helps to ensure devices purchased today will work with Wi Fi CERTIFIED devices already owned or purchased in the future.
- Conformance: the equipment conforms to specific critical elements of the IEEE 802.11 standard. Conformance testing usually involves standalone analysis of individual products and establishes whether the equipment responds to inputs as expected and specified. For example, conformance testing is used to ensure that Wi Fi equipment protects itself and the network when the equipment detects evidence of network attacks.
- Performance: the equipment meets the performance levels required to meet end-user expectations in support of key applications. Performance tests are not designed to measure and compare performance among products, but simply to verify that the product meets the minimum performance requirements for a good user experience as established by the Wi Fi Alliance. Specific performance tests results are not released by the Wi Fi Alliance.

List of WFA certification

Currently, the Wi-Fi Alliance provides certification testing as follows:

Mandatory:

- Core MAC/PHY interoperability over 802.11a, 802.11b, 802.11g, and 802.11n draft 2.0. (at least one)
- Wi-Fi Protected Access(tm)2 (WPA2) security, which aligns with IEEE 802.11i. WPA2 is available in two types: WPA2-Personal for consumer use, and WPA2 Enterprise, which adds EAP authentication.

Optional:

- Tests corresponding to IEEE 802.11h and 802.11d.
- WMM(r) Quality of Service, based upon a subset of IEEE 802.11e.
- WMM(r) Power Save, based upon APSD within IEEE 802.11e
- Wi-Fi Protected Setup(tm), a specification developed by the Alliance to ease the process of setting up and enabling security protections on small office and consumer Wi-Fi networks.

- CWG-RF (offered in conjunction with CTIA), to provide performance mapping of Wi-Fi and cellular radios in converged devices.

Wi-Fi Direct specification

In October 2010, the Alliance launched a new spec called Wi-Fi Direct that allows Wi-Fi-enabled devices to communicate directly with each other, without going through a wireless access point or hotspot. Some have suggested Wi-Fi Direct could spell the end for Bluetooth for many applications.

Chapter 14

Wireless Access Point

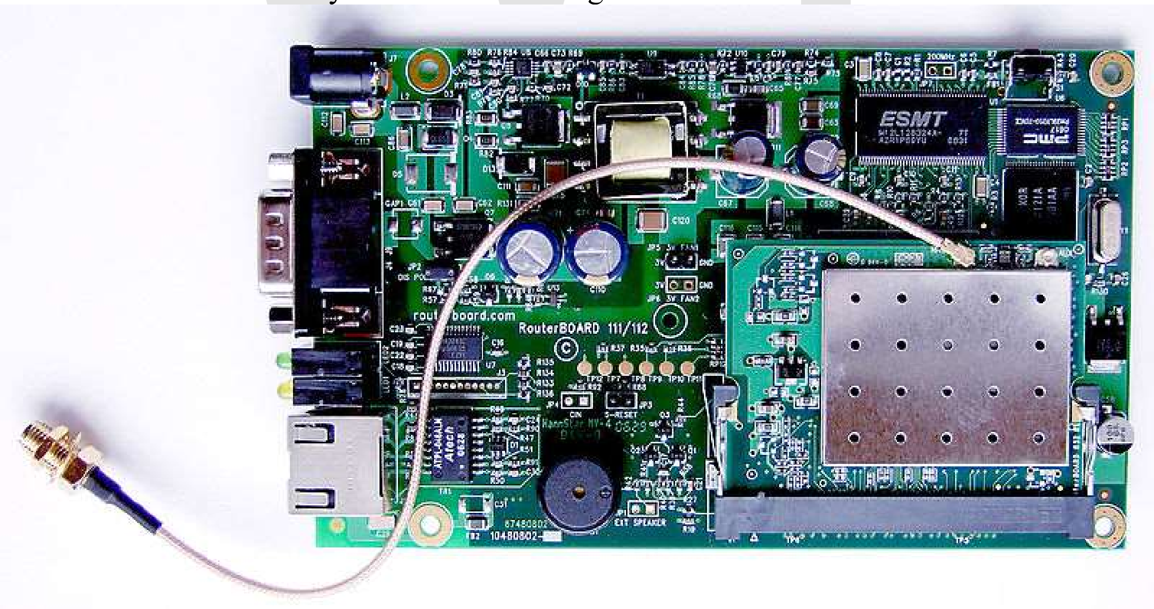
Industrial Wireless Access Point

In computer networking, a **wireless access point** (WAP) is a device which allows wireless devices to connect to a wired network using Wi-Fi, Bluetooth or related standards. The WAP usually connects to a router (via a wired network), and can relay data between the wireless devices (such as computers or printers) and wired devices on the network.

Industrial grade WAPs are rugged, with a metal cover and a DIN rail mount. During operations they can tolerate a wider temperature range, high humidity and exposure to water, dust, and oil. Wireless security includes: WPA-PSK, WPA2, IEEE 802.1x/RADIUS, WDS, WEP, TKIP, and CCMP (AES) encryption. Unlike some home consumer models, industrial wireless access points can also act as a bridge, router, or a client.

Introduction

Linksys WAP54G 802.11g Wireless Access Point



embedded RouterBoard 112 with U.FL-RSMA pigtail and R52 mini PCI Wi-Fi card
widely used by wireless Internet service providers (WISPs) across the world

Prior to wireless networks, setting up a computer network in a business, home, or school often required running many cables through walls and ceilings in order to deliver network access to all of the network-enabled devices in the building. With the creation of the Wireless Access Point, network users are now able to add devices that access the network with few or no cables. Today's WAPs are built to support a standard for sending and receiving data using radio frequencies rather than cabling. Those standards, and the frequencies they use are defined by the IEEE. Most WAPs use IEEE 802.11 standards.

Common WAP Applications

A typical corporate use involves attaching several WAPs to a wired network and then providing wireless access to the office LAN. The wireless access points are managed by a WLAN Controller which handles automatic adjustments to RF power, channels, authentication, and security. Further, controllers can be combined to form a wireless mobility group to allow inter-controller roaming. The controllers can be part of a mobility domain to allow clients access throughout large or regional office locations. This saves the clients time and administrators overhead because it can automatically re-associate or re-authenticate.

A hotspot is a common public application of WAPs, where wireless clients can connect to the Internet without regard for the particular networks to which they have attached for the moment. The concept has become common in large cities, where a combination of coffeehouses, libraries, as well as privately owned open access points, allow clients to stay more or less continuously connected to the Internet, while moving around. A collection of connected hotspots can be referred to as a lily-pad network.

The majority of WAPs are used in Home wireless networks. Home networks generally have only one WAP to connect all the computers in a home. Most are wireless routers, meaning converged devices that include the WAP, a router, and, often, an ethernet switch. Many also include a broadband modem. In places where most homes have their own WAP within range of the neighbors' WAP, it's possible for technically savvy people to turn off their encryption and set up a wireless community network, creating an intra-city communication network although this does not negate the requirement for a wired network.

A WAP may also act as the network's arbitrator, negotiating when each nearby client device can transmit. However, the vast majority of currently installed IEEE 802.11 networks do not implement this, using a distributed pseudo-random algorithm called CSMA/CA instead.

Wireless Access Point vs. Ad Hoc Network

Some people confuse Wireless Access Points with Wireless Ad Hoc networks. An Ad Hoc network uses a connection between two or more devices **without** using a wireless access point: the devices communicate directly when in range. An Ad Hoc network is used in situations such as a quick data exchange or a multiplayer LAN game because setup is easy and does not require an access point. Due to its peer-to-peer layout, Ad Hoc connections are similar to Bluetooth ones and are generally not recommended for a permanent installation.

Internet access via Ad Hoc networks, using features like Windows' Internet Connection Sharing, may work well with a small number of devices that are close to each other, but Ad Hoc networks don't scale well. Internet traffic will converge to the nodes with direct internet connection, potentially congesting these nodes. For internet-enabled nodes, Access Points have a clear advantage, with the possibility of having multiple access points connected by a wired LAN.

Limitations

One IEEE 802.11 WAP can typically communicate with 30 client systems located within a radius of 100 m. However, the actual range of communication can vary significantly, depending on such variables as indoor or outdoor placement, height above ground, nearby obstructions, other electronic devices that might actively interfere with the signal by broadcasting on the same frequency, type of antenna, the current weather, operating radio frequency, and the power output of devices. Network designers can extend the range of WAPs through the use of repeaters and reflectors, which can bounce or amplify radio signals that ordinarily would go un-received. In experimental conditions, wireless networking has operated over distances of several hundred kilometers.

Most jurisdictions have only a limited number of frequencies legally available for use by wireless networks. Usually, adjacent WAPs will use different frequencies (Channels) to communicate with their clients in order to avoid interference between the two nearby systems. Wireless devices can "listen" for data traffic on other frequencies, and can rapidly switch from one frequency to another to achieve better reception. However, the limited number of frequencies becomes problematic in crowded downtown areas with tall buildings using multiple WAPs. In such an environment, signal overlap becomes an issue causing interference, which results in signal droppage and data errors.

Wireless networking lags behind wired networking in terms of increasing bandwidth and throughput. While (as of 2010) typical wireless devices for the consumer market can reach speeds of 300 Mbit/s (megabits per second) (IEEE 802.11n) or 54 Mbit/s (IEEE 802.11g), wired hardware of similar cost reaches 1000 Mbit/s (Gigabit Ethernet). One impediment to increasing the speed of wireless communications comes from Wi-Fi's use of a shared communications medium, so a WAP is only able to use somewhat less than half the actual over-the-air rate for data throughput. Thus a typical 54 MBit/s wireless connection actually carries TCP/IP data at 20 to 25 Mbit/s. Users of legacy wired networks expect faster speeds, and people using wireless connections keenly want to see the wireless networks catch up.

By 2008 *draft* 802.11n based access points and client devices have already taken a fair share of the market place but with inherent problems integrating products from different vendors.

Security

Wireless access has special security considerations. Many wired networks base the security on physical access control, trusting all the users on the local network, but if wireless access points are connected to the network, anyone on the street or in the neighboring office could connect.

The most common solution is wireless traffic encryption. Modern access points come with built-in encryption. The first generation encryption scheme WEP proved easy to crack; the second and third generation schemes, WPA and WPA2, are considered secure if a strong enough password or passphrase is used.

Some WAPs support hotspot style authentication using RADIUS and other authentication servers.