Wireless Network and Wi-Fi Technology

(Concepts & Applications)

Precious Bertrand

Sudie Pearce

First Edition, 2012

ISBN 978-81-323-1496-7

Published by:
College Publishing House
4735/22 Prakashdeep Bldg,
Ansari Road, Darya Ganj,
Delhi - 110002
Email: info@wtbooks.com

Table of Contents

Chapter 1

Introduction to Wireless Network

Wireless network refers to any type of computer network that is wireless, and is commonly associated with a telecommunications network whose interconnections between nodes are implemented without the use of wires. Wireless telecommunications networks are generally implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves, for the carrier and this implementation usually takes place at the physical level or "layer" of the network.

Types of wireless connections

Wireless PAN

Wireless Personal Area Networks (WPANs) interconnect devices within a relatively small area, generally within reach of a person. For example, Bluetooth provides a WPAN for interconnecting a headset to a laptop. ZigBee also supports WPAN applications. Wi-Fi PANs are also getting popular as vendors have started integrating Wi-Fi in variety of consumer electronic devices. Intel My WiFi and Windows 7 virtual Wi-Fi capabilities have made Wi-Fi PANs simpler and easier to set up and configure.

Wireless LAN

A wireless local area network (WLAN) links two or more devices using a 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.

- Wi-Fi: Wi-Fi is increasingly used as a synonym for 802.11 WLANs, although it is technically a certification of interoperability between 802.11 devices.
- Fixed Wireless Data: This implements point to point links between computers or networks at two locations, often using dedicated microwave or laser beams over line of sight paths. It is often used in cities to connect networks in two or more buildings without physically wiring the buildings together.

Wireless MAN

Wireless Metropolitan area networks are a type of wireless network that connects several Wireless LANs.

- WiMAX is the term used to refer to wireless MANs and is covered in IEEE 802.16d/802.16e.

Wireless WAN

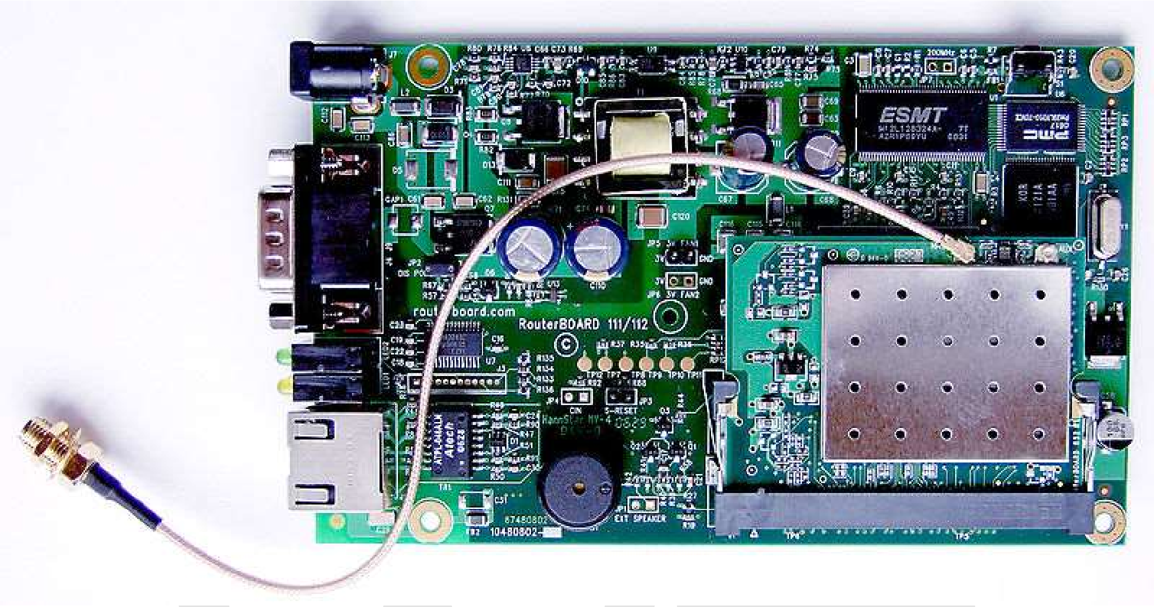
wireless wide area networks are wireless networks that typically cover large outdoor areas. These networks can be used to connect branch offices of business or as a public internet access system. They are usually deployed on the 2.4 GHz band. A typical system contains base station gateways, access points and wireless bridging relays. Other configurations are mesh systems where each access point acts as a relay also. When combined with renewable energy systems such as photo-voltaic solar panels or wind systems they can be stand alone systems.

Mobile devices networks

With the development of smart phones, cellular telephone networks routinely carry data in addition to telephone conversations:

- Global System for Mobile Communications (GSM): The GSM network is divided into three major systems: the switching system, the base station system, and the operation and support system. The cell phone connects to the base system station which then connects to the operation and support station; it then connects to the switching station where the call is transferred to where it needs to go. GSM is the most common standard and is used for a majority of cell phones.
- Personal Communications Service (PCS): PCS is a radio band that can be used by mobile phones in North America and South Asia. Sprint happened to be the first service to set up a PCS.
- D-AMPS: Digital Advanced Mobile Phone Service, an upgraded version of AMPS, is being phased out due to advancement in technology. The newer GSM networks are replacing the older system.

Uses



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.

Wireless networks have continued to develop and their uses have grown significantly. Cellular phones are part of huge wireless network systems. People use these phones daily to communicate with one another. Sending information overseas is possible through wireless network systems using satellites and other signals to communicate across the world. Emergency services such as the police department utilize wireless networks to communicate important information quickly. People and businesses use wireless networks to send and share data quickly whether it be in a small office building or across the world.

Another important use for wireless networks is as an inexpensive and rapid way to be connected to the Internet in countries and regions where the telecom infrastructure is poor or there is a lack of resources, as in most developing countries.

Compatibility issues also arise when dealing with wireless networks. Different components not made by the same company may not work together, or might require extra work to fix these issues. Wireless networks are typically slower than those that are directly connected through an Ethernet cable.

A wireless network is more vulnerable, because anyone can try to break into a network broadcasting a signal. Many networks offer WEP - Wired Equivalent Privacy - security systems which have been found to be vulnerable to intrusion. Though WEP does block some intruders, the security problems have caused some businesses to stick with wired networks until security can be improved. Another type of security for wireless networks is WPA - Wi-Fi Protected Access. WPA provides more security to wireless networks than a WEP security set up. The use of firewalls will help with security breaches which can help to fix security problems in some wireless networks that are more vulnerable.

Environmental concerns and health hazard

In recent times, there have been increased concerns about the safety of wireless communications, despite little evidence of health risks so far. The president of Lakehead University refused to agree to installation of a wireless network citing a California Public Utilities Commission study which said that the possible risk of tumors and other diseases due to exposure to electromagnetic fields (EMFs) needs to be further investigated.

Chapter 2

Bluetooth

Bluetooth logo

Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions) from fixed and mobile devices, creating personal area networks (PANs) with high levels of security. Created by telecoms vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization. Today Bluetooth is managed by the Bluetooth Special Interest Group.

Implementation

Bluetooth uses a radio technology called frequency-hopping spread spectrum, which chops up the data being sent and transmits chunks of it on up to 79 bands (1 MHz each) in the range 2402-2480 MHz. This range is in the globally unlicensed Industrial, Scientific and Medical (ISM) 2.4 GHz short-range radio frequency band.

Originally Gaussian frequency-shift keying (GFSK) modulation was the only modulation scheme available; subsequently, since the introduction of Bluetooth 2.0+EDR, π/4-DQPSK and 8DPSK modulation may also be used between compatible devices. Devices functioning with GFSK are said to be operating in basic rate (BR) mode where a gross data rate of 1 Mbit/s is possible. The term enhanced data rate (EDR) is used to describe π/4-DPSK and 8DPSK schemes, each giving 2 and 3 Mbit/s respectively. The combination of these (BR and EDR) modes in Bluetooth radio technology is classified as a "BR/EDR radio".

Bluetooth is a packet-based protocol with a master-slave structure. One master may communicate with up to 7 slaves in a piconet; all devices share the master's clock. Packet exchange is based on the basic clock, defined by the master, which ticks at 312.5 µs intervals. Two clock ticks make up a slot of 625 µs; two slots make up a slot pair of 1250 µs. In the simple case of single-slot packets the master transmits in even slots and receives in odd slots; the slave, conversely, receives in even slots and transmits in odd slots. Packets may be 1, 3 or 5 slots long but in all cases the master transmit will begin in even slots and the slave transmit in odd slots.

Bluetooth provides a secure way to connect and exchange information between devices such as faxes, mobile phones, telephones, laptops, personal computers, printers, Global Positioning System (GPS) receivers, digital cameras, and video game consoles.

The Bluetooth specifications are developed and licensed by the Bluetooth Special Interest Group (SIG). The Bluetooth SIG consists of more than 13,000 companies in the areas of telecommunication, computing, networking, and consumer electronics.

To be marketed as a Bluetooth device, it must be qualified to standards defined by the SIG.

Communication and connection

A master Bluetooth device can communicate with up to seven devices in a piconet. The devices can switch roles, by agreement, and the slave can become the master at any time.

At any given time, data can be transferred between the master and one other device (except for the little-used broadcast mode). The master chooses which slave device to address; typically, it switches rapidly from one device to another in a round-robin fashion.

The Bluetooth Core Specification provides for the connection of two or more piconets to form a scatternet, in which certain devices serve as bridges, simultaneously playing the master role in one piconet and the slave role in another.

Many USB Bluetooth adapters or "dongles" are available, some of which also include an IrDA adapter. Older (pre-2003) Bluetooth dongles, however, have limited capabilities, offering only the Bluetooth Enumerator and a less-powerful Bluetooth Radio incarnation. Such devices can link computers with Bluetooth with a distance of 100 meters, but they do not offer much in the way of services that modern adapters do.

Uses

Bluetooth is a standard wire-replacement communications protocol primarily designed for low power consumption, with a short range (power-class-dependent: 100 m, 10 m and 1 m, but ranges vary in practice; see table below) based on low-cost transceiver microchips in each device. Because the devices use a radio (broadcast) communications system, they do not have to be in line of sight of each other.

Class	Maximum Permitted Power		Range (approximate)
	mW	dBm	
Class 1	100	20	~100 meters
Class 2	2.5	4	~10 meters
Class 3	1	0	~1 meters

In most cases the effective range of class 2 devices is extended if they connect to a class 1 transceiver, compared to a pure class 2 network. This is accomplished by the higher sensitivity and transmission power of Class 1 devices.

Version	Data Rate
Version 1.2	1 Mbit/s
Version 2.0 + EDR	3 Mbit/s
Version 3.0 + HS	24 Mbit/s

While the Bluetooth Core Specification does mandate minimums for range, the range of the technology is application specific and is not limited. Manufacturers may tune their implementations to the range needed to support individual use cases.

Bluetooth profiles

To use Bluetooth wireless technology, a device must be able to interpret certain Bluetooth profiles, which are definitions of possible applications and specify general behaviors that Bluetooth enabled devices use to communicate with other Bluetooth devices. There are a wide range of Bluetooth profiles that describe many different types of applications or use cases for devices.

List of applications

A typical Bluetooth mobile phone headset

- Wireless control of and communication between a mobile phone and a handsfree headset. This was one of the earliest applications to become popular.
- Wireless networking between PCs in a confined space and where little bandwidth is required.
- Wireless communication with PC input and output devices, the most common being the mouse, keyboard and printer.
- Transfer of files, contact details, calendar appointments, and reminders between devices with OBEX.
- Replacement of traditional wired serial communications in test equipment, GPS receivers, medical equipment, bar code scanners, and traffic control devices.
- For controls where infrared was traditionally used.
- For low bandwidth applications where higher USB bandwidth is not required and cable-free connection desired.
- Sending small advertisements from Bluetooth-enabled advertising hoardings to other, discoverable, Bluetooth devices.
- Wireless bridge between two Industrial Ethernet (e.g., PROFINET) networks.
- Three seventh-generation game consoles, Nintendo's Wii and Sony's PlayStation 3 and PSP Go, use Bluetooth for their respective wireless controllers.
- Dial-up internet access on personal computers or PDAs using a data-capable mobile phone as a wireless modem like Novatel mifi.
- Short range transmission of health sensor data from medical devices to mobile phone, set-top box or dedicated telehealth devices.

- Allowing a DECT phone to ring and answer calls on behalf of a nearby cell phone
- Real-time location systems (RTLS), are used to track and identify the location of objects in real-time using “Nodes” or “tags” attached to, or embedded in the objects tracked, and “Readers” that receive and process the wireless signals from these tags to determine their locations
- Tracking livestock and detainees. According to a leaked diplomatic cable, King Abdullah of Saudi Arabia suggested "implanting detainees with an electronic chip containing information about them and allowing their movements to be tracked with Bluetooth. This was done with horses and falcons, the King said."

Bluetooth vs. Wi-Fi IEEE 802.11 in networking

Bluetooth and Wi-Fi have many applications: setting up networks, printing, or transferring files.

Wi-Fi is intended for resident equipment and its applications. The category of applications is outlined as WLAN, the wireless local area networks. Wi-Fi is intended as a replacement for cabling for general local area network access in work areas.

Bluetooth is intended for non-resident equipment and its applications. The category of applications is outlined as the wireless personal area network (WPAN). Bluetooth is a replacement for cabling in a variety of personally carried applications in any ambiance and can also support fixed location applications such as smart energy functionality in the home (thermostats, etc.).

Wi-Fi is wireless version of a traditional Ethernet network, and requires configuration to set up shared resources, transmit files, and to set up audio links (for example, headsets and hands-free devices). Wi-Fi uses the same radio frequencies as Bluetooth, but with higher power, resulting in a faster connection and better range from the base station. The nearest equivalents in Bluetooth are the DUN profile, which allows devices to act as modem interfaces, and the PAN profile, which allows for ad-hoc networking.

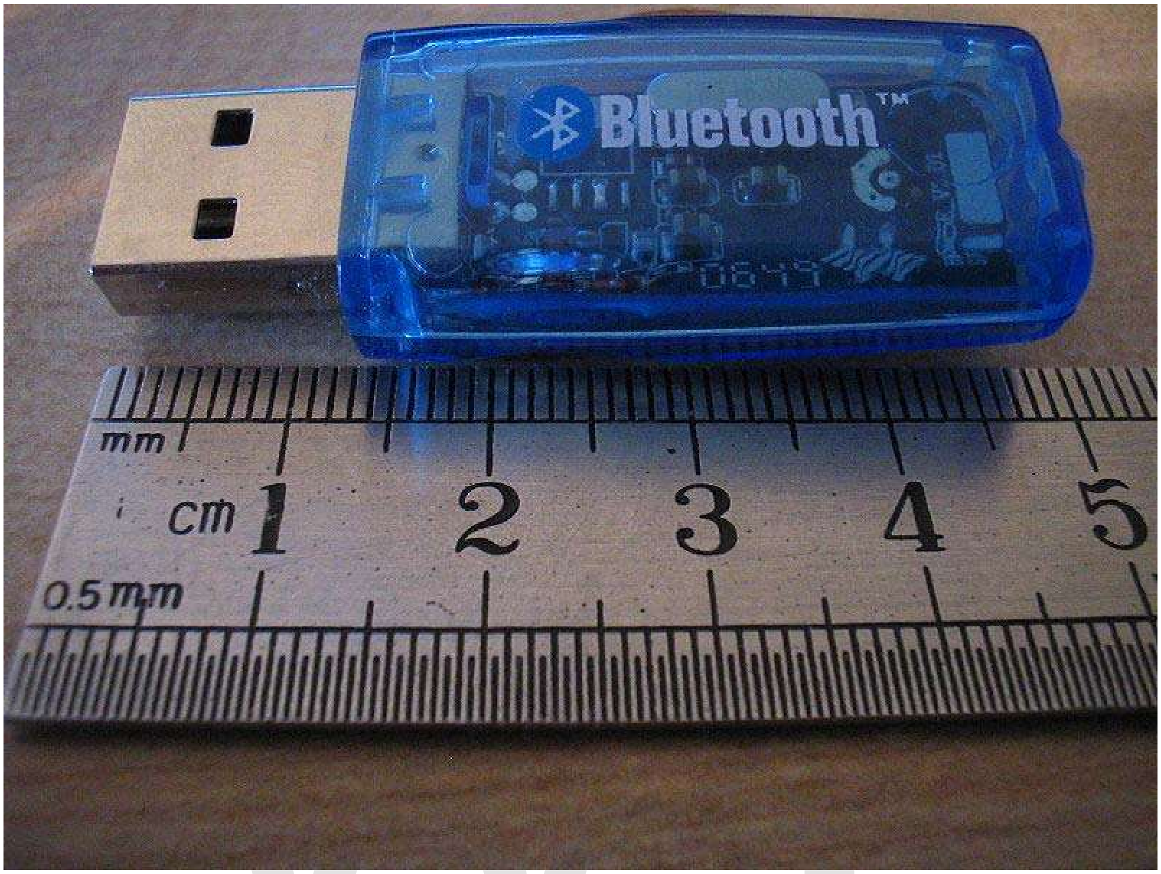
Bluetooth devices

A Bluetooth USB dongle with a 100 m range. The MacBook Pro, shown, also has a built in Bluetooth adaptor.

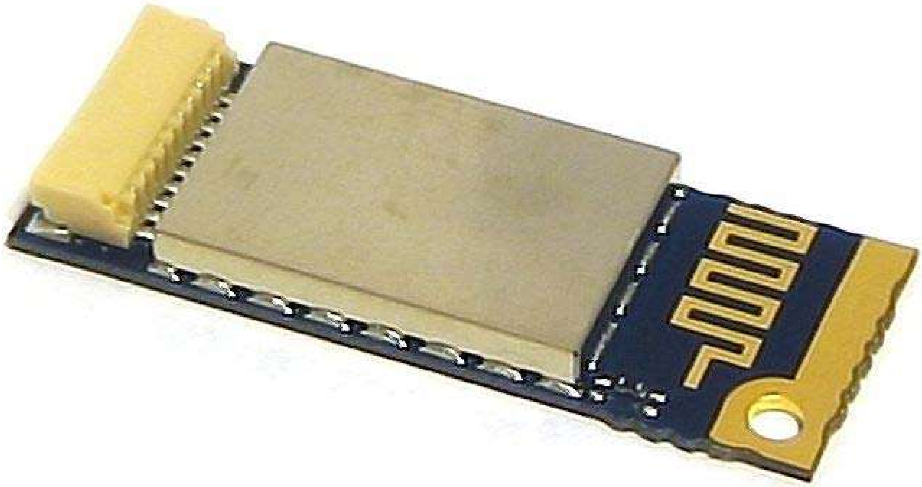
Bluetooth exists in many products, such as the iPod Touch, Lego Mindstorms NXT, PlayStation 3, PSP Go, telephones, the Nintendo Wii, and some high definition headsets, modems, and watches. The technology is useful when transferring information between two or more devices that are near each other in low-bandwidth situations. Bluetooth is commonly used to transfer sound data with telephones (i.e., with a Bluetooth headset) or byte data with hand-held computers (transferring files).

Bluetooth protocols simplify the discovery and setup of services between devices. Bluetooth devices can advertise all of the services they provide. This makes using services easier because more of the security, network address and permission configuration can be automated than with many other network types.

Computer requirements



A typical Bluetooth USB dongle



An internal notebook Bluetooth card (14×36×4 mm)

A personal computer that does not have embedded Bluetooth can be used with a Bluetooth adapter or "dongle" that will enable the PC to communicate with other Bluetooth devices (such as mobile phones, mice and keyboards). While some desktop computers and most recent laptops come with a built-in Bluetooth radio, others will require an external one in the form of a dongle.

Unlike its predecessor, IrDA, which requires a separate adapter for each device, Bluetooth allows multiple devices to communicate with a computer over a single adapter.

Operating system support

Apple has supported Bluetooth since Mac OS X v10.2 which was released in 2002.

For Microsoft platforms, Windows XP Service Pack 2 and SP3 releases have native support for Bluetooth 1.1, 2.0 and 2.0+EDR. Previous versions required users to install their Bluetooth adapter's own drivers, which were not directly supported by Microsoft. Microsoft's own Bluetooth dongles (packaged with their Bluetooth computer devices) have no external drivers and thus require at least Windows XP Service Pack 2. Windows Vista RTM/SP1 with the Feature Pack for Wireless or Windows Vista SP2 support Bluetooth 2.1+EDR. Windows 7 supports Bluetooth 2.1+EDR and Extended Inquiry Response (EIR).

The Windows XP and Windows Vista/Windows 7 Bluetooth stacks support the following Bluetooth profiles natively: PAN, SPP, DUN, HID, HCRP. The Windows XP stack can be replaced by a third party stack which may support more profiles or newer versions of Bluetooth. The Windows Vista/Windows 7 Bluetooth stack supports vendor-supplied additional profiles without requiring the Microsoft stack to be replaced.

Linux has two popular Bluetooth stacks, BlueZ and Affix. The BlueZ stack is included with most Linux kernels and was originally developed by Qualcomm. The Affix stack was developed by Nokia. FreeBSD features Bluetooth support since its 5.0 release. NetBSD features Bluetooth support since its 4.0 release. Its Bluetooth stack has been ported to OpenBSD as well.

Mobile phone requirements

A Bluetooth-enabled mobile phone is able to pair with many devices. To ensure the broadest support of feature functionality together with legacy device support, the Open Mobile Terminal Platform (OMTP) forum has published a recommendations paper, entitled "Bluetooth Local Connectivity".

Specifications and features

The Bluetooth specification was developed in 1994 by Jaap Haartsen and Sven Mattisson, who were working for Ericsson in Lund, Sweden. The specification is based on frequency-hopping spread spectrum technology.

The specifications were formalized by the Bluetooth Special Interest Group (SIG). The SIG was formally announced on May 20, 1998. Today it has a membership of over 13,000 companies worldwide. It was established by Ericsson, IBM, Intel, Toshiba, Motorola and Nokia, and later joined by many other companies.

Bluetooth v1.0 and v1.0B

Versions 1.0 and 1.0B had many problems, and manufacturers had difficulty making their products interoperable. Versions 1.0 and 1.0B also included mandatory Bluetooth hardware device address (BD_ADDR) transmission in the Connecting process (rendering anonymity impossible at the protocol level), which was a major setback for certain services planned for use in Bluetooth environments.

Bluetooth v1.1

- Ratified as IEEE Standard 802.15.1-2002
- Many errors found in the 1.0B specifications were fixed.
- Added support for non-encrypted channels.
- Received Signal Strength Indicator (RSSI).

Bluetooth v1.2

This version is backward compatible with 1.1 and the major enhancements include the following:

- Faster Connection and Discovery
- *Adaptive frequency-hopping spread spectrum (AFH)*, which improves resistance to radio frequency interference by avoiding the use of crowded frequencies in the hopping sequence.
- Higher transmission speeds in practice, up to 721 kbit/s, than in 1.1.
- Extended Synchronous Connections (eSCO), which improve voice quality of audio links by allowing retransmissions of corrupted packets, and may optionally increase audio latency to provide better support for concurrent data transfer.
- Host Controller Interface (HCI) support for three-wire UART.
- Ratified as IEEE Standard 802.15.1-2005
- Introduced Flow Control and Retransmission Modes for L2CAP.

Bluetooth v2.0 + EDR

This version of the Bluetooth Core Specification was released in 2004 and is backward compatible with the previous version 1.2. The main difference is the introduction of an Enhanced Data Rate (EDR) for faster data transfer. The nominal rate of EDR is about 3 Mbit/s, although the practical data transfer rate is 2.1 Mbit/s. EDR uses a combination of GFSK and Phase Shift Keying modulation (PSK) with two variants, π/4-DQPSK and 8DPSK. EDR can provide a lower power consumption through a reduced duty cycle.

The specification is published as "Bluetooth v2.0 + EDR" which implies that EDR is an optional feature. Aside from EDR, there are other minor improvements to the 2.0 specification, and products may claim compliance to "Bluetooth v2.0" without supporting the higher data rate. At least one commercial device states "Bluetooth v2.0 without EDR" on its data sheet.

Bluetooth v2.1 + EDR

Bluetooth Core Specification Version 2.1 + EDR is fully backward compatible with 1.2, and was adopted by the Bluetooth SIG on July 26, 2007.

The headline feature of 2.1 is secure simple pairing (SSP): this improves the pairing experience for Bluetooth devices, while increasing the use and strength of security.

2.1 allows various other improvements, including "Extended inquiry response" (EIR), which provides more information during the inquiry procedure to allow better filtering of devices before connection; sniff subrating, which reduces the power consumption in low-power mode

Bluetooth v3.0 + HS

Version 3.0 + HS of the Bluetooth Core Specification was adopted by the Bluetooth SIG on April 21, 2009. Bluetooth 3.0+HS supports theoretical data transfer speeds of up to 24 Mbit/s, though not over the Bluetooth link itself. Instead, the Bluetooth link is used for negotiation and establishment, and the high data rate traffic is carried over a colocated 802.11 link. Its main new feature is AMP (Alternate MAC/PHY), the addition of 802.11 as a high speed transport. Two technologies had been anticipated for AMP: 802.11 and UWB, but UWB is missing from the specification.

The High-Speed part of the specification is not mandatory, and hence only devices sporting the "+HS" will actually support the Bluetooth over Wifi high-speed data transfer. A Bluetooth 3.0 device without the HS suffix will not support High Speed, and needs to only support Unicast Connectionless Data (UCD), as shown in the Bluetooth 3.0+HS specification, Vol0, section 4.1 Specification Naming Conventions.

Alternate MAC/PHY

> Enables the use of alternative MAC and PHYs for transporting Bluetooth profile data. The Bluetooth radio is still used for device discovery, initial connection and profile configuration, however when large quantities of data need to be sent, the high speed alternate MAC PHY 802.11 (typically associated with Wi-Fi) will be used to transport the data. This means that the proven low power connection models of Bluetooth are used when the system is idle, and the low power per bit radios are used when large quantities of data need to be sent.

Unicast connectionless data

> Permits service data to be sent without establishing an explicit L2CAP channel. It is intended for use by applications that require low latency between user action

and reconnection/transmission of data. This is only appropriate for small amounts of data.

Enhanced Power Control

Updates the power control feature to remove the open loop power control, and also to clarify ambiguities in power control introduced by the new modulation schemes added for EDR. Enhanced power control removes the ambiguities by specifying the behaviour that is expected. The feature also adds closed loop power control, meaning RSSI filtering can start as the response is received. Additionally, a "go straight to maximum power" request has been introduced. This is expected to deal with the headset link loss issue typically observed when a user puts their phone into a pocket on the opposite side to the headset.

Bluetooth v4.0

On June 12, 2007, Nokia and Bluetooth SIG had announced that Wibree will be a part of the Bluetooth specification, as an ultra-low power Bluetooth technology.

On December 17, 2009, the Bluetooth SIG adopted Bluetooth low energy technology as the hallmark feature of the version 4.0. The provisional names *Wibree* and *Bluetooth ULP* (Ultra Low Power) are abandoned.

On April 21, 2010, the Bluetooth SIG completed the Bluetooth Core Specification version 4.0, which includes *Classic Bluetooth*, *Bluetooth high speed* and *Bluetooth low energy* protocols. Bluetooth high speed is based on Wi-Fi, and Classic Bluetooth consists of legacy Bluetooth protocols.

Bluetooth low energy

Bluetooth low energy is an alternative to the Bluetooth standard that was introduced in Bluetooth v4.0, and is aimed at very low power applications running off a coin cell. It allows two types of implementation, dual-mode and single-mode. In a dual-mode implementation, Bluetooth low energy functionality is integrated into an existing Classic Bluetooth controller. The resulting architecture shares much of Classic Bluetooth’s existing radio and functionality resulting in a minimal cost increase compared to Classic Bluetooth. Additionally, manufacturers can use current Classic Bluetooth (Bluetooth v2.1 + EDR or Bluetooth v3.0 + HS) chips with the new low energy stack, enhancing the development of Classic Bluetooth enabled devices with new capabilities.

Single-mode chips, which will enable highly integrated and compact devices, will feature a lightweight Link Layer providing ultra-low power idle mode operation, simple device discovery, and reliable point-to-multipoint data transfer with advanced power-save and secure encrypted connections at the lowest possible cost. The Link Layer in these controllers will enable Internet connected sensors to schedule Bluetooth low energy traffic between Bluetooth transmissions.

Future

Broadcast channel

Enables Bluetooth information points. This will drive the adoption of Bluetooth into mobile phones, and enable advertising models based on users pulling information from the information points, and not based on the object push model that is used in a limited way today.

Topology management

Enables the automatic configuration of the piconet topologies especially in scatternet situations that are becoming more common today. This should all be invisible to users of the technology, while also making the technology "just work."

QoS improvements

Enable audio and video data to be transmitted at a higher quality, especially when best effort traffic is being transmitted in the same piconet.

UWB for AMP

The high speed (AMP) feature of Bluetooth v3.0 is based on 802.11, but the AMP mechanism was designed to be usable with other radios as well. It was originally intended for UWB, but the WiMedia Alliance, the body responsible for the flavor of UWB intended for Bluetooth, announced in March 2009 that it was disbanding.

On March 16, 2009, the WiMedia Alliance announced it was entering into technology transfer agreements for the WiMedia Ultra-wideband (UWB) specifications. WiMedia has transferred all current and future specifications, including work on future high speed and power optimized implementations, to the Bluetooth Special Interest Group (SIG), Wireless USB Promoter Group and the USB Implementers Forum. After the successful completion of the technology transfer, marketing and related administrative items, the WiMedia Alliance will cease operations.

In October 2009 the Bluetooth Special Interest Group suspended development of UWB as part of the alternative MAC/PHY, Bluetooth v3.0 + HS solution. A small, but significant, number of former WiMedia members had not and would not sign up to the necessary agreements for the IP transfer. The Bluetooth SIG is now in the process of evaluating other options for its longer term roadmap.

Technical information

Bluetooth protocol stack

"Bluetooth is defined as a layer protocol architecture consisting of core protocols, cable replacement protocols, telephony control protocols, and adopted protocols." Mandatory protocols for all Bluetooth stacks are: LMP, L2CAP and SDP. Additionally, these protocols are almost universally supported: HCI and RFCOMM.

LMP (Link Management Protocol)

Used for control of the radio link between two devices. Implemented on the controller.

L2CAP (Logical Link Control & Adaptation Protocol)

Used to multiplex multiple logical connections between two devices using different higher level protocols. Provides segmentation and reassembly of on-air packets.

In Basic mode, L2CAP provides packets with a payload configurable up to 64kB, with 672 bytes as the default MTU, and 48 bytes as the minimum mandatory supported MTU.

In Retransmission & Flow Control modes, L2CAP can be configured for reliable or isochronous data per channel by performing retransmissions and CRC checks.

Bluetooth Core Specification Addendum 1 adds two additional L2CAP modes to the core specification. These modes effectively deprecate original Retransmission and Flow Control modes:

- **Enhanced Retransmission Mode** (ERTM): This mode is an improved version of the original retransmission mode. This mode provides a reliable L2CAP channel.
- **Streaming Mode** (SM): This is a very simple mode, with no retransmission or flow control. This mode provides an unreliable L2CAP channel.

Reliability in any of these modes is optionally and/or additionally guaranteed by the lower layer Bluetooth BDR/EDR air interface by configuring the number of retransmissions and flush timeout (time after which the radio will flush packets). In-order sequencing is guaranteed by the lower layer.

Only L2CAP channels configured in ERTM or SM may be operated over AMP logical links.

SDP (Service Discovery Protocol)

Service Discovery Protocol (SDP) allows a device to discover services supported by other devices, and their associated parameters. For example, when connecting a mobile phone to a Bluetooth headset, SDP will be used for determining which Bluetooth profiles are supported by the headset (Headset Profile, Hands Free Profile, Advanced Audio Distribution Profile (A2DP) etc.) and the protocol multiplexer settings needed to connect to each of them. Each service is identified by a Universally Unique Identifier (UUID), with official services (Bluetooth profiles) assigned a short form UUID (16 bits rather than the full 128)

HCI (Host/Controller Interface)

Standardised communication between the host stack (e.g., a PC or mobile phone OS) and the controller (the Bluetooth IC). This standard allows the host stack or controller IC to be swapped with minimal adaptation.

There are several HCI transport layer standards, each using a different hardware interface to transfer the same command, event and data packets. The most commonly used are USB (in PCs) and UART (in mobile phones and PDAs).

In Bluetooth devices with simple functionality (e.g., headsets) the host stack and controller can be implemented on the same microprocessor. In this case the HCI is optional, although often implemented as an internal software interface.

RFCOMM (Serial Port Emulation)

Radio frequency communications (RFCOMM) is a cable replacement protocol used to create a virtual serial data stream. RFCOMM provides for binary data transport and emulates EIA-232 (formerly RS-232) control signals over the Bluetooth baseband layer.

RFCOMM provides a simple reliable data stream to the user, similar to TCP. It is used directly by many telephony related profiles as a carrier for AT commands, as well as being a transport layer for OBEX over Bluetooth.

Many Bluetooth applications use RFCOMM because of its widespread support and publicly available API on most operating systems. Additionally, applications that used a serial port to communicate can be quickly ported to use RFCOMM.

BNEP (Bluetooth Network Encapsulation Protocol)

BNEP is used for transferring another protocol stack's data via an L2CAP channel. It's main purpose is the transmission of IP packets in the Personal Area Networking Profile. BNEP performs a similar function to SNAP in Wireless LAN.

AVCTP (Audio/Video Control Transport Protocol)

Used by the remote control profile to transfer AV/C commands over an L2CAP channel. The music control buttons on a stereo headset use this protocol to control the music player.

AVDTP (Audio/Video Distribution Transport Protocol)

Used by the advanced audio distribution profile (A2DP) to stream music to stereo headsets over an L2CAP channel. Intended to be used by video distribution profile.

Telephony control protocol

Telephony control protocol-binary (TCS BIN) is the bit-oriented protocol that defines the call control signaling for the establishment of voice and data calls between Bluetooth devices. Additionally, "TCS BIN defines mobility management procedures for handling groups of Bluetooth TCS devices."

TCS-BIN is only used by the cordless telephony profile, which failed to attract implementers. As such it is only of historical interest.

Adopted protocols

Adopted protocols are defined by other standards-making organizations and incorporated into Bluetooth's protocol stack, allowing Bluetooth to create protocols only when necessary. The adopted protocols include:

Point-to-Point Protocol (PPP)
    Internet standard protocol for transporting IP datagrams over a point-to-point link.
TCP/IP/UDP
    Foundation Protocols for TCP/IP protocol suite
Object Exchange Protocol (OBEX)
    Session-layer protocol for the exchange of objects, providing a model for object and operation representation
Wireless Application Environment/Wireless Application Protocol (WAE/WAP)
    WAE specifies an application framework for wireless devices and WAP is an open standard to provide mobile users access to telephony and information services.

Baseband Error Correction

Three types of error correction are implemented in Bluetooth systems,

- 1/3 rate forward error correction (FEC)
- 2/3 rate FEC
- Automatic repeat-request (ARQ)

Setting up connections

Any Bluetooth device in *discoverable mode* will transmit the following information on demand:

- Device name
- Device class
- List of services
- Technical information (for example: device features, manufacturer, Bluetooth specification used, clock offset)

Any device may perform an inquiry to find other devices to connect to, and any device can be configured to respond to such inquiries. However, if the device trying to connect knows the address of the device, it always responds to direct connection requests and transmits the information shown in the list above if requested. Use of a device's services may require pairing or acceptance by its owner, but the connection itself can be initiated by any device and held until it goes out of range. Some devices can be connected to only one device at a time, and connecting to them prevents them from connecting to other devices and appearing in inquiries until they disconnect from the other device.

Every device has a unique 48-bit address. However, these addresses are generally not shown in inquiries. Instead, friendly Bluetooth names are used, which can be set by the user. This name appears when another user scans for devices and in lists of paired devices.

Most phones have the Bluetooth name set to the manufacturer and model of the phone by default. Most phones and laptops show only the Bluetooth names and special programs are required to get additional information about remote devices. This can be confusing as, for example, there could be several phones in range named T610.

Pairing

Motivation

Many of the services offered over Bluetooth can expose private data or allow the connecting party to control the Bluetooth device. For security reasons it is therefore necessary to control which devices are allowed to connect to a given Bluetooth device. At the same time, it is useful for Bluetooth devices to automatically establish a connection without user intervention as soon as they are in range.

To resolve this conflict, Bluetooth uses a process called *pairing*, which is generally manually started by a device user—making that device's Bluetooth link visible to other devices. Two devices need to be *paired* to communicate with each other; the pairing process is typically triggered automatically the first time a device receives a connection request from a device with which it is not yet paired. Once a pairing has been established it is remembered by the devices, which can then connect to each without user intervention. When desired, the pairing relationship can later be removed by the user.

Implementation

During the pairing process, the two devices involved establish a relationship by creating a shared secret known as a *link key*. If a link key is stored by both devices they are said to be *paired* or *bonded*. A device that wants to communicate only with a bonded device can cryptographically authenticate the identity of the other device, and so be sure that it is the same device it previously paired with. Once a link key has been generated, an authenticated ACL link between the devices may be encrypted so that the data that they exchange over the airwaves is protected against eavesdropping.

Link keys can be deleted at any time by either device. If done by either device this will implicitly remove the bonding between the devices; so it is possible for one of the devices to have a link key stored but not be aware that it is no longer bonded to the device associated with the given link key.

Bluetooth services generally require either encryption or authentication, and as such require pairing before they allow a remote device to use the given service. Some services, such as the Object Push Profile, elect not to explicitly require authentication or encryption so that pairing does not interfere with the user experience associated with the service use-cases.

Pairing mechanisms

Pairing mechanisms have changed significantly with the introduction of Secure Simple Pairing in Bluetooth v2.1. The following summarizes the pairing mechanisms:

- **Legacy pairing**: This is the only method available in Bluetooth v2.0 and before. Each device must enter a PIN code; pairing is only successful if both devices enter the same PIN code. Any 16-byte UTF-8 string may be used as a PIN code, however not all devices may be capable of entering all possible PIN codes.
    - **Limited input devices**: The obvious example of this class of device is a Bluetooth Hands-free headset, which generally have few inputs. These devices usually have a *fixed PIN*, for example "0000" or "1234", that are hard-coded into the device.
    - **Numeric input devices**: Mobile phones are classic examples of these devices. They allow a user to enter a numeric value up to 16 digits in length.
    - **Alpha-numeric input devices**: PCs and smartphones are examples of these devices. They allow a user to enter full UTF-8 text as a PIN code. If pairing with a less capable device the user needs to be aware of the input limitations on the other device, there is no mechanism available for a capable device to determine how it should limit the available input a user may use.
- **Secure Simple Pairing** (SSP): This is required by Bluetooth v2.1. A Bluetooth v2.1 device may only use legacy pairing to interoperate with a v2.0 or earlier device. Secure Simple Pairing uses a form of public key cryptography, and has the following modes of operation:
    - **Just works**: As implied by the name, this method just works. No user interaction is required; however, a device may prompt the user to confirm the pairing process. This method is typically used by headsets with very limited IO capabilities, and is more secure than the fixed PIN mechanism which is typically used for legacy pairing by this set of limited devices. This method provides no man in the middle (MITM) protection.
    - **Numeric comparison**: If both devices have a display and at least one can accept a binary Yes/No user input, they may use Numeric Comparison. This method displays a 6-digit numeric code on each device. The user

    should compare the numbers to ensure they are identical. If the comparison succeeds, the user(s) should confirm pairing on the device(s) that can accept an input. This method provides MITM protection, assuming the user confirms on both devices and actually performs the comparison properly.
    - **Passkey Entry**: This method may be used between a device with a display and a device with numeric keypad entry (such as a keyboard), or two devices with numeric keypad entry. In the first case, the display is used to show a 6-digit numeric code to the user, who then enters the code on the keypad. In the second case, the user of each device enters the same 6-digit number. Both cases provide MITM protection.
    - **Out of band** (OOB): This method uses an external means of communication, such as Near Field Communication (NFC) to exchange some information used in the pairing process. Pairing is completed using the Bluetooth radio, but requires information from the OOB mechanism. This provides only the level of MITM protection that is present in the OOB mechanism.

SSP is considered simple for the following reasons:

- In most cases, it does not require a user to generate a passkey.
- For use-cases not requiring MITM protection, user interaction has been eliminated.
- For *numeric comparison*, MITM protection can be achieved with a simple equality comparison by the user.
- Using OOB with NFC will enable pairing when devices simply get close, rather than requiring a lengthy discovery process.

Security Concerns

Prior to Bluetooth v2.1, encryption is not required and can be turned off at any time. Moreover, the encryption key is only good for approximately 23.5 hours; using a single encryption key longer than this time allows simple XOR attacks to retrieve the encryption key.

- Turning off encryption is required for several normal operations, so it is problematic to detect if encryption is disabled for a valid reason or for a security attack.
- Bluetooth v2.1 addresses this in the following ways:
    - Encryption is required for all non-SDP (Service Discovery Protocol) connections
    - A new Encryption Pause and Resume feature is used for all normal operations requiring encryption to be disabled. This enables easy identification of normal operation from security attacks.
    - The encryption key is required to be refreshed before it expires.

Link keys may be stored on the device file system, not on the Bluetooth chip itself. Many Bluetooth chip manufacturers allow link keys to be stored on the device; however, if the device is removable this means that the link key will move with the device.

Air interface

The protocol operates in the license-free ISM band at 2.402-2.480 GHz. To avoid interfering with other protocols that use the 2.45 GHz band, the Bluetooth protocol divides the band into 79 channels (each 1 MHz wide) and changes channels up to 1600 times per second. Implementations with versions 1.1 and 1.2 reach speeds of 723.1 kbit/s. Version 2.0 implementations feature Bluetooth Enhanced Data Rate (EDR) and reach 2.1 Mbit/s. Technically, version 2.0 devices have a higher power consumption, but the three times faster rate reduces the transmission times, effectively reducing power consumption to half that of 1.x devices (assuming equal traffic load).

Security

Overview

Bluetooth implements confidentiality, authentication and key derivation with custom algorithms based on the SAFER+ block cipher. Bluetooth key generation is generally based on a Bluetooth PIN, which must be entered into both devices. This procedure might be modified if one of the devices has a fixed PIN (e.g., for headsets or similar devices with a restricted user interface). During pairing, an initialization key or master key is generated, using the E22 algorithm. The E0 stream cipher is used for encrypting packets, granting confidentiality and is based on a shared cryptographic secret, namely a previously generated link key or master key. Those keys, used for subsequent encryption of data sent via the air interface, rely on the Bluetooth PIN, which has been entered into one or both devices.

An overview of Bluetooth vulnerabilities exploits was published in 2007 by Andreas Becker.

In September 2008, the National Institute of Standards and Technology (NIST) published a Guide to Bluetooth Security that will serve as reference to organizations on the security capabilities of Bluetooth and steps for securing Bluetooth technologies effectively. While Bluetooth has its benefits, it is susceptible to denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. Users/organizations must evaluate their acceptable level of risk and incorporate security into the lifecycle of Bluetooth devices. To help mitigate risks, included in the NIST document are security checklists with guidelines and recommendations for creating and maintaining secure Bluetooth piconets, headsets, and smart card readers.

Bluetooth v2.1 - finalized in 2007 with consumer devices first appearing in 2009 - makes significant changes to Bluetooth's security, including pairing.

Bluejacking

Bluejacking is the sending of either a picture or a message from one user to an unsuspecting user through *Bluetooth* wireless technology. Common applications include short messages (e.g., "You’ve just been bluejacked!"). Bluejacking does not involve the removal or alteration of any data from the device. Bluejacking can also involve taking control of a mobile wirelessly and phoning a premium rate line, owned by the bluejacker.

History of security concerns

Early

In 2001, Jakobsson and Wetzel from Bell Laboratories discovered flaws in the Bluetooth pairing protocol and also pointed to vulnerabilities in the encryption scheme. In 2003, Ben and Adam Laurie from A.L. Digital Ltd. discovered that serious flaws in some poor implementations of Bluetooth security may lead to disclosure of personal data. In a subsequent experiment, Martin Herfurt from the trifinite.group was able to do a field-trial at the CeBIT fairgrounds, showing the importance of the problem to the world. A new attack called BlueBug was used for this experiment. In 2004 the first purported virus using Bluetooth to spread itself among mobile phones appeared on the Symbian OS. The virus was first described by Kaspersky Lab and requires users to confirm the installation of unknown software before it can propagate. The virus was written as a proof-of-concept by a group of virus writers known as "29A" and sent to anti-virus groups. Thus, it should be regarded as a potential (but not real) security threat to Bluetooth technology or Symbian OS since the virus has never spread outside of this system. In August 2004, a world-record-setting experiment showed that the range of Class 2 Bluetooth radios could be extended to 1.78 km (1.08 mile) with directional antennas and signal amplifiers. This poses a potential security threat because it enables attackers to access vulnerable Bluetooth devices from a distance beyond expectation. The attacker must also be able to receive information from the victim to set up a connection. No attack can be made against a Bluetooth device unless the attacker knows its Bluetooth address and which channels to transmit on.

2005

In January 2005, a mobile malware worm known as Lasco.A began targeting mobile phones using Symbian OS (Series 60 platform) using Bluetooth enabled devices to replicate itself and spread to other devices. The worm is self-installing and begins once the mobile user approves the transfer of the file (velasco.sis) from another device. Once installed, the worm begins looking for other Bluetooth enabled devices to infect. Additionally, the worm infects other .SIS files on the device, allowing replication to another device through use of removable media (Secure Digital, Compact Flash, etc.). The worm can render the mobile device unstable.

In April 2005, Cambridge University security researchers published results of their actual implementation of passive attacks against the PIN-based pairing between commercial

Bluetooth devices, confirming the attacks to be practicably fast and the Bluetooth symmetric key establishment method to be vulnerable. To rectify this vulnerability, they carried out an implementation which showed that stronger, asymmetric key establishment is feasible for certain classes of devices, such as mobile phones.

In June 2005, Yaniv Shaked and Avishai Wool published a paper describing both passive and active methods for obtaining the PIN for a Bluetooth link. The passive attack allows a suitably equipped attacker to eavesdrop on communications and spoof, if the attacker was present at the time of initial pairing. The active method makes use of a specially constructed message that must be inserted at a specific point in the protocol, to make the master and slave repeat the pairing process. After that, the first method can be used to crack the PIN. This attack's major weakness is that it requires the user of the devices under attack to re-enter the PIN during the attack when the device prompts them to. Also, this active attack probably requires custom hardware, since most commercially available Bluetooth devices are not capable of the timing necessary.

In August 2005, police in Cambridgeshire, England, issued warnings about thieves using Bluetooth enabled phones to track other devices left in cars. Police are advising users to ensure that any mobile networking connections are de-activated if laptops and other devices are left in this way.

2006

In April 2006, researchers from Secure Network and F-Secure published a report that warns of the large number of devices left in a visible state, and issued statistics on the spread of various Bluetooth services and the ease of spread of an eventual Bluetooth worm.

2007

In October 2007, at the Luxemburgish Hack.lu Security Conference, Kevin Finistere and Thierry Zoller demonstrated and released a remote root shell via Bluetooth on Mac OS X v10.3.9 and v10.4. They also demonstrated the first Bluetooth PIN and Linkkeys cracker, which is based on the research of Wool and Shaked.

Health concerns

Bluetooth uses the microwave radio frequency spectrum in the 2.402 GHz to 2.480 GHz range. Maximum power output from a Bluetooth radio is 100 mW, 2.5 mW, and 1 mW for Class 1, Class 2, and Class 3 devices respectively, which puts Class 1 at roughly the same level as mobile phones, and the other two classes much lower. Accordingly, Class 2 and Class 3 Bluetooth devices are considered less of a potential hazard than mobile phones, and Class 1 may be comparable to that of mobile phones : the maximum for a Class 1 is 100 mW for Bluetooth but 250 mW for UMTS W-CDMA, 1 W for GSM1800/1900 and 2 W for GSM850/900 for instance.

Bluetooth Innovation World Cup marketing initiative

The *Bluetooth* Innovation World Cup is an international competition encouraging the development of new innovations and ideas for applications leveraging the *Bluetooth* low energy wireless technology in sports, fitness and health care products. The *Bluetooth* Innovation World Cup is a marketing initiative of the Bluetooth Special Interest Group (SIG).

The aim of the competition is to stimulate new markets, creating new fields of applications and establishing Bluetooth low energy technology as the wireless data transfer standard for low energy applications is ordinary business in the competition of wireless standards. The initiative will go on for three years, having started 1 June 2009.

***Bluetooth* Innovation World Cup 2009**

The first international *Bluetooth* Innovation World Cup 2009 drew more than 250 international entries illustrating the abundance of opportunities for product development with the new *Bluetooth* low energy wireless technology.

The *Bluetooth* Innovation World Cup 2009 was sponsored by Nokia, Freescale Semiconductor, Texas Instruments, Nordic Semiconductor, STMicroelectronics and Brunel.

***Bluetooth* Innovator of the Year 2009**

On February 8, 2010, the Bluetooth SIG has awarded Edward Sazonov, Physical Activity Innovations LLC, the title of *Bluetooth* Innovator of the Year for 2009. Sazonov received this recognition at the official award ceremony held in-line with the Wearable Technologies Show at ispo 2010, the world’s largest trade show for sporting goods. The award includes a cash prize of €5,000 and a *Bluetooth* Qualification Program voucher (QDID) valued at up to US$ 10,000. Sazonov’s winning idea, The Fit Companion, is a small, unobtrusive sensor that when clipped-on to a user’s clothing or integrated in to a shoe, provides feedback about their physical activity. The data, transmitted via Bluetooth low energy technology, can help individuals to lose weight and achieve optimal physical activity. Intended for use in both training and daily activities like walking or performing chores, this simple, measuring device may offer a solution for reducing obesity.

***Bluetooth* Innovation World Cup 2010**

The Bluetooth Special Interest Group (SIG) announced the start of the second *Bluetooth* Innovation World Cup (IWC) on 1 June 2010. The 2010 *Bluetooth* Innovation World Cup has a focus on applications for the sports & fitness, health care and home information and control markets. The competition will close for registrations on September 15, 2010.

Chapter 3

Bluetooth Low Energy and Body Area Network

Bluetooth low energy

Bluetooth low energy (BLE) is a feature of Bluetooth 4.0 wireless radio technology, aimed at new, principally low-power and low-latency, applications for wireless devices within a short range (10 meters / 30 ft). This facilitates a wide range of applications and smaller form factor devices in the healthcare, fitness, security and home entertainment industries.

Lower power consumption

Devices using Bluetooth low energy wireless technology will consume a fraction of the power of other Bluetooth enabled products. In many cases, products will be able to operate more than a year on a button cell battery without recharging. In this way it will be possible to have, for example, small sensors operating continuously, (think of a temperature sensor) communicating with other devices, like a cellphone or a PDA. This may increase the concerns for privacy, as when the remote, low power, continuously on, sensor would be presence sensors or similar devices.

Some chip manufacturers do not disclose instantaneous power consumption data on data sheets. This specification item depends on the operational duty cycles. Therefore the authentic data may be obtained just with experimental board set-ups and respective firmware test environment. Respective test environment specification to normalize and directly compare the offered alternatives are not available (2008-10-19).

Bluetooth *vs* NFC

	Bluetooth V2.1	**BLE**	**NFC**
RFID mode	active	active	ISO 18000-3
Standardisation body	Bluetooth SIG	Bluetooth SIG	ISO/IEC
Network Standard	IEEE 802.15.1	IEEE 802.15.1	ISO 13157 etc.
Network Type	WPAN	WPAN	Point-to-point

Cryptography	available	available	not with RFID
Range	~30 m (class 2)	~50 m	< 0.2 m
Frequency	2.4-2.5 GHz	2.4-2.5 GHz	13.56 MHz
Bit rate	2.1 Mbit/s	~200 kbit/s	424 kbit/s
Set-up time	< 6 s	< 3 ms	< 0.1 s
Power consumption	varies with class	< 15 mA (xmit)	> 15mA (read)

Bluetooth and Near Field Communication (NFC) may be used both as short-range communication technologies. Integration with mobile phones is increasing, where Bluetooth is part of almost all phone types. To avoid the complicated configuration process, Bluetooth V4.0 low energy protocol has been added to scope of standard.

The former deficiency of Bluetooth behind NFC with set-up time has been compensated with much faster new Bluetooth low energy protocol stack.

There is no aim to make Bluetooth in the WPAN concept compatible with passive RFID. However Bluetooth defines a well standardized new class of active RFID which requires comparably lesser power than NFC in passive read mode.

History

In 2001, Nokia researchers determined that there were various scenarios that contemporary wireless technologies did not address. To address the problem, the Nokia Research Center started the development of a wireless technology adapted from the Bluetooth standard which would provide lower power usage and price while minimizing difference between Bluetooth and the new technology. The results were published in 2004 using the name Bluetooth Low End Extension. After further development with partners, e.g., within EU FP6 project MIMOSA, the technology was released to public in October 2006 with brand name Wibree. After negotiations with Bluetooth SIG members, in June 2007, an agreement was reached to include Wibree in future Bluetooth specification as a Bluetooth ultra-low-power technology, now known as Bluetooth low energy technology.

In December 2009, the Bluetooth SIG announced the adoption of Bluetooth low energy wireless technology as the hallmark feature of the Bluetooth Core Specification Version 4.0. Samples of sensors utilizing this specification are available from some silicon manufacturers today and shipments are anticipated to follow closely behind.

Integration of Bluetooth low energy technology with the Core Specification will be completed in early 2010 and the first Bluetooth low energy enabled products should be available before the end of the calendar year. Upon completion, mobile phone and PC manufacturers may enhance their Bluetooth product offerings with support for Bluetooth low energy wireless technology. End-user devices with Bluetooth v 4.0 are expected to reach the market in late 2010 or early 2011.

Actual status

The Bluetooth low energy specification is available to the general public as part of Bluetooth Core Specification Version 4.0. Actual stage of specification includes some optional features. No commonly published document currently discloses which of these options will be included in the decided chip implementations.

The Wibree technology was announced on 3 October 2006 by Nokia. Partners that currently license the technology and cooperate in defining the specification are Alpwise, Broadcom Corporation, CSR, Epson, Nordic Semiconductor, and Texas Instruments. Other contributors are Suunto and Taiyo Yuden.

The first Bluetooth low energy single-mode chip solutions were released to mass-market in October 2010, with more chips expected to follow in Q1-2011.

The first consumer products using Bluetooth low energy is expected to debut in first half of 2011.

Market demand

Bluetooth V2.1 watch, fitted with a phone vibrating alert for discreet notification

The Bluetooth SIG follows the market demand for low energy consumption respectively lesser battery wear out. This 2007 Bluetooth SIG adoption move for the 2001 Nokia 'Wibree' proposal was necessary to include low battery consumption operational modes for newly designed devices to communicate with other Bluetooth devices yet deployed. However, the compatibility depends on applications that run on existing Bluetooth devices and made capable for digesting the respective low energy transmissions with software updates. In addition to creating a market for sensors, watches and other existing devices, Bluetooth low energy's ability to connect low power devices to mobile phones offers a great variety of new applications. Comparable solutions with other industry standards (e.g. *ZigBee*) or international standards (e.g. IEEE 805.15.4) show the path.

The new protocol stack is being referred to as *Bluetooth low energy*. Nokia did apparently not offer the *WiBree* brand for common use . The *Bluetooth low energy* attribute prevents from impressions, that *Bluetooth ultra low power* might coincide with any type of deficiencies in functional power, transmission reach or transmission rate. However, the Bluetooth low energy chips will offer a well defined set of capabilities that do not replace or supersede the existing Bluetooth v2.x standards.

Technical details

BLE operates in the same spectrum range (2402-2480 MHz) as classic bluetooth, but uses a different set of channels. Instead of BT's 79 1 MHz wide channels, BLE has 40 2 MHz wide channels.

Bluetooth low energy is designed with two equally important implementation alternatives: single-mode and dual-mode. Small devices like tokens, watches and sports sensors based on a single-mode Bluetooth low energy implementation will enjoy the low-power consumption advantages enabled for highly integrated and compact devices. In dual-mode implementations Bluetooth low energy functionality is integrated into Classic Bluetooth circuitry. The architecture will share Classic Bluetooth technology radio and antenna, enhancing currently chips with the new low energy stack—enhancing the development of Classic Bluetooth devices with new capabilities.

Technical Specification	Classic Bluetooth	Bluetooth low energy
Distance/Range	100 m (330 ft)	200 m (660 ft)
Over the air data rate	1-3 Mb/s	1 Mb/s
Application throughput	0.7-2.1 Mb/s	0.26 Mb/s
Active slaves	7	Not defined; implementation dependent
Security	64/128-bit and application layer user defined	128-bit AES with Counter Mode CBC-MAC and application layer user

		defined
Robustness	Adaptive fast frequency hopping, FEC, fast ACK	Adaptive frequency hopping, Lazy Acknowledgement, 24-bit CRC, 32-bit Message Integrity Check
Latency (from a non connected state)	Typically 100 ms	6 ms
Total time to send data (det.battery life)	100 ms	6 ms
Voice capable	Yes	No
Network topology	Scatternet	Star-bus
Power consumption	1 as the reference	0.01 to 0.5 (depending on use case)
Peak current consumption	<30 mA	<20 mA (max 15 mA to run on coin cell battery)
Service discovery	Yes	Yes
Profile concept	Yes	Yes
Primary use cases	Mobile phones, gaming, headsets, stereo audio streaming, automotive, PCs, security, proximity, healthcare, sports & fitness, etc.	Mobile phones, gaming, PCs, watches, sports and fitness, healthcare, security & proximity, automotive, home electronics, automation, Industrial, etc.

More technical details may be obtained from official specification as published by the Bluetooth SIG. Note that power consumption is not part of the Bluetooth spec.

Compatibility

While Bluetooth low energy will be able to coexist with classic Bluetooth devices, it will *not* be able to communicate with them. Therefore, Bluetooth low energy is *not* backward compatible with classic Bluetooth devices, but it will be compatible with newer dual-mode devices. For example, for a mobile phone to be able to communicate with Bluetooth low energy devices in addition to classic Bluetooth devices such as Bluetooth headsets, a dual-mode chip is required. Classic Bluetooth hardware *cannot* be upgraded to dual-mode or low energy compatibility via a software upgrade.

Application profiles

Currently there are no application profiles commonly published. The specification of such profiles has to be expected prior to commonly available appliances.

Health care profiles

Main focus in health care with BLE is vital monitoring. The promoter of such applications is Continua Health Alliance as an industrial standardisation body.

Sporting profiles

Main focus in sports with BLE is locating as well as vital monitoring. The promoter of such applications is Bluetooth Special Interest Group (SIG) as an industrial standardisation body as well as Continua Health Alliance.

Use cases

Bluetooth low energy is the hallmark feature of v4.0 of the Bluetooth Core Specification. This enhancement to the Bluetooth wireless technology Core Specification that will enable new functionality and applications for remote controls, healthcare monitors, sports sensors and other devices. Bluetooth low energy will enhance existing use cases and will enable new ones, widening the applicability and functionality of Bluetooth.

The respective chips may be integrated into products such as tokens, watches, manual controls, wireless keyboards, gaming pads and body sensors, which may then connect to host devices such as mobile phones, personal digital assistants (PDAs) and personal computers (PCs).

However, currently in the tenth year after earliest publication with inventor Nokia in 2001 (Wibree) there is no implementing on chip-basis or on protocol-basis to any of the current PC-like or PDA-like products or with any mobile phones nor any of the announced appliance products neither disclosed nor announced. All announcement but one is recognised still just with Bluetooth SIG and not beyond (2010-01-27). The notified exception is with a wireless velo-odometer, probably not recognised as the *killer-application* with mobilephones.

Bluetooth low energy technology hence may extend any personal area network according to the intentions with IEEE 802.15 WPAN to include watches and toys, sports and health care equipment, human interface (HIDs) and entertainment devices.

Software updates

The respective applications with existing and deployed devices may be opened to Bluetooth low energy by updates. This will enable the Bluetooth software defined radio to receive signals from Bluetooth low energy devices. However, the capability to communicate in duplex mode is limited with the defined frequency allocation schemes for traditional Bluetooth. The common appliances such as mobile phones, personal digital assistants (PDAs) and personal computers (PCs) may then receive as host devices for complex applications the signals transmitted from Bluetooth low energy devices.

Bluetooth low energy technology hence may extend any personal area network according to the intentions with IEEE 802.15 (WPAN) to network personally carried simple devices with other appliances for complex local applications as well as for gateway support to transfer information to other networked entities.

Standardization

In the market of proprietary connectivity solutions, Bluetooth low energy technology differentiates itself through its:

- widely adopted industry standard for protocols (Bluetooth SIG)
- internationally adopted industry standard for transmission (IEEE 802.15.1)
- Low price through single chip integration
- Compatibility with yet deployed Bluetooth devices via updates

Body Area Network

A **Body Area Network (BAN)**, **Wireless Body Area Network (WBAN)** or **Body sensor network (BSN)** are terms used to describe the application of wearable computing devices . This will enable wireless communication between several miniaturized Body Sensor Units (BSU) and a single Body Central Unit (BCU) worn at the human body.

Concept

The rapid growth in physiological sensors, low power integrated circuits and wireless communication has enabled a new generation of wireless sensor networks. These wireless sensor networks are used to monitor traffic, crops, infrastructure and health. The Body Area Network field is an interdisciplinary area which could allow inexpensive and continuous health monitoring with real-time updates of medical records via Internet. A number of intelligent physiological sensors can be integrated into a wearable wireless body area network, which can be used for computer assisted rehabilitation or early detection of medical conditions. This area relies on the feasibility of implanting very small bio-sensors inside the human body that are comfortable and that don't impair normal activities. The implanted sensors in the human body will collect various physiological changes in order to monitor the patient's health status no matter their location. The information will be transmitted wirelessly to an external processing unit. This device will instantly transmit all information in real time to the doctors throughout the world. If an emergency is detected, the physicians will immediately inform the patient through the computer system by sending appropriate messages or alarms. Currently the level of information provided and energy resources capable of powering the sensors are limiting. While the technology is still in its primitive stage it is being widely researched and once adopted, is expected to be a breakthrough invention in healthcare, leading to concepts like telemedicine and mHealth becoming real.

Applications

Initial applications of BANs are expected to appear primarily in the healthcare domain, especially for continuous monitoring and logging vital parameters of patients suffering from chronic diseases such as diabetes, asthma and heart attacks.

- A BAN network in place on a patient can alert the hospital, even before he has a heart attack, through measuring changes in his vital signs.
- A BAN network on a diabetic patient could auto inject insulin though a pump, as soon as his insulin level declines, thus making the patient ‘doctor-free’ and virtually healthy.

Other applications of this technology include sports, military, or security. Extending the technology to new areas could also assist communication by seamless exchanges of information between individuals, or between individual and machines.

Components

A typical BAN or BSN requires vital sign monitoring sensors, motion detectors (through accelerometers) to help identify the location of the monitored individual and some form of communication, to transmit vital sign and motion readings to medical practitioners or care givers. A typical Body Area Network kit will consist of sensors, a Processor, a transceiver and a battery. Physiological sensors, such as ECG and SpO2 sensors, have been developed. Other sensors such as a blood pressure sensor, EEG sensor and a PDA for BSN interface are under development..

Challenges

Problems with the use of this technology could include:

- **Interoperability**: WBAN systems would have to ensure seamless data transfer across standards such as Bluetooth, ZigBee etc. to promote information exchange, plug and play device interaction. Further, the systems would have to be scalable, ensure efficient migration across networks and offer uninterrupted connectivity.
- **System Devices**: The sensors used in WBAN would have to be low on complexity, small in form factor, light in weight, power efficient, easy to use and reconfigurable. Further, the storage devices need to facilitate remote storage and viewing of patient data as well as access to external processing and analysis tools via the Internet.
- **System and device-level security**: Considerable effort would be required to make BAN transmission secure and accurate. It would have to be made sure that the patient’s data is only derived from each patient’s dedicated BAN system and is

not mixed up with other patient's data. Further, the data generated from WBAN should have secure and limited access.

- **Invasion of privacy**: People might consider the WBAN technology as a potential threat to freedom, if the applications go beyond 'secure' medical usage. Social acceptance would be key to this technology finding a wider application.
- **Sensor validation**: Pervasive sensing devices are subject to inherent communication and hardware constraints including unreliable wired/wireless network links, interference and limited power reserves. This may result in erroneous datasets being transmitted back to the end user. It is of the utmost importance especially within a healthcare domain that all sensor readings are validated. This helps to reduce false alarm generation and to identify possible weaknesses within the hardware and software design.
- **Data consistency**: Data residing on multiple mobile devices and wireless patient motes need to be collected and analysed in a seamless fashion. Within Body Area Networks, vital patient datasets may be fragmented over a number of nodes and across a number of networked PCs or Laptops. If a medical practitioner's mobile device does not contain all known information then the quality of patient care may degrade.
- **Interference**: The wireless link used for body sensors should reduce the interference and increase the coexistence of sensor node devices with other network devices available in the environment. This is especially important for large scale implementation of WBAN systems.

Chapter 4

Wireless Access Point and ExOR (Wireless Network Protocol)

Wireless access point

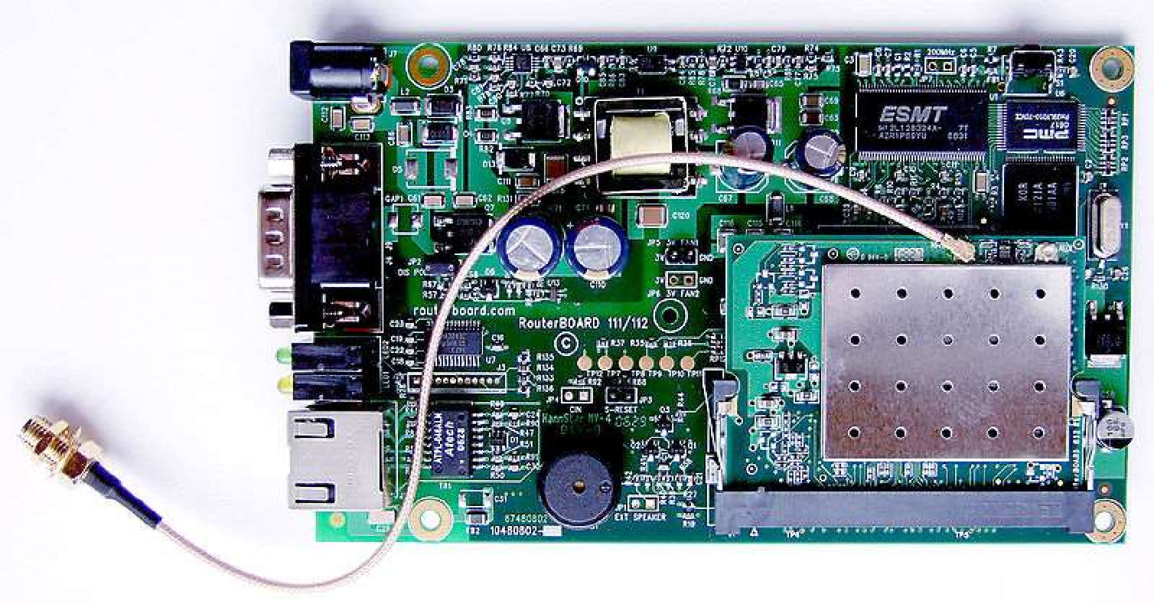
Industrial Wireless Access Point

In computer networking, a **wireless access point** (WAP) is a device that 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 home consumer models, industrial wireless access points can also be used 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 advent 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 Hot Spot 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 Hot Spots 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 without the need of wired networks.

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 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.

ExOR (wireless network protocol)

Extremely Opportunistic Routing (ExOR) is a combination of routing protocol and media access control for a wireless ad-hoc network, invented by Sanjit Biswas and Robert Morris of the MIT Artificial Intelligence Laboratory, and described in a 2005 Paper. Previously open source, , ExOR was available in 2005 but is no longer obtainable. The broadcast and retransmission strategies used by the algorithm were already described in the literature. ExOR is valuable because it can operate available digital radios to use some previously impractical algorithmic optimizations.

History

The algorithm is designed to convey packets of the Internet Protocol, so that it enables the maximum number of other services. At the time of invention, digital radios had widely replaced wireline internet services for portable devices. Specialized integrated circuits were widely available at low costs.

MIT at that time (2005) was involved with the One Laptop per Child project, an attempt to make an inexpensive low-power computer to help educate impoverished children. The advantages were thought to be reduced costs for digital copies of books and consumables like paper, with possible pedagogic improvements from the interactivity and flexibility. One of the crucial features of the laptop was to be a wireless ad-hoc network that would permit the laptops to cooperate to provide more resources than an individual computer could afford. A practical but superior network algorithm would directly help educate more children by reducing the cost and power needed by the laptop. A wireless ad-hoc network would cost less and use less power if it used standard radios (i.e. with integrated circuits for 802.11) and transferred more data over larger distances, with fewer intermediate radios.

This protocol was prototyped on RoofNet, and many authorities believe it is the media access protocol deployed by Meraki to wire San Francisco.

The Algorithm

The starting radio, the source, broadcasts a batch of packets. As timers in intermediate radios expire, radios further from the destination retransmit the packets that no closer radio has yet retransmitted.

Most of the complexity is to support this basic scheme. The timers in intermediate radios are set to an estimate of the transmission time that closer radios will need in order to transmit packets. The estimate is calculated based on the number of packets in the batch, and the probabilities of a correct transmission from each intermediate radio.

ExOR uses a conventional routing protocol "RRTc" to collect information about the probability of a successful transmission between each pair of digital radios in the network.

The authors were concerned that retransmitting packets could use up too much of the available radio time. ExOR therefore tries to reduce retransmissions of packets to the minimum possible. This accounts for ExOR's high efficiency.

First, from the routing information, the sending radio constructs a list of radios that might be able to forward data from the sending radio to the destination. The radios' numbers are placed in a list sorted by distance to the destination, from closest to furthest. The destination radio is at the head of the list. Also, the source radio starts a list of the packets in the batch in order to measure packets' progress. This "batch map" is an array of radio numbers, one per packet. Each radio number is the radio that transmitted that packet, and was closest to the destination radio. Each data packet has the list of radios, and packets placed in the front. The list saves space in each packet by using radio numbers rather than IP addresses. Then, the sending radio broadcasts the first batch of data packets. It starts a timer. Radios that receive a packet but are not in the list in the packet ignore the data packets. These radios throw away the packets as soon as the packets are received. Radios that are in the packet's list of radios save the data packets that they receive. They also update their batch map. When a radio times out, it transmits the packets that no radio closer to the destination has retransmitted. These packets include the radio's best available information about the progress of the packets in the batch (i.e. its batch map). In particular, each packet's batch map contains the retransmitter's radio number for each packet that it retransmits. When a radio receives a packet sent from a radio that is closer to the destination, it erases its own copy of that packet. There's no need for it to retransmit that packet. However, it also updates its batch map about the progress of the packets in the batch. In this way, the information about the progress of the packets flows backward toward the source as radios farther from the destination update their batch maps by eavesdropping on retransmissions.

Since the retransmissions closer to the source radio occur later, the packet progress information flows back to the source radio, even though no acknowledge packets are ever transmitted. At the end, there are usually a few packets that didn't go anywhere. These are sent by the most reliable route, without gambling on unreliable routes.

ExOR is more efficient with large blocks of data. These give more chances for a batch to find alternative routes. However, the batchmaps get larger, too. So, blocks of data more than 100,000 bytes are broken into groups of data packets called batches. Smaller messages are just sent by the most reliable route.

Since the major internet protocol TCP sends a stream of data, ExOR uses local proxy data servers to accumulate blocks of data.

Advantages and Disadvantages

Each packet is retransmitted a minimal number of times, and covers the longest possible distance on each transmission. Some time is wasted by having the receiver broadcast packet information, but this is far less than the normal routing schemes, which can retransmit when an acknowledge message is lost.

There are no acknowledge packets, and no collisions with them. This saves radio time.

The authors say that the protocol is roughly twice as efficient as normal routing protocols with fixed "optimal" routing.

The authors say that the variation in delivery times is 1/4 of other ad-hoc networks, and ascribe this to the algorithm's use of best available delivery times.

The authors arranged the test so that the protocol accumulates large blocks of data for transmission. The data shows a trade-off between the speed of the network's response and the efficiency of the radio system.

Response time in some games might be affected by larger amounts of buffering in high efficiency networks.

Testing

ExOR's efficiency estimates are based on a real implementation with a Linux routing toolkit called click. Experimental versions of the software were both simulated and installed on a rooftop network called "RoofNet" in Cambridge, Mass. This data was compared to published data for a similar network.

Chapter 5

Wireless Grid and Hidden Node Problem

Wireless grid

Wireless grids are wireless computer networks consisting of different types of electronic devices with the ability to share their resources with any other device in the network in an ad-hoc manner. A definition of the wireless grid can be given as: "Ad-hoc, distributed resource-sharing networks between heterogeneous wireless devices" The following key characteristics further clarify this concept:

- No centralized control
- Small, low powered devices
- Heterogeneous applications and interfaces
- New types of resources like cameras, GPS trackers and sensors
- Dynamic and unstable users / resources

The technologies that make up the wireless grid can be divided into two main categories; ad-hoc networking and grid computing.

(Wireless) Ad-hoc networking

In traditional networks, both wired and wireless, the connected devices, or nodes, depend on dedicated devices (edge devices) such as routers and/or servers for facilitating the throughput of information from one node to the other. These 'routing nodes' have the ability to determine where information is coming from and where it is supposed to go. They give out names and addresses (IP addresses) to each connected node and regulate the traffic between them. In wireless grids, such dedicated routing devices are not (always) available and the bandwidth that is permanently available to traditional networks has to be either 'borrowed' from an already existing network or publicly accessible bandwidth (open spectrum) has to be used.

A group addressing this problem is MANET (Mobile Ad-Hoc Network).

Resource sharing

One of the intended aspects of wireless grids is that it will facilitate the sharing of a wide variety of resources. These will include both technical as information resources. The former being bandwidth, QoS, and web services, but also computational power and data storage capacity. Information resources can include virtually any kind of data from databases and membership lists to pictures and directories.

Ad-hoc resource sharing between mobile devices in the wireless grid require for the devices to agree on sharing/communication protocols without the existence of dedicated servers.

Coordination Systems

Coordination Systems are the actual mechanisms that enable the sharing of resources between different devices. For different resources, devices use different coordination systems. Examples of such mechanisms are: SMB or NFS for sharing disk space and the distributed.net client for sharing processor cycles.

Trust Establishment

Before users are willing to share any resource, they demand a certain amount of trust between them and the users and/or systems they share resources with. The amount of trust required depends on the kind of information/resource that is to be shared. Sharing processor cycles requires less substantial trust then the sharing of personal information and commercial information can require another level of trust establishment altogether. There are systems currently in operation that can provide a certain amount of trust like the public key infrastructure that makes use of certificates; now often used in web based email systems, and Kerberos.

Resource discovery

Before any resource on a device in the grid can be utilized, those resources that are available must be discovered; all the devices that make up the grid and the resources they possess have to be identified. When a client enters the grid, such as a PDA, it has to be able to communicate to the other users that it is a PDA and it has a camera, GPS capabilities, a telephone function and various office applications such as a text editor. Protocols like UPnP and ZeroConf can detect a new node in the network when it enters. When detected, other users can send a query to the new device to find out what it has to offer. Commercial service providers can 'advertise' the resources they have to offer through IP multicasts. Within large grids containing thousands of nodes, a kind of 'friend of a friend' mechanism can be used. There is a myriad of standards that include resource description protocols. Standards as IETF's ZeroConf, Microsoft's UPnP, the Grid Resource Description Language (GRDL), the Web Services Description Language (WSDL) for describing various specific web services and parts of QoS that describe bandwidths all offer devices a way to describe and publish their specific resources and needs. There are also various different systems currently available that can gather these resource descriptions and structure them for other devices to use. The OpenGrid Services Architecture (OGSA) uses a Web service-style IndexService. The Web services community has defined UDDI which can makes a database of services that are available on the network, and JXTA uses ZeroConf to identify resources in a network. However, the problem with using these in wireless grids is that no stable publisher of these descriptions may exist.

Resource description

For any device to be able to use any resource, a way to identify and describe the resource has to be agreed on by all available devices. If, for instance, storage capacity is to be shared, it first has to be clear what the capacity of each device is and what the storage need is. As said, there are many techniques to describe certain resources but there is not one technique that is able to provide this service for all resources. The available techniques combined, however, cover most of what is needed.

Grid Computing

Grid computing came into existence as a manner of sharing heavy computational loads among multiple computers to be able to compute highly complex mathematical problems (a good real-world example being the SETI@Home project). However, it developed rapidly into a way of sharing virtually any resource that is available on any machine on the grid. Wired grids are now used to share not only computing power, but also hard disk space, data, and applications. The grid topology is highly flexible and easily scalable, allowing users to join and leave the grid without the hassle of time and resource hungry identification procedures, having to adjust their devices or install additional software on them. The goal of grid computing is described as "to provide flexible, secure and coordinated resource sharing among dynamic collections of individuals, institutions and resources" (McKnight, Howison, 2004).
It is intended to be a dynamic network without geographical, political, or cultural boundaries that offers real-time access to heterogeneous resources and still offer the same characteristics of the traditional distributed networks that are in use everywhere in our houses and offices. These characteristics being stability, scalability, and flexibility as the most important ones. Ian Foster offers a checklist for recognizing a grid.

A grid allows:

- Coordination of resources that are not subject to centralized control
- Use of standard, open, general-purpose protocols and interfaces
- Delivery of nontrivial qualities of service

The Wireless Grid

One of the biggest limitations of the wired grid is that users are forced to be in a fixed location as the devices they use are to be hard wired to the grid at all times. This also has a negative influence on the flexibility and scalability of the grid; devices can only join the grid in locations where the possibility exists to physically connect the device to the grid (i.e. there is the need for a hub or a switch to plug into).

One description of the wireless grid is "an augmentation of a wired grid that facilitates the exchange of information and the interaction between heterogeneous wireless devices" (Argawal, Norman & Gupta, 2004)

Argawal, Norman & Gupta (2004) identify three forces that drive the development of the wireless grid:

New user interaction modalities and form factors
Applications that exist on current wired grids need to be adapted to fit the devices used in wireless grids. These devices are usually hand held and therefore the user interface devices (screens, keyboards (if any)) are significantly smaller and availability of additional input devices like a mouse are limited. This means the traditional graphical interfaces found on PCs are not suitable.

Limited computing resources
Wireless devices do not possess the computing power nor the storage capacity of full size devices like a PC or laptop. Therefore wireless applications need to have access to additional computing resources to be able to offer the same functionality that wired networks do.

Additional new supporting infrastructure elements
In the case of an unforeseen event, there will be the need for major amounts of computational and communications bandwidths. An urban catastrophe, for example, would require a dynamic and adaptive wireless network to alert people within the population as well as those in the various coordination and aid services like the police, army, medical services, and government. Applications to provide for these bandwidths and 'instant' networks need to be addressed.

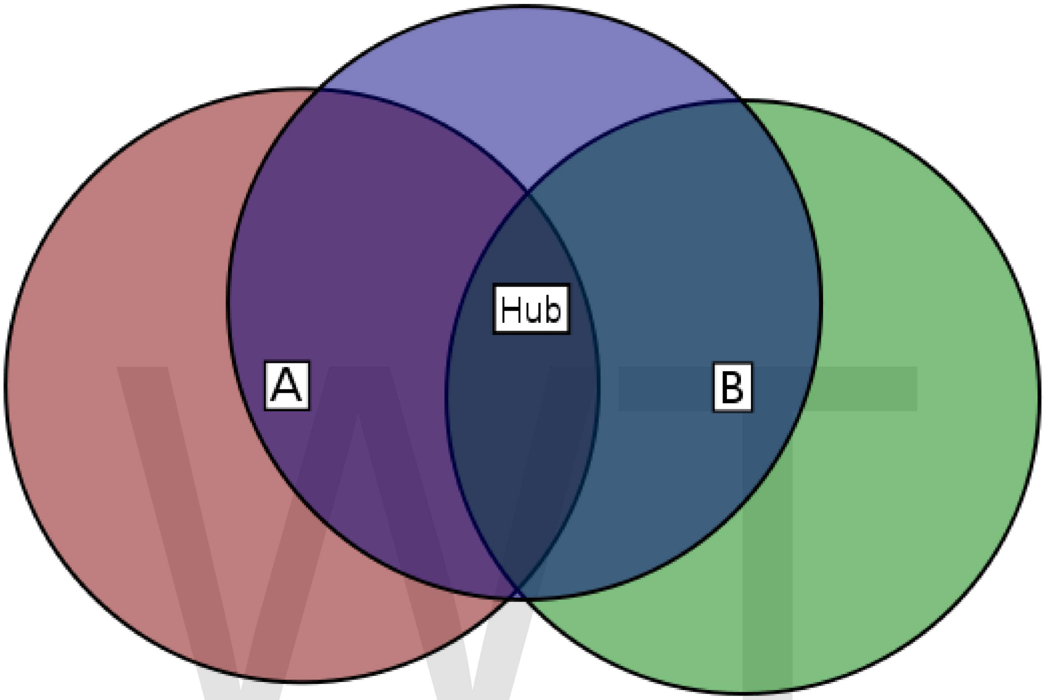
Wireless Grids infrastructure

The infrastructure of the wireless grid consists of three basic levels:

- The physical layer technologies and policies. The physical layer contains the spectrum on which the wireless devices can operate and communicate.
- Network infrastructure
- Middleware to provide communications between heterogeneous devices

Hidden node problem

In wireless networking, the **hidden node problem** or **hidden terminal problem** occurs when a node is visible from a wireless access point (AP), but not from other nodes communicating with said AP. This leads to difficulties in media access control.



In this example, A and B can each communicate with the hub, but are hidden from each other

Background

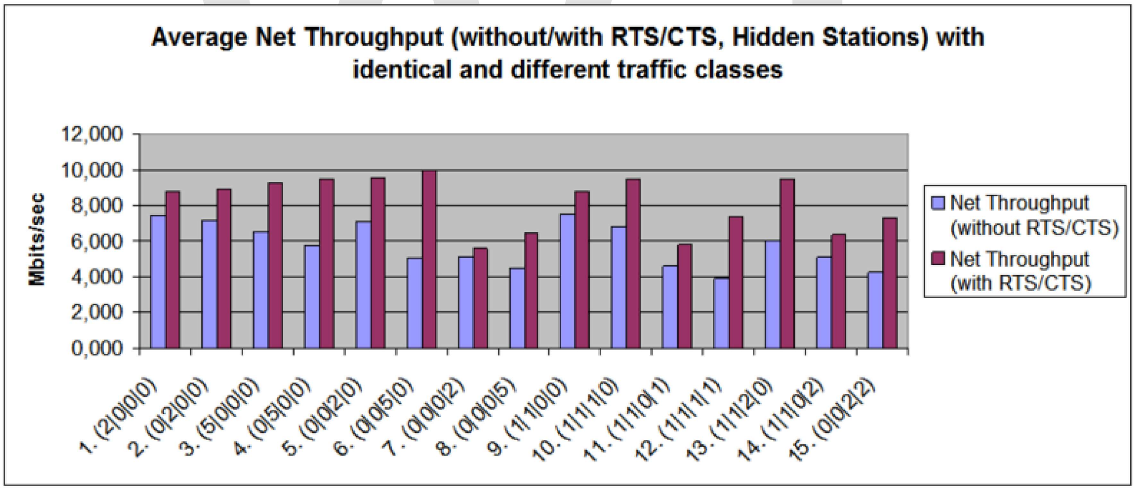
Hidden nodes in a wireless network refer to nodes that are out of range of other nodes or a collection of nodes. Take a physical star topology with an access point with many nodes surrounding it in a circular fashion: Each node is within communication range of the AP, but the nodes cannot communicate with each other, as they do not have a physical connection to each other. In a wireless network, it is likely that the node at the far edge of the access point's range, which is known as **A**, can see the access point, but it is unlikely that the same node can see a node on the opposite end of the access point's range, **B**. These nodes are known as *hidden*. The problem is when nodes **A** and **B** start to send packets simultaneously to the access point. Since node **A** and **B** can not sense the carrier, Carrier sense multiple access with collision avoidance (CSMA/CA) does not work, and collisions occur, scrambling data. To overcome this problem, handshaking is implemented in conjunction with the CSMA/CA scheme. The same problem exists in a MANET.

The hidden node problem can be observed easily in widespread (>50m radius) WLAN setups with many nodes that use directional antennas and have high upload. This is why IEEE 802.11 is suited for bridging the last mile for broadband access only to a very limited extent. Newer standards such as WiMAX assign time slots to individual stations, thus preventing multiple nodes from sending simultaneously and ensuring fairness even in over-subscription scenarios.

IEEE 802.11 uses 802.11 RTS/CTS acknowledgment and handshake packets to partly overcome the **hidden node problem**. RTS/CTS is not a complete solution and may decrease throughput even further, but adaptive acknowledgments from the base station can help too.

The comparison with hidden stations shows that RTS/CTS packages in each traffic class are profitable (even with short audio frames, which cause a high overhead on RTS/CTS frames).

In the experimental environment following traffic classes are included: data (not time critical), data (time critical), video, audio. Examples for notations: (0|0|0|2) means 2 audio stations; (1|1|2|0) means 1 data station (not time critical), 1 data station (time critical), 2 video stations.



Benchmarks: Net Throughput with/without RTS/CTS (Pommer, p.179)

The other methods that can be employed to solve hidden node problem are :

- Increase Transmitting Power From the Nodes
- Use omnidirectional antennas
- Remove obstacles
- Move the node
- Use protocol enhancement software
- Use antenna diversity

Increase Transmitting Power From the Nodes

Increasing the power (measured in milliwatts) of the nodes can solve the hidden node problem by allowing the cell around each node to increase in size, encompassing all of the other nodes. This configuration enables the non-hidden nodes to detect, or hear, the hidden node. If the non-hidden nodes can hear the hidden node, the hidden node is no longer hidden. Because wireless LANs use the CSMA/CA protocol, nodes will wait their turn before communicating with the access point.

Use omnidirectional antennas

Since nodes using directional antennas are nearly invisible to nodes that are not positioned in the direction the antenna is aimed at, directional antennas should be used only for very small networks (e.g., dedicated point-to-point connections). Use omnidirectional antennas for widespread networks consisting of more than two nodes.

Remove obstacles

Increasing the power on mobile nodes may not work if, for example, the reason one node is hidden is that there is a cement or steel wall preventing communication with other nodes. It is doubtful that one would be able to remove such an obstacle, but removal of the obstacle is another method of remedy for the hidden node problem. Keep these types of obstacles in mind when performing a site survey.

Move the node

Another method of solving the hidden node problem is moving the nodes so that they can all hear each other. If it is found that the hidden node problem is the result of a user moving his computer to an area that is hidden from the other wireless nodes, it may be necessary to have that user move again. The alternative to forcing users to move is extending the wireless LAN to add proper coverage to the hidden area, perhaps using additional access points.

Equalizing technology

Equalizing technology, which is completely compatible with 802.11, works by taking advantage of the natural inclination of Internet connections to back off when artificially restrained.

Equalizing constantly (every second) measures the total aggregate bandwidth throughput traversing the AP. If it senses the upper limit is being reached, Equalizing will then isolate the dominating flows and encourage them to back off by artificially restraining them. Thus freeing up the frequency for lesser powered remote nodes.

By keeping track of every flow going through the AP, Equalizing technology can make a determination of which ones are getting an unequal share of bandwidth and thus crowding out flows from weaker nodes.

Equalizing determines detrimental flows from normal ones by taking the following questions into consideration:

1. How persistent is the flow?
2. How many active flows are there?
3. How long has the flow been active?
4. How much total congestion is currently on the trunk?
5. How much bandwidth is the flow using relative to the link size?

The key to making this happen over 802.11 relies on the fact that if you slow a stream down, the application at the root cause will back off and also slow down. This can be done by the deploying equalzing technology after the access point without any changes to the 802.11 protocol since the throttling is actually done independent of the radio. The throttling of heavy streams happens between the AP and the connection to the Internet (or other external source).

Traffic Equalizing technologies are not universally applicable solutions to the hidden node problem. Rather, they are primarily a pragmatic fix to reduce symptoms without fixing the underlying problem.

Use protocol enhancement software

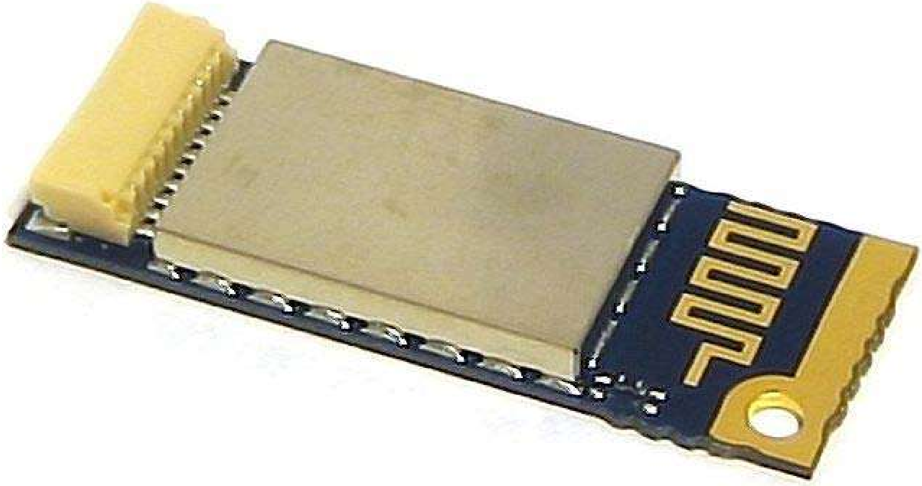
There are several software implementations of additional protocols that essentially implement a polling or token passing strategy. Then, a master (typically the access point) dynamically polls clients for data. Clients are not allowed to send data without the master's invitation. This eliminates the hidden node problem at the cost of increased latency and less maximum throughput.

Chapter 6

Wireless Network Interface Card and Linksys WRT54G Series

Wireless network interface card

A wireless network interface device with a USB interface and internal antenna



Bluetooth card

A **wireless network interface controller** (WNIC) is a network card which connects to a radio-based computer network, unlike a regular network interface controller (NIC) which connects to a wire-based network such as token ring or ethernet. A WNIC, just like a NIC, works on the Layer 1 and Layer 2 of the OSI Model. A WNIC is an essential component for wireless desktop computer. This card uses an antenna to communicate through microwaves. A WNIC in a desktop computer usually is connected using the PCI bus. Other connectivity options are USB and PC card. Integrated WNICs are also available, (typically in Mini PCI/PCI Express Mini Card form).

The term may also apply to a card using protocols other than Wi-Fi, such as one implementing Bluetooth connections.

Modes of operation

A WNIC can operate in two modes known as **infrastructure mode** and **ad hoc mode**.

Infrastructure mode

In an infrastructure mode network the WNIC needs an access point: all data is transferred using the access point as the central hub. All wireless nodes in an infrastructure mode network connect to an access point. All nodes connecting to the access point must have the same service set identifier (SSID) as the access point, and if the access point is enabled with WEP they must have the same WEP key or other authentication parameters.

Ad-hoc mode

In an ad-hoc mode network the WNIC does not require an access point, but rather can directly interface with all other wireless nodes directly. All the nodes in an ad-hoc network must have the same channel and SSID.

Specifications

WNICs are designed around the IEEE 802.11 standard which sets out low-level specifications for how all wireless networks operate. Earlier interface controllers are usually only compatible with earlier variants of the standard, while newer cards support both current and old standards.

Specifications commonly used in marketing materials for WNICs include:

- Wireless data transfer rates (measured in Mbit/s); these range from 2 Mbit/s to 54 Mbit/s.
- Wireless transmit power (measured in dBm)
- Wireless network standards (may include standards such as 802.11b, 802.11g, 802.11n, etc.) 802.11g offers data transfer speeds equivalent to 802.11a – up to 54 Mbit/s – and the wider 300-foot (91 m) range of 802.11b, and is backward compatible with 802.11b.

Most Bluetooth cards do not implement any form of the 802.11 standard.

Range

Wireless range may be substantially affected by objects in the way of the signal and by the quality of the antenna. Large electrical appliances, such as a refrigerators, fuse boxes, metal plumbing, and air conditioning units can impede a wireless network signal. The theoretical maximum range of Wi-Fi is only reached under ideal circumstances and true effective range is typically about half of the theoretical range. Specifically, the maximum throughput speed is only achieved at extremely close range (less than 25 feet (7.6 m) or so); at the outer reaches of a device's effective range, speed may decrease to around 1 Mbit/s before it drops out altogether. The reason is that wireless devices dynamically negotiate the top speed at which they can communicate without dropping too many data packets.

Linksys WRT54G series

Linksys WRT54G version 1.0

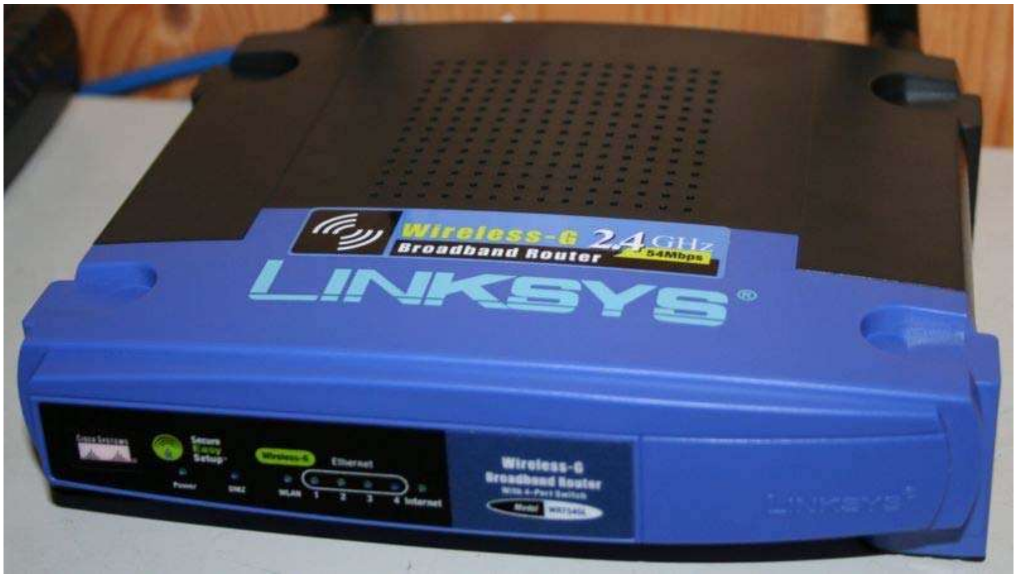
Linksys WRT54G (and variants **WRT54GS**, **WRT54GL**, and **WRTSL54GS**) is a Wi-Fi capable residential gateway from Linksys. The device is capable of sharing Internet connections among several computers via 802.3 Ethernet and 802.11b/g wireless data links.

WRT54G

The original **WRT54G** was first released in December 2002. It comes with a 4+1 port network switch (the Internet/WAN port is also in the same internal network switch, but on a different VLAN). The devices have two removable antennas connected through Reverse Polarity TNC connectors. The WRT54GC router is an exception and has an internal antenna with optional external antenna. As a cost-cutting measure, the design of the latest version of the WRT54G no longer has detachable antennas or TNC connectors. Instead, version 8 routers simply route thin wires into antenna 'shells' eliminating the connector. As a result, Linksys HGA7T and similar external antennas are no longer compatible with this model.

Hardware and revisions

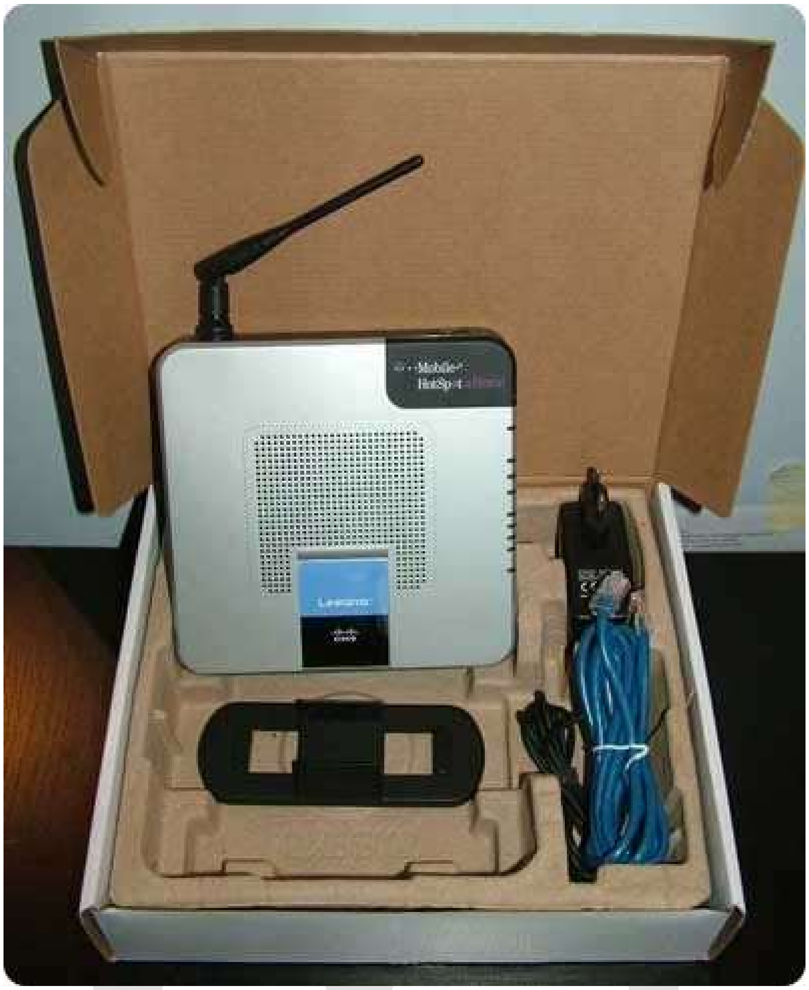
Linksys WRT54GS version 1.1



Linksys WRT54GL version 1.1

WRT54G version 2.0 with upgraded antennas

Linksys WRT54G-TM



Linksys WRT**U**54G-TM

Linksys WRT54GX version 2

Version	CPU	RAM	Flash memory	S/N Prefix	Power	Notes
1.0	Broadcom BCM4702 @ 125 MHz	16 MB	4 MB	CDF0 CDF1	5 V 2 A positive tip	20 front panel LEDs (including link/activity, collision detection and speed rating indicators for each Ethernet port). Wireless capability was provided by a Mini PCI card attached to the router motherboard
1.1	Broadcom BCM4710 @ 125 MHz	16 MB	4 MB	CDF2 CDF3	12 V 1 A	Front panel LEDs reduced to eight (one link/activity LED per port, plus one each for power, wireless, DMZ and WAN/Internet connectivity). Wireless chipset is

						integrated onto motherboard.
2.0	Broadcom BCM4712 @ 200 MHz	16 MB	4 MB	CDF5		Same as 1.1 with a CPU upgrade and greater wireless transmitter integration (fewer transmitter parts). Some of these have 32 MB of RAM but are locked to 16 MB in the firmware (can be unlocked to use all RAM.
2.1	Broadcom BCM4712 @ 216 MHz	16 MB	4 MB	CDF6		Same physical appearance as 1.1 and 2.0 models. Some of these models have 32 MB of RAM installed but have been locked to 16 MB by the manufacturer. Some models have two 16 MB MIRA P2V28S40BTP memory chips.
2.2	Broadcom BCM4712 @ 216 MHz	16 MB	4 MB	CDF7		Same physical appearance as 1.1 and 2.0 models. Switching chipset from ADMtek 6996L to Broadcom BCM5325EKQM. Some of these models have 32 MB of RAM installed but have been locked to 16 MB by the manufacturer. Some models have 16 MB Hynix HY5DU281622ET-J memory chips.
3.0	Broadcom BCM4712 @ 216 MHz	16 MB	4 MB	CDF8		Identical to 1.1 and later models, except for the CPU speed and an undocumented switch behind left front panel intended for use with a feature called "SecureEasySetup".
3.1	Broadcom BCM4712 @ 216 MHz	16 MB	4 MB	CDF9		The Version 3.1 hardware is essentially the same as the Version 3.0 hardware. Adds "SecureEasySetup" button.
4.0	Broadcom BCM5352 @ 200 MHz	16 MB	4 MB	CDFA		Switched to new SoC
5.0	Broadcom BCM5352 @ 200 MHz	8 MB	2 MB	CDFB	12 V 0.5 A	Switched to VxWorks OS and reduced Flash Memory and RAM; not compatible with most 3rd party firmware, although the "VxWorks killer" utility allows some 3rd party open source firmware to be loaded. Since less

					physical RAM is available in this and future models, the 3rd party firmware (popular open source projects) were modified into special "micro" versions.
5.1	Broadcom BCM5352 @ 200 MHz	8 MB	2 MB	CDFC	
5.2	Broadcom BCM5352 @ 200 MHz	8 MB	2 MB	CDFB	
6.0	Broadcom BCM5352 @ 200 MHz	8 MB	2 MB	CDFD	
7.0	Atheros AR2317 @ 240 MHz	8 MB	2 MB	CDFE	Switched to Atheros SoC
7.2	Broadcom BCM5354 @ 240 MHz	8 MB	2 MB	CDFK	Switched back to Broadcom based SoC; Samsung K4S641632K-UC75 (RAM); Samsung K801716UBC PI07 (Flash)
8.0	Broadcom BCM5354 @ 240 MHz	8 MB	2 MB	CDFF CDFG	Some units come with 16 MB of RAM. VxWorks killer works. Antennae cannot be removed.
8.1	Broadcom BCM5354 @ 240 MHz	8 MB	2 MB	MDF0	FCC ID: Q87-WRT54GV81. OS is Linux, no need for VxWorks killer. Antennae cannot be removed.
8.2	Broadcom BCM5354 @ 240 MHz	8 MB	2 MB	CDFJ	FCC ID: Q87-WRT54GV82. VxWorks killer does not work. Antennae cannot be removed.

WRT54GS

The **WRT54GS** is nearly identical to WRT54G except for additional RAM, flash memory, and SpeedBooster software. Versions 1 to 3 of this router have 8 MB of flash memory. Since most third parties' firmware only use up to 4 MB flash, a JFFS2-based read/write filesystem can be created and used on the remaining 4 MB free flash. This allows for greater flexibility of configurations and scripting, enabling this small router to both load balance multiple ADSL lines (multi homed) or to be run as a hardware layer 2 load balancer (with appropriate third party firmware).

Version	CPU	RAM	Flash memory	S/N Prefix	Notes
1.0	Broadcom BCM4712 @ 200 MHz	32 MB	8 MB	CGN0 CGN1	ADMtek 6996L switch. Added SpeedBooster technology (Broadcom Afterburner technology), claims to boost the throughput of 802.11g by 30% (for maximum boost needs SpeedBooster technology on the other side, but will boost standard 802.11g as well). Has LEDs for Power, DMZ, WLAN, Internet, and 1-4 Ports.
1.1	Broadcom BCM4712 @ 200 MHz	32 MB	8 MB	CGN2	Switched to Broadcom BCM4712 SoC and BCM5325E switch.
2.0	Broadcom BCM4712 @ 216 MHz	32 MB	8 MB	CGN3	10 LED Front Panel (two new ones behind Cisco logo button). Also capable of SecureEasySetup, but use of the logo button and lighting of the new LEDs behind it requires firmware upgrade. SoC chip REV1 or REV 2. The flash chip on this unit is Intel TE28F640.
2.1	Broadcom BCM4712 @ 216 MHz	32 MB	8 MB	CGN4	Radio chip is changed from BCM2050 to BCM2050KML.
3.0	Broadcom BCM5352 @ 200 MHz	32 MB	8 MB	CGN5	Switched to newer Broadcom SoC
4.0	Broadcom BCM5352 @ 200 MHz	16 MB	4 MB	CGN6	Reduced RAM & Flash (a very rare few have 32 MB/8 MB)
5.0	Broadcom BCM5352 @ 200 MHz	16 MB	2 MB	CGN7	Uses VxWorks OS and reduced Flash Memory; not compatible with most 3rd party firmware, although the "VxWorks killer" utility allows some 3rd party open source firmware to be loaded on this and future versions.
5.1	Broadcom	16 MB	2 MB	CGN8	

	BCM5352 @ 200 MHz				
6.0	Broadcom BCM5352 @ 200 MHz	16 MB	2 MB	CGN9	
7.0	Broadcom BCM5354 @ 240 MHz	16 MB	2 MB	CGNA CGNB CGNC	Switched to newer Broadcom SoC. Newest VxWorks killer works. Antennae can be removed. CGNB and CGNC antennae can be removed.
7.2	Broadcom BCM5354 @ 240 MHz	16 MB	2 MB	CGNE	FCC ID: Q87-WRT54GSV72. Some antennae can be removed. Some refurbished one have EN29LV160A 16 Mb (2 MiB) Flash and IS42S16800A or K4S281632IUC75 128 Mb (16MiB) RAM

WRT54GL

Linksys released the **WRT54GL** in 2005 to support third-party firmware based on Linux, after the original WRT54G line was switched from Linux to VxWorks, starting with version 5. The WRT54GL is technically a reissue of the version 4 WRT54G. Cisco was sued by the FSF for copyright infringement, but the case was settled.

Version	CPU	RAM	Flash memory	S/N Prefix	Notes
1.0	Broadcom BCM5352 @ 200 MHz	16 MB	4 MB	CL7A	New model line, released after the version 5 WRT54G, which returns to a Linux-based OS as opposed to the VxWorks firmware. SpeedBooster is not enabled in stock firmware, however third-party firmware will enable the feature. The hardware is essentially the same as the WRT54G version 4.0. One alteration is that the internal numbering scheme of the 4-port switch changed in this model, from 1 2 3 4, to 3 2 1 0.
1.1	Broadcom BCM5352 @ 200 MHz	16 MB	4 MB	CL7B CL7C CF7C	Detachable antennas. As of August, 2009, this version was shipping with firmware revision 4.30.11. This pre-loaded firmware allows the user to upload a 4 MB firmware image, whereas the pre-loaded firmware on version 1.0 limited the image to 3 MB. Firmware

version 4.30.14 is now available for both hardware versions. Fully supported by Tomato, OpenWrt, and DD-WRT.

WRTSL54GS

WRTSL54GS is similar to the **WRT54GS** while adding additional firmware features and a USB 2.0 port (referred to as StorageLink) which can be used for a USB hard disk or flash drive.

Unlike other models, the WRTSL54GS only has one antenna.

Version	CPU speed	RAM	Flash memory	S/N Prefix	Notes
1.0	Broadcom BCM4704 @ 264 MHz	32 MB	8 MB	CJK0	Released after the WRT54GS and WRT54GL. Uses Linux-based OS. Includes SpeedBooster support, additional firmware features, and an external USB 2.0 port (StorageLink) for network storage. Uses 8 MB of Intel TE28F640 flash with a Broadcom BCM4704 SoC and Broadcom BCM5325 Ethernet switch.
1.1	Broadcom BCM4704 @ 264 MHz	32 MB	8 MB	CJK11	Change from SoC rev 8 to rev 9 (unconfirmed)

WRT54GX

WRT54GX comes with SRX (Speed and Range eXpansion), which uses "True MIMO" technology. It has 3 antennae and was once marketed as a 'Pre-N' router, with 8 times the speed and 3 times the range over standard 802.11g routers.

Version	CPU speed	RAM	Flash memory	S/N Prefix	Notes
1.0	Broadcom BCM4704 @ 266 MHz	16 MB	4 MB	KBG5?	Wireless-G Broadband Router with SRX.
2.0	Realtek RTL8651B @ 200 MHz	32 MB	8 MB	KIO1?	Wireless-G Broadband Router with SRX.

WRT54GP2 and WRTP54G

WRT54GP2 has 1 or 2 antennae, and a built-in analog telephony adapter (ATA) with 2 phone lines, but only 3 network ports. "Vonage" **WRTP54G** has 1 antenna, 2 phone lines, 4 network ports — Same S/N Prefix

Version	Locked to	RAM	Flash memory	S/N Prefix	Notes
EA	Engin	32 MB	8 MB	CJJ0	Wireless-G Broadband Router with 2 Phone Ports. Uses the Sipura Chipset

WRT54GX2

WRT54GX2 has 2 antennae, and was advertised to have up to 6 times the speed and 2 times the range over standard 802.11g routers. Chipset Realtek. It is not compatible with DD-WRT .

WRT54GX4

WRT54GX4 has 3 moveable antennae, and is advertised to have 10 times the speed and 3 times the range of standard 802.11g routers. WRT54GX4-EU: chipset Realtek RTL8651B, radio chipset Airgo AGN303BB, flash S29GL064M90TFIR4. It does not appear to be compatible with DD-WRT .

WRT51AB

WRT series with 802.11a support. (First Generation)

Version	CPU speed	RAM	Flash memory	S/N Prefix	Notes
1.0	Broadcom BCM4702 @ 125 MHz	32 MB	4 MB	MCH0	2 mini-PCI Slots one A one B, Switch BCM5325A

WRT55AG

WRT54G series with 802.11a support.

Version	CPU speed	RAM	Flash memory	S/N Prefix	Notes
1.0	Broadcom BCM4710 @ 125 MHz	32 MB	4 MB	MDJ0	2 mini-PCI Slots
2.0	Atheros AR5001AP @ 200 MHz	16 MB	4 MB	MDJ1	

WTR54GS

The Linksys WTR54GS is a confusingly named derivative of the WRT54GS. It is a compact wireless travel router with SpeedBooster support that has only 1 LAN and 1

WAN Ethernet interfaces, but has 2 wireless interfaces. The WTR54GS has the ability to make an unencrypted wireless connection on one interface, and make open shared connections on the other wireless interface, or the LAN port. The default gateway IP address and default management address is 192.168.16.1.

Version	CPU	RAM	Flash memory	S/N Prefix	JTAG port	3rd party firmware support	Notes
1.0	Broadcom BCM5350 @ 200 MHz	16 MB (IC42S32400)	4 MB (29LV320ABTC)	SJH0	yes	DD-WRT v24 sp2 (mini or std)	
2.0	Broadcom BCM5350 @ 200 MHz	8 MB	2 MB	SJH1	no*	DD-WRT v24 sp2 (micro only)	*Some examples reportedly have a JTAG port, but most do not.
2.1	Broadcom BCM5350 @ 200 MHz	8 MB	2 MB	SJH2	no	DD-WRT v24 sp2 (micro only)	

WRT54G2

The WRT54G2 is the newest iteration of the WRT54G in a smaller, curved black case with internal antennae. This unit has a four port 10/100 switch and one WAN port.

Version	CPU	RAM	Flash memory	S/N Prefix	Notes
1.0	Broadcom BCM5354 @ 240 MHz	16 MB	2 MB	CSV	Two non-replaceable internal antennae. 3rd-party firmware: Fully compatible with DD-WRT (micro, micro-plus, and micro-plus with SSH editions). Not compatible with Tomato and other 3rd party firmware solutions at this time. Firmware: VxWorks

					FCC ID: Q87-WRT54G2V1
1.3	Broadcom BCM5354 @ 240 MHz	8 MB	2 MB	CSV	Hardware: Reduced system memory to 8 MB. 3rd-party firmware: Supported by DD-WRT. Firmware: VxWorks 5.5 FCC ID: Q87-WRT54G2V13
1.5	Atheros AR7240 @ 400 MHz	16 MB (W9412G6IH)	2 MB	CSV	Hardware: Reduced to one internal antenna; switched from Broadcom to Atheros chipset (AR7240-AH1E + AR9285-AL1E 3rd-party firmware: Not possible with DD-WRT. FCC ID: Q87-WRT54G2V15

WRT54GS2

The WRT54GS2 is the **WRT54G2** hardware with the VxWorks 5.5 Firmware including SpeedBooster. It has a sleek black design with 2 internal antennae. It includes a 4-port 10/100 switch and one 10/100 WAN port on the rear.

Version	CPU speed	RAM	Flash memory	S/N Prefix	Notes
1.0	Broadcom BCM5354 @ 240 MHz	8 MB	2 MB	CUQ	3rd-party firmware: Fully compatible with DD-WRT (micro)*. FCC ID:Q87-WRT54G2V1

* Note: 1.5 of the WRT54G2 is NOT supported by dd-wrt. Apparently it uses Atheros components that require more than the 2 MB of Flash Memory built-in for a dd-wrt solution.

WRT54GC

WRT54GC series with 802.11b/g support. This unit has a four port 10/100 switch and one WAN port. The "C" in the router number stands for compact, as the unit measures 4" by 4" by 1" with an internal antenna. The unit can be expanded with addition of HGA7S external antenna to boost range. Hardware Version 1.0 is the only option available in the United States since introduction in 2005.

Version 2.0 is shipping in, amongst other countries, the United Kingdom. This unit has 1 MB flash, 4 MB RAM and a non-detachable external antenna.

The internal hardware is based on a Marvell ARM914 ("Libertas") reference design which is probably identical to the SerComm IP806SM, Xterasys XR-2407G, Abocom ARM914, Hawking HWGR54 Revision M, and the Airlink 101 AR315W. By appropriately changing the value of the firmware byte 0x26, the WRT54GC can be cross-flashed with firmware based on the same reference platform.

There were reports in 2006 that a sister platform of the WRT54GC (the AR315W) was hacked to run Linux.

WRT54G3G/WRT54G3GV2 Mobile Broadband router

A variant which has 4 Ethernet ports, 1 Internet Wired port (For DSL/Cable connections) plus a PCMCIA slot for use with a Cellular Based PC Card "aircard". The V2 model has an additional 2 USB ports for 3G modem use and 1 other USB port which has yet to be put to use.

Model	Description	Alternative Firmware
WRT54G3G	A Vodafone branded unit locked to the Vodafone network supporting GPRS, UMTS and HSDPA but can be unlocked by flashing EM/EU version firmware.	Fully Supported by OpenWRT
WRT54G3G-ST	A Sprint Wireless (USA) unit which supports CDMA 1X and EVDO rev 0,A wireless Internet.	Fully Supported by OpenWRT
WRT54G3G-AT	AT&T (USA) version of the router which supports GPRS and HSDPA(UMTS Maybe?)	Fully Supported by OpenWRT
WRT54G3G-EU	European Union version supporting GPRS, UMTS and HSDPA.	Fully Supported by OpenWRT
WRT54G3GV2-VF	A Vodafone branded unit which supports full HSDPA up to 7.2 Mbit/s and seems not to be locked to the Vodafone network (Via setting APN, User and Password manually) but does not work with all USB dongles (T-Mobile: Web'N-Walk-Stick III (Huawei 172) and IV (Huawei 176 - has ext. Antenna port) are well supported, out of the box. Huawei E220 is also supported - firmware upgrade maybe needed).	Partial Supported by customization of Linksys GPL code and supported by OpenWRT. NOTE: Due to changes in the CFE (bootloader) it is not fully supported yet. You should not try it without a serial console.

Other Cellular Providers
To use this router with other cellular providers, one must use an Alternative Firmware provider. The Stock Firmware does not support cellular providers, even though one does have the exact supported aircard. e.g.: Telus Mobility (CANADA) uses the Sierra Wireless Aircard 595 which is supported by this router, but because it is from Telus Mobility and not from Sprint (USA), it will never load the card into the router to make it operational. This is only true for the Sprint and AT&T branded models.

WRT54G-TM and WRTU54G-TM

The WRT54G-TM (TM stands for T-Mobile) is also called the T-Mobile "Hotspot@Home" service. It allows calls to be made via T-Mobile's GSM network or via Wi-Fi Unlicensed Mobile Access (UMA), using the same telephone and phone number (a special dual-mode phone designed for the service is required e.g. Blackberry Pearl 8120). Additionally, once a call is in progress, one may transition from Wi-Fi to GSM (and vice versa) seamlessly, as Wi-Fi signal comes and goes, such as when entering or exiting a home or business. A special router is not needed to use the service, but the T-Mobile branded routers are supposed to enhance the telephone's battery life. This is the only known tweak to the TM version of the firmware. The hardware appears similar to that of the WRT54GL, except it has 32 MB RAM and 8 MB flash memory.

The WRT54G-TM having a serial number that starts with C061 has these specifications:

- Broadcom BCM5352EKPBG CPU
- 32 MB RAM (Hynix HY5DU561622ETP-D43)
- 8 MB Flash (JS28f640)
- Uses the same BINs that the WRT54GS v3.0 does

Version	CPU speed	RAM	Flash memory	S/N Prefix	Notes
WRT54G-TM	Broadcom BCM5352 @ 200 MHz	32 MB	8 MB	CO61	T-Mobile Edition WRT54GS V3.0 (Renamed WRT54G-TM). It is possible to upgrade to third-party firmware via JTAG or by replacing the CFS and uploading a new firmware over TFTP. Instructions for the CFS/TFTP method can be found easily on the Internet , and other third-party firmwares can be easily applied afterwards. The Tomato Firmware also works on the WRT54G-TM.
WRTU54G-TM	Infineon ADM8668 @ 200 MHz	64 MB	8 MB	QMF00H	T-Mobile Edition Model: WRTU54G-TM. This version has two RJ-11 telephone ports and two

SIM card slots. The WRTU54G-TM is not supported by DD-WRT. It can be flashed, and work is being done to port OpenWRT to this board

WRT54G-RG

The WRT54G-RG (RG stands for Rogers) is also called the Rogers TalkSpot Voice-Optimized Router. It works with Rogers' Talkspot UMA service, which allows calls to be made via Rogers' cellular network or via Wi-Fi Unlicensed Mobile Access (UMA), using the same telephone and phone number. A UMA-compatible phone is required. The WRT54G-RG and the WRT54G-TM are identical in terms of hardware.

Version	CPU speed	RAM	Flash memory	S/N Prefix	Notes
WRT54G-RG	Broadcom BCM5352 @ 200 MHz	32 MB	8 MB	CDF1	FCC ID: Q87-WT54GV40. The WRT54G-RG is supported by DD-WRT.

Third-party firmware projects

After Linksys was required to release the WRT54G's firmware source code under terms of the GNU General Public License, there have been many third party projects enhancing that code as well as some entirely new projects using the hardware in these devices. Three of the most widely used are DD-WRT, Tomato and OpenWRT.

Hardware versions affect firmware compatibility

As of January 2006, most third-party firmware is no longer compatible with version 5 of both the WRT54G and the WRT54GS. The amount of flash memory in the version 5 devices has been reduced to 2 MB, too small for current Linux-based third-party firmware.

Some users have succeeded in flashing and running a stripped down but fully functional version of DD-WRT called 'micro' on a version 5 WRT54G. An easier method not requiring any disassembly of the device has since been devised for flashing v5-v8 to DD-WRT.

To support third-party firmware, Linksys has re-released the WRT54G v4, under the new model name **WRT54GL** (the 'L' in this name allegedly stands for 'Linux'). It is also possible to replace the 2 MB flash chip in the WRT54G with a 4 MB flash chip. The Macronix International 29LV320BTC-90 is a suitable part although others may work as well. The user must first install a JTAG header and use a JTAG cable to backup the firmware, then replace the chip and restore the firmware with the JTAG cable. After testing for proper functionality of the modified unit, 3rd party firmware can be flashed using the JTAG cable and a suitable image file.

CPU

According to OpenWrt, the Linksys WRT54G series use several different processors, all of them 32-bit MIPS architecture processors, most manufactured by Broadcom.

Default settings

- IP address: 192.168.1.1 (WRT54G-TM and WRT54G-RG: 192.168.0.1)
- Web interface username: "root" for most routers, no user name on some
- Password: "admin"

Chapter 7

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.

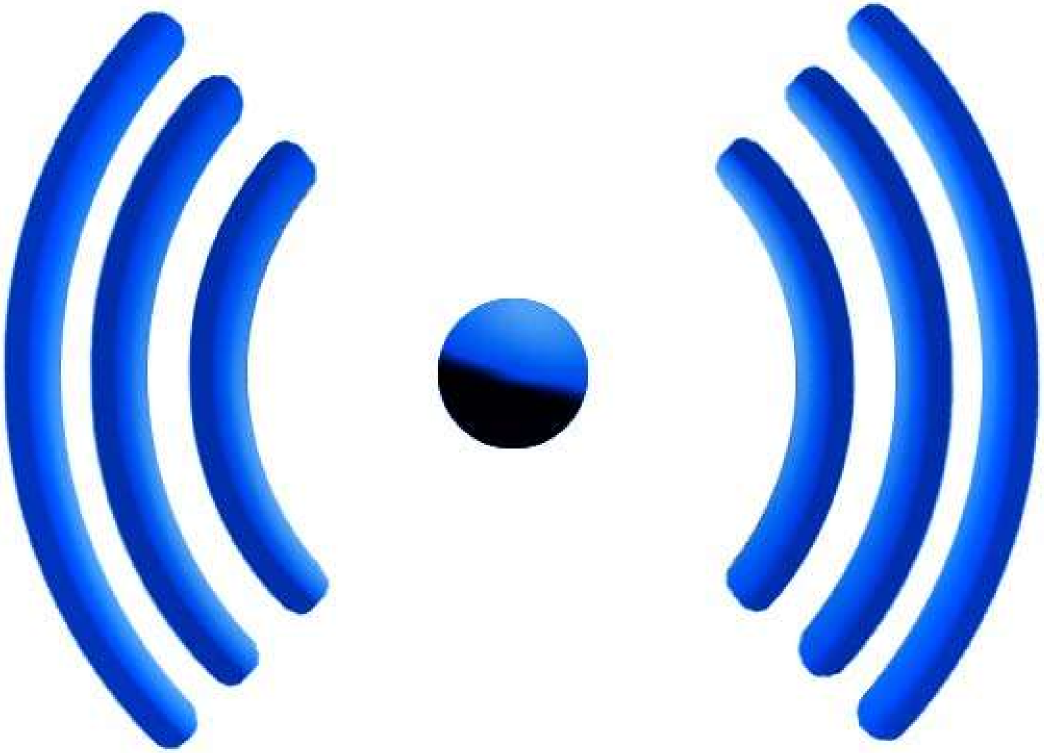
Here we, focuses on the certification and approvals process and the general growth of wireless networking under the protocols certified by the Wi-Fi Alliance. Non-Wi-Fi-Alliance wireless technologies intended for fixed points such as Motorola Canopy are usually described as fixed wireless. Non-Wi-Fi-Alliance 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 detern
wireless internet status.

How to operate:

Press the button four red indic hts shou his means the device
is searching for a signal.
If the signal bar lights fla n 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 secon lashing), a weak wireless sign
has been detected. A wireless con ion 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
signal. 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

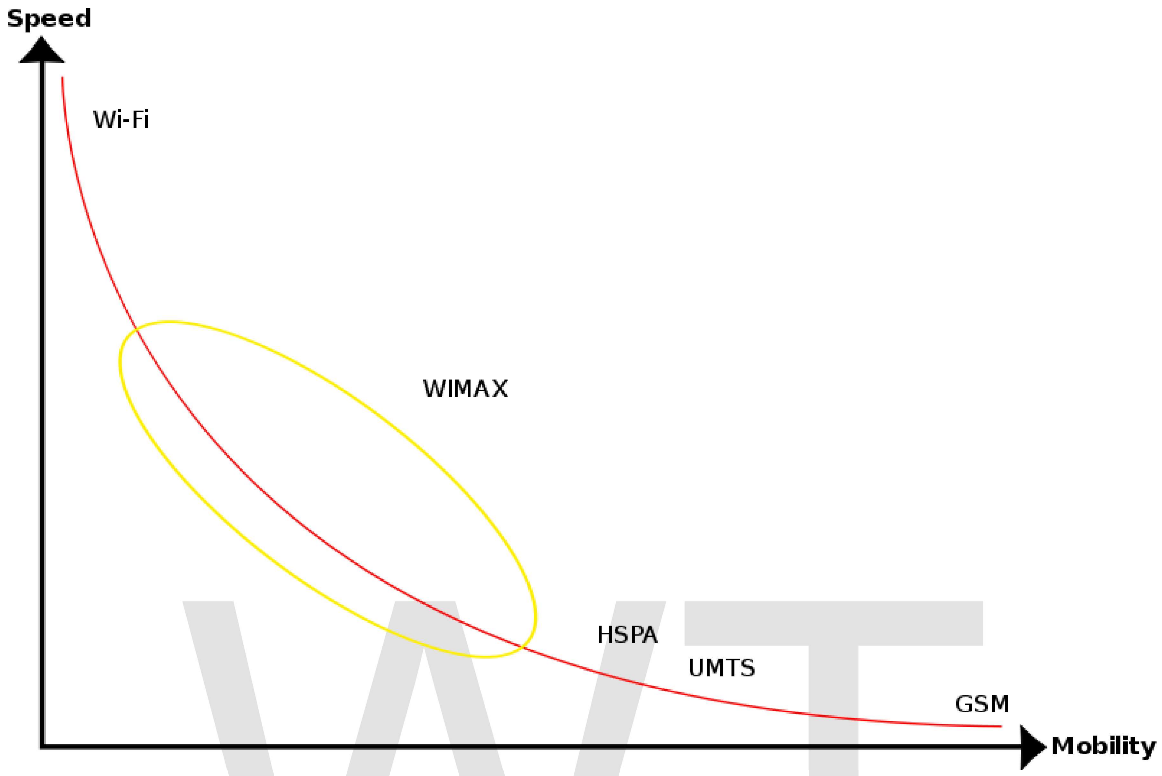
Wi-Fi networks have limited range. A typical wireless router using 802.11b or 802.11g with a stock antenna might have a range of 32 m (120 ft) indoors and 95 m (300 ft) outdoors. The IEEE 802.11n however, can exceed that range by more than two times. Range also varies with frequency band. Wi-Fi in the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

Mobility



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.

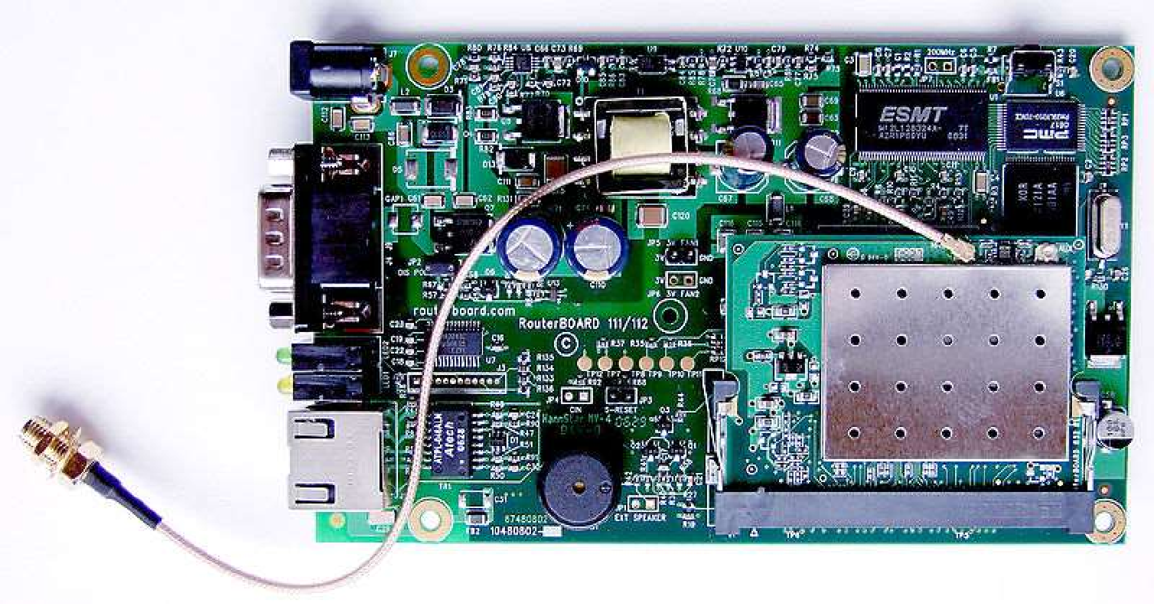
Channel pollution

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

USB wireless adapter

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

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.

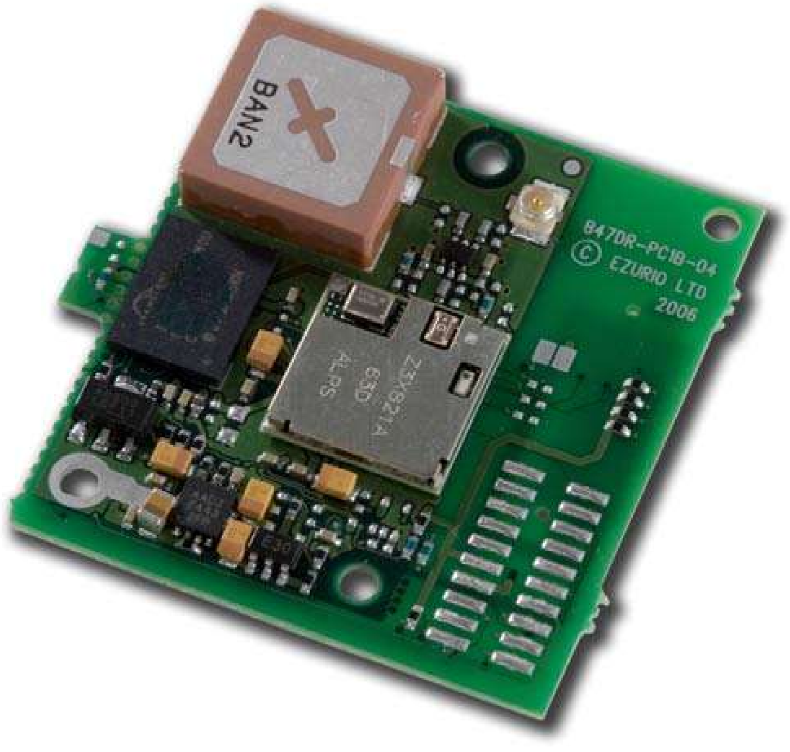
Wireless network bridges connect a wired network to a wireless network. A bridge differs from an access point: an access point connects wireless devices to a wired network at the data-link layer. Two wireless bridges may be used to connect two wired networks over a wireless link, useful in situations 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 8

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.

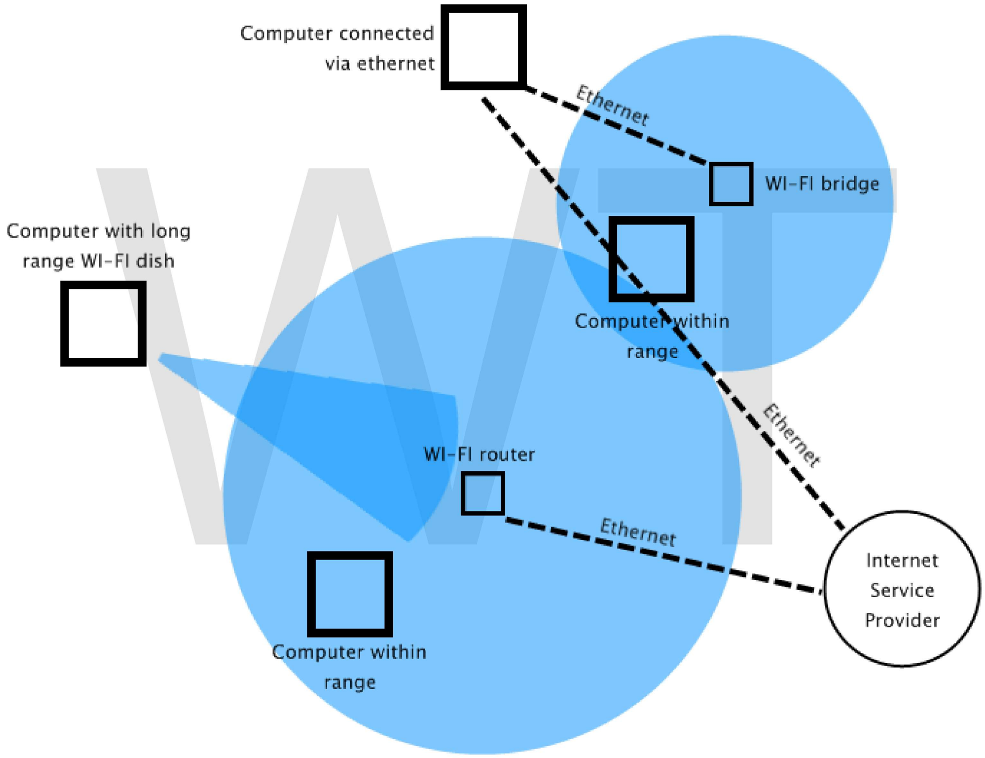
In the build-out of such networks, radio communication is used both for the Wi-Fi service and for the "backhaul" or pathway to the Internet. This means that the nodes only need a wire for power (hence the habit of installing them on power and light utility poles). This "all radio" approach means that 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 9

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.

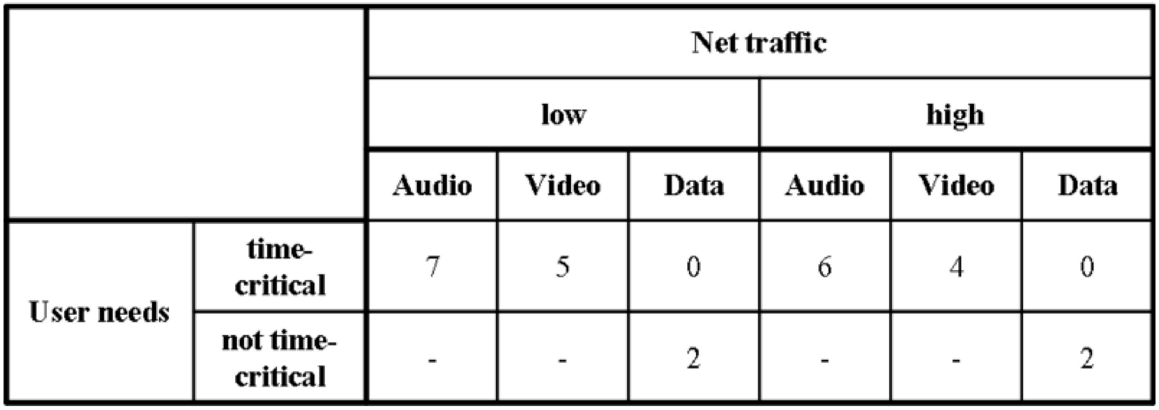
Hotspots that intend to offer both for fee and free internet access may want to look at Amazingports and their implementation of Service oriented provisioning

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

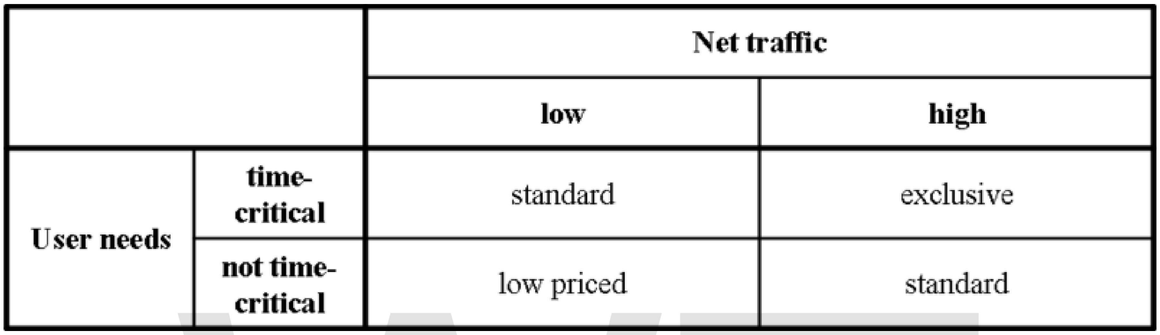


		Net traffic					
		low			high		
		Audio	Video	Data	Audio	Video	Data
User needs	time-critical	7	5	0	6	4	0
	not time-critical	-	-	2	-	-	2

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 10

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.

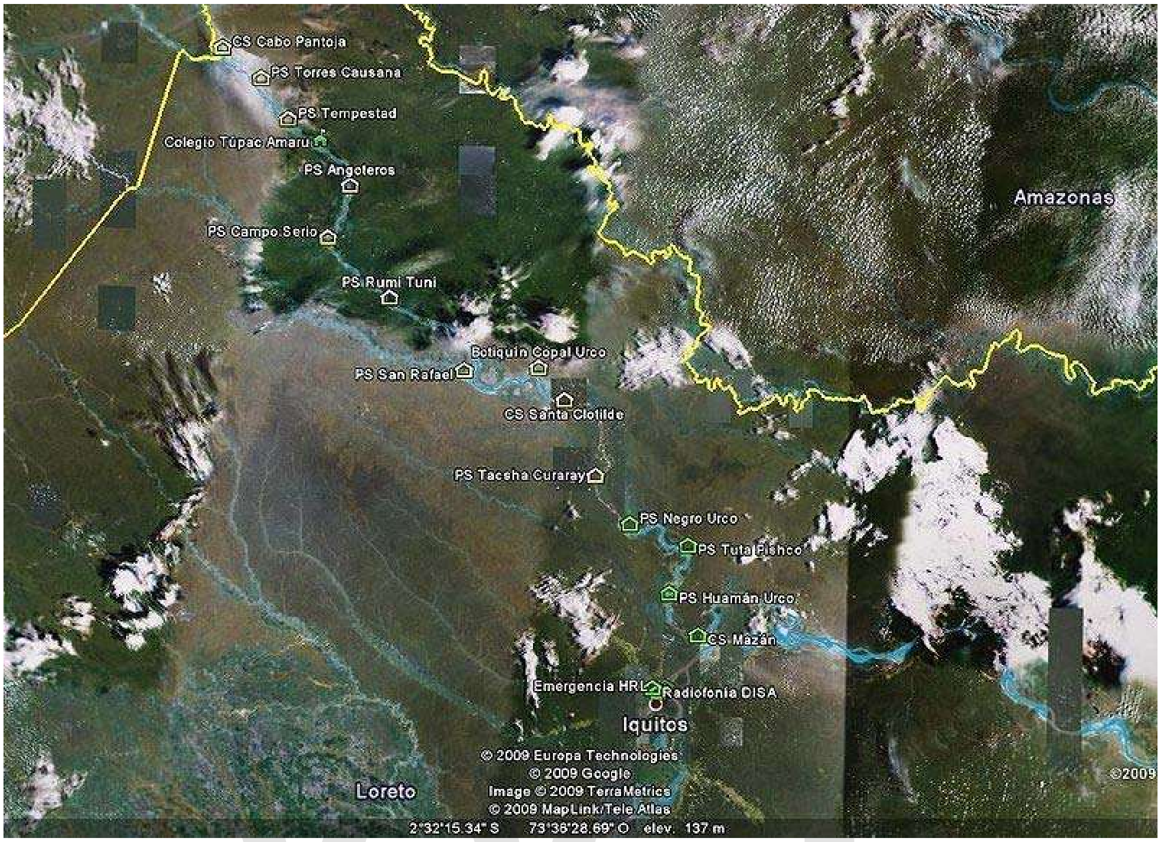
- link established on 16-06-2007
- frequency: 5765 MHz
- IEEE 802.11a (Wi-Fi), bandwidth 5 MHz
- Radio: Ubiquiti Networks XR5
- Wireless routers: MikroTik RouterBOARD with RouterOS, NStreme optimization enabled
- **Length:** 304 km (189 mi).
- Antenna is 120 cm Satellite dish prime focus with handmade 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 11

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 12

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 13

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 14

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).