

Bra att veta om trådlöst

Contents

Articles

Comparison of mobile phone standards	1
3G	6
CDMA2000	11
3GPP Long Term Evolution	13
Router	24
Machine-to-Machine	29
Input/output	32
RS-232	33
RS-422	42
EIA-485	44
Modbus	48
Virtual private network	53
Layer 2 Tunneling Protocol	58
Network address translation	63
Wi-Fi	70
Service set (802.11 network)	80
Wireless access point	82
Wired Equivalent Privacy	84
Wi-Fi Protected Access	88
Power over Ethernet	91
Antenna (radio)	98

References

Article Sources and Contributors	114
Image Sources, Licenses and Contributors	118

Article Licenses

License	120
---------	-----

Comparison of mobile phone standards

Global System for Mobile Communications (GSM, around 80–85 % market share) and IS-95 (around 10–15 % market share^[1]) are the two most prevalent mobile communication technologies. Both technologies have to solve the same problem: to divide the finite RF spectrum among multiple users.

TDMA (Time Division Multiple Access—underlying technology used in GSM's 2G) does it by chopping up the channel into sequential time slices. Each user of the channel takes turns to transmit and receive signals. In reality, only one person is actually using the channel at a specific moment. This is analogous to time-sharing on a large computer server.

CDMA (Code Division Multiple Access Underlying technology used in GSM's 3G and IS-95's 2G) on the other hand, uses a special type of digital modulation called spread spectrum which spreads the voice data over a very wide channel in pseudorandom fashion. The receiver undoes the randomization to collect the bits together and produce the sound.

For comparison, imagine a cocktail party, where couples are talking to each other in a single room. The room represents the available bandwidth. In GSM, a speaker takes turns talking to a listener. The speaker talks for a short time and then stops to let another pair talk. There is never more than one speaker talking in the room, no one has to worry about two conversations mixing. In CDMA, any speaker can talk at any time; however each uses a different language. Each listener can only understand the language of their partner. As more and more couples talk, the background noise (representing the *noise floor*) gets louder, but because of the difference in languages, conversations do not mix.

Comparison table

Feature	NMT	GSM	UMTS (3GSM)	IS-95 (CDMA one)	CDMA 2000
Technology	FDMA	TDMA	W-CDMA	CDMA	CDMA
Generation	1G	2G	3G	2G	3G
Digital	No	Yes	Yes	Yes	Yes
Year of First Use	1981	1991	2001	1995	2000 / 2002
Worldwide market share *Valid non-biased source still required	0%	72%	12%	0.6%	12%
Roaming	Scandinavia	Worldwide, 200+ countries	Worldwide	Limited	Limited
Handset interoperability	None	SIM card	SIM card	None	RUIM (not commonly implemented)
Operator locking	Monopoly	Unlockable	Unlockable	ESN	ESN
Common Interference	None	Interferes with some electronics, such as amplifiers	None	None	None

Signal quality/coverage area	Good coverage due to low frequencies	Good coverage indoors on 850/900 MHz. Repeaters possible. 35 km hard limit.	Smaller cells and lower indoors coverage on 2100 MHz; equivalent coverage indoors and superior range to GSM on 850/900 MHz.	Unlimited cell size, low transmitter power permits large cells	Unlimited cell size, low transmitter power permits large cells
Frequency utilization/Call density	Very low density	0.2 MHz = 8 timeslots. Each timeslot can hold up to 2 calls through interleaving.	5 MHz = 2 Mbit/s. Each call uses 1.8-12 kbit/s depending on chosen quality and audio complexity.	? Comparable to UMTS	? Comparable to UMTS
Battery life	Low, due to high transmitter power (1 watt)	Very good due to simple protocol, good coverage and mature, power-efficient chipsets.	Lower due to high demands of WCDMA power control and young chipsets.	Lower due to high demands of CDMA power control.	Lower due to high demands of CDMA power control and young chipsets.
Handoff	Hard	Hard	Soft	Soft	Soft
Breathing	No	No	Yes	Yes	Yes
Intellectual property	Scandinavian telecom operators	Concentrated among a few manufacturers	Concentrated among a few manufacturers	Qualcomm	Qualcomm

Advantages of 2G GSM

- GSM is mature; this maturity means a more stable network with robust features.
- Less signal deterioration inside buildings.
- Ability to use repeaters.
- Talktime is generally higher in GSM phones due to the pulse nature of transmission.
- The availability of Subscriber Identity Modules allows users to switch networks and handsets at will, aside from a subsidy lock.
- GSM covers virtually all parts of the world so international roaming is not a problem.
- The much bigger number of subscribers globally creates a better network effect for GSM handset makers, carriers and end users.

Disadvantages of 2G GSM

- Pulse nature of TDMA transmission used in 2G interferes with some electronics, especially certain audio amplifiers. 3G uses W-CDMA now.
- Intellectual property is concentrated among a few industry participants, creating barriers to entry for new entrants and limiting competition among phone manufacturers.
- GSM has a fixed maximum cell site range of 35 km, which is imposed by technical limitations.^[2]

Advantages of IS-95

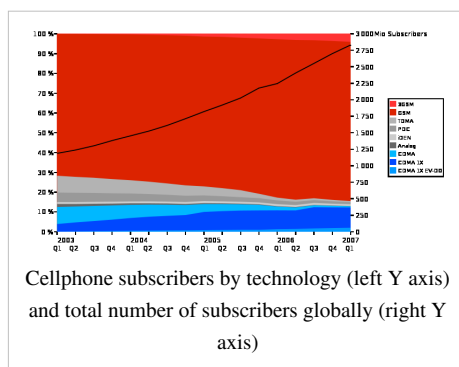
- Capacity is IS-95's biggest asset; it can accommodate more users per MHz of bandwidth than any other technology.
- Has no built-in limit to the number of concurrent users.
- Uses precise clocks that do not limit the distance a tower can cover.^[3]
- Consumes less power and covers large areas so cell size in IS-95 is larger.
- Able to produce a reasonable call with lower signal (cell phone reception) levels.
- Uses soft handoff, reducing the likelihood of dropped calls.
- IS-95's variable rate voice coders reduce the rate being transmitted when speaker is not talking, which allows the channel to be packed more efficiently.
- Has a well-defined path to higher data rates.

Disadvantages of IS-95

- Most technologies are patented and must be licensed from Qualcomm.
- *Breathing* of base stations, where coverage area shrinks under load. As the number of subscribers using a particular site goes up, the range of that site goes down.
- Because IS-95 towers interfere with each other, they are normally installed on much shorter towers. Because of this, IS-95 may not perform well in hilly terrain.
- IS-95 covers a smaller portion of the world, and IS-95 phones are generally unable to roam internationally.
- Manufacturers are often hesitant to release IS-95 devices due to the smaller market, so features are sometimes late in coming to IS-95 devices.
- Even barring subsidy locks, CDMA phones are linked by ESN to a specific network, thus phones are typically not portable across providers.

Development of the Market Share of Mobile Standards

This graphic compares the market shares of the different mobile standards.



In a fast growing market, GSM/3GSM (red) grows faster than the market and is gaining market share, the CDMA family (blue) grows at about the same rate as the market, while other technologies (grey) are being phased out.

Comparison of wireless Internet standards

As a reference, a comparison of mobile and non-mobile wireless Internet standards follows.

Comparison of Mobile Internet Access methods ()

Standard	Family	Primary Use	Radio Tech	Downlink (Mbit/s)	Uplink (Mbit/s)	Notes
LTE	UMTS/4GSM	General 4G	OFDMA/MIMO/SC-FDMA	100 (in 20MHz bandwidth)	50 (in 20 MHz bandwidth)	LTE-Advanced update expected to offer peak rates of at least 1 Gbit/s fixed speeds and 100 Mbit/s to mobile users.
WiMAX	802.16	Mobile Internet	MIMO-SOFDMA	128 (in 20MHz bandwidth)	56 (in 20MHz bandwidth)	WiMAX update IEEE 802.16m expected to offer peak rates of at least 1 Gbit/s fixed speeds and 100Mbit/s to mobile users.
Flash-OFDM	Flash-OFDM	Mobile Internet mobility up to 200mph (350km/h)	Flash-OFDM	5.3 10.6 15.9	1.8 3.6 5.4	Mobile range 18miles (30km) extended range 34 miles (55km)
HIPERMAN	HIPERMAN	Mobile Internet	OFDM	56.9	56.9	
Wi-Fi	802.11 (11n)	Mobile Internet	OFDM/MIMO	288.9*		Antenna, RF front end enhancements and minor protocol timer tweaks have helped deploy long range P2P networks compromising on radial coverage, throughput and/or spectra efficiency (310km [4] & 382km [5]) (*can support 600 when set at 40MHz channel width).
iBurst	802.20	Mobile Internet	HC-SDMA/TDD/MIMO	95	36	Cell Radius: 3–12 km Speed: 250kmph Spectral Efficiency: 13 bits/s/Hz/cell Spectrum Reuse Factor: "1"
EDGE Evolution	GSM	Mobile Internet	TDMA/FDD	1.9	0.9	3GPP Release 7
UMTS W-CDMA HSDPA+HSUPA HSPA+	UMTS/3GSM	General 3G	CDMA/FDD CDMA/FDD/MIMO	0.384 14.4 56	0.384 5.76 22	HSDPA widely deployed. Typical downlink rates today 2 Mbit/s, ~200 kbit/s uplink; HSPA+ downlink up to 56 Mbit/s.
UMTS-TDD	UMTS/3GSM	Mobile Internet	CDMA/TDD	16	16	Reported speeds according to IPWireless [6] using 16QAM modulation similar to HSDPA+HSUPA
1xRTT	CDMA2000	Mobile phone	CDMA	0.144	0.144	Succeeded by EV-DO for data use, but still is used for voice and as a failover for EV-DO

EV-DO 1x Rev. 0 EV-DO 1x Rev.A EV-DO Rev.B	CDMA2000	Mobile Internet	CDMA/FDD	2.45 3.1 4.9xN	0.15 1.8 1.8xN	Rev B note: N is the number of 1.25 MHz chunks of spectrum used. EV-DO is not designed for voice, and requires a fallback to 1xRTT when a voice call is placed or received.
---	----------	-----------------	----------	----------------------	----------------------	---

Notes: All speeds are theoretical maximums and will vary by a number of factors, including the use of external antennae, distance from the tower and the ground speed (e.g. communications on a train may be poorer than when standing still). Usually the bandwidth is shared between several terminals. The performance of each technology is determined by a number of constraints, including the spectral efficiency of the technology, the cell sizes used, and the amount of spectrum available. For more information, see *Comparison of wireless data standards*. See also Comparison of mobile phone standards, Spectral efficiency comparison table and OFDM system comparison table.

See also

- Comparison of wireless data standards
- Spectral efficiency comparison table
- SMS - contain the content of its standardization

References

- [1] "Subscriber statistics end Q1 2007" (http://web.archive.org/web/20070927162249/http://www.gsmworld.com/news/statistics/pdf/gsm_stats_q1_07.pdf). Archived from the original (http://www.gsmworld.com/news/statistics/pdf/gsm_stats_q1_07.pdf) on 2007-09-27. . Retrieved 2007-09-22.
- [2] <http://www.arcx.com/sites/faq.htm>
- [3] Frequently Asked PCS Questions (<http://www.arcx.com/sites/faq.htm>)
- [4] <http://www.alvarion.com/index.php/en/news-a-events/global-press-releases/948-worlds-longest-wi-fi-connection-made-by-the-swedish-space-corporation>
- [5] <http://www.eslared.org.ve/articulos/Long%20Distance%20WiFi%20Trial.pdf>
- [6] <http://www.ipwireless.com/technology/>

3G

International Mobile Telecommunications-2000 (IMT — 2000), better known as **3G** or **3rd Generation**, is a generation of standards for mobile phones and mobile telecommunications services fulfilling specifications by the International Telecommunication Union.^[1] Application services include wide-area wireless voice telephone, mobile Internet access, video calls and mobile TV, all in a mobile environment. Compared to the older 2G and 2.5G standards, a 3G system must allow simultaneous use of speech and data services, and provide peak data rates of at least 200 kbit/s according to the IMT-2000 specification. Recent 3G releases, often denoted 3.5G and 3.75G, also provide mobile broadband access of several Mbit/s to laptop computers and smartphones.

The following standards are typically branded 3G:

- the UMTS system, first offered in 2001, standardized by 3GPP, used primarily in Europe, Japan, China (however with a different radio interface) and other regions predominated by GSM 2G system infrastructure. The cell phones are typically UMTS and GSM hybrids. Several radio interfaces are offered, sharing the same infrastructure:
 - The original and most widespread radio interface is called W-CDMA.
 - The TD-SCDMA radio interface, was commercialised in 2009 and is only offered in China.
 - The latest UMTS release, HSPA+, can provide peak data rates up to 56 Mbit/s in the downlink in theory (28 Mbit/s in existing services) and 22 Mbit/s in the uplink.
- the CDMA2000 system, first offered in 2002, standardized by 3GPP2, used especially in North America and South Korea, sharing infrastructure with the IS-95 2G standard. The cell phones are typically CDMA2000 and IS-95 hybrids. The latest release EVDO Rev B offers peak rates of 14.7 Mbit/s downstreams.

The above systems and radio interfaces are based on kindred spread spectrum radio transmission technology. While the GSM EDGE standard ("2.9G"), DECT cordless phones and Mobile WiMAX standards formally also fulfill the IMT-2000 requirements and are approved as 3G standards by ITU, these are typically not branded 3G, and are based on completely different technologies.

A new generation of cellular standards has appeared approximately every tenth year since 1G systems were introduced in 1981/1982. Each generation is characterized by new frequency bands, higher data rates and non backwards compatible transmission technology. The first release of the 3GPP Long Term Evolution (LTE) standard does not completely fulfill the ITU 4G requirements called IMT-Advanced. First release LTE is not backwards compatible with 3G, but is a pre-4G or 3.9G technology, however sometimes branded "4G" by the service providers. WiMAX is another technology verging on or marketed as 4G.

Overview

The 3G (UMTS and CDMA2000) research and development projects started in 1992. In 1999, ITU approved five radio interfaces for IMT-2000 as a part of the ITU-R M.1457 Recommendation; WiMAX was added in 2007.^[2]

There are **evolutionary standards** that are backwards-compatible extensions to pre-existing 2G networks as well as **revolutionary standards** that require all-new networks and frequency allocations.^[3] The latter group is the UMTS family, which consists of standards developed for IMT-2000, as well as the independently developed standards DECT and WiMAX, which were included because they fit the IMT-2000 definition.

Overview of 3G/IMT-2000 standards^[4]

ITU IMT-2000	common name(s)		bandwidth of data	pre-4G	duplex	channel	description	geographical areas
TDMA Single-Carrier (IMT-SC)	EDGE (UWC-136)		EDGE Evolution	none	FDD	TDMA	evolutionary upgrade to GSM/GPRS ^[5]	worldwide, except Japan and South Korea
CDMA Multi-Carrier (IMT-MC)	CDMA2000		EV-DO	UMB ^[6]		CDMA	evolutionary upgrade to cdmaOne (IS-95)	Americas, Asia, some others
CDMA Direct Spread (IMT-DS)	UMTS ^[7]	W-CDMA ^[8]	HSPA	LTE			family of revolutionary standards.	worldwide
CDMA TDD (IMT-TC)		TD-CDMA ^[9]			Europe			
		TD-SCDMA ^[10]			China			
FDMA/TDMA (IMT-FT)	DECT		none			FDMA/TDMA	short-range; standard for cordless phones	Europe, USA
IP-OFDMA			WiMAX (IEEE 802.16)			OFDMA		worldwide

[1] Clint Smith, Daniel Collins. "3G Wireless Networks", page 136. 2000.

[2] ITU. "ITU Radiocommunication Assembly approves new developments for its 3G standards" (http://www.itu.int/newsroom/press_releases/2007/30.html). *press release*. . Retrieved 1 June 2009.

[3] ITU. "What really is a Third Generation (3G)(3G) Mobile Technology" (http://www.itu.int/ITU-D/imt-2000/Documents/IMT2000/What_really_3G.pdf) (PDF). . Retrieved 1 June 2009.

[4] ITU-D Study Group 2. "Guidelines on the smooth transition of existing mobile networks to IMT-2000 for developing countries (GST); Report on Question 18/2" (http://www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG02.18-1-2006-PDF-E.pdf). . Retrieved 1 June 2009.

[5] Can also be used as an upgrade to PDC or D-AMPS.

[6] development halted in favour of LTE. Qualcomm halts UMB project (<http://www.reuters.com/article/marketsNews/idUSN1335969420081113?rpc=401&>), Reuters, 13 November 2008

[7] also known as FOMA; 3GPP notes that "there currently existed many different names for the same system (eg FOMA, W-CDMA, UMTS, etc)"; "Draft summary minutes, decisions and actions from 3GPP Organizational Partners Meeting#6, Tokyo, 9 October 2001" (http://www.3gpp.org/ftp/op/OP_07/DOCS/pdf/OP6_13r1.pdf) (PDF). p. 7. . UMTS is the common name for a standard that encompasses multiple air interfaces.

[8] also known as UTRA-FDD; W-CDMA is sometimes used as a synonym for UMTS, ignoring the other air interface options.

[9] also known as UTRA-TDD 3.84 Mcps high chip rate (HCR)

[10] also known as UTRA-TDD 1.28 Mcps low chip rate (LCR)

While EDGE fulfills the 3G specifications, most GSM/UMTS phones report EDGE ("2.75G") and UMTS ("3G") functionality.

History

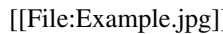
The first pre-commercial 3G network was best launched by NTT DoCoMo in Japan branded FOMA, in May 2001 on a pre-release of W-CDMA technology.^[1] The first commercial launch of 3G was also by NTT DoCoMo in Japan on 1 October 2001, although it was initially somewhat limited in scope;^{[2] [3]} broader availability was delayed by apparent concerns over reliability.^[4] The second network to go commercially live was by SK Telecom in South Korea on the 1xEV-DO technology in January 2002. By May 2002 the second South Korean 3G network was by KT on EV-DO and thus the Koreans were the first to see competition among 3G operators.

The first European pre-commercial network was at the Isle of Man by Manx Telecom, the operator then owned by British Telecom, and the first commercial network in Europe was opened for business by Telenor in December 2001 with no commercial handsets and thus no paying customers. These were both on the W-CDMA technology.

The first commercial United States 3G network was by Monet Mobile Networks, on CDMA2000 1x EV-DO technology, but this network provider later shut down operations. The second 3G network operator in the USA was Verizon Wireless in October 2003 also on CDMA2000 1x EV-DO. AT&T Mobility is also a true 3G network, having completed its upgrade of the 3G network to HSPA.

The first pre-commercial demonstration network in the southern hemisphere was built in Adelaide, South Australia by m.Net Corporation in February 2002 using UMTS on 2100 MHz. This was a demonstration network for the 2002 IT World Congress. The first commercial 3G network was launched by Hutchison Telecommunications branded as *Three* in March 2003.

Eritel Launched the first 3G network in Africa

By June 2007, the 200 millionth 3G subscriber had been connected. Out of 3 billion mobile phone subscriptions worldwide this is only 6.7%. In the countries where 3G was launched first – Japan and South Korea – 3G penetration is over 70%.^[5] In Europe the leading country is Italy with a third of its subscribers migrated to 3G. Other leading countries by 3G migration include UK, Austria, Australia and Singapore at the 20% migration level. A confusing statistic is counting CDMA2000 1x RTT customers as if they were 3G customers. If using this definition, then the total 3G subscriber base would be 475 million at June 2007 and 15.8% of all subscribers worldwide. 

Adoption

In December 2007, 190 3G networks were operating in 40 countries and 154 HSDPA networks were operating in 71 countries, according to the Global Mobile Suppliers Association (GSA). In Asia, Europe, Canada and the USA, telecommunication companies use W-CDMA technology with the support of around 100 terminal designs to operate 3G mobile networks.

Roll-out of 3G networks was delayed in some countries by the enormous costs of additional spectrum licensing fees. (See Telecoms crash.) In many countries, 3G networks do not use the same radio frequencies as 2G, so mobile operators must build entirely new networks and license entirely new frequencies; an exception is the United States where carriers operate 3G service in the same frequencies as other services. The license fees in some European countries were particularly high, bolstered by government auctions of a limited number of licenses and sealed bid auctions, and initial excitement over 3G's potential. Other delays were due to the expenses of upgrading equipment for the new systems.

Europe

In Europe, mass market commercial 3G services were introduced starting in March 2003 by 3 (Part of Hutchison Whampoa) in the UK and Italy. The European Union Council suggested that the 3G operators should cover 80% of the European national populations by the end of 2005.

Canada

In Canada, Bell Mobility, SaskTel^[6] and Telus launched a 3G EVDO network in 2005.^[7] Rogers Wireless was the first to implement UMTS technology, with HSDPA services in eastern Canada in late 2006.^[8] Realizing they would miss out on roaming revenue from the 2010 Winter Olympics, Bell and Telus formed a joint venture and rolled out a shared HSDPA network using Nokia Siemens technology.

Iraq

Mobitel Iraq is the first mobile 3G operator in Iraq. It was launched commercially on February 2007.

Philippines

3G services were made available in the Philippines on December 2008.^[9]

Syria

MTN Syria is the first mobile 3G operator in Syria. It was launched commercially on May 2010.

China

China announced in May 2008, that the telecoms sector was re-organized and three 3G networks would be allocated so that the largest mobile operator, China Mobile, would retain its GSM customer base. China Unicom would retain its GSM customer base but relinquish its CDMA2000 customer base, and launch 3G on the globally leading W-CDMA (UMTS) standard. The CDMA2000 customers of China Unicom would go to China Telecom, which would then launch 3G on the CDMA2000 1x EV-DO standard. This meant that China would have all three main cellular technology 3G standards in commercial use. Finally in January 2009, Ministry of industry and Information Technology of China awarded licenses of all three standards: TD-SCDMA to China Mobile, W-CDMA to China Unicom and CDMA2000 to China Telecom. The launch of 3G occurred on 1 October 2009, to coincide with the 60th Anniversary of the Founding of the People's Republic of China..

North Korea

North Korea has had a 3G network since 2008, which is called **Koryolink**, a joint venture between Egyptian company Orascom Telecom Holding and the state-owned Korea Post and Telecommunications Corporation (KPTC) is North Korea's only 3G Mobile operator, and one of only two mobile companies in the country. According to Orascom quoted in *BusinessWeek*, the company had 125,661 subscribers in May 2010. The Egyptian company owns 75 percent of Koryolink, and is known to invest in infrastructure for mobile technology in developing nations. It covers Pyongyang, and five additional cities and eight highways and railways. Its only competitor - SunNet, uses GSM technology and suffers from poor call quality and disconnections.^[10] Phone numbers on the network are prefixed with +850 (0)192.^[11]

Africa

The first African use of 3G technology was a 3G videocall made in Johannesburg on the Vodacom network in November 2004. The first commercial launch was by Emtel-ltd in Mauritius in 2004. In late March 2006, a 3G service was provided by the new company Wana in Morrocco. In East Africa (Tanzania) in 2007 a 3G service was provided by Vodacom Tanzania.

India

In 2008, India entered the 3G arena with the launch of 3G enabled Mobile and Data services by Government owned Bharat Sanchar Nigam Ltd. (BSNL). Later, MTNL launched 3G in Delhi and Mumbai. Nationwide auction of 3G wireless spectrum was announced in April 2010.

The first Private-sector service provider that launched 3G services is Tata Docomo, on November 5, 2010. And the second is by Reliance Communications, December 13, 2010. Other providers like Bharati Airtel, Vodafone, Idea and Aircel are expected to launch 3G services by January 2011. (Nov 20 th 2010 Now peak level 3G technology Spectrum)

Features

Data rates

ITU has not provided a clear definition of the data rate users can expect from 3G equipment or providers. Thus users sold 3G service may not be able to point to a standard and say that the rates it specifies are not being met. While stating in commentary that "it is expected that IMT-2000 will provide higher transmission rates: a minimum data rate of 2 Mbit/s for stationary or walking users, and 384 kbit/s in a moving vehicle,"^[12] the ITU does not actually clearly specify minimum or average rates or what modes of the interfaces qualify as 3G, so various rates are sold as 3G intended to meet customers expectations of broadband data.

Security

3G networks offer greater security than their 2G predecessors. By allowing the UE (User Equipment) to authenticate the network it is attaching to, the user can be sure the network is the intended one and not an impersonator. 3G networks use the KASUMI block crypto instead of the older A5/1 stream cipher. However, a number of serious weaknesses in the KASUMI cipher have been identified.^[13]

In addition to the 3G network infrastructure security, end-to-end security is offered when application frameworks such as IMS are accessed, although this is not strictly a 3G property.

Applications

The bandwidth and location information available to 3G devices gives rise to applications not previously available to mobile phone users. Some of the applications are:

- **Mobile TV** – a provider redirects a TV channel directly to the subscriber's phone where it can be watched.
- **Video on demand** – a provider sends a movie to the subscriber's phone.
- **Video conferencing** – subscribers can see as well as talk to each other.
- **Tele-medicine** – a medical provider monitors or provides advice to the potentially isolated subscriber.
- **Location-based services** – a provider sends localized weather or traffic conditions to the phone, or the phone allows the subscriber to find nearby businesses or friends.

Evolution

Both 3GPP and 3GPP2 are currently working on extensions to 3G standard that are based on an all-IP network infrastructure and using advanced wireless technologies such as MIMO, these specifications already display features characteristic for IMT-Advanced (4G), the successor of 3G. However, falling short of the bandwidth requirements for 4G (which is 1 Gbit/s for stationary and 100 Mbit/s for mobile operation), these standards are classified as 3.9G or Pre-4G.

3GPP plans to meet the 4G goals with LTE Advanced, whereas Qualcomm has halted development of UMB in favour of the LTE family.^[1]

On 14 December 2009, Telia Sonera announced in an official press release that "We are very proud to be the first operator in the world to offer our customers 4G services."^[14] With the launch of their LTE network, initially they are offering *pre-4G* (or *beyond 3G*) services in Stockholm, Sweden and Oslo, Norway.

References

- [1] "The history of UMTS and 3G development" (<http://www.umtsworld.com/umts/history.htm>). .
- [2] "World's first 3G launch on 1 October severely restricted (hktc.com)" (<http://info.hktc.com/imm/01100401/info14.htm>). .
- [3] "broadbandmag.co.uk/3G grinds to a start" (<http://www.broadbandmag.co.uk/analysis/3G/3G.html>). .
- [4] "DoCoMo Delays 3G Launch" (<http://www.wired.com/techbiz/media/news/2001/04/43253>). .
- [5] "Plus 8 Star presentation, "Is 3G a Dog or a Demon – Hints from 7 years of 3G Hype in Asia"" (<http://www.plus8star.com/?p=123>). Plus8star.com. 2008-06-11. . Retrieved 2010-09-06.
- [6] http://www.nortel.com/corporate/news/newsreleases/2005b/06_30_05_sasktel.html
- [7] <http://www.cellphones.ca/news/post001469/>
- [8] Kapica Jack (2006-11-02). "Rogers unveils new wireless network" (<http://www.theglobeandmail.com/news/technology/article853485.ece>). The Globe and Mail. . Retrieved 2010-03-22.
- [9] <http://www.physorg.com/news9436.html>
- [10] "Cell phone demand stays strong in North Korea" (<http://www.businessweek.com/idg/2010-05-13/cell-phone-demand-stays-strong-in-north-korea.html>). Business Week. 2009-12-08. . Retrieved 2010-09-06.
- [11] Telephone numbers in North Korea
- [12] "Cellular Standards for the Third Generation" (<http://www.itu.int/osg/spu/imt-2000/technology.html#Cellular Standards for the Third Generation>). ITU. 1 December 2005. .
- [13] "Security for the Third Generation (3G) Mobile System" (http://www.isrc.rhul.ac.uk/useca/OtherPublications/3G_UMTS Security.pdf). Network Systems & Security Technologies. .
- [14] "first in the world with 4G services" (<http://www.teliaSonera.com/News-and-Archive/Press-releases/2009/TeliaSonera-first-in-the-world-with-4G-services/>). TeliaSonera. 2009-12-14. . Retrieved 2010-09-06.

CDMA2000

CDMA2000 (also known as **IMT Multi-Carrier (IMT-MC)**) is a family of 3G^[1] mobile technology standards, which use CDMA channel access, to send voice, data, and signaling data between mobile phones and cell sites. The set of standards includes: **CDMA2000 1X**, **CDMA2000 EV-DO Rev. 0**, **CDMA2000 EV-DO Rev. A**, and **CDMA2000 EV-DO Rev. B**^[2]. All are approved radio interfaces for the ITU's IMT-2000. CDMA2000 has a relatively long technical history and is backward-compatible with its previous 2G iteration IS-95 (cdmaOne). In the United States, *CDMA2000* is a registered trademark of the Telecommunications Industry Association (TIA-USA)^[3]. The successor to CDMA2000 is LTE, part of the competing 3GPP family.^[4]



Huawei CDMA2000 EVDO USB wireless modem

1X

CDMA2000 1X (IS-2000), also known as **1x** and **1xRTT**, is the core CDMA2000 wireless air interface standard. The designation "1x", meaning *1 times Radio Transmission Technology*, indicates the same RF bandwidth as IS-95: a duplex pair of 1.25 MHz radio channels. 1xRTT almost doubles the capacity of IS-95 by adding 64 more traffic channels to the forward link, orthogonal to (in quadrature with) the original set of 64. The 1X standard supports packet data speeds of up to 153 kbps with real world data transmission averaging 60–100 kbps in most commercial applications.^[5] IMT-2000 also made changes to the data link layer for the greater use of data services, including medium and link access control protocols and QoS. The IS-95 data link layer only provided "best effort delivery" for data and circuit switched channel for voice (i.e., a voice frame once every 20 ms).

1xEV-DO

CDMA2000 1xEV-DO (Evolution-Data Optimized), often abbreviated as **EV-DO** or **EV**, is a telecommunications standard for the wireless transmission of data through radio signals, typically for broadband Internet access. It uses multiplexing techniques including code division multiple access (CDMA) as well as time division multiple access (TDMA) to maximize both individual user's throughput and the overall system throughput. It is standardized by 3rd Generation Partnership Project 2 (3GPP2) as part of the CDMA2000 family of standards and has been adopted by many mobile phone service providers around the world – particularly those previously employing CDMA networks. It is also used on the Globalstar satellite phone network.^[6]

Networks

The CDMA Development Group states that, as of November 2009, there are 308 operators in 116 countries offering CDMA2000 1X and 1xEV-DO service.^[7]

History

The intended 4G successor to CDMA2000 was UMB (Ultra Mobile Broadband), however in November 2008, Qualcomm announced it was ending development of the technology, favoring LTE instead.^[8]

References

- [1] http://www.itu.int/ITU-D/imt-2000/Documents/IMT2000/What_really_3G.pdf
- [2] CDMA2000 explanation (<http://www.cdg.org/technology/3g.asp>), cdg.org, November 17, 2009
- [3] CDMA2000 trademark application (<http://tess2.uspto.gov/bin/showfield?f=doc&state=4001:kets67.2.3>), uspto.gov, November 17, 2009
- [4] Qualcomm halts UMB project (<http://www.reuters.com/article/marketsNews/idUSN1335969420081113?rpc=401&>), Reuters, November 13th, 2008
- [5] 1X features/speeds (http://www.cdg.org/technology/3g_1X.asp), cdg.org, November 17, 2009
- [6] Globalstar GSP 1700 satphone also loaded with EVDO (<http://www.engadgetmobile.com/2006/11/09/globalstar-gsp-1700-satphone-also-loaded-with-ev-do/>)
- [7] http://www.cdg.org/technology/cdma_technology/cdma_stats.asp
- [8] Qualcomm halts UMB project (<http://www.reuters.com/article/marketsNews/idUSN1335969420081113?rpc=401&>), Reuters, November 13th, 2008

External links

- CDMA2000 Development Group (CDG) (<http://www.cdg.org/>)
- 3GPP2 (<http://www.3gpp2.org/>) Standards and specifications
- TIA (<http://www.tiaonline.org>) Standards documentation

3GPP Long Term Evolution

3GPP Long Term Evolution (LTE), is the latest standard in the mobile network technology tree that produced the GSM/EDGE and UMTS/HSDPA network technologies ^[1], ^[2]. It is a project of the 3rd Generation Partnership Project (3GPP), operating under a name trademarked by one of the associations within the partnership, the European Telecommunications Standards Institute.

The current generation of mobile telecommunication networks are collectively known as 3G (for "third generation"). Although LTE is often marketed as 4G, first-release LTE does not fully comply with the IMT Advanced 4G requirements. The pre-4G standard is a step toward LTE Advanced, a 4th generation standard (4G)^[3] of radio technologies designed to increase the capacity and speed of mobile telephone networks. LTE Advanced is backwards compatible with LTE and uses the same frequency bands, while LTE is not backwards compatible with 3G systems.

MetroPCS, Verizon Wireless and AT&T Mobility in the United States and several worldwide carriers announced plans, beginning in 2009, to convert their networks to LTE. The world's first publicly available LTE-service was opened by TeliaSonera in the two Scandinavian capitals Stockholm and Oslo on the 14th of December 2009. LTE is a set of enhancements to the Universal Mobile Telecommunications System (UMTS) which was introduced in 3rd Generation Partnership Project (3GPP) Release 8. Much of 3GPP Release 8 focuses on adopting 4G mobile communication's technology, including an all-IP flat networking architecture. On August 18, 2009, the European Commission announced it will invest a total of €18 million into researching the deployment of LTE and the certified 4G system LTE Advanced.^[4]

While it is commonly seen as a mobile telephone or common carrier development, LTE is also endorsed by public safety agencies in the US^[5] as the preferred technology for the new 700 MHz public-safety radio band. Agencies in some areas have filed for waivers^[6] hoping to use the 700 MHz^[7] spectrum with other technologies in advance of the adoption of a nationwide standard.

Overview

The LTE specification provides downlink peak rates of at least 100 Mbps, an uplink of at least 50 Mbps and RAN round-trip times of less than 10 ms. LTE supports scalable carrier bandwidths, from 1.4 MHz to 20 MHz and supports both frequency division duplexing (FDD) and time division duplexing (TDD).

Part of the LTE standard is the System Architecture Evolution, a flat IP-based network architecture designed to replace the GPRS Core Network and ensure support for, and mobility between, some legacy or non-3GPP systems, for example GPRS and WiMax respectively.^[8]

The main advantages with LTE are high throughput, low latency, plug and play, FDD and TDD in the same platform, an improved end-user experience and a simple architecture resulting in low operating costs. LTE will also support seamless passing to cell towers with older network technology such as GSM, cdmaOne, UMTS, and CDMA2000. The next step for LTE evolution is LTE Advanced and is currently being standardized in 3GPP Release 10. A complete end-to-end description of Release 10 can be found at ^[9]

Current state

Much of the standard addresses upgrading 3G UMTS to 4G mobile communications technology, which is essentially a mobile broadband system with enhanced multimedia services built on top.

The standard includes:

- Peak download rates of 326.4 Mbit/s for 4x4 antennae, and 172.8 Mbit/s for 2x2 antennae (utilizing 20 MHz of spectrum).^[10]
- Peak upload rates of 86.4 Mbit/s for every 20 MHz of spectrum using a single antenna.^[10]
- Five different terminal classes have been defined from a voice centric class up to a high end terminal that supports the peak data rates. All terminals will be able to process 20 MHz bandwidth.
- At least 200 active users in every 5 MHz cell. (Specifically, 200 active data clients)
- Sub-5 ms latency for small IP packets
- Increased spectrum flexibility, with supported spectrum slices as small as 1.4 MHz and as large as 20 MHz (W-CDMA requires 5 MHz slices, leading to some problems with roll-outs of the technology in countries where 5 MHz is a commonly allocated amount of spectrum, and is frequently already in use with legacy standards such as 2G GSM and cdmaOne.) Limiting sizes to 5 MHz also limited the amount of bandwidth per handset
- In the 900 MHz frequency band to be used in rural areas, supporting an optimal cell size of 5 km, 30 km sizes with reasonable performance, and up to 100 km cell sizes supported with acceptable performance. In city and urban areas, higher frequency bands (such as 2.6 GHz in EU) are used to support high speed mobile broadband. In this case, cell sizes may be 1 km or even less.
- Good support for mobility. High performance mobile data is possible at speeds of up to 350 km/h, or even up to 500 km/h, depending on the frequency band used.^[11]
- Co-existence with legacy standards (users can transparently start a call or transfer of data in an area using an LTE standard, and, should coverage be unavailable, continue the operation without any action on their part using GSM/GPRS or W-CDMA-based UMTS or even 3GPP2 networks such as cdmaOne or CDMA2000)
- Support for MBSFN (Multicast Broadcast Single Frequency Network). This feature can deliver services such as Mobile TV using the LTE infrastructure, and is a competitor for DVB-H-based TV broadcast.

A large amount of the work is aimed at simplifying the architecture of the system, as it transits from the existing UMTS circuit + packet switching combined network, to an all-IP flat architecture system.

Timetable

- In early 2008, LTE test equipment began shipping from several vendors, and at the Mobile World Congress 2008 in Barcelona Ericsson demonstrated the world's first end-to-end mobile call enabled by LTE on a small handheld device.^[12] Motorola demonstrated an LTE RAN standard compliant eNodeB and LTE chipset at the same event.
- In December 2008, the Rel-8 specification was frozen for new features, meaning only essential clarifications and corrections were permitted.
- In January 2009, the ASN.1 code was frozen. The Rel-8 standard was complete enough that hardware designers had been designing chipsets, test equipment, and base stations for some time. LTE standards development continues with 3GPP Release 9, which was frozen in December 2009. Updates to all 3GPP specifications are made every quarter and can be found at the 3GPP web site.
- On December 14, 2009, the world's first publicly available LTE service was opened by TeliaSonera in the two Scandinavian capitals Stockholm and Oslo.
- On February 10, 2010, AT&T U.S. announced its rollout of LTE service in 2011.
- On May 11, 2010, TeliaSonera, Telenor, and TDC Network announced an LTE network expected to be online in Denmark in 1Q 2011.
- On May 28, 2010, Russian operator Scartel announced the launch of an LTE network in Kazan by the end of the 2010.^[13]

- On June 1, 2010, Thailand's National Telecommunications Commission announced it will hold an auction for LTE license to 3 mobile service providers in September 2010. LTE service will be online by 4Q 2010.
- On August 30, 2010, Scartel launched an LTE network in Kazan, but the LTE network was closed (shut down) on the next day because of license absence.
- On August 31, 2010, Kenya's Safaricom announced plans to roll out LTE technology within two months.
- In August 2010, Alcatel-Lucent and Texas Energy Network, LLC (TEN), a new startup founded by Gregory M. Casey, former Executive Vice President at Qwest Communications, successfully tested an LTE base station working over a range of 12 km by simulating energy industry video and field operation activity. The tests were conducted within the Permian Basin, in the Artesian area of southeastern New Mexico.
- On September 2010, Nepal's first privately owned GSM mobile operator, Ncell-part of TeliaSonera , announced plans to rollout 4G service nation wide.
- On September 15, 2010, Bernie McMonagle, a Verizon Wireless Senior federal sales executive, announced that Verizon plans to have their entire 3G footprint switched over to 4G, so all of their customers can take advantage of the faster speeds, by the end of 2013.^[14]
- On September 16, 2010, Verizon Wireless announced that its LTE network would roll out in 30 "National Football League Cities" in the United States before the end of 2010.^[15]
- On September 21, 2010, MetroPCS began to roll out its LTE network in Las Vegas, Nevada.^[16]
- On September 29, 2010, MetroPCS rolled out LTE services in Dallas/Fort Worth, Texas.^[17]
- On October 26, 2010, Ericsson Nikola Tesla in cooperation with T-Mobile Croatia started testing the LTE network in Croatia.

On Desember 1,2010 Vodafone Germany started the commercial Sale of LTE products especially for residence in the countryside.

An "All IP Network" (AIPN)

Next generation networks are based upon Internet Protocol (IP). See, for example, the Next Generation Mobile Networks Alliance (NGMN).^[18]

In 2004, 3GPP proposed IP as the future for next generation networks and began feasibility studies into All IP Networks (AIPN). Proposals developed included recommendations for 3GPP Release 7 (2005),^[19] which are the foundation of higher level protocols such as LTE. These recommendations are part of the 3GPP System Architecture Evolution (SAE). Some aspects of All-IP networks, however, were already defined as early as release 4.^[20]

E-UTRAN Air Interface

E-UTRAN is the air interface of LTE. Its main features are:

- Peak download rates up to 292 Mbit/s and upload rates up to 71 Mbit/s depending on the user equipment category.
- Low data transfer latencies (sub-5 ms latency for small IP packets in optimal conditions), lower latencies for handover and connection setup time than with previous radio access technologies.
- Support for terminals moving at up to 350 km/h or 500 km/h depending on the frequency band.
- Support for both FDD and TDD duplexes as well as half-duplex FDD with the same radio access technology
- Support for all frequency bands currently used by IMT systems by ITU-R.
- Flexible bandwidth: 1.4 MHz, 3 MHz, 5 MHz, 15 MHz and 20 MHz are standardized.
- Support for cell sizes from tens of metres radius (femto and picocells) up to 100 km radius macrocells
- Simplified architecture: The network side of EUTRAN is composed only by the eNodeBs
- Support for inter-operation with other systems (e.g. GSM/EDGE, UMTS, CDMA2000, WiMAX...)
- Packet switched radio interface.

Technology demonstrations

- In September 2006, Siemens Networks (today Nokia Siemens Networks) showed in collaboration with Nomor Research the first live emulation of an LTE network to the media and investors. As live applications two users streaming an HD-TV video in the downlink and playing an interactive game in the uplink have been demonstrated.^[21]
- The first presentation of an LTE demonstrator with HDTV streaming (>30 Mbit/s), video supervision and Mobile IP-based handover between the LTE radio demonstrator and the commercially available HSDPA radio system was shown during the ITU trade fair in Hong Kong in December 2006 by Siemens Communication Department.
- In February 2007, Ericsson demonstrated for the first time in the world LTE with bit rates up to 144 Mbit/s^[22]
- In September 2007, NTT docomo demonstrated LTE data rates of 200 Mbit/s with power consumption below 100 mW during the test.^[23]
- In November 2007, Infineon presented the world's first RF transceiver named SMARTi LTE supporting LTE functionality in a single-chip RF silicon processed in CMOS^{[24] [25]}
- At the February 2008 Mobile World Congress:
 - Huawei demonstrated Long Term Evolution ("LTE") applications by means of multiplex HDTV services and mutual gaming that has transmission speeds of 100 Mbit/s.
 - Motorola demonstrated how LTE can accelerate the delivery of personal media experience with HD video demo streaming, HD video blogging, Online gaming and VoIP over LTE running a RAN standard compliant LTE network & LTE chipset.^[26]
 - Ericsson EMP (now ST-Ericsson) demonstrated the world's first end-to-end LTE call on handheld^[12] Ericsson demonstrated LTE FDD and TDD mode on the same base station platform.
 - Freescale Semiconductor demonstrated streaming HD video with peak data rates of 96 Mbit/s downlink and 86 Mbit/s uplink.^[27]
 - NXP Semiconductors (now a part of ST-Ericsson) demonstrated a multi-mode LTE modem as the basis for a software-defined radio system for use in cellphones.^[28]
 - picoChip and Mimoon demonstrated a base station reference design. This runs on a common hardware platform (multi-mode / software defined radio) with their WiMAX architecture.^[29]
- In April 2008, Motorola demonstrated the first EV-DO to LTE hand-off - handing over a streaming video from LTE to a commercial EV-DO network and back to LTE.^[30]
- In April 2008, LG Electronics and Nortel demonstrated LTE data rates of 50 Mbit/s while travelling at 110 km/h.^[31]
- In April 2008 Ericsson unveiled its M700 mobile platform, the world's first commercially available LTE-capable platform, with peak data rates of up to 100 Mbit/s in the downlink and up to 50 Mbit/s in the uplink. The first products based on M700 will be data devices such as laptop modems, Expresscards and USB modems for notebooks, as well other small-form modems suitable for consumer electronic devices. Commercial release is set for 2009, with products based on the platform expected in 2010.
- In November 2008 Motorola demonstrated industry first over-the-air LTE session in 700 MHz spectrum.^[32]
- Researchers at Nokia Siemens Networks and Heinrich Hertz Institut have demonstrated LTE with 100 Mbit/s Uplink transfer speeds.^[33]
- At the February 2009 Mobile World Congress:
 - Huawei demonstrated the world's first unified frequency-division duplex and time-division duplex (FDD/TDD) long-term evolution (LTE) solution.
 - Aricent gave a demonstration of LTE eNodeB layer2 stacks.
 - Setcom Streaming a Video^[34]
 - Infineon demonstrated a single-chip 65 nm CMOS RF transceiver providing 2G/3G/LTE functionality^[35]

- Launch of ng Connect program, a multi-industry consortium founded by Alcatel-Lucent to identify and develop wireless broadband applications.^[36]
- Motorola provided LTE drive tour on the streets of Barcelona to demonstrate LTE system performance in a real-life metropolitan RF environment^[37]
- In May 2009 Setcom Streaming HD Video at GSMA MWC and LTE World Summit
- In July 2009 Nujira demonstrated efficiencies of more than 60% for an 880 MHz LTE Power Amplifier^[38]
- In August 2009, Nortel and LG Electronics demonstrated the first successful handoff between CDMA and LTE networks in a standards-compliant manner^[39]
- In August 2009, Alcatel-Lucent receives FCC certification for LTE base stations for the 700 MHz spectrum band.^[40]
- In September 2009, Nokia Siemens Networks demonstrated world's first LTE call on standards-compliant commercial software.^[41]
- In October 2009, Ericsson and Samsung demonstrated interoperability between the first ever commercial LTE device and the live network in Stockholm, Sweden.^[42]
- In October 2009, Alcatel-Lucent's Bell Labs, Deutsche Telekom Laboratories, the Fraunhofer Heinrich-Hertz Institut and antenna supplier Kathrein conducted live field tests of a technology called Coordinated Multipoint Transmission (CoMP) aimed at increasing the data transmission speeds of Long Term Evolution (LTE) and 3G networks.^[43]
- In November 2009, Alcatel-Lucent completed first live LTE call using 800 MHz spectrum band set aside as part of the European Digital Dividend (EDD).^[44]
- In November 2009, Nokia Siemens Networks and LG completed first end-to-end interoperability testing of LTE.^[45]
- On December 14, 2009, the first commercial LTE deployment was in the Scandinavian capitals Stockholm and Oslo by the Swedish-Finnish network operator TeliaSonera and its Norwegian brandname NetCom (Norway). TeliaSonera incorrectly branded the network "4G". The modem devices on offer were manufactured by Samsung (dongle GT-B3710), and the network infrastructure created by Huawei (in Oslo) and Ericsson (in Stockholm). TeliaSonera plans to roll out nationwide LTE across Sweden, Norway and Finland.^[46] TeliaSonera used spectral bandwidth of 10 MHz (out of the maximum 20 MHz), and Single-Input and Single-Output transmission. The deployment should have provided a physical layer net bitrates of up to 50 Mbit/s downlink and 25 Mbit/s in the uplink. Introductory tests showed a TCP goodput of 42.8 Mbit/s downlink and 5.3 Mbit/s uplink in Stockholm.^[47]
- In December 2009, ST-Ericsson and Ericsson first to achieve LTE and HSPA mobility with a multimode device.^[48]
- In January 2010, Alcatel-Lucent and LG complete a live handoff of an end-to-end data call between Long Term Evolution (LTE) and CDMA networks.^[49]
- In February 2010, Nokia Siemens Networks and Vodafone Italy complete the first LTE call in Italy. The test was undertaken with commercial hardware and software. During the call a throughput of about 70 Mbit/s downlink and 19 Mbit/s uplink have been reached.
- In February 2010, Nokia Siemens Networks and Movistar test the LTE in Mobile World Congress 2010 in Barcelona, Spain, with both indoor and outdoor demonstrations.^[50]
- In May 2010, Mobile TeleSystems (MTS) and Huawei showed an indoor LTE network at "Sviaz-Expocomm 2010" in Moscow, Russia.^[51] MTS expects to start a trial LTE service in Moscow by the beginning of 2011. Earlier, MTS has received a license to build an LTE network in Uzbekistan, and intends to commence a test LTE network in Ukraine in partnership with Alcatel-Lucent.
- At the Shanghai Expo 2010 in May 2010, Motorola demonstrated a live LTE in conjunction with China Mobile. This included video streams and a drive test system using TD-LTE.^[52]
- As of 12/10/2010 DirecTV has teamed up with Verizon Wireless for a test of high-speed Long Term Evolution (LTE) wireless technology in a few homes in Pennsylvania, designed to deliver an integrated Internet and TV

bundle. Verizon Wireless said it launched LTE wireless services (for data, no voice) in 38 markets where more than 110 million Americans live on Sunday, Dec. 5.^[53]

- Indonesian cellular operator PT XL Axiata Tbk. held a first phase trial service LTE-4G with vendor partner Ericsson at December 2010. Besides downloading a huge data, test are also conducted to support the activities of broadcasting TV in the form of direct broadcast (live report), the first in Indonesia to use LTE-based devices.^[54]

Carrier adoption

Most carriers supporting GSM or HSPA networks can be expected to upgrade their networks to LTE at some stage. A complete list of commercial contracts can be found at:^[55]

- The world's first publicly available LTE-service was opened by TeliaSonera in the two Scandinavian capitals Stockholm and Oslo on the 14th of December 2009
- In January 2009 TeliaSonera signed a contract for an LTE network with Huawei covering Oslo, Norway. Under the agreement, Huawei will provide an end-to-end LTE solution including LTE base stations, core network and OSS (Operating Support System). The Huawei contract was cancelled in January 2010 and a new contract was signed with Ericsson.
- AT&T Mobility has stated that they intend to upgrade to LTE as their 4G technology in 2011, but will introduce HSPA+ as bridge standards.^[56]
- In January 2009 Ericsson and TeliaSonera announced the signing of a commercial LTE network. The roll-out of the 4G mobile broadband network will offer the highest data rates ever realized, with the best interactivity and quality. This network will cover Sweden's capital Stockholm and the contract is Ericsson's first for commercial deployment of LTE.
- T-Mobile, Vodafone, France Télécom and Telecom Italia Mobile have also announced or talked publicly about their commitment to LTE.
- In August 2009 Telefónica selected six countries to field-test LTE in the succeeding months: Spain, the United Kingdom, Germany and the Czech Republic in Europe, and Brazil and Argentina in Latin America.^[57]
- On November 24, 2009 Telecom Italia announced^[58] the first outdoor pre-commercial experimentation in the world, deployed in Torino and totally integrated into the 2G/3G network currently in service.
- The Dutch telecom provider KPN announced that it will use LTE for its 4G network.^[59]
- AlMadar Aljadeed, the biggest Libyan mobile phone operator, has announced that it will be adopting the LTE technology passing straight from 2G technology to 4G.^[60]
- The Belgian telecom provider Telenet has announced that it will be testing LTE on specific locations.^[61] The Belgian telecom provider Belgacom will be preparing their network for LTE.^[62]
- On March 18, 2010 Australian telecommunications carrier Telstra announced LTE trials lasting six months involving Motorola, Nokia, Ericsson and Siemens beginning in May 2010^[63]
- On October 6, 2010 Canadian provider Rogers Communications Inc announced that Ottawa, Canada's national capital, will be the site of LTE trials. Rogers said it will expand on this testing and move to a comprehensive technical trial of LTE on both low- and high-band frequencies across the Ottawa area.^[64]

Despite initial development of the rival UMB standard, which was designed as an upgrade path for CDMA networks, most operators of networks based upon the latter system have also announced their intent to migrate to LTE, resulting in discontinuation of UMB development.

- Verizon Wireless completed its first test LTE data calls in August 2009 and plans to deploy LTE beginning in 2010 with system-wide deployment completed in 2013.^[65]
- Bell Mobility has stated their intention to use LTE as a future upgrade to their HSPA+ network.^[66]
- Telus Mobility has announced that it will adopt LTE as its 4G wireless standard.^[67]
- MetroPCS recently announced that it would be using LTE for its upcoming 4G network.^[68]

- The newly formed China Telecom/China Unicom^[69] and Japan's KDDI^[70] have announced they have chosen LTE as their 4G network technology.

Some newcomers to the mobile phone market are or will be using LTE for their networks.

- Cox Communications has its first tower for wireless LTE network build-out.^[71] Wireless services should launch late 2009.
- The Irish telco Digiweb is currently operating a 4G service in the Dublin area. It shall be noted though that Digiweb employs Flash-OFDM technology and not LTE.
- Zain KSA Telecom Company has announced its plans to "build the largest 4G network in the globe" when it signed on Sunday Feb. 14 2010, at its HQ office, an agreement with three global giants in the provision of 4G Long Term Evolution (LTE): Motorola, Ericsson and Huawei. The agreement covered the implementation of phase one of the 4G LTE covering 4 major cities: Riyadh, Jeddah, Dammam and Al-Khobar.^[72]
- Maxis Communications Malaysia is currently testing LTE with its technology partners, Alcatel-Lucent and Huawei demonstrated an LTE connection with peak download speed of 60 and 104 Mbit/s, using both 10 MHz and 20 MHz bandwidth channels.^[73]
- Sprint Nextel On July 13, 2010 announced possibly constructing their own LTE network despite already using WiMAX as their 4G standard.^[74]
- On September 7, 2010 CenterNet and Mobyland, two Polish operators, have announced that they've launched a first commercial LTE network using 20 MHz of spectrum on the 1800 MHz band.^[75]
- Estonian Mobile phone operator EMT has opened 4G service for public use based on LTE standard on 16th of December 2010.^[76]

Frequency bands

The LTE standard can be used with many different frequency bands. There are planned 700 MHz deployments in North America (Verizon); 900, 1800, 2600 MHz in Europe; 1800 and 2600 MHz in Asia; 1800 MHz in Australia.^[77]
[78]

The situation is similar to the GSM standard that is deployed worldwide on many GSM frequency bands, from which most popular are: 850, 900, 1800, 1900 MHz. That is why phones from one country often do not work in other countries. For example, one needs at least a quad-band handset (850/900/1800/1900) to be sure their phone will work in both North America and Europe. Consumers have the same problem with 3G technologies - the UMTS standard is deployed worldwide on 14 different UMTS frequency bands. For this reason, even 3G-supporting phones will most likely provide fast internet access in no more than one region, even when it is a GSM quad-band phone and voice services will work, internet access will be slow.

Handsets and mobile modems stated to support 4G LTE will most likely support only a subset of LTE bands, so will not work with the other.

References

- [1] "An Introduction to LTE" (<http://sites.google.com/site/lteencyclopedia/home>). 3GPP LTE Encyclopedia. . Retrieved 2010-12-03.
- [2] "Long Term Evolution (LTE): A Technical Overview" ([http://www.motorola.com/staticfiles/Business/Solutions/Industry Solutions/Service Providers/Wireless Operators/LTE/_Document/Static Files/6834_MotDoc_New.pdf](http://www.motorola.com/staticfiles/Business/Solutions/Industry%20Solutions/Service%20Providers/Wireless%20Operators/LTE/_Document/Static%20Files/6834_MotDoc_New.pdf)). Motorola. . Retrieved 2010-07-03.
- [3] "Mobile telecommunications standards" (http://en.wikipedia.org/wiki/Template:Mobile_telecommunications_standards). Wikipedia. . Retrieved 2010-06-16.
- [4] "European Commission pumps €18 million into LTE research | Wireless News" (<http://www.betanews.com/article/European-Commission-pumps-a18-million-into-LTE-research/1250618141>). Betanews. . Retrieved 2010-03-24.
- [5] "NPSTC Votes To Endorse LTE Technology for Broadband Network" (http://www.npstc.org/documents/Press_Release_NPSTC_Endorses_LTE_Standard_090610.pdf). *National Public Safety Telecommunications Council*. June 10, 2009. .
- [6] "PS Docket No. 06-229" (http://www.fcc.gov/Daily_Releases/Daily_Business/2009/db0814/DA-09-1819A1.pdf). *Federal Communications Commission*. August 14, 2009. .

- [7] "700 MHz Public Safety Spectrum" (<http://www.fcc.gov/pshs/public-safety-spectrum/700-MHz/>). Fcc.gov. 2009-06-12. . Retrieved 2010-03-24.
- [8] *LTE – an introduction* (http://www.ericsson.com/res/docs/whitepapers/lte_overview.pdf). Ericsson. 2009. .
- [9] *LTE – An End-to-End Description of Network Architecture and Elements* (<http://sites.google.com/site/lteencyclopedia/lte-network-infrastructure-and-elements>). 3GPP LTE Encyclopedia. 2009. .
- [10] Rumney, Moray. "3GPP LTE: Introducing Single-Carrier FDMA" (<http://cp.literature.agilent.com/litweb/pdf/5989-7898EN.pdf>). Agilent Technologies. .
- [11] Sesia, Toufik, Baker: *LTE - The UMTS Long Term Evolution; From Theory to Practice*, page 11. Wiley, 2009.
- [12] Ericsson to make World-first demonstration of end-to-end LTE call on handheld devices at Mobile World Congress, Barcelona (<http://www.ericsson.com/ericsson/press/releases/20080210-1190029.shtml>)
- [13] Scartel to launch "\$30-\$40m" LTE network in Kazan (http://www.marchmontnews.com/story.php?story_id=13016)
- [14] Verizon's LTE Network Launching in 30 NFL Cities by End of the Year (<http://www.slashgear.com/verizons-lte-network-launching-in-30-nfl-cities-by-end-of-the-year-16102731/>)
- [15] Verizon Wireless to Launch 4G LTE Service in 30 U.S. Cities (<http://www.eweek.com/c/a/Mobile-and-Wireless/Verizon-Wireless-to-Launch-4G-LTE-Service-in-30-US-Cities-417341/>)
- [16] http://www.philly.com/philly/business/technology/20100921_ap_metropcsfiresupcuttingedgewirelessnetwork.html
- [17] <http://investor.metropcs.com/phoenix.zhtml?c=177745&p=irol-newsArticle&ID=1475926>
- [18] <http://www.ngmn.org> Next Generation Mobile Networks Alliance
- [19] 3GPP TR 22.978 All-IP network (AIPN) feasibility study (<http://www.3gpp.org/ftp/Specs/html-info/22978.htm>)
- [20] 3GPP Work Item 31067 (<http://www.3gpp.org/specs/WorkItem-info/WI--31067.htm>)
- [21] Nomor Research: World's first LTE demonstration (<http://www.nomor.de/home/company/lte-demo-details>)
- [22] Ericsson demonstrates live LTE at 144Mbps (<http://www.ericsson.com/ericsson/press/releases/20070209-1103814.shtml>)
- [23] NTT DoCoMo develops low power chip for 3G LTE handsets (<http://www.electronicweekly.com/Articles/2007/09/14/42179/ntt-docomo-develops-low-power-chip-for-3g-lte-handsets.htm>)
- [24] Infineon Ships One Billion RF-Transceivers; Introduces Next-Generation LTE Chip (<http://www.infineon.com/cms/en/corporate/press/news/releases/2007/INFCOM200711-019.html>)
- [25] SMARTi LTE Specifications (<http://www.infineon.com/cms/de/product/channel.html?channel=db3a3043163797a6011649c97e7a0734>)
- [26] "Motorola Media Center - Press Releases" (http://www.motorola.com/mediacenter/news/detailpf.jsp?globalObjectId=9249_9178_23). Motorola.com. 2008-02-07. . Retrieved 2010-03-24.
- [27] Gardner, W. David. "Freescale Semiconductor To Demo LTE In Mobile Handsets", *Information Week*, February 8, 2008. (<http://www.informationweek.com/hardware/showArticle.jhtml?articleID=206106780>)
- [28] Walko, John "NXP powers ahead with programmable LTE modem", *EETimes*, January 30, 2008. (<http://www.eetimes.com/conf/3gsm/showArticle.jhtml?articleID=206100262&kc=6437>)
- [29] Walko, John "PicoChip, MimoOn team for LTE ref design", *EETimes*, February 4, 2008. (<http://eetimes.eu/showArticle.jhtml?articleID=206103517>)
- [30] "Motorola Media Center - Press Releases" (http://www.motorola.com/mediacenter/news/detailpf.jsp?globalObjectId=9422_9351_23). Motorola.com. 2008-03-26. . Retrieved 2010-03-24.
- [31] Nortel and LG Electronics Demo LTE at CTIA and with High Vehicle Speeds:: Wireless-Watch Community (<http://wireless-watch.com/2008/04/06/nortel-and-lg-electronics-demo-lte-at-ctia-and-with-high-vehicle-speeds/>)
- [32] "Motorola Media Center - Motorola Demonstrates Industry First Over-the-Air LTE Session in 700MHz Spectrum" (<http://mediacenter.motorola.com/content/detail.aspx?ReleaseID=5591>). Mediacenter.motorola.com. 2008-11-03. . Retrieved 2010-03-24.
- [33] Researchers demo 100 Mbit/s MIMO with SDMA / virtual MIMO technology (<http://www.presseecho.de/informationstechnologie/PR277867.htm>)
- [34] Mr. Markku Niiranen, Setcom Managing Director, Malta (<http://www.youtube.com/watch?v=Gv9QIJWBoK0>)
- [35] "Infineon Introduces Two New RF-Chips for LTE and 3G - SMARTi LU for Highest Data Rates with LTE and SMARTi UEmicro for Lowest Cost 3G Devices - Infineon Technologies" (<http://www.infineon.com/cms/en/corporate/press/news/releases/2009/INFWLS200901-024.html>). Infineon.com. 2009-01-14. . Retrieved 2010-03-24.
- [36] "MWC: Alcatel-Lucent focusing on cross-industry collaboration" (http://telephonyonline.com/wireless/news/Alcatel-Lucent_NG_Connect/). Telephonyonline.com. . Retrieved 2010-03-24.
- [37] "Motorola Media Center - Press Releases - Motorola Brings LTE to Life on the Streets of Barcelona" (<http://mediacenter.motorola.com/content/detail.aspx?NewsAreaID=2&ReleaseID=10757>). Mediacenter.motorola.com. 2009-02-16. . Retrieved 2010-03-24.
- [38] "achieves best ever LTE transmitter efficiency" (http://www.nujira.com/news_item.asp?nid=53). Nujira. 2009-07-16. . Retrieved 2010-03-24.
- [39] "News Releases: Nortel and LG Electronics Complete World's First 3GPP Compliant Active Handover Between CDMA and LTE Networks" (http://www2.nortel.com/go/news_detail.jsp?cat_id=-8055&oid=100260833). Nortel. 2009-08-27. . Retrieved 2010-03-24.
- [40] "Alcatel-Lucent gains LTE/700 MHz certification - RCR Wireless News" (<http://www.rcrwireless.com/article/20090824/WIRELESS/908249995/alcatel-lucent-gains-lte-700-mhz-certification>). Rcrwireless.com. 2009-08-24. . Retrieved 2010-03-24.

- [41] "World's first LTE call on commercial software" (<http://www.nokiasiemensnetworks.com/press/press-releases/worlds-first-lte-call-commercial-software>). Nokia Siemens Networks. 2009-09-17. . Retrieved 2010-03-24.
- [42] "Light Reading Mobile - 4G/LTE - Ericsson, Samsung Make LTE Connection - Telecom News Analysis" (http://www.unstrung.com/document.asp?doc_id=183528&). Unstrung.com. . Retrieved 2010-03-24.
- [43] October 17, 2009 — 12:26am ET (2009-10-17). "Alca-Lu says new antenna technology boosts LTE, 3G data speeds" (<http://www.fiercebroadbandwireless.com/story/alca-lu-says-new-antenna-technology-boosts-lte-3g-data-speeds/2009-10-17#ixzz0XfYnDKUk>). FierceBroadbandWireless. . Retrieved 2010-03-24.
- [44] "Alcatel-lucent completes first 800mhz live lte call" (<http://www.theinquirer.net/inquirer/news/1562918/alcatel-lucent-completes-800mhz-live-lte>). The Inquirer. 2010-01-11. . Retrieved 2010-03-24.
- [45] "and LG complete first end-to-end interoperability testing of LTE" (<http://www.nokiasiemensnetworks.com/press/press-releases/nokia-siemens-networks-and-lg-complete-first-end-end-interoperability-testing-l>). Nokia Siemens Networks. 2009-11-24. . Retrieved 2010-03-24.
- [46] NetCom.no (<https://netcom.no/mobiltbredband/4g/4Gengelsk.html>) - NetCom 4G (in English)
- [47] Daily Mobile Blog (<http://dailymobile.se/2009/12/15/teliasonera-s-4g-speed-test-looking-good/>)
- [48] "ST-Ericsson" (http://www.stericsson.com/press_releases/LTE_HSPA.jsp). ST-Ericsson. . Retrieved 2010-03-24.
- [49] "Alcatel-Lucent and LG Electronics Complete a Live Handoff of an End-to-End Data Call Between Long Term Evolution (LTE) and CDMA networks" ([http://www.yourcommunicationnews.com/alcatel-lucent+and+lg+electronics+complete+a+live+handoff+of+an+end-to-end+data+call+between+long+term+evolution+\(lte\)+and+cdma+networks_44225.html](http://www.yourcommunicationnews.com/alcatel-lucent+and+lg+electronics+complete+a+live+handoff+of+an+end-to-end+data+call+between+long+term+evolution+(lte)+and+cdma+networks_44225.html)). Your Communication News. 2010-01-08. . Retrieved 2010-03-24.
- [50] "4G Wireless Evolution - Telefonica and Nokia Siemens Demonstrate Live LTE in a Real Network Environment" (<http://4g-wirelessevolution.tmcnet.com/topics/4g-wirelessevolution/articles/75590-telefonica-nokia-siemens-demonstrate-live-lte-a-real.htm>). 4g-wirelessevolution.tmcnet.com. 2010-02-15. . Retrieved 2010-03-24.
- [51] "MTS and Huawei showcase LTE at Sviaz-Expocomm 2010" (http://www.company.mts.ru/press-centre/press_release/2010-05-11-1382205/) (in Russian). Mobile TeleSystems. 2010-05-11. . Retrieved 2010-05-22.
- [52] "Motorola and CMCC LTE live network at Shanghai Expo 2010" (<http://mediacenter.motorola.com/content/detail.aspx?ReleaseID=12724&NewsAreaId=17>). .
- [53] "DirecTV Tests LTE With Verizon Wireless" (http://www.multichannel.com/article/460950-DirecTV_Tests_LTE_With_Verizon_Wireless.php). .
- [54] <http://www.trendingtech.info/technology/xl-test-4g-technology/>
- [55] "LTE Commercial Contracts" (<http://sites.google.com/site/teencyclopedia/lte-equipment-manufacturers>). . Retrieved 2010-12-10.
- [56] "AT&T develops wireless broadband plans" (<http://web.archive.org/web/20080610191131/http://www.telecoms.com/itmgcontent/tcoms/news/articles/20017502859.html>). Archived from the original (<http://www.telecoms.com/itmgcontent/tcoms/news/articles/20017502859.html>) on 2008-06-10. . Retrieved 2008-08-25.
- [57] "Telefónica drives fourth generation mobile technology by commissioning six advanced pilot trials" (http://pressoffice.telefonica.com/documentos/nprensa/Piloto_LTE_EN.pdf). . Retrieved 2009-10-02.
- [58] "Telecom accende la rete mobile di quarta generazione" ([http://www.ilsole24ore.com/art/SoleOnLine4/Tecnologia e Business/2009/11/telecom-lte-sperimentazione-torino.shtml?uuid=48bf8c08-d84b-11de-bef4-cdc18202a3e3&DocRulesView=Libero](http://www.ilsole24ore.com/art/SoleOnLine4/Tecnologia%20e%20Business/2009/11/telecom-lte-sperimentazione-torino.shtml?uuid=48bf8c08-d84b-11de-bef4-cdc18202a3e3&DocRulesView=Libero)). Il Sole 24 ORE. . Retrieved 2010-03-24.
- [59] KPN drops Wimax and chooses LTE (dutch) (<http://tweakers.net/nieuws/62830/kpn-schiet-wimax-af-en-kiest-voor-lte.html>)
- [60] Almadar (http://www.almadar.ly/news.aspx?m_id=541)
- [61] <http://hugin.info/136600/R/1390518/348549.pdf>
- [62] "Belgacom maakt netwerk klaar voor lte | Mobile | Tweakers.net Nieuws" (<http://tweakers.net/nieuws/65977/belgacom-maakt-netwerk-klaar-voor-lte.html>). Tweakers.net. . Retrieved 2010-03-24.
- [63] Crozier, Ry (2010-03-18). "Video: Telstra outlines LTE trial roadmap - Networking - Technology - News" (<http://www.itnews.com.au/News/169891,telstra-outlines-lte-trial-roadmap.aspx>). Itnews.com.au. . Retrieved 2010-03-24.
- [64] "Rogers launches first LTE technical trial in Ottawa" (<http://www.reuters.com/article/idUSSGE6950MG20101006>). reuters.com. 2010-10-06. .
- [65] Berg, Andrew (2009-08-17). "Verizon Completes LTE Data Calls" (<http://www.wirelessweek.com/News-Verizon-LTE-Data-Calls-081709.aspx>). *WirelessWeek* (Advantage Business Media). . Retrieved 2009-08-18.
- [66] Bell announces strategic 3G wireless network investment, maximizing consumer choice in mobile data and confirming its path forward to 4G LTE wireless (<http://www.bce.ca/en/news/releases/bm/2008/10/10/74991.html>)
- [67] reportonbusiness.com: Wireless sales propel Telus results (<http://www.reportonbusiness.com/servlet/story/RTGAM.20080808.wtelus0808/BNStory/Business/home>)
- [68] MetroPCS Chooses LTE For 4G Wireless Network (<http://www.informationweek.com/news/mobility/wifiwimax/showArticle.jhtml?articleID=210003630>)
- [69] CDMA operators will choose LTE, says ZTE (http://www.telecomasia.net/article.php?id_article=9140&id_sector=12)
- [70] Japan's KDDI Selects LTE Core as Next-Generation Mobile Broadband Solution from Hitachi and Nortel (<http://www.foxbusiness.com/story/markets/industries/telecom/japans-kddi-selects-lte-core-generation-mobile-broadband-solution-hitachi/>)

- [71] Cox goes with LTE-ready CDMA (<http://www.fiercebroadbandwireless.com/story/cox-goes-lte-ready-cdma-700-mhz-band/2009-03-30>)
- [72] Zain KSA builds the largest 4G network in the globe (http://www.sa.zain.com/autoforms/portal/home/corporate/press-releases/largest4gnetwork?AF_language=en)
- [73] (<http://www.mmail.com.my/content/42265-tech-shorts>)
- [74] Maisto, Michelle. "Sprint Considering LTE, Merger with T-Mobile." *eweek.com*. (<http://www.eweek.com/c/a/Mobile-and-Wireless/Sprint-Considering-LTE-Merger-with-T-Mobile-768696/>)
- [75] "4th commercial LTE network running in Poland" (<http://lteworld.org/news/4th-commercial-lte-network-running-poland>). *LTE World*. 2010-09-07. . Retrieved 2010-09-08.
- [76] (<https://www.emt.ee/web/www/uudised/-/uudis/2318083>), Press Release (in Estonian), Accessed on 22.12.2010
- [77] 1800 MHz - The LTE spectrum band that was almost forgotten (<http://4gtrends.com/?p=4307>)
- [78] CSL begins dual-band 1800/2600 LTE rollout (<http://www.telecomasia.net/content/csl-begins-dual-band-18002600-lte-rollout>)

Further reading

- Chris Johnson, "LTE in BULLETS (<http://www.lte-bullets.com>)", CreateSpace, 2010, ISBN 978-1452834641
- Erik Dahlman, Stefan Parkvall, Johan Sköld, Per Beming, "3G Evolution - HSPA and LTE for Mobile Broadband", 2nd edition, Academic Press, 2008, ISBN 978-0-12-374538-5
- Stefania Sesia, Issam Toufik, and Matthew Baker, "LTE - The UMTS Long Term Evolution - From Theory to Practice", John Wiley & Sons, 2009, ISBN 978-0-470-69716-0
- Borko Furht, Syed A. Ahson, "Long Term Evolution: 3GPP LTE Radio And Cellular Technology", Crc Press, 2009, ISBN 978-1-4200-7210-5
- F. Khan, "LTE for 4G Mobile Broadband - Air Interface Technologies and Performance", Cambridge University Press, 2009
- Mustafa Ergen, "Mobile Broadband - Including WiMAX and LTE", Springer, NY, 2009
- H. Ekström, A. Furuskär, J. Karlsson, M. Meyer, S. Parkvall, J. Torsner, and M. Wahlqvist, "Technical Solutions for the 3G Long-Term Evolution," *IEEE Commun. Mag.*, vol. 44, no. 3, March 2006, pp. 38–45
- E. Dahlman, H. Ekström, A. Furuskär, Y. Jading, J. Karlsson, M. Lundevall, and S. Parkvall, "The 3G Long-Term Evolution - Radio Interface Concepts and Performance Evaluation," *IEEE Vehicular Technology Conference (VTC) 2006 Spring*, Melbourne, Australia, May 2006
- K. Fazel and S. Kaiser, *Multi-Carrier and Spread Spectrum Systems: From OFDM and MC-CDMA to LTE and WiMAX*, 2nd Edition, John Wiley & Sons, 2008, ISBN 978-0-470-99821-2
- Agilent Technologies, "LTE and the Evolution to 4G Wireless: Design and Measurement Challenges (<http://www.agilent.com/find/ltebook>)", John Wiley & Sons, 2009 ISBN 978-0-470-68261-6
- Sajal Kumar Das, John Wiley & Sons (April 2010): "Mobile Handset Design", ISBN 978-0470824672 .
- Miriam Bank, M. Bank, B. Hill, U. Mahlab "OFDMA systems, pilot signals and Doppler effect", *The IUP J. of Telecommunications*, 2(2), 2010 (7-13),

External links

- LTE homepage (<http://www.3gpp.org/article/lte>) from the 3GPP website
- LTE A-Z Description (<http://sites.google.com/site/lteencyclopedia/home>) 3GPP LTE Encyclopedia
- LTE Equipment Manufacturers (<http://sites.google.com/site/lteencyclopedia/lte-equipment-manufacturers>) List of 3GPP LTE Equipment Manufacturers and Commercial Contracts
- LinkedIn.com (<http://www.linkedin.com/groups?gid=1180727>), Public LTE Discussion Forum]
- LTE Portal (<http://www.lteportal.com/>) - 3GPP LTE / LTE-Advanced Technology - dedicated portal created for information sharing, collaboration, and networking.

Industry reaction

- "Mobile Broadband: The Global Evolution of UMTS/HSPA - 3GPP Release 7 and Beyond" by 3G Americas (http://www.3gamericas.org/English/pdfs/wp_UMTS_Rel7_Beyond_FINAL.pdf)
- Experience LTE by Motorola (<http://business.motorola.com/experiencelte/lte-experience.html>)
- Verizon Wireless Global LTE Deployment Plans (http://news.vzw.com/LTE/Dick_Lynch_MWC_Final.pdf)

White papers and other information

- EDGE, HSPA, LTE: Broadband Innovation (http://www.rysavvy.com/Articles/2007_09_Rysavvy_3GAmericas.pdf) (PDF)
- Balancing cost vs capacity for LTE (<http://www.mentum.com/blog/>)
- "LTE performance for initial deployments" by Nokia Siemens Networks (http://www.nokiasiemensnetworks.com/NR/rdonlyres/4B75329B-3750-4BBB-8320-7113613AAB64/0/LTE_measurement_A4_1302.pdf)
- LTE Comparison with GSM and UMTS (<http://sites.google.com/site/lteencyclopedia/lte-radio-link-budgeting-and-rf-planning/lte-link-budget-comparison/>)
- An Introduction – Ericsson White Paper - (http://www.ericsson.com/news/090601_lte_introduction_20100510174714;) "The Long Term Evolution of 3G" on Ericsson Review, no. 2, 2005 (http://www.ericsson.com/technology/research_papers/wireless_access/doc/the_3g_long_term_evolution_radio_interface.pdf)
- "3G Long-Term Evolution" by Dr. Erik Dahlman at Ericsson Research (http://www.signal.uu.se/Research/PCCWIP/Tunisia/WIP05_EAB.pdf)
- "Long-Term 3G Evolution - Radio Access" by Dr. Stefan Parkvall at Ericsson Research (http://www.calit2.net/events/pdfs/S3G_Stefan_Parkvall.pdf)
- "3GPP Long-Term Evolution / System Architecture Evolution: Overview" by Ulrich Barth at Alcatel (http://www.ikr.uni-stuttgart.de/Content/itg/fg524/Meetings/2006-09-29-Ulm/01-3GPP_LTE-SAE_Overview_Sep06.pdf)
- "3GPP LTE & 3GPP2 LTE Standardization" by Dr. Lee, HyeonWoo at Samsung Electronics (<http://www.krnet.or.kr/board/include/download.asp?no=30&db=program&fileno=2>)
- "Trends in Mobile Network Architectures" by Dr. Michael Schopp at Siemens Networks (<http://www.comnets.uni-bremen.de/typo3site/uploads/media/ITG-FA52-Schopp-Bremen-Nov-2006.pdf>)
- "Overview of the 3GPP LTE Physical Layer" by James Zyren and Dr. Wes McCoy, Freescale Semiconductor (http://www.freescale.com/files/wireless_comm/doc/white_paper/3GPPEVOLUTIONWP.pdf)
- "Growing momentum brings LTE closer to becoming a commercial reality" (http://www.ericsson.com/broadband/facts_opinions/index_industry_news.shtml)
- 3GPP LTE - series of pages looking at different aspects of 3G LTE (<http://www.radio-electronics.com/info/cellular/telecomms/lte-long-term-evolution/3g-lte-basics.php>)
- LTE technology introduction (<http://www.rohde-schwarz.com/appnote/1MA111.pdf>)
- Alcatel-Lucent's online magazine on 4G/LTE (<http://www2.alcatel-lucent.com/enrich/en/v3i2/>)
- LTE Encyclopedia (<http://sites.google.com/site/lteencyclopedia/>)
- Steepest Ascent LTE Toolbox & LTE Blockset (http://www.steepestascent.com/content/default.asp?page=s2_10)
- LTE and the Evolution to 4G Wireless Design and Measurement Challenges - "LTE Security" (http://www.3g4g.co.uk/Lte/LTE_Security_WP_0907_Agilent.pdf)
- Role of Crypto in Mobile Communications "LTE Security" (<https://www.cosic.esat.kuleuven.be/ecrypt/courses/end/slides-28/9-niemi.pdf>)
- « Alcatel-Lucent chair on Flexible Radio» (<http://www.supelec.fr/flexible-radio-chair.html>), working on the concept of LTE small cells
- Coexistence Digital TV and LTE (<http://www.rohde-schwarz.com/appnote/1MA176.pdf>)

- LTE in Doppler Effect condition, see: www.ofdma-manfred.com and www.hit.ac.il/staff/bank_m ([http://www.hit.ac.il/ac/files/bank_m/Articles/17 Las vegas doppler.pdf](http://www.hit.ac.il/ac/files/bank_m/Articles/17%20Las%20vegas%20doppler.pdf))
- The LTE / LTE-Advanced Guide (http://lteportal.com/LTE_Business_Guide/) A semi-annual publication on LTE / LTE-Advanced - May and November 2010 publications are now available.]

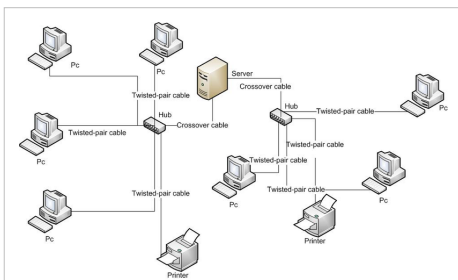
Router

A **router** interconnects two or more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another. When multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks.

Application

When multiple routers are used in a large collection of interconnected networks, the routers exchange information, so that each router can build up a reference table showing the preferred paths between any two systems on the interconnected networks.

A router can have many interface connections, for different physical types of network (such as copper cables, fiber optic, or wireless transmission). It may contain firmware for different networking protocol standards. Each network interface device is specialized to convert computer signals from one protocol standard to another.



Two small computer networks connected with HUBS, these are not ROUTERS, but simply connectors between computers. SWITCHES may be used to connect HUBS together to help transfer signals more efficiently between groups of users.



A Cisco ASM/2-32EM router deployed at CERN in 1987.

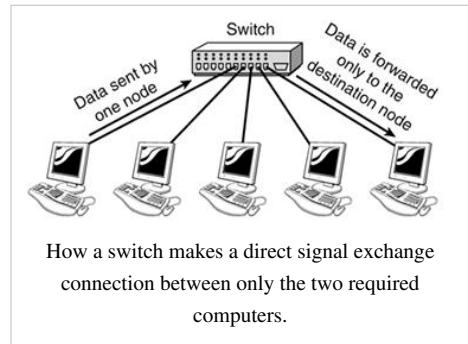


Juniper SRX210 service gateway router

Routers can be used to connect two or more logical subnets, each having a different network address. The subnets addresses in the router do not necessarily map directly to the physical interfaces of the router.^[1] The term "layer 3 switching" is often used interchangeably with the term "routing". The term switching is generally used to refer to data forwarding between two network devices with the same network address. This is also called layer 2 switching or LAN switching.

Conceptually, a router operates in two operational planes (or sub-systems).^[2]

- **Control plane:** where a router builds an address table (called routing table) that records where a packet should be forwarded, and through which physical interface. It does this by using either statically configured statements (called static routes), or alternatively, by exchanging information with other routers in the network through a dynamical routing protocol.
- **Forwarding plane:** The router actually forwards traffic, (called data packets in Internet Protocol language) from incoming interfaces to outgoing interfaces destination addresses that the packet header contains. It performs this function by following rules derived from the routing table that has been recorded in the control plane.



Routers may provide connectivity inside enterprises, between enterprises and the Internet, and inside internet service providers (ISPs). The largest routers (for example the Cisco CRS-1 or Juniper T1600) interconnect ISPs, are used inside ISPs, or may be used in very large enterprise networks. The smallest routers provide connectivity for small and home offices.

Routers for Internet connectivity and internal use

Routers intended for ISP and major enterprise connectivity almost invariably exchange routing information using the Border Gateway Protocol (BGP). RFC 4098^[3] defines several types of BGP-speaking routers according to the routers' functions:

- **Edge router (ER):** An ER is placed at the edge of an ISP network. The router speaks external BGP (EBGP) to a BGP speaker in another provider or large enterprise Autonomous System(AS). This type of router is also called PE (Provider Edge) routers.
- **Subscriber edge router (SER):** An SER is located at the edge of the subscriber's network, it speaks EBGP to its provider's AS(s). It belongs to an end user (enterprise) organization. This type of router is also called CE (Customer Edge) routers.
- **Inter-provider border router:** Interconnecting ISPs, this is a BGP-speaking router that maintains BGP sessions with other BGP speaking routers in other providers' ASes.
- **Core router:** A *core router* is one that resides within an AS as back bone to carry traffic between edge routers.

Within an ISP: Internal to the provider's AS, such a router speaks internal BGP (IBGP) to that provider's edge routers, other intra-provider core routers, or the provider's inter-provider border routers.

"Internet backbone:" The Internet does not have a clearly identifiable backbone, as did its predecessors. See default-free zone (DFZ). Nevertheless, the major ISPs' routers make up what many would consider the core. These ISPs operate all four types of the BGP-speaking routers described here. In ISP usage, a "core" router is internal to an ISP, and used to interconnect its edge and border routers. Core routers may also have specialized functions in virtual private networks based on a combination of BGP and Multi-Protocol Label Switching (MPLS).^[4]

Routers are also used for port forwarding for private servers.



A typical home router showing the ADSL telephone line and ETHERNET network cable connections.

History

The very first device that had fundamentally the same functionality as a router does today, i.e a packet switch, was the Interface Message Processor (IMP); IMPs were the devices that made up the ARPANET, the first packet switching network. The idea for a router (although they were called "gateways" at the time) initially came about through an international group of computer networking researchers called the International Network Working Group (INWG). Set up in 1972 as an informal group to consider the technical issues involved in connecting different networks, later that year it became a subcommittee of the International Federation for Information Processing.^[5]

These devices were different from most previous packet switches in two ways. First, they connected dissimilar kinds of networks, such as serial lines and local area networks. Second, they were connectionless devices, which had no role in assuring that traffic was delivered reliably, leaving that entirely to the hosts (although this particular idea had been previously pioneered in the CYCLADES network).

The idea was explored in more detail, with the intention to produce a real prototype system, as part of two contemporaneous programs. One was the initial DARPA-initiated program, which created the TCP/IP architecture of today.^[6] The other was a program at Xerox PARC to explore new networking technologies, which produced the PARC Universal Packet system, although due to corporate intellectual property concerns it received little attention outside Xerox until years later.^[7]

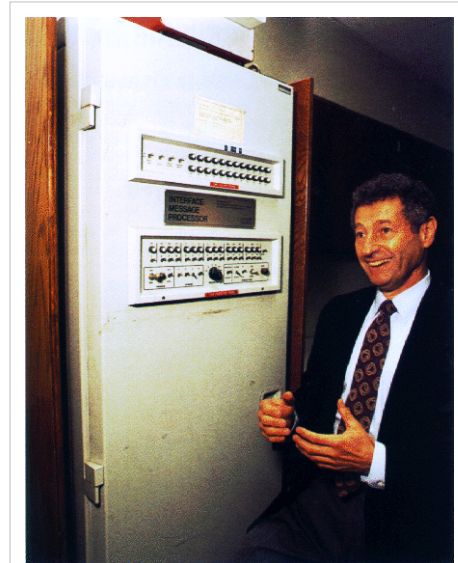
The earliest Xerox routers came into operation sometime after early 1974. The first true IP router was developed by Virginia Strazisar at BBN, as part of that DARPA-initiated effort, during 1975-1976. By the end of 1976, three PDP-11-based routers were in service in the experimental prototype Internet.^[8]

The first multiprotocol routers were independently created by staff researchers at MIT and Stanford in 1981; the Stanford router was done by William Yeager, and the MIT one by Noel Chiappa; both were also based on PDP-11s.^{[9] [10] [11] [12]}

As virtually all networking now uses IP at the network layer, multiprotocol routers are largely obsolete, although they were important in the early stages of the growth of computer networking, when several protocols other than TCP/IP were in widespread use. Routers that handle both IPv4 and IPv6 arguably are multiprotocol, but in a far less variable sense than a router that processed AppleTalk, DECnet, IP, and Xerox protocols.

In the original era of routing (from the mid-1970s through the 1980s), general-purpose mini-computers served as routers. Although general-purpose computers can perform routing, modern high-speed routers are highly specialized computers, generally with extra hardware added to accelerate both common routing functions, such as packet forwarding and specialised functions such as IPsec encryption.

Still, there is substantial use of Linux and Unix machines, running open source routing code, for routing research and other applications. While Cisco's operating system was independently designed, other major router operating



Leonard Kleinrock and the first IMP.



Avaya ERS 8600 (2010)

systems, such as those from Juniper Networks and Extreme Networks, are extensively modified but still have Unix ancestry.

Enterprise routers

All sizes of routers may be found inside enterprises. The most powerful routers tend to be found in ISPs and academic & research facilities. Large businesses may also need powerful routers.

A three-layer model is in common use, not all of which need be present in smaller networks.^[13]

Access

Access routers, including 'small office/home office' (SOHO) models, are located at customer sites such as branch offices that do not need hierarchical routing of their own. Typically, they are optimized for low cost. Some SOHO routers are capable of running alternative free Linux-based firmwares like OpenWrt.

Distribution

Distribution routers aggregate traffic from multiple access routers, either at the same site, or to collect the data streams from multiple sites to a major enterprise location. Distribution routers often are responsible for enforcing quality of service across a WAN, so they may have considerable memory, multiple WAN interfaces, and substantial processing intelligence.

They may also provide connectivity to groups of servers or to external networks. In the latter application, the router's functionality must be carefully considered as part of the overall security architecture. Separate from the router may be a firewall or VPN concentrator, or the router may include these and other security functions.

Core

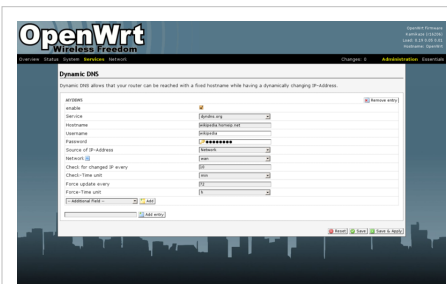
In enterprises, a core router may provide a "collapsed backbone" interconnecting the distribution tier routers from multiple buildings of a campus, or large enterprise locations. They tend to be optimized for high bandwidth.

Forwarding plane (a.k.a. data plane)

For pure Internet Protocol (IP) forwarding function, a router is designed to minimize the state information on individual packets. The main purpose of a router is to connect multiple networks and forward packets destined either for its own networks or other networks. A router is considered a Layer 3 device because its primary forwarding decision is based on the information in the Layer 3 IP packet, specifically the destination IP address. This process is known as routing. When each router receives a packet, it searches its routing table to find the best match between the destination IP address of the packet and one of the network addresses in the routing table. Once a match is found, the packet is encapsulated in the layer 2 data link frame for that outgoing interface. A router does not look into the actual data contents that the packet carries, but only at the layer 3 addresses to make a forwarding decision, plus optionally other information in the header for hint on, for example, QoS. Once a packet is forwarded, the router does not retain any historical information about the packet, but the forwarding action can be collected into the statistical data, if so configured.



Linksys by Cisco WRT54GL SoHo Router



A screenshot of the LuCI web interface used by OpenWrt. Here it is being used to configure Dynamic DNS.

Forwarding decisions can involve decisions at layers other than the IP internetwork layer or OSI layer 3. A function that forwards based on data link layer, or OSI layer 2, information, is properly called a bridge or switch. This function is referred to as layer 2 switching, as the addresses it uses to forward the traffic are layer 2 addresses in the OSI layer model.

Besides making decision as which interface a packet is forwarded to, which is handled primarily via the routing table, a router also has to manage congestion, when packets arrive at a rate higher than the router can process. Three policies commonly used in the Internet are tail drop, random early detection, and weighted random early detection. Tail drop is the simplest and most easily implemented; the router simply drops packets once the length of the queue exceeds the size of the buffers in the router. Random early detection (RED) probabilistically drops datagrams early when the queue exceeds a pre-configured size of the queue until a pre-configured max when it becomes tail drop. Weighted random early detection requires a weight on the average queue size to act upon when the traffic is about to exceed the pre-configured size, so that short bursts will not trigger random drops.

Another function a router performs is to decide which packet should be processed first when multiple queues exist. This is managed through Quality of service (QoS), which is critical when VoIP (Voice over IP) is deployed, so that delays between packets do not exceed 150ms to maintain the quality of voice conversations.

Yet another function a router performs is called "policy based routing" where special rules are constructed to override the rules derived from the routing table when a packet forwarding decision is made.

These functions may be performed through the same internal paths that the packets travel inside the router. Some of the functions may be performed through an application-specific integrated circuit (ASIC) to avoid overhead caused by multiple CPU cycles, and others may have to be performed through the CPU as these packets need special attention that cannot be handled by an ASIC.

References

- [1] Requirements for IPv4 Routers (<ftp://ftp.rfc-editor.org/in-notes/rfc1812.txt>), RFC 1812, F. Baker, June 1995
- [2] Requirements for Separation of IP Control and Forwarding (<ftp://ftp.rfc-editor.org/in-notes/rfc3654.txt>), RFC 3654, H. Khosravi & T. Anderson, November 2003
- [3] Terminology for Benchmarking BGP Device Convergence in the Control Plane (<ftp://ftp.rfc-editor.org/in-notes/rfc4098.txt>), RFC 4098, H. Berkowitz *et al.*, June 2005
- [4] BGP/MPLS VPNs (<ftp://ftp.rfc-editor.org/in-notes/rfc2547.txt>), RFC 2547, E. Rosen and Y. Rekhter, April 2004
- [5] Davies, Shanks, Heart, Barker, Despres, Detwiler, and Riml, "Report of Subgroup 1 on Communication System", INWG Note #1.
- [6] Vinton Cerf, Robert Kahn, "A Protocol for Packet Network Intercommunication" (<http://ieeexplore.ieee.org/iel5/8159/23818/01092259.pdf>), IEEE Transactions on Communications, Volume 22, Issue 5, May 1974, pp. 637 - 648.
- [7] David Boggs, John Shoch, Edward Taft, Robert Metcalfe, "Pup: An Internetwork Architecture" (<http://ieeexplore.ieee.org/iel5/8159/23925/01094684.pdf>), IEEE Transactions on Communications, Volume 28, Issue 4, April 1980, pp. 612- 624.
- [8] Craig Partridge, S. Blumenthal, "Data networking at BBN" (<http://ieeexplore.ieee.org/iel5/85/33687/01603444.pdf>); IEEE Annals of the History of Computing, Volume 28, Issue 1; January–March 2006.
- [9] Valley of the Nerds: Who Really Invented the Multiprotocol Router, and Why Should We Care? (http://www.pbs.org/cringely/pulpit/1998/pulpit_19981210_000593.html), Public Broadcasting Service, Accessed August 11, 2007.
- [10] Router Man (<http://www.networkworld.com/supp/2006/anniversary/032706-routerman.html?t5>), NetworkWorld, Accessed June 22, 2007.
- [11] David D. Clark, "M.I.T. Campus Network Implementation", CCNG-2, Campus Computer Network Group, M.I.T., Cambridge, 1982; pp. 26.
- [12] Pete Carey, "A Start-Up's True Tale: Often-told story of Cisco's launch leaves out the drama, intrigue", San Jose Mercury News, December 1, 2001.
- [13] Oppenheimer, Pr (2004). *Top-Down Network Design*. Indianapolis: Cisco Press. ISBN 1587051524.

External links

- Internet Engineering Task Force, the Routing Area ([http://www.ietf.org/html.charters/wg-dir.html#Routing Area](http://www.ietf.org/html.charters/wg-dir.html#RoutingArea))
- Internet Corporation for Assigned Names and Numbers (<http://www.icann.org/>)
- North American Network Operators Group (<http://www.nanog.org/>)
- Réseaux IP Européens (European IP Networks) (<http://www.ripe.net/>)
- American Registry for Internet Numbers (<http://www.arin.net/>)
- Router Default IP and Username Database (<http://www.routeripaddress.com/>)
- Asia-Pacific Network Information Center (<http://www.apnic.net/>)
- Latin American Network Information Center (<http://www.lacnic.net/>)
- African Region Internet Registry (<http://www.afrinic.net/>)
- Wireless Network Switching Subsystem (<http://www.entryboot.com/wireless-network--switching-subsystem.php>)

Machine-to-Machine

Machine-to-Machine (M2M) refers to technologies that allow both wireless and wired systems to communicate with other devices of the same ability.^[1] ^[2] As defined by Numerex,^[3] M2M uses a *device* (such as a sensor or meter) to capture an *event* (such as temperature, inventory level, etc.), which is relayed through a *network* (wireless, wired or hybrid) to an *application* (software program), that translates the captured event into *meaningful information* (for example, items need to be restocked). This is accomplished through the use of telemetry, the language machines use when in communication with each other. Such communication was originally accomplished by having a remote network of machines relay information back to a central hub for analysis, which would then be rerouted into a system like a personal computer.^[4]

However, modern M2M communication has expanded beyond a one-to-one connection and changed into a system of networks that transmits data to personal appliances. The expansion of wireless networks across the world has made it far easier for M2M communication to take place and has lessened the amount of power and time necessary for information to be communicated between machines.^[5] These networks also allow an array of new business opportunities and connections between consumers and producers in terms of the products being sold.^[6]

In recent years, SMS has become an increasingly important transmission mechanism for M2M communication,^[7] with the ubiquity of GSM and the relatively low cost of SMS being cited as advantages. Concerns have been raised over the reliability of SMS as an M2M channel,^[8] however the rise of direct Signaling System 7 (SS7) connected SMS gateways, which can offer increased reliability and the ability to confirm delivery, have allayed many of these fears.

History

The origin of M2M communications is cloudy because of the many different possibilities of its inception. It began around the year 2000, possibly earlier, when cellular technology first began to learn to connect directly to other computer systems. An example of an early use is OnStar's system of communication.^[9]

The year 2009 was important to the development of M2M technology, both in the U.S., and in Europe. In the United States, AT&T and Jasper Wireless entered into an agreement to both support the creation of M2M devices jointly. In conjunction, they have stated that they will be trying to further connections between consumer electronics and M2M wireless networks, which would create a boost in speed, connectivity, and overall power of such devices.^[10]

In Europe, the Norwegian incumbent Telenor concluded ten years of M2M research by setting up two entities serving the upper (services) and lower (connectivity) parts of the value-chain. Telenor Connexion^[11] in Sweden

draws on Vodafone's former research capabilities in subsidiary Europolitan and is a market leader in Europe's market for services across such typical markets as logistics, fleet management, car safety, healthcare, and smart metering of electricity consumption.^[12] Telenor Objects has a similar role supplying connectivity to M2M networks across Europe. In December, 2009, Spanish Telefonica announced that they are also setting up a M2M entity in Madrid.^[13]

In early 2010 in the U.S., AT&T, KPN, Rogers, Telcel / America Movil, Jasper Wireless began to work together in the creation of a M2M site, which will serve as a hub for developers in the field of M2M communication electronics.^[14] In February 2010, Vodafone, Verizon Wireless and nPhase (a joint partnership of Qualcomm and Verizon) announced their strategic alliance to provide global M2M solutions that would offer their customers an easy way to roll out M2M solutions across Europe and the US.^[15] In March 2010, Sprint and Axeda Corporation announced their strategic alliance for global M2M solutions.^[16] Partnerships like these make it easier, faster and more cost-efficient for businesses to use M2M. In June 2010, mobile messaging operator tyntec announced the availability of its high-reliability SMS services for M2M applications.

According to the independent wireless analyst firm Berg Insight, the number of cellular network connections worldwide used for M2M communication was 47.7 million in 2008. The company forecasts that the number of M2M connections will grow to 187 million by 2014.^[17]

A research study from the E-Plus Group^[18] shows that in 2010 2.3 million M2M SIM-cards will be in the German market. According to the study, this figure will rise in 2013 to over 5 million SIM-cards. The main growth driver is segment "tracking and tracing" with an expected average growth rate of 30 percent. The fastest growing M2M segment in Germany, with an average annual growth of 47 percent, will be the consumer electronics segment.

Applications

Wireless networks that are all interconnected can serve to improve production and efficiency in various areas, including machinery that works on building cars and on letting the developers of products know when certain products need to be taken in for maintenance and for what. Such information serves to streamline products that consumers buy and works to keep them all working at highest efficiency.^[6]

Another application is to use wireless technology to monitor systems, such as utility meters. This would allow the owner of the meter to know if certain elements have been tampered with, which serves as a quality method to stop fraud.^[19]

A third application is to use wireless networks to update digital billboards. This allows advertisers to display different messages based on time of day or day-of-week, and allows quick global changes for messages, such as pricing changes for gasoline.

Open M2M initiatives

- BITXML^[20] (protocol)
- M2MXML^[21] (protocol)
- COOS Project^[22] (connectivity initiative)

References

- [1] "Machine-to-Machine (M2M) Communication Challenges Established (U)SIM Card Technology" - GD (http://www.gi-de.com/portal/page?_pageid=44,139339&_dad=portal&_schema=PORTAL)
- [2] "Machine to Machine (M2M) Technology in Demand Responsive Commercial Buildings" ([http://74.125.155.132/search?q=cache:3aeLbEcgvOgJ:drcc.lbl.gov/pubs/LBNL_55087.pdf+what+is+\"machine+to+machine\"&cd=40&hl=en&ct=clnk&gl=us](http://74.125.155.132/search?q=cache:3aeLbEcgvOgJ:drcc.lbl.gov/pubs/LBNL_55087.pdf+what+is+\))
- [3] "M2M: The Internet of 50 Billion Devices" (<http://www.huawei.com/publications/view.do?id=6083&cid=11392&pid=10664>), *WinWin Magazine*, January 2010.
- [4] "Machine-to-Machine (M2M) Communications" (<http://www.mobilein.com/M2M.htm>), *MobileIN*.

- [5] "How Machine-to-Machine Communication Works" (<http://communication.howstuffworks.com/m2m-communication.htm>), HowStuffWorks.com
- [6] "When Machines Speak" ([http://books.google.com/books?id=2TkEAAAAMBAJ&pg=PA20&dq="Machine+to+Machine"&cd=3#v=onepage&q="Machine+to+Machine"&f=false](http://books.google.com/books?id=2TkEAAAAMBAJ&pg=PA20&dq=)), *InfoWorld*.
- [7] <http://www.160characters.org/news.php?action=view&nid=2919>
- [8] ref: <http://www.m2minformation.com/communication-methods-m2m/sms-m2m>
- [9] "The Rise of the Machine-to-Machine Sector" (<http://www.itbusinessedge.com/cm/community/features/interviews/blog/the-rise-of-the-machine-to-machine-sector/?cs=39847>), *IT Business Edge*.
- [10] "AT&T, Jasper Wireless Join Forces to Connect New Categories of Consumer Electronics and Business Devices to Nation's Fastest Network" (<http://www.jasperwireless.com/050709.html>), Jasper Wireless.
- [11] About us (<http://www.telenorconnexion.com/about-us>) - Telenor Connexion. Retrieved October 20, 2010.
- [12] Telenor Connexion Expands Machine-to-Machine Services Using Cisco IP NGN Infrastructure (http://newsroom.cisco.com/dlls/2010/prod_020910d.html) - Cisco Systems, February 9, 2010.
- [13] Global products and services development (http://www.telefonica.com/en/innovation/html/desa_productos_servicios/desa_productos_servicios.shtml) - Telefonica. Retrieved October 20, 2010.
- [14] M2M.com (<http://www.m2m.com>)
- [15] Vodafone, Verizon Wireless and nPhase announce strategic alliance to provide global M2M solutions (http://enterprise.vodafone.com/insight_news/2010-03-12_vodafone_wins_a_five_year_contract_with_deutsche_post_dhl_for_fully_managed_network.jsp?icmp=wikipedia_deutsche_win_managed), Vodafone press release, 12 March 2010.
- [16] Sprint and Axeda Announce Alliance for Global M2M Solutions (http://investors.sprint.com/phoenix.zhtml?c=127149&p=irol-newsArticle_newsroom&ID=1403399&highlight=), Sprint press release
- [17] The Global Wireless M2M Market (http://www.berginsight.com/ShowReport.aspx?m_m=3&id=95), Berg Insight.
- [18] <http://www.telecompaper.com/news/article.aspx?cid=760808>
- [19] "Gemalto's Innovative Machine-to-Machine Solution Receives '2009 SmartGrid Product of the Year' Award" (http://www.tradingmarkets.com/news/stock-alert/tmkt_gemalto-s-innovative-machine-to-machine-solution-receives-2009-smartgrid-product-of-the-year-award-829231.html), *Trading Markets* press release
- [20] <http://www.bitxml.org/>
- [21] <http://sourceforge.net/projects/m2mxml/>
- [22] <http://www.coosproject.org/maven-site/1.0.0/project-info.html>

External links

- "What is M2M Communications" (<http://www.m2mcomm.com/about/what-is-m2m/index.html>) at M2M Comm
- "Machine-to-Machine (M2M) and RFID available through Bharatbook" (<http://www.prlog.org/10573459-machine-to-machine-m2m-and-rfid-available-through-bharatbook.html>) - PRLog press release
- "Sync My Ride, and Only Mine" (<http://www.m2mmag.com/news/articles/article.aspx?ID=8256>), M2M Magazine
- "Ericsson reflects on the future of a Networked World at the Abu Dhabi Media Summit 2010" (<http://www.albawaba.com/en/countries/UAE/262579>), Al Bawaba
- "How Satellite Tracking Systems Can Both Save and Make Money" (http://www.industryweek.com/articles/how_satellite_tracking_systems_can_both_save_and_make_money_21304.aspx?SectionID=4), *Industry Week*
- "Low-Cost Security Monitoring Using Satellite Telecommunication" (<http://www.satmos.com/documents/esa-satmos.pdf>), "ESA"
- Machine-to-Machine M2M Technology (<http://www.adaptivem2m.com/>) Adaptive M2M | Machine-to-Machine Communication

Input/output

In computing, **input/output**, or **I/O**, refers to the communication between an information processing system (such as a computer), and the outside world, possibly a human, or another information processing system. Inputs are the signals or data received by the system, and outputs are the signals or data sent from it. The term can also be used as part of an action; to "perform I/O" is to perform an input or output operation. I/O devices are used by a person (or other system) to communicate with a computer. For instance, a keyboard or a mouse may be an input device for a computer, while monitors and printers are considered output devices for a computer. Devices for communication between computers, such as modems and network cards, typically serve for both input and output.

Note that the designation of a device as either input or output depends on the perspective. Mouse and keyboards take as input physical movement that the human user outputs and convert it into signals that a computer can understand. The output from these devices is input for the computer. Similarly, printers and monitors take as input signals that a computer outputs. They then convert these signals into representations that human users can see or read. For a human user the process of reading or seeing these representations is receiving input. These interactions between computers and humans is studied in a field called human–computer interaction.

In computer architecture, the combination of the CPU and main memory (i.e. memory that the CPU can read and write to directly, with individual instructions) is considered the brain of a computer, and from that point of view any transfer of information from or to that combination, for example to or from a disk drive, is considered I/O. The CPU and its supporting circuitry provide memory-mapped I/O that is used in low-level computer programming in the implementation of device drivers. An I/O algorithm is one designed to exploit locality and perform efficiently when data reside on secondary storage, such as a disk drive.

Interface

I/O Interface is required whenever the I/O device is driven by the processor. The interface must have necessary logic to interpret the device address generated by the processor. Handshaking should be implemented by the interface using appropriate commands like (BUSY,READY,WAIT), and the processor can communicate with I/O device through the interface. If different data formats are being exchanged, the interface must be able to convert serial data to parallel form and vice-versa. There must be provision for generating interrupts and the corresponding type numbers for further processing by the processor if required

A computer that uses memory-mapped I/O accesses hardware by reading and writing to specific memory locations, using the same assembler language instructions that computer would normally use to access memory.

Higher-level implementation

Higher-level operating system and programming facilities employ separate, more abstract I/O concepts and primitives. For example, most operating systems provide application programs with the concept of files. The C and C++ programming languages, and operating systems in the Unix family, traditionally abstract files and devices as streams, which can be read or written, or sometimes both. The C standard library provides functions for manipulating streams for input and output.

In the context of the ALGOL 68 programming language, the *input* and *output* facilities are collectively referred to as *transput*. The *ALGOL 68* transput library recognizes the following standard files/devices: stand in, stand out, stand errors and stand back.

An alternative to special primitive functions is the I/O monad, which permits programs to just describe I/O, and the actions are carried out outside the program. This is notable because the I/O functions would introduce side-effects to any programming language, but now purely functional programming is practical.

Addressing mode

There are many ways through which data can be read or stored in the memory. Each method is an addressing mode, and has its own advantages and limitations.

There are many type of addressing modes such as direct addressing, indirect addressing, immediate addressing, index addressing, based addressing, based-index addressing, implied addressing, etc.

Direct address

In this type of address of the data is a part of the instructions itself. When the processor decodes the instruction, it gets the memory address from where it can be read/store the required information.

Mov Reg. [Addr]

Here the `Addr` operand points to a memory location which holds the data and copies it into the specified Register.

Indirect address

Here the address can be stored in a register. The instructions will have the register which has the address. So to fetch the data, the instruction must be decoded appropriate register selected. The contents of the register will be treated as the address using this address appropriate memory location is selected and data is read/written.

Port-mapped I/O

Port-mapped I/O usually requires the use of instructions which are specifically designed to perform I/O operations.

RS-232

In telecommunications, **RS-232** (Recommended Standard 232) is a standard for serial binary single-ended data and control signals connecting between a *DTE* (Data Terminal Equipment) and a *DCE* (Data Circuit-terminating Equipment). It is commonly used in computer serial ports. The standard defines the electrical characteristics and timing of signals, the meaning of signals, and the physical size and pinout of connectors.

Scope of the standard

The Electronics Industries Association (EIA) standard RS-232-C^[1] as of 1969 defines:

- Electrical signal characteristics such as voltage levels, signaling rate, timing and slew-rate of signals, voltage withstand level, short-circuit behavior, and maximum load capacitance.
- Interface mechanical characteristics, pluggable connectors and pin identification.
- Functions of each circuit in the interface connector.
- Standard subsets of interface circuits for selected telecom applications.

The standard does not define such elements as

- character encoding (for example, ASCII, Baudot code or EBCDIC)
- the framing of characters in the data stream (bits per character, start/stop bits, parity)
- protocols for error detection or algorithms for data compression
- bit rates for transmission, although the standard says it is intended for bit rates lower than 20,000 bits per second. Many modern devices support speeds of 115,200 bit/s and above
- power supply to external devices.

Details of character format and transmission bit rate are controlled by the serial port hardware, often a single integrated circuit called a UART that converts data from parallel to asynchronous start-stop serial form. Details of

voltage levels, slew rate, and short-circuit behavior are typically controlled by a line driver that converts from the UART's logic levels to RS-232 compatible signal levels, and a receiver that converts from RS-232 compatible signal levels to the UART's logic levels.

History

RS-232 was first introduced in 1962.^[2] The original DTEs were electromechanical teletypewriters and the original DCEs were (usually) modems. When electronic terminals (smart and dumb) began to be used, they were often designed to be interchangeable with teletypes, and so supported RS-232. The C revision of the standard was issued in 1969 in part to accommodate the electrical characteristics of these devices.

Since application to devices such as computers, printers, test instruments, and so on was not considered by the standard, designers implementing an RS-232 compatible interface on their equipment often interpreted the requirements idiosyncratically. Common problems were non-standard pin assignment of circuits on connectors, and incorrect or missing control signals. The lack of adherence to the standards produced a thriving industry of breakout boxes, patch boxes, test equipment, books, and other aids for the connection of disparate equipment. A common deviation from the standard was to drive the signals at a reduced voltage: the standard requires the transmitter to use +12 V and -12 V, but requires the receiver to distinguish voltages as low as +3 V and -3 V. Some manufacturers therefore built transmitters that supplied +5 V and -5 V and labeled them as "RS-232 compatible."

Later personal computers (and other devices) started to make use of the standard so that they could connect to existing equipment. For many years, an RS-232-compatible port was a standard feature for serial communications, such as modem connections, on many computers. It remained in widespread use into the late 1990s. In personal computer peripherals it has largely been supplanted by other interface standards, such as USB. RS-232 is still used to connect older designs of peripherals, industrial equipment (such as PLCs), console ports and special purpose equipment such as a cash drawer for a cash register.

The standard has been renamed several times during its history as the sponsoring organization changed its name, and has been variously known as EIA RS-232, EIA 232, and most recently as TIA 232. The standard continued to be revised and updated by the Electronic Industries Alliance and since 1988 by the Telecommunications Industry Association (TIA).^[3] Revision C was issued in a document dated August 1969. Revision D was issued in 1986. The current revision is *TIA-232-F Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*, issued in 1997. Changes since Revision C have been in timing and details intended to improve harmonization with the CCITT standard V.24, but equipment built to the current standard will interoperate with older versions.

Related ITU-T standards include **V.24** (circuit identification) and **V.28** (signal voltage and timing characteristics).

Limitations of the standard

Because the application of RS-232 has extended far beyond the original purpose of interconnecting a terminal with a modem, successor standards have been developed to address the limitations. Issues with the RS-232 standard include:^[4]

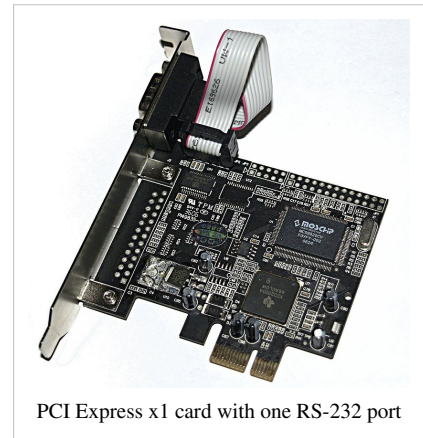
- The large voltage swings and requirement for positive and negative supplies increases power consumption of the interface and complicates power supply design. The voltage swing requirement also limits the upper speed of a compatible interface.
- Single-ended signaling referred to a common signal ground limits the noise immunity and transmission distance.
- Multi-drop connection among more than two devices is not defined. While multi-drop "work-arounds" have been devised, they have limitations in speed and compatibility.
- Asymmetrical definitions of the two ends of the link make the assignment of the role of a newly developed device problematic; the designer must decide on either a DTE-like or DCE-like interface and which connector pin

assignments to use.

- The handshaking and control lines of the interface are intended for the setup and takedown of a dial-up communication circuit; in particular, the use of handshake lines for flow control is not reliably implemented in many devices.
- No method is specified for sending power to a device. While a small amount of current can be extracted from the DTR and RTS lines, this is only suitable for low power devices such as mice.
- The 25-way connector recommended in the standard is large compared to current practice.

Role in modern personal computers

In the book *PC 97 Hardware Design Guide*,^[5] Microsoft deprecated support for the RS-232 compatible serial port of the original IBM PC design. Today, RS-232 has mostly been replaced in personal computers by USB for local communications. Compared with RS-232, USB is faster, uses lower voltages, and has connectors that are simpler to connect and use. Both standards have software support in popular operating systems. USB is designed to make it easy for device drivers to communicate with hardware. However, there is no direct analog to the terminal programs used to let users communicate directly with serial ports. USB is more complex than the RS-232 standard because it includes a protocol for transferring data to devices. This requires more software to support the protocol used. RS-232 only standardizes the voltage of signals and the functions of the physical interface pins. Serial ports of personal computers are also sometimes used to directly control various hardware devices, such as relays or lamps, since the control lines of the interface can be easily manipulated by software. This isn't feasible with USB, which requires some form of receiver to decode the serial data.



PCI Express x1 card with one RS-232 port

As an alternative, USB docking ports are available which can provide connectors for a keyboard, mouse, one or more serial ports, and one or more parallel ports. Corresponding device drivers are required for each USB-connected device to allow programs to access these USB-connected devices as if they were the original directly-connected peripherals. Devices that convert USB to RS-232 may not work with all software on all personal computers and may cause a reduction in bandwidth along with higher latency.

Personal computers may use a serial port to interface to devices such as uninterruptible power supplies. In some cases, serial data is not exchanged, but the control lines are used to signal conditions such as loss of power or low battery alarms.

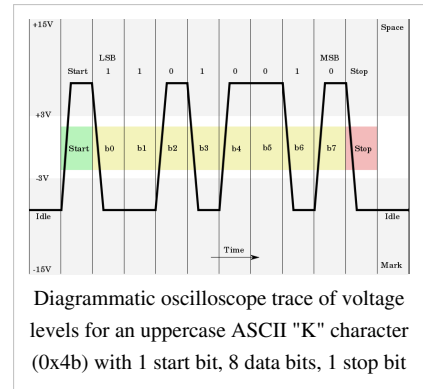
Many fields (for example, laboratory automation, surveying) provide a continued demand for RS-232 I/O due to sustained use of very expensive but aging equipment. It is often far cheaper to continue to use RS-232 than it is to replace the equipment. Additionally, modern industrial automation equipment, such as PLCs, VFDs, servo drives, and CNC equipment are programmable via RS-232. Some manufacturers have responded to this demand: Toshiba re-introduced the DE-9M connector on the Tecra laptop.

Standard details

In RS-232, user data is sent as a time-series of bits. Both synchronous and asynchronous transmissions are supported by the standard. In addition to the data circuits, the standard defines a number of control circuits used to manage the connection between the DTE and DCE. Each data or control circuit only operates in one direction, that is, signaling from a DTE to the attached DCE or the reverse. Since transmit data and receive data are separate circuits, the interface can operate in a full duplex manner, supporting concurrent data flow in both directions. The standard does not define character framing within the data stream, or character encoding.

Voltage levels

The RS-232 standard defines the voltage levels that correspond to logical one and logical zero levels for the data transmission and the control signal lines. Valid signals are plus or minus 3 to 15 volts; the ± 3 V range near zero volts is not a valid RS-232 level. The standard specifies a maximum open-circuit voltage of 25 volts: signal levels of ± 5 V, ± 10 V, ± 12 V, and ± 15 V are all commonly seen depending on the power supplies available within a device. RS-232 drivers and receivers must be able to withstand indefinite short circuit to ground or to any voltage level up to ± 25 volts. The slew rate, or how fast the signal changes between levels, is also controlled.



For data transmission lines (TxD, RxD and their secondary channel equivalents) logic one is defined as a negative voltage, the signal condition is called marking, and has the functional significance. Logic zero is positive and the signal condition is termed spacing. Control signals are logically inverted with respect to what one sees on the data transmission lines. When one of these signals is active, the voltage on the line will be between $+3$ to $+15$ volts. The inactive state for these signals is the opposite voltage condition, between -3 and -15 volts. Examples of control lines include request to send (RTS), clear to send (CTS), data terminal ready (DTR), and data set ready (DSR).

Because the voltage levels are higher than logic levels typically used by integrated circuits, special intervening driver circuits are required to translate logic levels. These also protect the device's internal circuitry from short circuits or transients that may appear on the RS-232 interface, and provide sufficient current to comply with the slew rate requirements for data transmission.

Because both ends of the RS-232 circuit depend on the ground pin being zero volts, problems will occur when connecting machinery and computers where the voltage between the ground pin on one end, and the ground pin on the other is not zero. This may also cause a hazardous ground loop. Use of a common ground limits RS-232 to applications with relatively short cables. If the two devices are far enough apart or on separate power systems, the local ground connections at either end of the cable will have differing voltages; this difference will reduce the noise margin of the signals. Balanced, differential, serial connections such as USB, RS-422 and RS-485 can tolerate larger ground voltage differences because of the differential signaling.^[6]

Unused interface signals terminated to ground will have an undefined logic state. Where it is necessary to permanently set a control signal to a defined state, it must be connected to a voltage source that asserts the logic 1 or logic 0 level. Some devices provide test voltages on their interface connectors for this purpose.

Connectors

RS-232 devices may be classified as Data Terminal Equipment (DTE) or Data Communication Equipment (DCE); this defines at each device which wires will be sending and receiving each signal. The standard recommended but did not make mandatory the D-subminiature 25 pin connector. In general and according to the standard, terminals and computers have male connectors with DTE pin functions, and modems have female connectors with DCE pin functions. Other devices may have any combination of connector gender and pin definitions. Many terminals were manufactured with female terminals but were sold with a cable with male connectors at each end; the terminal with its cable satisfied the recommendations in the standard.

Presence of a 25 pin D-sub connector does not necessarily indicate an RS-232-C compliant interface. For example, on the original IBM PC, a male D-sub was an RS-232-C DTE port (with a non-standard current loop interface on reserved pins), but the female D-sub connector was used for a parallel Centronics printer port. Some personal computers put non-standard voltages or signals on some pins of their serial ports.

The standard specifies 20 different signal connections. Since most devices use only a few signals, smaller connectors can often be used.

Pinouts

The following table lists commonly-used RS-232 signals and pin assignments.^[7] For variations see Serial port.

Signal			Origin		DB-25 pin
Name	Typical purpose	Abbreviation	DTE	DCE	
Data Terminal Ready	OOB control signal: Tells DCE that DTE is ready to be connected.	DTR	●		20
Data Carrier Detect	OOB control signal: Tells DTE that DCE is connected to telephone line.	DCD		●	8
Data Set Ready	OOB control signal: Tells DTE that DCE is ready to receive commands or data.	DSR		●	6
Ring Indicator	OOB control signal: Tells DTE that DCE has detected a ring signal on the telephone line.	RI		●	22
Request To Send	OOB control signal: Tells DCE to prepare to accept data from DTE.	RTS	●		4
Clear To Send	OOB control signal: Acknowledges RTS and allows DTE to transmit.	CTS		●	5
Transmitted Data	Data signal: Carries data from DTE to DCE.	TxD	●		2
Received Data	Data signal: Carries data from DCE to DTE.	RxD		●	3
Common Ground		GND	common		7
Protective Ground		PG	common		1

The signals are named from the standpoint of the DTE. The ground signal is a common return for the other connections. The DB-25 connector includes a second "protective ground" on pin 1. Connecting this to pin 7 (signal reference ground) is a common practice but not essential.

Data can be sent over a secondary channel (when implemented by the DTE and DCE devices), which is equivalent to the primary channel. Pin assignments are described in following table:

Signal	Pin
Common Ground	7 (same as primary)
Secondary Transmitted Data (STD)	14
Secondary Received Data (SRD)	16
Secondary Request To Send (SRTS)	19
Secondary Clear To Send (SCTS)	13
Secondary Carrier Detect (SDCD)	12

Cables

The standard does not define a maximum cable length but instead defines the maximum capacitance that a compliant drive circuit must tolerate. A widely-used rule-of-thumb indicates that cables more than 50 feet (15 metres) long will have too much capacitance, unless special cables are used. By using low-capacitance cables, full speed communication can be maintained over larger distances up to about 1,000 feet.^[8] For longer distances, other signal standards are better suited to maintain high speed.

Since the standard definitions are not always correctly applied, it is often necessary to consult documentation, test connections with a breakout box, or use trial and error to find a cable that works when interconnecting two devices.

Connecting a fully-standard-compliant DCE device and DTE device would use a cable that connects identical pin numbers in each connector (a so-called "straight cable"). "Gender changers" are available to solve gender mismatches between cables and connectors. Connecting devices with different types of connectors requires a cable that connects the corresponding pins according to the table above. Cables with 9 pins on one end and 25 on the other are common. Manufacturers of equipment with 8P8C connectors usually provide a cable with either a DB-25 or DE-9 connector (or sometimes interchangeable connectors so they can work with multiple devices). Poor-quality cables can cause false signals by crosstalk between data and control lines (such as Ring Indicator). If a given cable will not allow a data connection, especially if a Gender changer is in use, a Null modem may be necessary.

Conventions

For functional communication through a serial port interface, conventions of bit rate, character framing, communications protocol, character encoding, data compression, and error detection, not defined in RS 232, must be agreed to by both sending and receiving equipment. For example, consider the serial ports of the original IBM PC. This implementation used an 8250 UART using asynchronous start-stop character formatting with 7 or 8 data bits per frame, usually ASCII character coding, and data rates programmable between 75 bits per second and 115,200 bits per second. Data rates above 20,000 bits per second are out of the scope of the standard, although higher data rates are sometimes used by commercially manufactured equipment. In the particular case of the IBM PC, baud rates were programmable with arbitrary values, so that a PC could be connected to, for example, MIDI music controllers (31,250 bits per second) or other devices not using the rates typically used with modems. Since most devices do not have automatic baud rate detection, users must manually set the baud rate (and all other parameters) at both ends of the RS-232 connection.

RTS/CTS handshaking

In older versions of the specification, RS-232's use of the RTS and CTS lines is asymmetric: The DTE asserts RTS to indicate a desire to transmit to the DCE, and the DCE asserts CTS in response to grant permission. This allows for half-duplex modems that disable their transmitters when not required, and must transmit a synchronization preamble to the receiver when they are re-enabled. This scheme is also employed on present-day RS-232 to RS-485 converters, where the RS-232's RTS signal is used to ask the converter to take control of the RS-485 bus - a concept that doesn't otherwise exist in RS-232. There is no way for the DTE to indicate that it is unable to accept data from the DCE.

A non-standard symmetric alternative, commonly called "RTS/CTS handshaking," was developed by various equipment manufacturers: CTS indicates permission from the DCE for the DTE to send data to the DCE (and is controlled by the DCE independent of RTS), and RTS indicates permission from the DTE for the DCE to send data to the DTE. This was eventually codified in version RS-232-E (actually TIA-232-E by that time) by defining a new signal, "RTR (Ready to Receive)," which is CCITT V.24 circuit 133. TIA-232-E and the corresponding international standards were updated to show that circuit 133, when implemented, shares the same pin as RTS (Request to Send), and that when 133 is in use, RTS is assumed by the DCE to be ON at all times.^[9]

Thus, with this alternative usage, one can think of RTS asserted (positive voltage, logic 0) meaning that the DTE is indicating it is "ready to receive" from the DCE, rather than requesting permission from the DCE to send characters to the DCE.

Note that equipment using this protocol must be prepared to buffer some extra data, since a transmission may have begun just before the control line state change.

3-wire and 5-wire RS-232

A minimal "3-wire" RS-232 connection consisting only of transmit data, receive data, and ground, is commonly used when the full facilities of RS-232 are not required. Even a two-wire connection (data and ground) can be used if the data flow is one way (for example, a digital postal scale that periodically sends a weight reading, or a GPS receiver that periodically sends position, if no configuration via RS-232 is necessary). When only hardware flow control is required in addition to two-way data, the RTS and CTS lines are added in a 5-wire version.

Seldom used features

The EIA-232 standard specifies connections for several features that are not used in most implementations. Their use requires the 25-pin connectors and cables, and of course both the DTE and DCE must support them.

Signal rate selection

The DTE or DCE can specify use of a "high" or "low" signaling rate. The rates as well as which device will select the rate must be configured in both the DTE and DCE. The prearranged device selects the high rate by setting pin 23 to ON.

Loopback testing

Many DCE devices have a loopback capability used for testing. When enabled, signals are echoed back to the sender rather than being sent on to the receiver. If supported, the DTE can signal the local DCE (the one it is connected to) to enter loopback mode by setting pin 18 to ON, or the remote DCE (the one the local DCE is connected to) to enter loopback mode by setting pin 21 to ON. The latter tests the communications link as well as both DCE's. When the DCE is in test mode it signals the DTE by setting pin 25 to ON.

A commonly used version of loopback testing doesn't involve any special capability of either end. A hardware loopback is simply a wire connecting complementary pins together in the same connector (see *loopback*).

Loopback testing is often performed with a specialized DTE called a bit error rate tester (or BERT).

Timing signals

Some synchronous devices provide a clock signal to synchronize data transmission, especially at higher data rates. Two timing signals are provided by the DCE on pins 15 and 17. Pin 15 is the transmitter clock, or send timing (ST); the DTE puts the next bit on the data line (pin 2) when this clock transitions from OFF to ON (so it is stable during the ON to OFF transition when the DCE registers the bit). Pin 17 is the receiver clock, or receive timing (RT); the DTE reads the next bit from the data line (pin 3) when this clock transitions from ON to OFF.

Alternatively, the DTE can provide a clock signal, called transmitter timing (TT), on pin 24 for transmitted data. Again, data is changed when the clock transitions from OFF to ON and read during the ON to OFF transition. TT can be used to overcome the issue where ST must traverse a cable of unknown length and delay, clock a bit out of the DTE after another unknown delay, and return it to the DCE over the same unknown cable delay. Since the relation between the transmitted bit and TT can be fixed in the DTE design, and since both signals traverse the same cable length, using TT eliminates the issue. TT may be generated by looping ST back with an appropriate phase change to align it with the transmitted data. ST loop back to TT lets the DTE use the DCE as the frequency reference, and correct the clock to data timing.

Related standards

Other serial signaling standards may not interoperate with standard-compliant RS-232 ports. For example, using the TTL levels of near +5 and 0 V puts the mark level in the undefined area of the standard. Such levels are sometimes used with NMEA 0183-compliant GPS receivers and depth finders.

A 20 mA current loop uses the absence of 20 mA current for high, and the presence of current in the loop for low; this signaling method is often used for long-distance and optically isolated links. Connection of a current-loop device to a compliant RS-232 port requires a level translator. Current-loop devices can supply voltages in excess of the withstand voltage limits of a compliant device. The original IBM PC serial port card implemented a 20 mA current-loop interface, which was never emulated by other suppliers of plug-compatible equipment.

Other serial interfaces similar to RS-232:

- RS-422 (a high-speed system similar to RS-232 but with differential signaling)
- RS-423 (a high-speed system similar to RS-422 but with unbalanced signaling)
- RS-449 (a functional and mechanical interface that used RS-422 and RS-423 signals - it never caught on like RS-232 and was withdrawn by the EIA)
- RS-485 (a descendant of RS-422 that can be used as a bus in multidrop configurations)
- MIL-STD-188 (a system like RS-232 but with better impedance and rise time control)
- EIA-530 (a high-speed system using RS-422 or RS-423 electrical properties in an EIA-232 pinout configuration, thus combining the best of both; supersedes RS-449)
- EIA/TIA-561 8 Position Non-Synchronous Interface Between Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange
- EIA/TIA-562 Electrical Characteristics for an Unbalanced Digital Interface (low-voltage version of EIA/TIA-232)
- TIA-574 (standardizes the 9-pin D-subminiature connector pinout for use with EIA-232 electrical signalling, as originated on the IBM PC/AT)
- SpaceWire (high-speed serial system designed for use on board spacecraft)

Development tools

When developing and/or troubleshooting RS-232, close examination of hardware signals can be very important to find problems. A serial line analyzer is a device similar to a logic analyzer but specialized for RS-232's voltage levels, connectors, and, where used, clock signals. The serial line analyzer can collect, store, and display the data and control signals, allowing developers to view them in detail. Some simply display the signals as waveforms; more elaborate versions include the ability to decode characters in ASCII or other common codes and to interpret common protocols used over RS-232 such as SDLC, HDLC, DDCMP, and X.25. Serial line analyzers are available as standalone units, as software and interface cables for general-purpose logic analyzers, and as programs that run in common personal computers.

References

- [1] Electronics Industries Association, "EIA Standard RS-232-C Interface Between Data Terminal Equipment and Data Communication Equipment Employing Serial Data Interchange", August 1969, reprinted in Telebyte Technology *Data Communication Library*, Greenlawn NY, 1985, no ISBN
- [2] RS232 Data Interface Tutorial (<http://www.arcelect.com/rs232.htm>)
- [3] TIA Web site (<http://www.tiaonline.org/business/about/>)
- [4] Paul Horowitz and Winfield Hill, *The Art of Electronics Second Edition*, Cambridge University Press, Cambridge MA, 1989, ISBN 0-521-37095-7, pages 723-726 for discussion of RS 232 limitations and application issues.
- [5] *PC 97 Hardware Design Guide* (<http://www.microsoft.com/whdc/archive/pcguides.mspx>). Redmond, Washington, USA: Microsoft Press. 1997. ISBN 1-57231-381-1. .
- [6] National Semiconductor Application Note AN-1031 "TIA/EIA-422-B Overview", January 2000, National Semiconductor Inc. (<http://www.national.com/an/AN/AN-1031.pdf>) page - evaluate the combination of cable length and data rate.
- [7] Joakim Ögren. "Serial (PC 9)" ([http://www.hardwarebook.info/Serial_\(PC_9\)](http://www.hardwarebook.info/Serial_(PC_9))). .
- [8] Tony Lawrence. "Serial Wiring" (<http://aplawrence.com/Unixart/serial.art.html>). .
- [9] ca...@gauss.llnl.gov (Casey Leedom) (1990-02-20). "[news:<49249@lll-winken.LLNL.GOV> Re: EIA-232 full duplex RTS/CTS flow control standard proposal]". [news:comp.dcom.modems comp.dcom.modems]. (Web link) (<http://groups.google.com/group/comp.dcom.modems/msg/39042605325cc765?dmode=source>). Retrieved on 2008-04-30.

RS-422

RS422	
Standard	EIA RS-422
Physical Media	Twisted Pair
Network Topology	Point-to-point, Multi-dropped
Maximum Devices	10 (1 driver & 10 receivers)
Maximum Distance	1200 metres (4000 feet)
Mode of Operation	Differential
Maximum Baud Rate	100Kbps - 10Mbps
Voltage Levels	-6V to +6V (maximum Voltage)
Mark(1)	Negative Voltages
Space(0)	Positive voltages
Available Signals	Tx+, Tx-, Rx+, Rx- (Full Duplex)
Connector types	Not specified, Commonly Screw terminals

RS-422 is a common short form and former official title of American National Standards Institute (ANSI) standard **ANSI/TIA/EIA-422-B** and its international equivalent **ITU-T Recommendation T-REC-V.11**,^[1] also known as **X.27**. These technical standards specify the electrical characteristics of the balanced voltage digital interface circuit^[2]. RS-422 provides for data transmission, using balanced or differential signaling, with unidirectional/non-reversible, terminated or non-terminated transmission lines, point to point, or multi-drop. In contrast to EIA-485 (which is multi-point instead of multi-drop), EIA-422/V.11 does not allow multiple drivers but only multiple receivers.

The current title of the ANSI standard is *TIA-422 Electrical Characteristics of Balanced Voltage Differential Interface Circuits* and is now in revision B, published in May 1994, and was reaffirmed by the Telecommunications Industry Association in 2005.

Several key advantages offered by this standard include the differential receiver, a differential driver and data rates as high as 10 megabaud at 12 metres (40 ft). The specification itself does not set an upper limit on data rate, but rather shows how signal rate degrades with cable length. The figure plotting this stops at 10 Mbit/s.

EIA-422 only specifies the electrical signaling characteristics of a single balanced signal. Protocols and pin assignments are defined in other specifications. The mechanical connections for this interface are specified by EIA-530 (DB-25 connector) or EIA-449 (DC-37 connector), however devices exist which have 4 screw-posts to implement the transmit and receive pair only. The maximum cable length is 1200 m. Maximum data rates are 10 Mbit/s at 12 m or 100 kbit/s at 1200 m. EIA-422 cannot implement a truly multi-point communications network (such as with EIA-485), however one driver can be connected to up to ten receivers.

A common use of EIA-422 is for RS-232 extenders. In video editing studios it is used to link control signals for all video and audio players/recorders to a central control board. Also, an RS-232-compatible variant of RS-422 using a mini-DIN-8 connector was widely used on Macintosh hardware until it was replaced by Intel's Universal Serial Bus on the iMac in 1998.

EIA-422 can interoperate with interfaces designed to MIL-STD-188-114B, but they are not identical. EIA-422 uses a nominal 0 to 5 volt signal while MIL-STD-188-114B uses a signal symmetric about 0 V. However the tolerance for common mode voltage in both specifications allows them to interoperate. Care must be taken with the termination network.

EIA-423 is a similar specification for unbalanced signaling.

When used in relation to communications wiring, RS-422 wiring refers to cable made of 2 sets of twisted pair, often with each pair being shielded, and a ground wire. While a double pair cable may be practical for many RS-422 applications, the RS-422 specification only defines one signal path and does not assign any function to it. Any complete cable assembly (i.e. with connectors) should be labeled with the specification that defined the signal function and mechanical layout of the connector, such as RS-449.

References

This article was originally based on material from the Free On-line Dictionary of Computing, which is licensed under the GFDL.

[1] <http://www.itu.int/rec/T-REC-V.11/en> V.11 ITU Recommendation T-REC-V.11

[2] TIA/EIA STANDARD, *Electrical Characteristics of Balanced Voltage Digital Interface Circuits, TIA/EIA-422-B*, May 1994

External links

- The Telecommunications Industry Association (<http://www.tiaonline.org/>)
- National Semiconductor Application Note AN-1031 "TIA/EIA-422-B Overview", January 2000, National Semiconductor Inc., retrieved from (<http://www.national.com/an/AN/AN-1031.pdf>)
- National Semiconductor Application Note AN-759 "Comparing EIA-485 and EIA-422-A Line Drivers and Receivers in Multipoint Applications", February 1991, National Semiconductor Inc., retrieved from (<http://www.national.com/an/AN/AN-759.pdf>)
- National Semiconductor Application Note AN-214 "Transmission Line Drivers and Receivers or TIA/EIA Standards RS-422 and RS-423" August 1993, National Semiconductor Inc., retrieved from (<http://www.national.com/an/AN/AN-214.pdf>)
- Maxim IC Application Note 723 "Selecting and Using RS-232, RS-422, and RS-485 Serial Data Standards" Dec 2000,

Maxim Integrated Products, Inc., retrieved from (http://www.maxim-ic.com/appnotes.cfm/appnote_number/723)

- Texas Instruments Application Report "422 and 485 Standards Overview and System Configurations" June 2002, Texas Instruments, retrieved from (<http://focus.ti.com/lit/an/slla070d/slla070d.pdf>)
- Texas Instruments Application Report SLLA067B "Comparing Bus Solutions" October 2009, Texas Instruments, retrieved from (<http://focus.ti.com/lit/an/slla067b/slla067b.pdf>)
- RS422 (http://www.usconverters.com/index.php?main_page=index&cPath=65) devices at U.S. Converters

EIA-485

RS-485	
Standard	EIA RS-485
Physical Media	Twisted Pair
Network Topology	Point-to-point, Multi-dropped, Multi-point
Maximum Devices	32 (32 drivers and 32 receivers)
Maximum Distance	1200 metres (4000 feet)
Mode of Operation	Differential
Maximum Baud Rate	100 kbit/s - 10 Mbit/s
Voltage Levels	-5 V to +5 V (max)
Mark(1)	Positive Voltages (B-A > +200 mV)
Space(0)	negative voltages (B-A < -200 mV)
Available Signals	Tx+/Rx+, Tx-/Rx- (Half Duplex) Tx+, Tx-, Rx+, Rx- (Full Duplex)
Connector types	Not specified.

EIA-485, also known as *TIA/EIA-485* or *RS-485*, is a standard defining the electrical characteristics of drivers and receivers for use in balanced digital multipoint systems. The standard is published by the ANSI Telecommunications Industry Association/Electronic Industries Alliance (TIA/EIA). Digital communications networks implementing the EIA-485 standard can be used effectively over long distances and in electrically noisy environments. Multiple receivers may be connected to such a network in a linear, multi-drop configuration. These characteristics make such networks useful in industrial environments and similar applications.

Overview

EIA-485 only specifies electrical characteristics of the driver and the receiver. It does not specify or recommend any communications protocol. EIA-485 enables the configuration of inexpensive local networks and multidrop communications links. It offers high data transmission speeds (35 Mbit/s up to 10 m and 100 kbit/s at 1200 m). Since it uses a differential balanced line over twisted pair (like EIA-422), it can span relatively large distances (up to 4000 feet or just over 1200 meters).

In contrast to EIA-422, which has a single driver circuit which cannot be switched off, EIA-485 drivers need to be put in transmit mode explicitly by asserting a signal to the driver. This allows EIA-485 to implement linear topologies using only two wires. The equipment located along a set of EIA-485 wires are interchangeably called nodes, stations and devices. ^[1]

The recommended arrangement of the wires is as a connected series of point-to-point (multidropped) nodes, a line or bus, not a star, ring, or multiply-connected network. Ideally, the two ends of the cable will have a termination resistor connected across the two wires. Without termination resistors, reflections of fast driver edges can cause multiple data edges that can cause data corruption. Termination resistors also reduce electrical noise sensitivity due to the lower impedance, and bias resistors (see below) are required. The value of each termination resistor should be equal to the cable impedance (typically, 120 ohms for twisted pairs).

Star and ring topologies are not recommended because of signal reflections or excessively low or high termination impedance. But if a star configuration is unavoidable, such as when controlling multiple pan-tilt-zoom video cameras from a central video surveillance hub, special EIA-485 star/hub repeaters are available which bidirectionally listen

for data on each span and then retransmit the data onto all other spans.

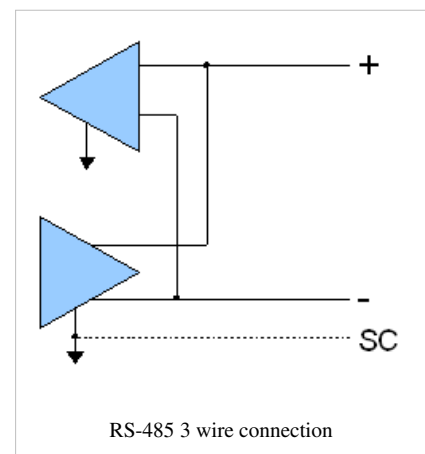
Somewhere along the set of wires, pull up or pull down resistors are established to Fail-safe bias each data line/wire when the lines are not being driven by any device. This way, the lines will be biased to known voltages and nodes will not interpret the noise from undriven lines as actual data; without biasing resistors, the data lines float in such a way that electrical noise sensitivity is greatest when all device stations are silent or unpowered.^[2]

Master-slave arrangement

Often in a master-slave arrangement when one device dubbed "the master" initiates all communication activity, the master device itself provides the bias and not the slave devices. In this configuration, the master device is typically centrally located along the set of EIA-485 wires, so it would be two slave devices located at the physical end of the wires that would provide the termination. The master device itself would provide termination if it were located at a physical end of the wires, but that is often a bad design^[3] as the master would be better located at a halfway point between the slave devices. Note that it is not a good idea to apply the bias at multiple node locations, because, by doing so, the effective bias resistance is lowered, which could possibly cause a violation of the EIA-485 specification and cause communications to malfunction. By keeping the biasing with the master, slave device design is simplified and this situation is avoided.

Three-wire connection

Even though the data is transmitted over a 2-wire twisted pair bus, all EIA-485 transceivers interpret the voltage levels of the differential signals with respect to a third common voltage. Without this common reference, a set of transceivers may interpret the differential signals incorrectly. In a typical setup, this third voltage is implied in the power supply common/ground connection. However, fundamentally speaking, there is nothing requiring this common voltage to be the same as the power supply. In fact, certain MS/TP (Master Slave / Token Passing) wiring requires full isolation between the various EIA-485 devices and have to run the third wire for the common connection.^[4]



Full duplex operation

EIA-485, like EIA-422 can be made full-duplex by using four wires. Since EIA-485 is a multi-point specification, however, this is not necessary in many cases. EIA-485 and EIA-422 can interoperate with certain restrictions.

Converters between EIA-485 and other formats are available to allow a personal computer to communicate with remote devices. By using "Repeaters" and "Multi-Repeaters" very large RS-485 networks can be formed. The Application Guidelines for TIA/EIA-485-A has one diagram called "Star Configuration. Not recommended." Using an RS-485 "Multi-Repeater" can allow for "Star Configurations" with "Home Runs" (or multi-drop) connections similar to Ethernet Hub/Star implementations (with greater distances). Hub/Star systems (with "Multi-Repeaters") allow for very maintainable systems, without violating any of the RS-485 specifications. Repeaters can also be used to extend the distance or number of nodes on a network.

Applications

EIA-485 signals are used in a wide range of computer and automation systems. In a computer system, SCSI-2 and SCSI-3 may use this specification to implement the physical layer for data transmission between a controller and a disk drive. EIA-485 is used for low-speed data communications in commercial aircraft cabins vehicle bus. It requires minimal wiring, and can share the wiring among several seats, reducing weight.

EIA-485 is used as the physical layer underlying many standard and proprietary automation protocols used to implement Industrial Control Systems, including the most common versions of Modbus and Profibus. These are used in programmable logic controllers and on factory floors. Since it is differential, it resists electromagnetic interference from motors and welding equipment.

In theatre and performance venues EIA-485 networks are used to control lighting and other systems using the DMX512 protocol.

EIA-485 is also used in building automation as the simple bus wiring and long cable length is ideal for joining remote devices. It may be used to control video surveillance systems or to interconnect security control panels and devices such as access control card readers.

Although many applications use EIA-485 signal levels, the speed, format, and protocol of the data transmission is not specified by EIA-485. Interoperation even of similar devices from different manufacturers is not assured by compliance with the signal levels alone.

Connectors

EIA-485 does not specify any connector or pinout. Circuits may be terminated on screw terminals, D-subminiature connectors, or other types of connectors.

Signs of common mistakes

From a software engineer's perspective, miswired RS-485 can lead to spurious characters because a spurious mark bit is seen. A bus without good pull up and pull down resistors will be noise-sensitive. These can be system-wide (albeit trivial) problems that require looking beyond just the CPU that is being programmed.

Pin labeling

The EIA-485 differential line consists of two pins:

- **A** aka '-' aka **TxD-/RxD-** aka **inverting** pin
- **B** aka '+' aka **TxD+/RxD+** aka **non-inverting** pin
- **SC** aka **G** aka **reference** pin

The SC line is the optional voltage reference connection. This is the reference potential used by the transceiver to measure the A and B voltages.

The B line is positive (compared to A) when the line is idle (i.e., data is 1).

In addition to the **A** and **B** connections, the EIA standard also specifies a third interconnection point called **C**, which is the common signal reference ground.

These names are all in use on various equipment, but the actual standard released by EIA only uses the names **A** and **B**. However, despite the unambiguous standard, there is much confusion about which is which:

The EIA-485 signaling specification states that signal **A** is the **inverting** or '-' pin and signal **B** is the **non-inverting** or '+' pin.^[5]

This is in conflict with the A/B naming used by a number of differential transceiver manufacturers, including, among others:

- Texas Instruments, as seen in their application handbook on EIA-422/485 communications (A=non-inverting, B=inverting)
- Intersil, as seen in their data sheet for the ISL4489 transceiver^[6]
- Maxim, as seen in their data sheet for the MAX483 transceiver^[7]

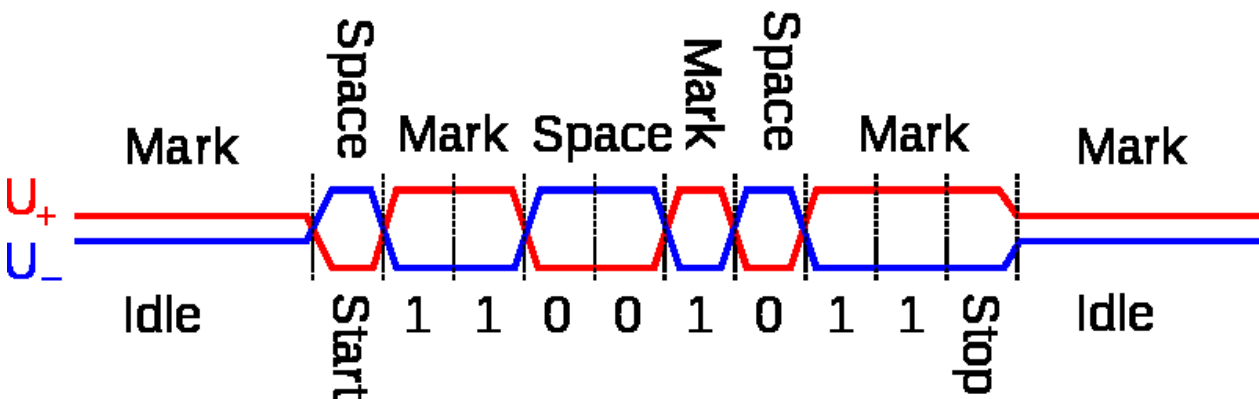
These manufacturers are incorrect, but their practice is in widespread use.

Therefore, care must be taken when using A/B naming.

The standard does not discuss cable shielding, but makes some recommendations on preferred methods of interconnecting the signal reference common and equipment case grounds.

Waveform example

The graph below shows potentials of the '+' and '-' pins of an EIA-485 line during transmission of one byte (0xD3, least significant bit first) of data using an asynchronous start-stop method.



References

- [1] Engineering Department, Electronic Industries Association, *EIA Standard RS-485 Electrical Characteristics of Generators and Receivers for Use in Balanced Multipoint Systems*, reprinted in Telebyte Technology "Data Communication Library" Greenlawn NY, 1985, no ISBN, no Library of Congress card number
- [2] <http://www.national.com/an/AN/AN-847.pdf>
- [3] <http://www.ccontrols.com.cn/pdf/Extv9n2.pdf>
- [4] <http://www.chipkin.com/articles/rs485-cables-why-you-need-3-wires-for-2-two-wire-rs485>
- [5] http://www.bb-europe.com/tech_articles/polarities_for_differential_pair_signals.asp
- [6] <http://www.intersil.com/data/fn/fn6074.pdf>
- [7] <http://datasheets.maxim-ic.com/en/ds/MAX1487-MAX491.pdf>

External links

- Guidelines for Proper Wiring of an RS-485 (TIA/EIA-485-A) Network (http://www.maxim-ic.com/appnotes.cfm?appnote_number=763&CMP=WP-1)
- Technical library of RS-485 articles and application notes (http://www.bb-elec.com/technical_library.asp)
- RS232 to RS485 cable scheme (http://pinouts.ru/SerialPortsCables/rs485_cable_pinout.shtml)
- Practical information about implementing RS485 (<http://www.lammertbies.nl/comm/info/RS-485.html>)
- Implementation of RS485 standard in the Linux OS (<http://retis.sssup.it/~scordino/code/rs485.html>)

Modbus

Modbus is a serial communications protocol published by Modicon in 1979 for use with its programmable logic controllers (PLCs). It has become a de facto standard communications protocol in industry, and is now the most commonly available means of connecting industrial electronic devices.^[1] The main reasons for the extensive use of Modbus over other communications protocols are:

1. It is openly published and royalty-free
2. Relatively easy industrial network to deploy
3. It moves raw bits or words without placing many restrictions on vendors

Modbus allows for communication between many devices connected to the same network, for example a system that measures temperature and humidity and communicates the results to a computer. Modbus is often used to connect a supervisory computer with a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems.

Suppliers large and small, system integrators, end users, open source developers, educators and other interested parties can become Modbus organization members. Some of the prominent members are SoftDEL Systems, Precision Digital Corporation, Motor Protection Electronics, FieldServer Technologies and many more^[2]

Protocol versions

Versions of the Modbus protocol exist for serial port and for Ethernet and other networks that support the Internet protocol suite. Most Modbus devices communicate over a serial EIA-485 physical layer [3]. There are many variants of Modbus protocols

- *Modbus RTU* — This is used in serial communication & makes use of a compact, binary representation of the data for protocol communication. The RTU format follows the commands/data with a cyclic redundancy check checksum as an error check mechanism to ensure the reliability of data. Modbus RTU is the most common implementation available for Modbus. A Modbus RTU message must be transmitted continuously without inter-character hesitations. Modbus messages are framed (separated) by idle (silent) periods.
- *Modbus ASCII* — This is used in serial communication & makes use of ASCII characters for protocol communication. The ASCII format uses a longitudinal redundancy check checksum. Modbus ASCII messages are framed by leading colon (':') and trailing newline (CR/LF).
- *Modbus TCP/IP or Modbus TCP* — This is a modbus variant used for communications over TCP/IP networks. It does not require a checksum calculation as lower layer takes care of the same.
- *Modbus over TCP/IP or Modbus over TCP* — This is a modbus variant that differs from Modbus TCP in that a checksum is included in the payload as with Modbus RTU.
- *Modbus Plus (Modbus+, MB+ or MBP)* — An extended version, Modbus Plus (Modbus+ or MB+), also exists, but remains proprietary to SCHNEIDER ELECTRIC. It requires a dedicated co-processor to handle fast HDLC-like token rotation. It uses twisted pair at 1 Mbit/s and includes transformer isolation at each node, which makes it transition/edge triggered instead of voltage/level triggered. Special interfaces are required to connect Modbus Plus to a computer, typically a card made for the ISA (SA85), PCI or PCMCIA bus.

Data model and function calls are identical for the first 4 variants of protocols; only the encapsulation is different. However the variants are not interoperable as the frame formats are different.

Communication and devices

Each device intended to communicate using Modbus is given a unique address. In serial and MB+ networks only the node assigned as the Master may initiate a command, but on Ethernet, any device can send out a Modbus command, although usually only one master device does so. A Modbus command contains the Modbus address of the device it is intended for. Only the intended device will act on the command, even though other devices might receive it (an exception is specific broadcastable commands sent to node 0 which are acted on but not acknowledged). All Modbus commands contain checking information, ensuring that a command arrives undamaged. The basic Modbus commands can instruct an RTU to change a value in one of its registers, control or read an I/O port, as well as commanding the device to send back one or more values contained in its registers.

There are many modems and gateways that support Modbus, as it is a very simple protocol and often copied. Some of them were specifically designed for this protocol. Different implementations use wireline, wireless communication and even SMS or GPRS. Typical problems the designers have to overcome include high latency and timing problems.

Frame Format

All modbus variants choose different frame formats ^[1].

Modbus RTU Frame Format		
Name	Length	Function
Start	3.5c idle	at least 3-1/2 character times of silence (MARK condition)
Address	8 bits	Station Address
Function	8 bits	Indicates the function codes like read coils / inputs
Data	n * 8 bits	Data + length will be filled depending on the message type
CRC Check	16 bits	Error checks
End	3.5c idle	at least 3-1/2 character times of silence between frames

Modbus ASCII Frame Format		
Name	Length	Function
Start	1 char	starts with colon (:) (ASCII value is 3A hex)
Address	2 chars	Station Address
Function	2 chars	Indicates the function codes like read coils / inputs
Data	n chars	Data +length will be filled depending on the message type
LRC Check	2 chars	Error checks
End	2 chars	carriage return – line feed(CRLF) pair (ASCII values of 0D & 0A hex)

Modbus TCP Frame Format		
Name	Length	Function
Transaction Identifier	2 bytes	<i>For synchronization between messages of server & client</i>
Protocol Identifier	2 bytes	<i>Zero for MODBUS/TCP</i>
Length Field	2 bytes	<i>Number of remaining bytes in this frame</i>
Unit Identifier	1 byte	<i>Slave Address (255 if not used)</i>
Function code	1 byte	<i>Function codes as in other variants</i>
Data bytes	n bytes	<i>Data as response or commands</i>

Unit identifier is used with MODBUS/TCP devices that are composites of several MODBUS devices, e.g. on MODBUS/TCP to MODBUS RTU gateways. In such case, the unit identifier tells the Slave Address of the device behind the gateway. Natively MODBUS/TCP-capable devices usually ignore the Unit Identifier.

Supported Function Codes

Modbus function codes / data types includes the following types ^[4] Most commonly used are given in *italics*.

- *01 Read Coil Status*
- *02 Read Input Status*
- *03 Read Holding Registers*
- *04 Read Input Registers*
- *05 Force Single Coil*
- *06 Preset Single Register*
- 07 Read Exception Status
- 08 Diagnostics
- 09 Program 484
- 10 Poll 484
- 11 Fetch Communication Event Counter
- 12 Fetch Communication Event Log
- 13 Program Controller
- 14 Poll Controller
- *15 Force Multiple Coils*
- *16 Preset Multiple Registers*
- 17 Report Slave ID
- 18 Program 884/M84
- 19 Reset Comm. Link
- 20 Read General Reference
- 21 Write General Reference
- 22 Mask Write 4X Register
- 23 Read/Write 4X Registers
- 24 Read FIFO Queue

Implementations

Almost all implementations have variations from the official standard. Different varieties might not communicate correctly between equipment of different suppliers. Some of the most common variations are:

- Data types
 - Floating point IEEE
 - 32-bit integer
 - 8-bit data
 - Mixed data types
 - Bit fields in integers
 - Multipliers to change data to/from integer. 10, 100, 1000, 256 ...
- Protocol extensions
 - 16-bit slave addresses
 - 32-bit data size (1 address = 32 bits of data returned.)
 - Word swapped data

Limitations

- Since Modbus was designed in the late 1970s to communicate to programmable logic controllers, the number of data types is limited to those understood by PLCs at the time. Large binary objects are not supported.
- No standard way exists for a node to find the description of a data object, for example, to determine if a register value represents a temperature between 30 and 175 degrees.
- Since Modbus is a master/slave protocol, there is no way for a field device to "report by exception" (except over Ethernet TCP/IP, called open-mbus)- the master node must routinely poll each field device, and look for changes in the data. This consumes bandwidth and network time in applications where bandwidth may be expensive, such as over a low-bit-rate radio link.
- Modbus is restricted to addressing 247 devices on one data link, which limits the number of field devices that may be connected to a master station (once again Ethernet TCP/IP proving the exception).
- Modbus transmissions must be contiguous which limits the types of remote communications devices to those that can buffer data to avoid gaps in the transmission.
- Modbus protocol provides no security against unauthorized commands or interception of data. ^[5]

Trade group

The *Modbus organization* is a trade association for the promotion and development of Modbus protocol.

References

- [1] Bill Drury, *Control Techniques Drives and Controls Handbook (2nd Edition)* . 2009, Institution of Engineering and Technology, Online version available at: http://knovel.com/web/portal/browse/display?_EXT_KNOVEL_DISPLAY_bookid=2995&VerticalID=0, page 508 and following
- [2] "Modbus members list" (<http://www.modbus.com/about.php>)
- [3] <http://www.obvius.com/documentation/faq/modbus.html>
- [4] Gordon Clarke, Deon Reynders *Practical Modern Scada Protocols: Dnp3, 60870.5 and Related Systems* ,Newnes, 2004 ISBN 0750657995 pages 47-51
- [5] Charles Palmer, Sujeet Sheno (ed) *Critical Infrastructure Protection III: Third IFIP WG 11. 10 International Conference, Hanover, New Hampshire, USA, March 23-25, 2009, Revised Selected Papers* Springer, 2009 ISBN 3642047971, page 87

External links

- (http://www.modbus.org/docs/PI_MBUS_300.pdf)
- Detailed Protocol Description (<http://www.modbus.org/specs.php>)
- Modbus Organization site (<http://www.modbus.org>)
- Protocol explanation for Java developers (<http://jamod.sourceforge.net/kbase/protocol.html>)
- A basic explanation on how modbus works (<http://www.simplymodbus.ca/FAQ.htm>)
- Industrial Ethernet Blog (<http://www.industrial-ethernet.org>)
- Free Modbus Master Simulator software (<http://en.radzio.dxp.pl/modbus-master-simulator/>)
- Free Modbus Device Testing Software (<http://www.globalmultimedia.in/modnet.htm>)

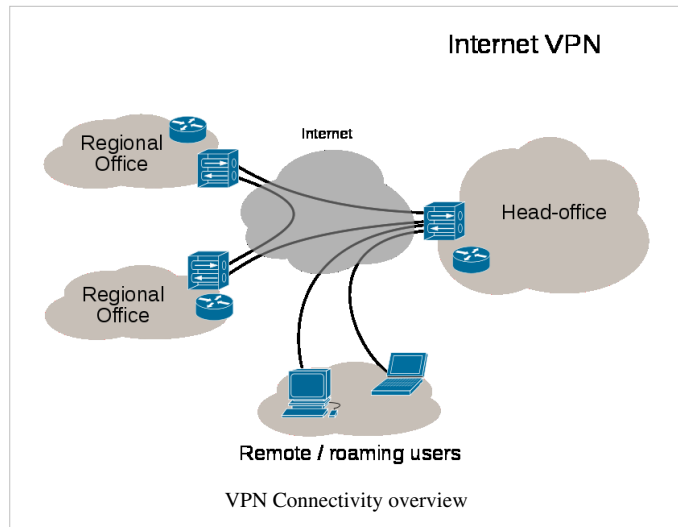
Open-source software

- An Open Source Modbus library in C for GNU/Linux, Mac OS X, FreeBSD, and QNX (<http://copyleft.free.fr/wordpress/index.php/libmodbus>)
- QModBus (<http://qmodbus.sourceforge.net/>) is a graphical Modbus master application for Linux and Windows.
- Free Modbus ASCII/RTU and TCP for microcontrollers (<http://freemodbus.berlios.de>). In C. New site location is <http://www.freemodbus.org> (<http://www.freemodbus.org/>). A commercially supported version is available at <http://www.embedded-solutions.at> (<http://www.embedded-solutions.at/>).
- Protocol::Modbus in Perl (<http://search.cpan.org/~cosimo/Protocol-Modbus-0.05/lib/Protocol/Modbus.pm>)
- Modbus::Client in Perl (<http://search.cpan.org/~dvklein/Modbus-Client-1.03/lib/Modbus/Client.pm>)
- Modbus master in Ruby (<http://www.messen-und-deuten.de/modbus.html>). Public domain sample code, can easily be re-implemented in other scripting languages.
- rmodbus (<http://rmodbus.herokuapp.com>). Free implementation of ModBus protocol in pure Ruby.
- jamod (<http://jamod.sourceforge.net/>). Implementation of ModBus protocol in Java.
- Modbus4J (<http://sourceforge.net/projects/modbus4j/>). Implementation of the ModBus protocol in Java. Part of the Mango M2M project.
- ModBus-Droid (<http://www.bencatlin.com/software-projects/modbus-droid/>). Modbus Scanner for Android based on a modified version of the Modbus4J library.
- node-modbus-stack (<https://github.com/TooTallNate/node-modbus-stack>). Open-source implementation of the Modbus protocol, written in JavaScript for NodeJS.
- pymodbus (<http://code.google.com/p/pymodbus/>). Free implementation of ModBus protocol in Python.
- modbus-tk (<http://code.google.com/p/modbus-tk/>). Another implementation of Modbus Protocol in Python
- MBLogic - Free implementation of Modbus/TCP in Python (<http://mblogic.sourceforge.net>)

Virtual private network

A **virtual private network (VPN)** is a computer network that uses a public telecommunication infrastructure such as the Internet to provide remote offices or individual users with secure access to their organization's network. It aims to avoid an expensive system of owned or leased lines that can be used by only one organization.

It encapsulates data transfers between two or more networked devices which are not on the same private network so as to keep the transferred data private from other devices on one or more intervening local or wide area networks. There are many different classifications, implementations, and uses for VPNs.



History

Until the end of the 1990s networked computers were connected through expensive leased lines and/or dial-up phone lines.

Virtual Private Networks reduce network costs because they avoid a need for many leased lines that individually connect to the Internet. Users can exchange private data securely, making the expensive leased lines unnecessary.^[1]

VPN technologies have myriad protocols, terminologies and marketing influences that define them. For example, VPN technologies can differ in:

- The protocols they use to tunnel the traffic
- The tunnel's termination point, i.e., customer edge or network provider edge
- Whether they offer site-to-site or remote access connectivity
- The levels of security provided
- The OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity

Some classification schemes are discussed in the following sections.

Security Mechanisms

Secure VPNs use cryptographic tunneling protocols to provide confidentiality by blocking intercepts and packet sniffing, allowing sender authentication to block identity spoofing, and provide message integrity by preventing message alteration.

Secure VPN protocols include the following:

- IPsec (Internet Protocol Security) was originally developed for IPv6, which requires it. This standards-based security protocol is also widely used with IPv4. L2TP frequently runs over IPsec.
- Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic, as it does in the OpenVPN project, or secure an individual connection. A number of vendors provide remote access VPN capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules.
- Datagram Transport Layer Security (DTLS), is used in Cisco's next-generation VPN product, Cisco AnyConnect VPN, to solve the issues SSL/TLS has with tunneling over TCP.

- Microsoft Point-to-Point Encryption (MPPE) works with their PPTP and in several compatible implementations on other platforms.
- Microsoft introduced Secure Socket Tunneling Protocol (SSTP) in Windows Server 2008 and Windows Vista Service Pack 1. SSTP tunnels Point-to-Point Protocol (PPP) or L2TP traffic through an SSL 3.0 channel.
- MPVPN (Multi Path Virtual Private Network). Ragula Systems Development Company owns the registered trademark "MPVPN".^[2]
- Secure Shell (SSH) VPN -- OpenSSH offers VPN tunneling to secure remote connections to a network or inter-network links. This should not be confused with port forwarding. OpenSSH server provides limited number of concurrent tunnels and the VPN feature itself does not support personal authentication.^{[3] [4] [5]}

Authentication

Tunnel endpoints must authenticate before secure VPN tunnels can establish.

User-created remote access VPNs may use passwords, biometrics, two-factor authentication or other cryptographic methods.

Network-to-network tunnels often use passwords or digital certificates, as they permanently store the key to allow the tunnel to establish automatically and without intervention.

Routing

Tunneling protocols can be used in a point-to-point topology that would theoretically not be considered a VPN, because a VPN by definition is expected to support arbitrary and changing sets of network nodes. But since most router implementations support a software-defined tunnel interface, customer-provisioned VPNs often are simply defined tunnels running conventional routing protocols.

On the other hand provider-provided VPNs (PPVPNs) need to support coexisting multiple VPNs, hidden from one another, but operated by the same service provider.

PPVPN Building blocks

Depending on whether the PPVPN runs in layer 2 or layer 3, the building blocks described below may be L2 only, L3 only, or combine them both. Multiprotocol Label Switching (MPLS) functionality blurs the L2-L3 identity.

RFC 4026 generalized the following terms to cover L2 and L3 VPNs, but they were introduced in RFC 2547.^[6]

Customer edge device. (CE)

a device at the customer premises, that provides access to the PPVPN. Sometimes it's just a demarcation point between provider and customer responsibility. Other providers allow customers to configure it.

Provider edge device (PE)

A PE is a device, or set of devices, at the edge of the provider network, that presents the provider's view of the customer site. PEs are aware of the VPNs that connect through them, and maintain VPN state.

Provider device (P)

A P device operates inside the provider's core network, and does not directly interface to any customer endpoint. It might, for example, provide routing for many provider-operated tunnels that belong to different customers' PPVPNs. While the P device is a key part of implementing PPVPNs, it is not itself VPN-aware and does not maintain VPN state. Its principal role is allowing the service provider to scale its PPVPN offerings, as, for example, by acting as an aggregation point for multiple PEs. P-to-P connections, in such a role, often are high-capacity optical links between major locations of provider.

User-visible PPVPN services

This section deals with the types of VPN considered in the IETF; some historical names were replaced by these terms.

OSI Layer 1 services

Virtual private wire and private line services (VPWS and VPLS)

In both of these services, the service provider does not offer a full routed or bridged network, but provides components to build customer-administered networks. VPWS are point-to-point while VPLS can be point-to-multipoint. They can be Layer 1 emulated circuits with no data link structure.

The customer determines the overall customer VPN service, which also can involve routing, bridging, or host network elements.

An unfortunate acronym confusion can occur between Virtual Private Line Service and Virtual Private LAN Service; the context should make it clear whether "VPLS" means the layer 1 virtual private line or the layer 2 virtual private LAN.

OSI Layer 2 services

Virtual LAN

A Layer 2 technique that allows for the coexistence of multiple LAN broadcast domains, interconnected via trunks using the IEEE 802.1Q trunking protocol. Other trunking protocols have been used but have become obsolete, including Inter-Switch Link (ISL), IEEE 802.10 (originally a security protocol but a subset was introduced for trunking), and ATM LAN Emulation (LANE).

Virtual private LAN service (VPLS)

Developed by IEEE, VLANs allow multiple tagged LANs to share common trunking. VLANs frequently comprise only customer-owned facilities. The former is a layer 1 technology that supports emulation of both point-to-point and point-to-multipoint topologies. The method discussed here extends Layer 2 technologies such as 802.1d and 802.1q LAN trunking to run over transports such as Metro Ethernet.

As used in this context, a VPLS is a Layer 2 PPVPN, rather than a private line, emulating the full functionality of a traditional local area network (LAN). From a user standpoint, a VPLS makes it possible to interconnect several LAN segments over a packet-switched, or optical, provider core; a core transparent to the user, making the remote LAN segments behave as one single LAN.^[7]

In a VPLS, the provider network emulates a learning bridge, which optionally may include VLAN service.

Pseudo wire (PW)

PW is similar to VPWS, but it can provide different L2 protocols at both ends. Typically, its interface is a WAN protocol such as Asynchronous Transfer Mode or Frame Relay. In contrast, when aiming to provide the appearance of a LAN contiguous between two or more locations, the Virtual Private LAN service or IPLS would be appropriate.

IP-only LAN-like service (IPLS)

A subset of VPLS, the CE devices must have L3 capabilities; the IPLS presents packets rather than frames. It may support IPv4 or IPv6.

OSI Layer 3 PPVPN architectures

This section discusses the main architectures for PPVPNs, one where the PE disambiguates duplicate addresses in a single routing instance, and the other, virtual router, in which the PE contains a virtual router instance per VPN. The former approach, and its variants, have gained the most attention.

One of the challenges of PPVPNs involves different customers using the same address space, especially the IPv4 private address space.^[8] The provider must be able to disambiguate overlapping addresses in the multiple customers' PPVPNs.

BGP/MPLS PPVPN

In the method defined by RFC 2547, BGP extensions advertise routes in the IPv4 VPN address family, which are of the form of 12-byte strings, beginning with an 8-byte Route Distinguisher (RD) and ending with a 4-byte IPv4 address. RDs disambiguate otherwise duplicate addresses in the same PE.

PEs understand the topology of each VPN, which are interconnected with MPLS tunnels, either directly or via P routers. In MPLS terminology, the P routers are Label Switch Routers without awareness of VPNs.

Virtual router PPVPN

The Virtual Router architecture,^{[9] [10]} as opposed to BGP/MPLS techniques, requires no modification to existing routing protocols such as BGP. By the provisioning of logically independent routing domains, the customer operating a VPN is completely responsible for the address space. In the various MPLS tunnels, the different PPVPNs are disambiguated by their label, but do not need routing distinguishers.

Virtual router architectures do not need to disambiguate addresses, because rather than a PE router having awareness of all the PPVPNs, the PE contains multiple virtual router instances, which belong to one and only one VPN.

Plaintext Tunnels

Some virtual networks may not use encryption to protect the data contents. While VPNs often provide security, an unencrypted overlay network does not neatly fit within the secure or trusted categorization. For example a tunnel set up between two hosts that used Generic Routing Encapsulation (GRE) would in fact be a virtual private network, but neither secure nor trusted.

Besides the GRE example above, native plaintext tunneling protocols include Layer 2 Tunneling Protocol (L2TP) when it is set up without IPsec and Point-to-Point Tunneling Protocol (PPTP) or Microsoft Point-to-Point Encryption (MPPE).

Trusted delivery networks

Trusted VPNs do not use cryptographic tunneling, and instead rely on the security of a single provider's network to protect the traffic.

- Multi-Protocol Label Switching (MPLS) is often used to overlay VPNs, often with quality-of-service control over a trusted delivery network.
- Layer 2 Tunneling Protocol (L2TP)^[11] which is a standards-based replacement, and a compromise taking the good features from each, for two proprietary VPN protocols: Cisco's Layer 2 Forwarding (L2F)^[12] (obsolete as of 2009) and Microsoft's Point-to-Point Tunneling Protocol (PPTP).^[13]

From the security standpoint, VPNs either trust the underlying delivery network, or must enforce security with mechanisms in the VPN itself. Unless the trusted delivery network runs among physically secure sites only, both trusted and secure models need an authentication mechanism for users to gain access to the VPN.

VPNs in mobile environments

Mobile VPNs are used in a setting where an endpoint of the VPN is not fixed to a single IP address, but instead roams across various networks such as data networks from cellular carriers or between multiple Wi-Fi access points.^[14] Mobile VPNs have been widely used in public safety, where they give law enforcement officers access to mission-critical applications, such as computer-assisted dispatch and criminal databases, as they travel between different subnets of a mobile network.^[15] They are also used in field service management and by healthcare organizations,^[16] among other industries.

Increasingly, mobile VPNs are being adopted by mobile professionals and white-collar workers who need reliable connections.^[16] They allow users to roam seamlessly across networks and in and out of wireless-coverage areas without losing application sessions or dropping the secure VPN session. A conventional VPN cannot survive such events because the network tunnel is disrupted, causing applications to disconnect, time out,^[14] or fail, or even cause the computing device itself to crash.^[16]

Instead of logically tying the endpoint of the network tunnel to the physical IP address, each tunnel is bound to a permanently associated IP address at the device. The mobile VPN software handles the necessary network authentication and maintains the network sessions in a manner transparent to the application and the user.^[14] The Host Identity Protocol (HIP), under study by the Internet Engineering Task Force, is designed to support mobility of hosts by separating the role of IP addresses for host identification from their locator functionality in an IP network. With HIP a mobile host maintains its logical connections established via the host identity identifier while associating with different IP addresses when roaming between access networks.

References

- [1] Feilner, Markus. "Chapter 1 - VPN—Virtual Private Network". OpenVPN: Building and Integrating Virtual Private Networks: Learn How to Build Secure VPNs Using this Powerful Open Source Application. Packt Publishing.
- [2] Trademark Applications and Registrations Retrieval (TARR) (<http://tarr.uspto.gov/servlet/tarr?regser=serial&entry=78063238&action=Request+Status>)
- [3] OpenBSD ssh manual page, VPN section (<http://www.openbsd.org/cgi-bin/man.cgi?query=ssh#SSH-BASED+VIRTUAL>)
- [4] Unix Toolbox section on SSH VPN (<http://cb.vu/unixtoolbox.xhtml#vpn>)
- [5] Ubuntu SSH VPN how-to (https://help.ubuntu.com/community/SSH_VPN)
- [6] E. Rosen & Y. Rekhter (March 1999). "RFC 2547 BGP/MPLS VPNs" (<http://www.ietf.org/rfc/rfc2547.txt>). Internet Engineering Task Force (IETF).
- [7] *Ethernet Bridging (OpenVPN)* (<http://openvpn.net/index.php/access-server/howto-openvpn-as/214-how-to-setup-layer-2-ethernet-bridging.html>),
- [8] Address Allocation for Private Internets (<http://www.ietf.org/rfc/rfc1918.txt>), RFC 1918, Y. Rekhter *et al.*, February 1996
- [9] RFC 2917, *A Core MPLS IP VPN Architecture*
- [10] RFC 2918, K. Muthukrishnan & A. Malis (September 2000)
- [11] Layer Two Tunneling Protocol "L2TP" (<http://www.ietf.org/rfc/rfc2661.txt>), RFC 2661, W. Townsley *et al.*, August 1999
- [12] IP Based Virtual Private Networks (<http://www.ietf.org/rfc/rfc2341.txt>), RFC 2341, A. Valencia *et al.*, May 1998
- [13] Point-to-Point Tunneling Protocol (PPTP) (<http://www.ietf.org/rfc/rfc2637.txt>), RFC 2637, K. Hamzeh *et al.*, July 1999
- [14] Phifer, Lisa. "Mobile VPN: Closing the Gap" (http://searchmobilecomputing.techtarget.com/tip/0,289483,sid40_gci1210989_mem1,00.html), *SearchMobileComputing.com*, July 16, 2006.
- [15] Willett, Andy. "Solving the Computing Challenges of Mobile Officers" ([http://www.officer.com/print/Law-Enforcement-Technology/Solving-the-Computing-Challenges-of-Mobile-Officers/1\\$30992](http://www.officer.com/print/Law-Enforcement-Technology/Solving-the-Computing-Challenges-of-Mobile-Officers/1$30992)), *www.officer.com*, May, 2006.
- [16] Cheng, Roger. "Lost Connections" (<http://online.wsj.com/article/SB119717610996418467.html>), *The Wall Street Journal*, December 11, 2007.

External links

- JANET UK "Different Flavours of VPN: Technology and Applications" (<http://www.ja.net/documents/development/vpn/different-flavours-of-vpn-web.pdf>)
- Virtual Private Network Consortium - a trade association for VPN vendors (<http://www.vpnc.org/>)
- CShip VPN-Wiki/List (http://en.cship.org/wiki/Virtual_Private_Network)
- Virtual Private Networks (<http://www.microsoft.com/vpn>) on Microsoft TechNet
- Creating VPNs with IPsec and SSL/TLS (<http://www.linuxjournal.com/article/9916>) Linux Journal article by Rami Rosen
- Setting up vpn with PPTP (<http://techtalk.pipitlabs.com/configure-linux-as-pptp-gateway>)
- Setting up vpn with IPSEC/L2TP (<http://techtalk.pipitlabs.com/configure-l2tpdipsec-vpn-in-linux>)
- QuickTun (<http://wiki.ucis.nl/QuickTun>) Simple VPN software based on D.J. Bernstein's NaCl cryptography library

Layer 2 Tunneling Protocol

In computer networking, **Layer 2 Tunneling Protocol (L2TP)** is a tunneling protocol used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy.^[1]

Although L2TP acts like a Data Link Layer protocol in the OSI model, L2TP is in fact a Session Layer protocol,^[2] and uses the registered UDP port 1701. (*see List of TCP and UDP port numbers*).

History and future

Published in 1999 as proposed standard RFC 2661, L2TP has its origins primarily in two older tunneling protocols for PPP: Cisco's Layer 2 Forwarding Protocol (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). A new version of this protocol, L2TPv3, was published as proposed standard RFC 3931 in 2005. L2TPv3 provides additional security features, improved encapsulation, and the ability to carry data links other than simply PPP over an IP network (e.g., Frame Relay, Ethernet, ATM, etc).

Description

The entire L2TP packet, including payload and L2TP header, is sent within a UDP datagram. It is common to carry Point-to-Point Protocol (PPP) sessions within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec (discussed below).

The two endpoints of an L2TP tunnel are called the *LAC (L2TP Access Concentrator)* and the *LNS (L2TP Network Server)*. The LAC is the initiator of the tunnel while the LNS is the server, which waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional. To be useful for networking, higher-level protocols are then run through the L2TP tunnel. To facilitate this, an *L2TP session (or call)* is established within the tunnel for each higher-level protocol such as PPP. Either the LAC or LNS may initiate sessions. The traffic for each session is isolated by L2TP, so it is possible to set up multiple virtual networks across a single tunnel. MTU should be considered when implementing L2TP.

The packets exchanged within an L2TP tunnel are categorised as either *control packets* or *data packets*. L2TP provides reliability features for the control packets, but no reliability for data packets. Reliability, if desired, must be provided by the nested protocols running within each session of the L2TP tunnel.

Tunneling models

An L2TP tunnel can extend across an entire PPP session or only across one segment of a two-segment session. This can be represented by four different tunneling models, namely [3] [4] [5]

- *voluntary tunnel*
- *compulsory tunnel — incoming call*
- *compulsory tunnel — remote dial*
- *L2TP multi-hop connection*

L2TP packet structure

An L2TP packet consists of :

Bits 0–15	Bits 16–31
Flags and Version Info	Length (opt)
Tunnel ID	Session ID
Ns (opt)	Nr (opt)
Offset Size (opt)	Offset Pad (opt).....
Payload data	

Field meanings:

Flags and version

control flags indicating data/control packet and presence of length, sequence, and offset fields.

Length (optional)

Total length of the message in bytes, present only when length flag is set.

Tunnel ID

Indicates the identifier for the control connection.

Session ID

Indicates the identifier for a session within a tunnel.

Ns (optional)

sequence number for this data or control message, beginning at zero and incrementing by one (modulo 2^{16}) for each message sent. Present only when sequence flag set.

Nr (optional)

sequence number for expected message to be received. Nr is set to the Ns of the last in-order message received plus one (modulo 2^{16}). In data messages, Nr is reserved and, if present (as indicated by the S bit), MUST be ignored upon receipt..

Offset Size (optional)

Specifies where payload data is located past the L2TP header. If the offset field is present, the L2TP header ends after the last byte of the offset padding. This field exists if the offset flag is set.

Offset Pad (optional)

Variable length, as specified by the offset size. Contents of this field are undefined.

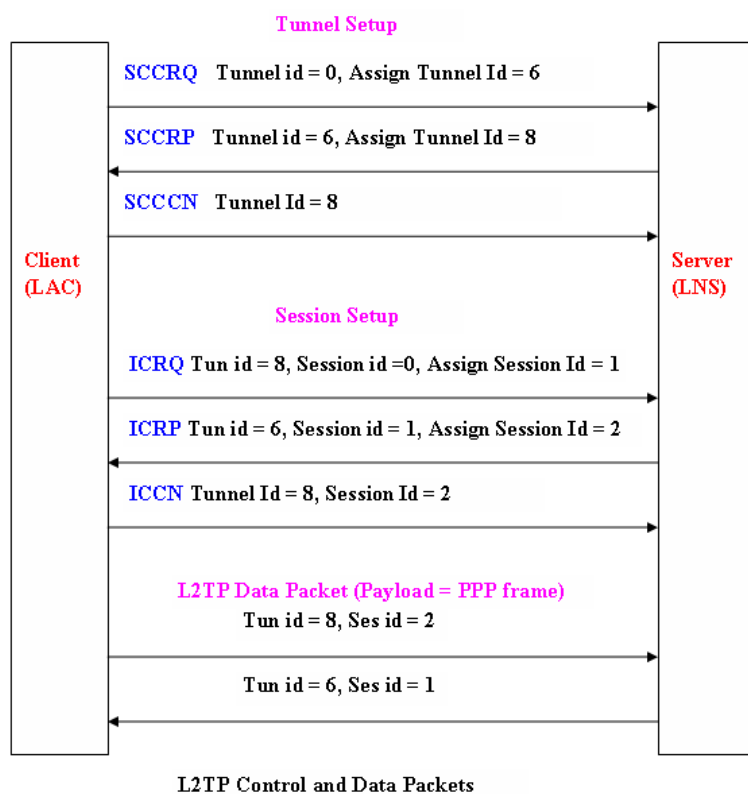
Payload data

Variable length (Max payload size = Max size of UDP packet – size of L2TP header)

L2TP packet exchange

At the time of setup of L2TP connection, many control packets are exchanged between server and client to establish tunnel and session for each direction. One peer requests the other peer to assign a specific tunnel and session id through these control packets. Then using this tunnel and session id, data packets are exchanged with the compressed PPP frames as payload.

The list of L2TP Control messages exchanged between LAC and LNS, for handshaking before establishing a tunnel and session in voluntary tunneling method are



L2TP/IPsec

Because of the lack of confidentiality inherent in the L2TP protocol, it is often implemented along with IPsec. This is referred to as L2TP/IPsec, and is standardized in IETF RFC 3193. The process of setting up an L2TP/IPsec VPN is as follows:

1. Negotiation of IPsec security association (SA), typically through *Internet key exchange* (IKE). This is carried out over UDP port 500, and commonly uses either a shared password (so-called "pre-shared keys"), public keys, or X.509 certificates on both ends, although other keying methods exist.
2. Establishment of Encapsulating Security Payload (ESP) communication in transport mode. The IP protocol number for ESP is 50 (compare TCP's 6 and UDP's 17). At this point, a secure channel has been established, but no tunneling is taking place.
3. Negotiation and establishment of L2TP tunnel between the SA endpoints. The actual negotiation of parameters takes place over the SA's secure channel, within the IPsec encryption. L2TP uses UDP port 1701.

When the process is complete, L2TP packets between the endpoints are encapsulated by IPsec. Since the L2TP packet itself is wrapped and hidden within the IPsec packet, no information about the internal private network can be garnered from the encrypted packet. Also, it is not necessary to open UDP port 1701 on firewalls between the endpoints, since the inner packets are not acted upon until after IPsec data has been decrypted and stripped, which

only takes place at the endpoints.

A potential point of confusion in L2TP/IPsec is the use of the terms '*tunnel*' and '*secure channel*'. The term '*tunnel*' refers to a channel which allows untouched packets of one network to be transported over another network. In the case of L2TP/PPP, it allows L2TP/PPP packets to be transported over IP. A '*secure channel*' refers to a connection within which the confidentiality of all data is guaranteed. In L2TP/IPsec, first IPsec provides a secure channel, then L2TP provides a tunnel.

Windows implementation

Windows Vista provides two new configuration utilities that attempt to make using L2TP without IPsec easier, both described in sections that follow below:

- an MMC snap-in called "Windows Firewall with Advanced Security" (WFWAS), located in Control Panel → Administrative Tools
- the "netsh advfirewall" command-line tool

Both these configuration utilities are not without their difficulties, and unfortunately, there is very little documentation about both "netsh advfirewall" and the IPsec client in WFWAS. One of the aforementioned difficulties is that it is not compatible with NAT. Another problem is that servers must be specified only by IP address in the new Vista configuration utilities; the hostname of the server cannot be used, so if the IP address of the IPsec server changes, all clients will have to be informed of this new IP address (which also rules out servers that addressed by utilities such as DynDNS).

L2TP in ADSL networks

L2TP is often used as a tunneling mechanism to resell ADSL endpoint connectivity at layer 2. An L2TP tunnel would sit between the user and the ISP the connection would be resold to, so the reselling ISP would not appear as doing the transport.

L2TP in cable networks

L2TP is used by the cable Internet provider as a tunnelling mechanism to sell endpoint connectivity. The L2TP tunnel sits between the user and the ISP. Again, the reselling cable provider doesn't appear as doing the transport.

References

- [1] IETF (1999), RFC 2661, Layer Two Tunneling Protocol "L2TP"
- [2] Cisco Systems, Inc., Cisco Active Network Abstraction Technology Support and Information Model Reference Manual, Version 3.6, Chapter 9 (http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.6/master_tech/9l2tp.pdf), Layer 2 Tunnel Protocol "L2TP"
- [3] <http://publib.boulder.ibm.com/infocenter/series/v5r3/index.jsp?topic=/rzaiz/rzaiymultihop.htm>
- [4] http://www.cisco.com/en/US/tech/tk827/tk369/tk388/tsd_technology_support_sub-protocol_home.html
- [5] <http://technet2.microsoft.com/WindowsServer/en/library/04bd5817-0e41-46b7-9dda-d6340fce514f1033.mspx>

External links

Implementations

- Cisco: Cisco L2TP documentation (http://www.cisco.com/en/US/docs/ios/12_0t/12_0t1/feature/guide/l2tpT.html), also read Technology brief from Cisco (http://www.cisco.com/warp/public/cc/pd/iosw/tech/l2pro_tc.htm)
- Open source and Linux: xl2tpd (<http://www.xelerance.com/software/xl2tpd/>), Linux RP-L2TP (<http://sourceforge.net/projects/rp-l2tp/>), OpenL2TP (<http://sourceforge.net/projects/openl2tp/>), l2tpns (<http://>

- l2tpns.sourceforge.net/), l2tpd (<http://sourceforge.net/projects/l2tpd/>) (inactive), Linux L2TP/IPsec server (<http://www.zeroshell.net/eng/vpndetails/>), FreeBSD multi-link PPP daemon (<http://mpd.sourceforge.net/>)
- Microsoft: built-in client included with Windows 2000 and higher; Microsoft L2TP/IPsec VPN Client (<http://www.microsoft.com/technet/prodtechnol/windows2000serv/support/vpnclientag.msp>) for Windows 98/Windows Me/Windows NT 4.0
 - Apple: built-in client included with Mac OS X 10.3 and higher.
 - Setting up IPSEC/L2TP in Linux (<http://techtalk.pipitlabs.com/configure-l2tpdipsec-vpn-in-linux>)

Internet standards and extensions

- RFC 2341 *Cisco Layer Two Forwarding (Protocol) "L2F"* (a predecessor to L2TP)
- RFC 2637 *Point-to-Point Tunneling Protocol (PPTP)* (a predecessor to L2TP)
- RFC 2661 *Layer Two Tunneling Protocol "L2TP"*
- RFC 2809 *Implementation of L2TP Compulsory Tunneling via RADIUS*
- RFC 2888 *Secure Remote Access with L2TP*
- RFC 3070 *Layer Two Tunneling Protocol (L2TP) over Frame Relay*
- RFC 3145 *L2TP Disconnect Cause Information*
- RFC 3193 *Securing L2TP using IPsec*
- RFC 3301 *Layer Two Tunneling Protocol (L2TP): ATM access network*
- RFC 3308 *Layer Two Tunneling Protocol (L2TP) Differentiated Services*
- RFC 3355 *Layer Two Tunneling Protocol (L2TP) Over ATM Adaptation Layer 5 (AAL5)*
- RFC 3371 *Layer Two Tunneling Protocol "L2TP" Management Information Base*
- RFC 3437 *Layer Two Tunneling Protocol Extensions for PPP Link Control Protocol Negotiation*
- RFC 3438 *Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers: Internet Assigned Numbers Authority (IANA) Considerations Update*
- RFC 3573 *Signaling of Modem-On-Hold status in Layer 2 Tunneling Protocol (L2TP)*
- RFC 3817 *Layer 2 Tunneling Protocol (L2TP) Active Discovery Relay for PPP over Ethernet (PPPoE)*
- RFC 3931 *Layer Two Tunneling Protocol - Version 3 (L2TPv3)*
- RFC 4045 *Extensions to Support Efficient Carrying of Multicast Traffic in Layer-2 Tunneling Protocol (L2TP)*
- RFC 4951 *Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover"*

Other

- IANA assigned numbers for L2TP (<http://www.iana.org/assignments/l2tp-parameters>)
 - L2TP Extensions Working Group (l2tpext) (<http://www.ietf.org/html.charters/l2tpext-charter.html>) - (*where future standardization work is being coordinated*)
 - Using Linux as an L2TP/IPsec VPN client (<http://www.jacco2.dds.nl/networking/linux-l2tp.html>)
 - Configuring L2TP VPN in Windows (http://alivevpn.com/l2tp_vpn_account_settings)
-

Network address translation

In computer networking, **network address translation** (NAT) is the process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device for the purpose of remapping one IP address space into another.

Most often today, NAT is used in conjunction with *network masquerading* (or *IP masquerading*) which is a technique that hides an entire IP address space, usually consisting of private network IP addresses (RFC 1918), behind a single IP address in another, often public address space. This mechanism is implemented in a routing device that uses stateful translation tables to map the "hidden" addresses into a single IP address and readdresses the outgoing Internet Protocol (IP) packets on exit so that they appear to originate from the router. In the reverse communications path, responses are mapped back to the originating IP address using the rules ("state") stored in the translation tables. The translation table rules established in this fashion are flushed after a short period unless new traffic refreshes their state.

As described, the method enables communication through the router only when the conversation originates in the masqueraded network, since this establishes the translation tables. For example, a web browser in the masqueraded network can browse a website outside, but a web browser outside could not browse a web site in the masqueraded network. However, most NAT devices today allow the network administrator to configure translation table entries for permanent use. This feature is often referred to as "static NAT" or port forwarding and allows traffic originating in the "outside" network to reach designated hosts in the masqueraded network.

Because of the popularity of this technique (see below), the term *NAT* has become virtually synonymous with the method of IP masquerading.

Network address translation has serious consequences, both drawbacks and benefits, on the quality of Internet connectivity and requires careful attention to the details of its implementation. As a result, many methods have been devised to alleviate the issues encountered. See the article on *NAT traversal*.

Overview

In the mid-1990s NAT became a popular tool for alleviating the consequences of IPv4 address exhaustion. It has become a standard, indispensable feature in routers for home and small-office Internet connections.

Most systems using NAT do so in order to enable multiple hosts on a private network to access the Internet using a single public IP address (see gateway). However, NAT breaks the originally envisioned model of IP end-to-end connectivity across the Internet, introduces complications in communication between hosts, and affects performance.

NAT obscures an internal network's structure: all traffic appears to outside parties as if it originated from the gateway machine.

Network address translation involves over-writing the source or destination IP address and usually also the TCP/UDP port numbers of IP packets as they pass through the router. Checksums (both IP and TCP/UDP) must also be rewritten as a result of these changes.

In a typical configuration, a local network uses one of the designated "private" IP address subnets (RFC 1918). Private Network Addresses are 192.168.x.x, 172.16.x.x through 172.31.x.x, and 10.x.x.x (or using CIDR notation, 192.168/16, 172.16/12, and 10/8), and a router on that network has a private address (such as 192.168.0.1) in that address space. The router is also connected to the Internet with a single "public" address (known as "overloaded" NAT) or multiple "public" addresses assigned by an ISP. As traffic passes from the local network to the Internet, the source address in each packet is translated on the fly from the private addresses to the public address(es). The router tracks basic data about each active connection (particularly the destination address and port). When a reply returns to the router, it uses the connection tracking data it stored during the outbound phase to determine where on the internal network to forward the reply; the TCP or UDP client port numbers are used to demultiplex the packets in the case of

overloaded NAT, or IP address and port number when multiple public addresses are available, on packet return.

Basic NAT and PAT

There are two levels of network address translation.

- **Basic NAT.** This involves IP address translation only, not port mapping.
- **PAT (Port Address Translation).** Also called simply "NAT" or "Network Address Port Translation, NAPT".

This involves the translation of both IP addresses and port numbers.

All Internet packets have a source IP address and a destination IP address. Both or either of the source and destination addresses may be translated.

Some Internet packets do not have port numbers: for example, ICMP packets. However, the vast bulk of Internet traffic is TCP and UDP packets, which do have port numbers. Packets which do have port numbers have both a source port number and a destination port number. Both or either of the source and destination ports may be translated.

NAT which involves translation of the source IP address and/or source port is called **source NAT** or **SNAT**. This re-writes the IP address and/or port number of the computer which originated the packet.

NAT which involves translation of the destination IP address and/or destination port number is called **destination NAT** or **DNAT**. This re-writes the IP address and/or port number corresponding to the destination computer.

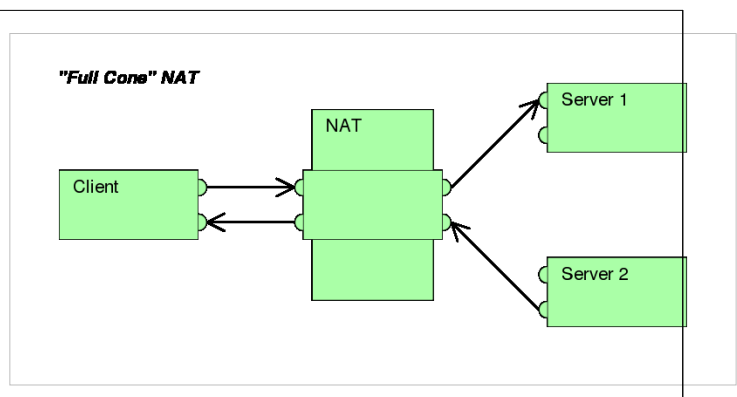
SNAT and DNAT may be applied simultaneously to Internet packets.

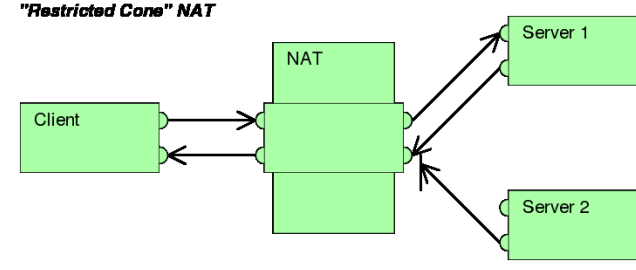
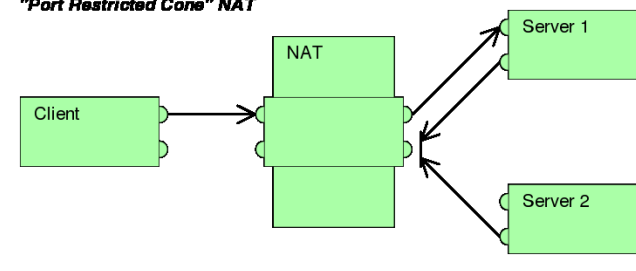
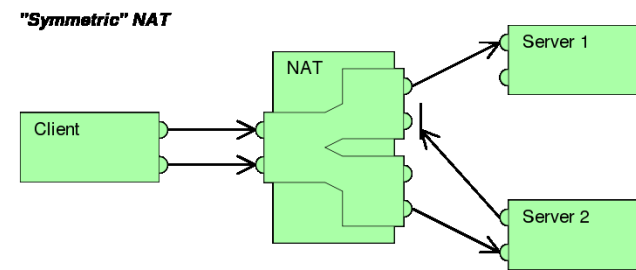
Types of NAT

Network address translation is implemented in a variety of schemes of translating addresses and port numbers, each affecting application communication protocols differently. In some application protocols that use IP address information, the application running on a node in the masqueraded network needs to determine the external address of the NAT, i.e., the address that its communication peers detect, and, furthermore, often needs to examine and categorize the type of mapping in use. For this purpose, the Simple traversal of UDP over NATs (STUN) protocol was developed (RFC 3489, March 2003). It classified NAT implementation as *full cone NAT*, *(address) restricted cone NAT*, *port restricted cone NAT* or *symmetric NAT* and proposed a methodology for testing a device accordingly. However, these procedures have since been deprecated from standards status, as the methods have proven faulty and inadequate to correctly assess many devices. New methods have been standardized in RFC 5389 (October 2008) and the STUN acronym now represents the new title of the specification: *Session Traversal Utilities for NAT*.

Full-cone NAT, also known as *one-to-one NAT*

- Once an internal address (iAddr:iPort) is mapped to an external address (eAddr:ePort), any packets from iAddr:iPort will be sent through eAddr:ePort.
- Any external host can send packets to iAddr:iPort by sending packets to eAddr:ePort.



<p>(Address) restricted cone NAT</p> <ul style="list-style-type: none"> Once an internal address ($iAddr:iPort$) is mapped to an external address ($eAddr:ePort$), any packets from $iAddr:iPort$ will be sent through $eAddr:ePort$. An external host ($hAddr:any$) can send packets to $iAddr:iPort$ by sending packets to $eAddr:ePort$ only if $iAddr:iPort$ has previously sent a packet to $hAddr:any$. "Any" means the port number doesn't matter. 	<p>"Restricted Cone" NAT</p> 
<p>Port-restricted cone NAT</p> <p>Like an address restricted cone NAT, but the restriction includes port numbers.</p> <ul style="list-style-type: none"> Once an internal address ($iAddr:iPort$) is mapped to an external address ($eAddr:ePort$), any packets from $iAddr:iPort$ will be sent through $eAddr:ePort$. An external host ($hAddr:hPort$) can send packets to $iAddr:iPort$ by sending packets to $eAddr:ePort$ only if $iAddr:iPort$ has previously sent a packet to $hAddr:hPort$. 	<p>"Port Restricted Cone" NAT</p> 
<p>Symmetric NAT</p> <ul style="list-style-type: none"> Requests from internal IP address and port combinations to different external IP address and port pairs are mapped to the external NAT address on a unique port. This also applies to all requests from the same host to different destinations. Only an external host that receives a packet from an internal host can send a packet back. 	<p>"Symmetric" NAT</p> 

This terminology has been the source of much confusion, as it has proven inadequate at describing real-life NAT behavior.^[1] Many NAT implementations combine these types, and it is therefore better to refer to specific individual NAT behaviors instead of using the Cone/Symmetric terminology. Especially, most NAT translators combine *symmetric NAT* for outgoing connections with *static port mapping*, where incoming packets to the external address and port are redirected to a specific internal address and port. Some products can redirect packets to several internal hosts, e.g. to divide the load between a few servers. However, this introduces problems with more sophisticated communications that have many interconnected packets, and thus is rarely used.

Many NAT implementations follow the *port preservation* design especially for TCP, which is to say that they use the same values as internal and external port numbers. NAT *port preservation* for outgoing TCP connections is especially important for TCP NAT traversal, because programs usually bind distinct TCP sockets to ephemeral ports for distinct TCP connections, rendering NAT port prediction impossible for TCP. On the other hand, for UDP, NATs do not need to have *port preservation* because applications usually reuse the same UDP socket to send packets to distinct hosts, making port prediction straightforward, as it is the same source port for each packet. Furthermore, *port preservation* in NAT for TCP allows P2P protocols to offer less complexity and less latency because there is no need to use a third party to discover the NAT port since the application already knows the NAT port.^[2] However, if two internal hosts attempt to communicate with the same external host using the same port number, the external port number used by the second host will be chosen at random. Such NAT will be sometimes perceived as (*address*)

restricted cone NAT and other times as *symmetric NAT*.

Recent studies have shown that roughly 70% of clients in P2P networks employ some form of NAT.^[3]

NAT and TCP/UDP

"Pure NAT", operating on IP alone, may or may not correctly parse protocols that are totally concerned with IP information, such as ICMP, depending on whether the payload is interpreted by a host on the "inside" or "outside" of translation. As soon as the protocol stack is climbed, even with such basic protocols as TCP and UDP, the protocols will break unless NAT takes action beyond the network layer.

IP has a checksum in each packet header, which provides error detection only for the header. IP datagrams may become fragmented and it is necessary for a NAT to reassemble these fragments to allow correct recalculation of higher-level checksums and correct tracking of which packets belong to which connection.

The major transport layer protocols, TCP and UDP, have a checksum that covers all the data they carry, as well as the TCP/UDP header, plus a "pseudo-header" that contains the source and destination IP addresses of the packet carrying the TCP/UDP header. For an originating NAT to successfully pass TCP or UDP, it must recompute the TCP/UDP header checksum based on the translated IP addresses, not the original ones, and put that checksum into the TCP/UDP header of the first packet of the fragmented set of packets. The receiving NAT must recompute the IP checksum on every packet it passes to the destination host, and also recognize and recompute the TCP/UDP header using the retranslated addresses and pseudo-header. This is not a completely solved problem. One solution is for the receiving NAT to reassemble the entire segment and then recompute a checksum calculated across all packets.

Originating host may perform Maximum transmission unit (MTU) path discovery (RFC 1191) to determine the packet size that can be transmitted without fragmentation, and then set the "don't fragment" bit in the appropriate packet header field.

Destination network address translation (DNAT)

DNAT is a technique for transparently changing the destination IP address of an en-route packet and performing the inverse function for any replies. Any router situated between two endpoints can perform this transformation of the packet.

DNAT is commonly used to publish a service located in a private network on a publicly accessible IP address. This use of DNAT is also called port forwarding.

SNAT

The meaning of the term *SNAT* varies by vendor. Many vendors have proprietary definitions for *SNAT*. A common expansion is *Source NAT*, the counterpart of *Destination NAT (DNAT)*. Microsoft uses the acronym for *Secure NAT*, in regard to the ISA Server extension discussed below. For Cisco Systems, *SNAT* means *Stateful NAT*.

The Internet Engineering Task Force (IETF) defines *SNAT* as *Softwires Network Address Translation*. This type of NAT is named after the Softwires working group that is charged with the standardization of discovery, control and encapsulation methods for connecting IPv4 networks across IPv6 networks and IPv6 networks across IPv4 networks.

Dynamic network address translation

Dynamic NAT, just like static NAT, is not common in smaller networks but is found within larger corporations with complex networks. The way dynamic NAT differs from static NAT is that where static NAT provides a one-to-one internal to public static IP address mapping, dynamic NAT doesn't make the mapping to the public IP address static and usually uses a group of available public IP addresses.

Applications affected by NAT

Some Application Layer protocols (such as FTP and SIP) send explicit network addresses within their application data. FTP in active mode, for example, uses separate connections for control traffic (commands) and for data traffic (file contents). When requesting a file transfer, the host making the request identifies the corresponding data connection by its network layer and transport layer addresses. If the host making the request lies behind a simple NAT firewall, the translation of the IP address and/or TCP port number makes the information received by the server invalid. The Session Initiation Protocol (SIP) controls Voice over IP (VoIP) and suffers the same problem. SIP may use multiple ports to set up a connection and transmit voice stream via RTP. IP addresses and port numbers are encoded in the payload data and must be known prior to the traversal of NATs. Without special techniques, such as STUN, NAT behavior is unpredictable and communications may fail.

Application Layer Gateway (ALG) software or hardware may correct these problems. An ALG software module running on a NAT firewall device updates any payload data made invalid by address translation. ALGs obviously need to understand the higher-layer protocol that they need to fix, and so each protocol with this problem requires a separate ALG.

Another possible solution to this problem is to use NAT traversal techniques using protocols such as STUN or ICE, or proprietary approaches in a session border controller. NAT traversal is possible in both TCP- and UDP-based applications, but the UDP-based technique is simpler, more widely understood, and more compatible with legacy NATs. In either case, the high level protocol must be designed with NAT traversal in mind, and it does not work reliably across symmetric NATs or other poorly-behaved legacy NATs.

Other possibilities are UPnP (Universal Plug and Play) or NAT-PMP (NAT Port Mapping Protocol), but these require the cooperation of the NAT device.

Most traditional client-server protocols (FTP being the main exception), however, do not send layer 3 contact information and therefore do not require any special treatment by NATs. In fact, avoiding NAT complications is practically a requirement when designing new higher-layer protocols today.

NATs can also cause problems where IPsec encryption is applied and in cases where multiple devices such as SIP phones are located behind a NAT. Phones which encrypt their signaling with IPsec encapsulate the port information within the IPsec packet meaning that NA(P)T devices cannot access and translate the port. In these cases the NA(P)T devices revert to simple NAT operation. This means that all traffic returning to the NAT will be mapped onto one client causing the service to fail. There are a couple of solutions to this problem: one is to use TLS, which operates at level 4 in the OSI Reference Model and therefore does not mask the port number; another is to Encapsulate the IPsec within UDP - the latter being the solution chosen by TISPAN to achieve secure NAT traversal.

The DNS protocol vulnerability announced by Dan Kaminsky on 2008 July 8 is indirectly affected by NAT port mapping. To avoid DNS server cache poisoning, it is highly desirable to not translate UDP source port numbers of outgoing DNS requests from a DNS server which is behind a firewall which implements NAT. The recommended work-around for the DNS vulnerability is to make all caching DNS servers use randomized UDP source ports. If the NAT function de-randomizes the UDP source ports, the DNS server will be made vulnerable.

Drawbacks

Hosts behind NAT-enabled routers do not have end-to-end connectivity and cannot participate in some Internet protocols. Services that require the initiation of TCP connections from the outside network, or stateless protocols such as those using UDP, can be disrupted. Unless the NAT router makes a specific effort to support such protocols, incoming packets cannot reach their destination. Some protocols can accommodate one instance of NAT between participating hosts ("passive mode" FTP, for example), sometimes with the assistance of an application-level gateway (see below), but fail when both systems are separated from the Internet by NAT. Use of NAT also complicates tunneling protocols such as IPsec because NAT modifies values in the headers which interfere with the integrity checks done by IPsec and other tunneling protocols.

End-to-end connectivity has been a core principle of the Internet, supported for example by the Internet Architecture Board. Current Internet architectural documents observe that NAT is a violation of the End-to-End Principle, but that NAT does have a valid role in careful design.^[4] There is considerably more concern with the use of IPv6 NAT, and many IPv6 architects believe IPv6 was intended to remove the need for NAT.^[5]

Because of the short-lived nature of the stateful translation tables in NAT routers, devices on the internal network lose IP connectivity typically within a very short period of time unless they implement NAT keep-alive mechanisms by frequently accessing outside hosts. This dramatically shortens the power reserves on battery-operated hand-held devices and has thwarted more widespread deployment of such IP-native Internet-enabled devices.

Some Internet service providers (ISPs), especially in Russia, Asia and other "developing" regions provide their customers only with "local" IP addresses, due to a limited number of external IP addresses allocated to those entities. Thus, these customers must access services external to the ISP's network through NAT. As a result, the customers cannot achieve true end-to-end connectivity, in violation of the core principles of the Internet as laid out by the Internet Architecture Board.

Benefits

The primary benefit of IP-masquerading NAT is that it has been a practical solution to the impending exhaustion of IPv4 address space. Even large networks can be connected to the Internet with as little as a single IP address. The more common arrangement is having machines that require end-to-end connectivity supplied with a routable IP address, while having machines that do not provide services to outside users behind NAT with only a few IP addresses used to enable Internet access.

Some^[6] have also called this exact benefit a major drawback, since it delays the need for the implementation of IPv6, :

"[...] it is possible that its [NAT's] widespread use will significantly delay the need to deploy IPv6. [...]
It is probably safe to say that networks would be better off without NAT [...]"

Examples of NAT software

- iptables: the Linux packet filter and NAT (interface for NetFilter)
- IPFilter: Solaris, NetBSD, FreeBSD, xMach.
- PF (firewall): The OpenBSD Packet Filter.
- Netfilter Linux packet filter framework
- Internet Connection Sharing (ICS): Windows NAT+DHCP since W98SE
- WinGate: like ICS plus lots of control

References

- [1] François Audet; and Cullen Jennings (January 2007) (text). *RFC 4787 Network Address Translation (NAT) Behavioral Requirements for Unicast UDP* (<http://www.ietf.org/rfc/rfc4787.txt>). IETF. . Retrieved 2007-08-29.
- [2] "Characterization and Measurement of TCP Traversal through NATs and Firewalls" (<http://nutss.gforge.cis.cornell.edu/pub/imc05-tcpnat/>). December 2006..
- [3] "Illuminating the shadows: Opportunistic network and web measurment" (<http://illuminati.coralcdn.org/stats/>). December 2006..
- [4] R. Bush; and D. Meyer; RFC 3439, *Some Internet Architectural Guidelines and Philosophy* (<http://www.ietf.org/rfc/rfc3439.txt>), December 2002
- [5] G. Van de Velde *et al.*; RFC 4864, *Local Network Protection for IPv6* (<http://tools.ietf.org/rfc/rfc4864.txt>), May 2007
- [6] Larry L. Peterson; and Bruce S. Davie; *Computer Networks: A Systems Approach*, Morgan Kaufmann, 2003, pp. 328-330, ISBN 1-55860-832-X

External links

- NAT-Traversal Test and results (<http://natatest.net.in.tum.de>)
- Characterization of different TCP NATs (<http://nutss.net/pub/imc05-tcpnat/>) – Paper discussing the different types of NAT
- Anatomy: A Look Inside Network Address Translators – Volume 7, Issue 3, September 2004 (http://www.cisco.com/en/US/about/ac123/ac147/archived_issues/ipj_7-3/anatomy.html)
- Jeff Tyson, HowStuffWorks: *How Network Address Translation Works* (<http://computer.howstuffworks.com/nat.htm/printable>)
- NAT traversal techniques in multimedia Networks (<http://www.newport-networks.com/whitepapers/nat-traversal1.html>) – White Paper from Newport Networks
- Peer-to-Peer Communication Across Network Address Translators (<http://www.brynosaurus.com/pub/net/p2pnat/>) (PDF) (<http://www.brynosaurus.com/pub/net/p2pnat.pdf>) – NAT traversal techniques for UDP and TCP
- RFC 5128 - Informational - State of Peer-to-Peer (P2P) Communications across Network Address Translators (NATs)
- RFC 4008 – Standards Track – Definitions of Managed Objects for Network Address Translators (NAT)
- RFC 3022 – Traditional IP Network Address Translator (Traditional NAT)
- RFC 1631 – Obsolete – The IP Network Address Translator (NAT)
- *Speak Freely* End of Life Announcement (<http://www.fourmilab.ch/speakfree/unix/>) – John Walker's discussion of why he stopped developing a famous program for free Internet communication, part of which is directly related to NAT
- natd (http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/network-natd.html)
- SNAT, DNAT and OCS2007R2 (<http://www.cainetworks.com/support/training/snat-dnat-ocs.html>) – discussing the SNAT in Microsoft OCS 2007R2
- Alternative Taxonomy
 - Static NAT (<http://publib.boulder.ibm.com/infocenter/iserics/v5r3/index.jsp?topic=/rzajw/rzajwstatic.htm>)
 - Dynamic NAT (<http://publib.boulder.ibm.com/infocenter/iserics/v5r3/index.jsp?topic=/rzajw/rzajwdynamic.htm>)
 - Masquerade NAT (<http://publib.boulder.ibm.com/infocenter/iserics/v5r3/index.jsp?topic=/rzajw/rzajwaddmasq.htm>)
- Network Address TRanslation - NAT (<http://blog.ipexpert.com/2009/09/07/network-address-translation-nat/>)

Wi-Fi

Wi-Fi (pronounced /'waɪfaɪ/) is a trademark of the Wi-Fi Alliance. 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 — 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.

This article focuses on the certification and approvals process and the general growth of wireless networking under the protocols certified by the Wi-Fi Alliance. For more on the technologies, see the appropriate articles with IEEE, ANSI, IETF, W3 and ITU prefixes (acronyms for the accredited standards organizations that have created formal technology standards for the protocols by which devices communicate). 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.^{[1] [2]} 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.^[3]

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.^[4]

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^[5]) or *Hi-Fi* (used since 1950^[5]). Even the Wi-Fi Alliance itself has often used the phrase *Wireless Fidelity* in its press releases^{[6] [7]} and documents,^{[8] [9]} the term also appears in a white paper on Wi-Fi from ITAA.^[10] However, based on Phil Belanger's^[11] statement, the term Wi-Fi was never supposed to mean anything at all.^{[12] [13]}

The term *Wi-Fi*, first used commercially in August 1999,^[14] 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'".^{[12] [13] [15]} 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",^[12] 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*.^{[8] [9]} There was no official statement related to the dropping of the term.

The yin-yang logo indicates the certification of a product for interoperability.^[8]

Uses

Internet access

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.^[16]

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.^[17] As of 2010 the Czech Republic had 1150 Wi-Fi based wireless Internet service providers.^{[18] [19]}



A roof-mounted Wi-Fi antenna

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 many mobile phones can also create wireless connections via tethering on iPhone, Android, Symbian, and WinMo.^[20]

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 bathrooms, kitchens and garden sheds.

City-wide Wi-Fi

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,^[21] and Minneapolis has generated \$1.2 million profit annually for their provider.^[22]

In May, 2010, London, UK Mayor Boris Johnson pledged London-wide Wi-Fi by 2012.^[23] Both the City of London, UK^[24] and Islington^[25] already have extensive outdoor Wi-Fi coverage.

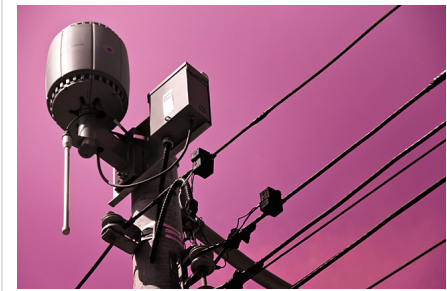


An outdoor Wi-Fi access point in Minneapolis

Campus-wide Wi-Fi

Carnegie Mellon University built the first wireless Internet network in the world at their Pittsburgh campus in 1994,^[26] 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 State's first major university to offer completely wireless Internet access across the entire campus in 2000.^[27]



An outdoor Wi-Fi access point in Toronto

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 pending specification called *Wi-Fi Direct* for file transfers and media sharing through a new discovery- and security-methodology.^[28]

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

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.



A keychain-size Wi-Fi detector

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.^[29] 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.

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.

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.^[30] 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^[31] 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^[32] 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.

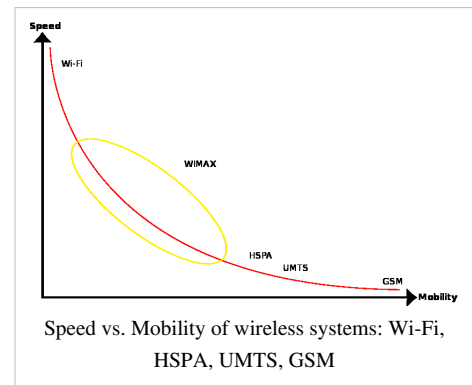
Due to the complex nature of radio propagation at typical Wi-Fi frequencies, particularly the effects of signal reflection off trees and buildings, algorithms can only approximately predict Wi-Fi signal strength for any given area in relation to a transmitter.^[33] This effect does not apply equally to long-range Wi-Fi, since longer links typically operate from towers that broadcast above the surrounding foliage.

Mobility

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^[34] or other large entities (such as universities) seek to provide large area coverage.

Hardware

Standard devices

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.

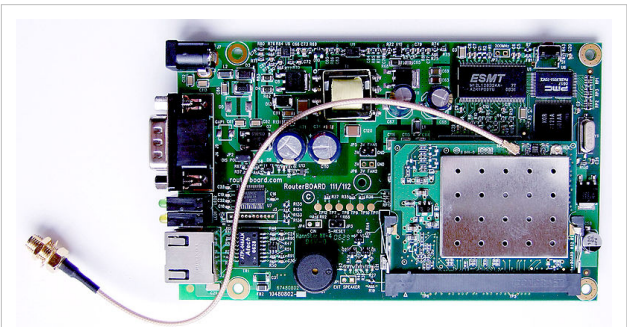
Wireless adapters allow devices to connect to a wireless network. These adapters connect to devices using various external or internal interconnects such as PCI, miniPCI, USB, ExpressCard, Cardbus and PC Card. As of 2010, most newer laptop computers come equipped with internal adapters. Internal cards 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-extendors or wireless repeaters can extend the range of an existing wireless network. Strategically placed range-extendors 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



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



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



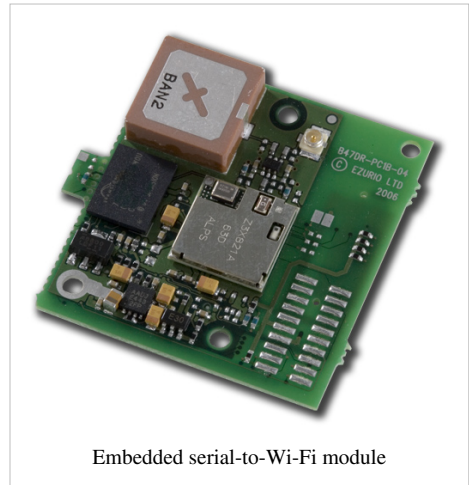
USB wireless adapter

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.^{[35] [36]} The Swedish Space Agency transferred data 420 km (260 mi), using 6 watt amplifiers to reach an overhead stratospheric balloon.^[37]

Embedded systems

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.^[38] 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.^[39]

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



Embedded serial-to-Wi-Fi module

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.^[40]

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.^[41]

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.^[42] 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,^[43] 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, as of 2009.

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,^[44] 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.^[45] A Florida court case determined that owner laziness was not to be a valid excuse.^[46]

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 (see DHCP and Zeroconf) this could possibly lead wireless users to send sensitive data to the wrong middle-man when seeking a destination (*see Man-in-the-middle attack*). 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.

Notes

- [1] . The Wi-Fi Alliance has also develop some core technology that has expanded the applicability of Wi-Fi, including a simple set up protocol (Wi-Fi Protected Set Up) and a peer to peer connectivity technology (Wi-Fi Peer to Peer) "Wi-Fi Alliance: Organization" (<http://www.wi-fi.org/organization.php>). www.wi-fi.org. . Retrieved 2009-10-22.
- [2] "Wi-Fi Alliance: White Papers" (<http://www.wi-fi.org/wp/wifi-alliance-certification/>). www.wi-fi.org. . Retrieved 2009-10-22.
- [3] "Wi-Fi Alliance: Programs" (http://www.wi-fi.org/certification_programs.php). www.wi-fi.org. . Retrieved 2009-10-22.
- [4] GainSpan specifically designs for Wi-Fi technology between Wi-Fi devices. Extremely useful. "GainSpan low-power, embedded Wi-Fi" (http://www.gainspan.com/technology/technology_overview.php). www.gainspan.com. . Retrieved 2010.
- [5] *Oxford English Dictionary* (2 ed.). Oxford: Oxford University Press. 1989. ISBN 0198611862.
- [6] "Wireless Ethernet Compatibility Alliance (WECA) Awards New Wi-Fi Interoperability Certification" (http://www.wi-fi.org/news_articles.php?f=media_news&news_id=64). Wi-Fi Alliance. 2000-05-08. . Retrieved 2009-11-30.
- [7] "Six Wi-Fi Interoperability Certifications Awarded By The Wireless Ethernet Compatibility Alliance (WECA)" (http://www.wi-fi.org/news_articles.php?f=media_news&news_id=62). Wi-Fi Alliance. 2000-07-19. . Retrieved 2009-11-30.
- [8] "Securing Wi-Fi Wireless Networks with Today's Technologies" (http://www.wi-fi.org/files/wp_4_Securing_Wireless_Networks_2-6-03.pdf). Wi-Fi Alliance. 2003-02-06. . Retrieved 2009-11-30.
- [9] "WPA™ Deployment Guidelines for Public Access Wi-Fi® Networks" (http://www.wi-fi.org/files/wp_6_WPA_Deployment_for_Public_Access_10-28-04.pdf). Wi-Fi Alliance. 2004-10-28. . Retrieved 2009-11-30.
- [10] "Wireless Fidelity (WiFi) Technology" (<http://www.itaa.org/isec/docs/innovation/wifiwhitepaper.pdf>). ITAA. January 2004. . Retrieved 2009-11-30.
- [11] Phil Belanger is the founding member of the Wi-Fi Alliance.
- [12] "Wi-Fi isn't short for 'Wireless Fidelity'" (http://www.boingboing.net/2005/11/08/wifi_isnt_short_for_.html). boingboing.net. . Retrieved 2007-08-31.
- [13] "Wireless Fidelity' Debunked" (<http://www.wi-fiplanet.com/columns/article.php/3674591>). Wi-Fi Planet. 2007-04-27. . Retrieved 2007-08-31.
- [14] U.S. Patent and Trademark Office.
- [15] "What is the True Meaning of Wi-Fi?" (<http://www.teleclick.ca/2005/12/what-is-the-true-meaning-of-wi-fi/>). Teleclick. . Retrieved 2007-08-31.
- [16] "Switch on for Square Mile wi-fi" (<http://news.bbc.co.uk/2/hi/technology/6577307.stm>). news.bbc.co.uk. 2007-04-23. . Retrieved 2007-11-08.

- [17] "MuniWireless » City Initiatives Directory" (<http://www.muniwireless.com/initiatives/2008/01/02/7483/>). www.muniwireless.com. . Retrieved 2008-03-12.
- [18] "Wi-Fi: Poskytovatelé bezdrátového připojení" (<http://translate.google.com/translate?u=http://www.internetprovsechny.cz/wifi-poskytovatele.php&hl=cs&ie=UTF8&sl=cs&tl=en>). [internetprovsechny.cz](http://www.internetprovsechny.cz). . Retrieved 2010-09-10.
- [19] "Bezdrátové připojení k internetu" (<http://translate.google.com/translate?u=http://www.bezdratovepripojeni.cz&hl=cs&ie=UTF8&sl=cs&tl=en>). [bezdratovepripojeni.cz](http://www.bezdratovepripojeni.cz). . Retrieved 2008-05-18.
- [20] "Mifi vs Joikuspot" (<http://www.mificlub.com/2010/07/mifi-vs-joikuspot/>). [mificlub.com](http://www.mificlub.com). . Retrieved 2010-10-09.
- [21] "Sunnyvale Uses MetroFi" (http://www.unstrung.com/document.asp?doc_id=85119&WT.svl=wire1_1). [unstrung.com](http://www.unstrung.com). . Retrieved 2008-07-16.
- [22] "Minneapolis moves ahead with wireless" (<http://www.startribune.com/business/111286134.html>). The Star Tribune. December 5, 2010. . Retrieved December 5, 2010.
- [23] "London-wide wi-fi by 2012 pledge" (http://news.bbc.co.uk/2/hi/uk_news/england/london/8692103.stm). *BBC News*. 2010-05-19. . Retrieved 2010-05-19.
- [24] "City of London Fires Up Europe's Most Advanced Wi-Fi Network" (<http://www.govtech.com/dc/118717>). www.govtech.com. . Retrieved 2007-05-14.
- [25] "London gets a mile of free Wi-Fi" (<http://www.zdnet.co.uk/news/networking/2005/04/18/london-gets-a-mile-of-free-wi-fi-39195421/>). [zdnet.co.uk](http://www.zdnet.co.uk). . Retrieved 200-04-18.
- [26] "Wi-Fi Origins" (<http://www.cmu.edu/homepage/computing/2009/summer/wi-fi-origins.shtml>). . Retrieved 2008-07-16.
- [27] <http://www.drexel.edu/catalog/general/aboutuniversity.htm>
- [28] "Wi-Fi Direct allows device-to-device links" (<http://www.networkworld.com/news/2009/101409-wi-fi-direct.html?hpg1=bn>). .
- [29] "Wi-Fi Finder" (<http://www.jiwire.com/search-hotspot-locations.htm>). [jiwire.com](http://www.jiwire.com). . Retrieved 2008-04-20.
- [30] "802.11n Delivers Better Range" (<http://www.wi-fiplanet.com/tutorials/article.php/3680781>). *Wi-Fi Planet*. 2007-05-31. .
- [31] FCC Sec.15.249 Operation within the bands 902–928 MHz, 2400–2483.5 MHz, 5725–5875 MHz, and 24.0–24.25 GHz. (<http://www.hallikainen.com/FccRules/2007/15/249/>)
- [32] See for example IEEE Standard 802.15.4 section 1.2 scope
- [33] "WiFi Mapping Software: Footprint" (<http://www.alryca.net/node/20>). Alyrica Networks, Inc.. . Retrieved 2008-04-27.
- [34] Wilson, Tracy V.. "How Municipal WiFi Works" (<http://computer.howstuffworks.com/municipal-wifi.htm>). computer.howstuffworks.com. . Retrieved 2008-03-12.
- [35] "Ermanno Pietrosemoli has set a new record for the longest communication Wi-Fi link" (<http://interred.wordpress.com/2007/06/18/ermanno-pietrosemoli-has-set-a-new-record-for-the-longest-communication-wi-fi-link/>). . Retrieved 2008-03-10.
- [36] "Wireless technology is irreplaceable for providing access in remote and scarcely populated regions" (<http://www.apc.org/en/news/strategic/world/wireless-technology-irreplaceable-providing-access/>). . Retrieved 2008-03-10.
- [37] "Long Distance WiFi Trial" ([http://www.eslared.org.ve/articulos/Long Distance WiFi Trial.pdf](http://www.eslared.org.ve/articulos/Long%20Distance%20WiFi%20Trial.pdf)) (PDF). . Retrieved 2008-03-10.
- [38] "Quatech Rolls Out Airborne Embedded 802.11 Radio for M2M Market" (<http://edageek.com/2008/04/18/embedded-wifi-radio/>). . Retrieved 2008-04-29.
- [39] "CIE article on embedded WiFi for M2M applications" (<http://www.cieonline.co.uk/cie2/articlen.asp?pid=1810&id=19742>). . Retrieved 2008-08-27.
- [40] "802.11 X Wireless Network in a Business Environment -- Pros and Cons." (<http://networkbits.net/wireless-printing/80211-g-pros-cons-of-a-wireless-network-in-a-business-environment/>). [NetworkBits.net](http://networkbits.net). . Retrieved 2008-04-08.
- [41] Bernstein, Daniel J. (2002). "DNS forgery" (<http://cr.yp.to/djbdns/forgery.html>). . Retrieved 2010-03-24. "An attacker with access to your network can easily forge responses to your computer's DNS requests."
- [42] Mateti, Prabhaker (2005). "Hacking Techniques in Wireless Networks" (http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm#_Toc77524658). Dayton, Ohio: Department of Computer Science and Engineering Wright State University. . Retrieved 2010-02-28.
- [43] "Wireless Vulnerabilities & Exploits" (<http://www.wirelessve.org/entries/show/WVE-2005-0020>). [wirelessve.org](http://www.wirelessve.org). . Retrieved 2008-04-15.
- [44] NoCat's goal is to bring you Infinite Bandwidth Everywhere for Free (<http://nocat.net/>)
- [45] "Let's Warchalk" (http://www.blackbeltjones.com/warchalking/warchalking0_9.pdf) (PDF). Matt Jones. . Retrieved 2008-10-09.
- [46] See the wikinews article mentioned in this section.

References

Further reading

- *Wireless Networking in the Developing World* (PDF book)

External links

- The Wi-Fi Alliance (<http://wi-fi.org/>)

Service set (802.11 network)

Service Set means all the devices associated with a specific local or enterprise 802.11 wireless LAN(s). There are a few interrelated terms associated with service sets.

Service Set identifier (SSID)

Service set identifier, or **SSID**, is a name that identifies a particular 802.11 wireless LAN. A client device receives broadcast messages from all access points within range advertising their SSIDs. The client device can then either manually or automatically—based on configuration—select the network with which to associate. The SSID can be up to 32 characters long. As the SSID displays to users, it normally consists of human-readable characters. However, the standard does not require this. The SSID is defined as a sequence of 1–32 octets each of which may take any value.

It is legitimate for multiple access points to share the same SSID if they provide access to the same network as part of an extended service set.

Some wireless access points support broadcasting multiple SSIDs, allowing the creation of Virtual Access Points, partitioning a single physical access point into several virtual access points, each of which can have a different set of security and network settings. This is not yet part of the 802.11 standard.

Basic service set

The **basic service set (BSS)** is the basic building block of an IEEE 802.11 wireless LAN (according to the IEEE 802.11-1999 standard). In Infrastructure mode a single access point (AP) together with all associated stations (STAs) is called a BSS.^[1] This is not to be confused with the coverage of an AP, which is called Basic Service Area (BSA). An AP acts as a master to control the stations within that BSS. In ad hoc mode a set of synchronized STAs, one of which acts as master, forms a BSS. Each BSS is identified by a BSSID. The most basic BSS consists of one AP and one STA.

Independent Basic Service Set (IBSS)

With 802.11 it is possible to create an ad-hoc network of client devices without a controlling Access Point called an Independent Basic Service Set (IBSS), in which case the SSID is chosen by the client device that starts the network, and broadcasting of the SSID is performed in a pseudo-random order by all devices that are members of the network.

Extended service set

An **Extended Service Set (ESS)** is a set of one or more interconnected BSSs and integrated local area networks (LANs) that appear as a single BSS to the logical link control layer at any station associated with one of those BSSs.

The set of interconnected BSSs must have a common service set identifier (SSID). They can work on the same channel, or work on different channels to boost aggregate throughput.

Basic service set identifier (BSSID)

A related field is the BSSID or Basic Service Set Identifier, which uniquely identifies each BSS (the SSID however, can be used in multiple, possibly overlapping, BSSs). In an infrastructure BSS, the BSSID is the MAC address of the wireless access point (WAP). In an IBSS, the BSSID is a locally administered MAC address generated from a 46-bit random number. The individual/group bit of the address is set to 0. The universal/local bit of the address is set to 1.

A BSSID with a value of all 1s is used to indicate the broadcast BSSID. A broadcast BSSID may only be used during probe requests.

Security of broadcasting SSID

Many access points allow a user to turn off the broadcast of the SSID. With many network client devices, this results in the detected network displaying as an unnamed network and the user would need to manually enter the correct SSID to connect to the network.

Unfortunately, turning off the broadcast of the SSID may lead to a false sense of security. The method discourages only casual wireless snooping, but does not stop a person trying to attack the network.^[2]

It is not secure against determined crackers, because every time someone connects to the network, the SSID is transmitted in cleartext even if the wireless connection is otherwise encrypted. An eavesdropper can passively sniff the wireless traffic on that network undetected (with software like Kismet), and wait for someone to connect, revealing the SSID. Alternatively, there are faster (albeit detectable) methods where a cracker spoofs a "disassociate frame" as if it came from the wireless bridge, and sends it to one of the clients connected; the client immediately re-connects, revealing the SSID.^[3]

As disabling SSID doesn't offer protection against determined crackers, proven security methods should be used such as requiring 802.11i/WPA2.^[4]

References

- [1] "IEEE Std 802.11-2007, Section 3.16, p. 6" (<http://standards.ieee.org/getieee802/download/802.11-2007.pdf>). 2007-06-12. . Retrieved 2008-05-07.
- [2] Robert Moskowitz (2003). "Debunking the Myth of SSID Hiding" (http://www.library.cornell.edu/dlit/ds/links/cit/redrover/ssid/wp_ssid_hiding.pdf). International Computer Security Association. . Retrieved 2008-02-06.
- [3] Joshua Bardwell; Devin Akin (2005). *CWNA Official Study Guide* (Third ed.). McGraw-Hill. p. 334. ISBN 0072255382.
- [4] "What is a Wireless Network's SSID?" (http://kbserver.netgear.com/kb_web_files/N100683.asp). *Netgear*. . Retrieved 2008-02-06.

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.



Industrial Wireless Access Point

Introduction

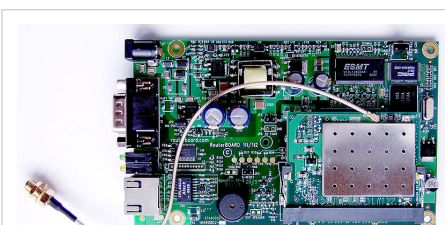
Prior to wireless networks, setting up a computer network in a business, home, or school often required running many cables through walls and ceilings in order to deliver network access to all of the network-enabled devices in the building. With the advent of the Wireless Access Point, network users 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.



Linksys WAP54G 802.11g Wireless Access Point

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.



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

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.

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is a deprecated security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 protocol in 1997, it was intended to provide confidentiality comparable to that of a traditional wired network, but is susceptible to eavesdropping.^[1]

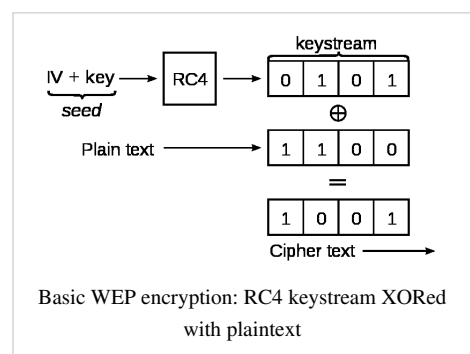
Since 2001, several serious weaknesses in the protocol have been identified by cryptanalysts with the result that today a WEP connection can be cracked with readily available software within minutes.^[2] In response to vulnerabilities the IEEE created a new 802.11i task force, by 2003 the Wi-Fi Alliance announced that WEP had been superseded by Wi-Fi Protected Access (WPA), which was a subset of then upcoming 802.11i amendment. Finally in 2004, with the ratification of the full 802.11i standard (i.e., WPA2), the IEEE declared that both WEP-40 and WEP-104 "have been deprecated as they fail to meet their security goals".^[3] Despite its weaknesses, WEP is still widely in use and is often the first security choice presented to users by router configuration tools.^{[4] [5]}

WEP is often inaccurately referred to as *Wireless Encryption Protocol*.

Encryption details

WEP was included as the privacy of the original IEEE 802.11 standard ratified in September 1999.^[1] WEP uses the stream cipher RC4 for confidentiality,^[6] and the CRC-32 checksum for integrity.^[7] It was deprecated as a wireless privacy mechanism in 2004, but for legacy purposes is still documented in the current standard.^[1]

Standard 64-bit WEP uses a 40 bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. At the time that the original WEP standard was being drafted, U.S. Government export restrictions on cryptographic technology limited the key size. Once the restrictions were lifted, all of the major manufacturers eventually implemented an extended 128-bit WEP protocol using a 104-bit key size (WEP-104).



A 128-bit WEP key is almost always entered by users as a string of 26 hexadecimal (base 16) characters (0-9 and A-F). Each character represents four bits of the key. 26 digits of four bits each gives 104 bits; adding the 24-bit IV produces the final 128-bit WEP key.

A 256-bit WEP system is available from some vendors, and as with the 128-bit key system, 24 bits of that is for the IV, leaving 232 actual bits for protection. These 232 bits are typically entered as 58 hexadecimal characters. $(58 \times 4 = 232 \text{ bits}) + 24 \text{ IV bits} = 256\text{-bit WEP key}$.

Key size is not the only major security limitation in WEP.^[8] Cracking a longer key requires interception of more packets, but there are active attacks that stimulate the necessary traffic. There are other weaknesses in WEP, including the possibility of IV collisions and altered packets,^[6] that are not helped at all by a longer key.

Authentication

Two methods of authentication can be used with WEP: Open System authentication and Shared Key authentication.

For the sake of clarity, we discuss WEP authentication in the Infrastructure mode (that is, between a WLAN client and an Access Point), but the discussion applies to the ad-Hoc mode as well.

In Open System authentication, the WLAN client need not provide its credentials to the Access Point during authentication. Thus, any client, regardless of its WEP keys, can authenticate itself with the Access Point and then attempt to associate. In effect, no authentication (in the true sense of the term) occurs. After the authentication and association, WEP can be used for encrypting the data frames. At this point, the client needs to have the right keys.

In Shared Key authentication, the WEP key is used for authentication. A four-way challenge-response handshake is used:

1. The client station sends an authentication request to the Access Point.
2. The Access Point sends back a clear-text challenge.
3. The client has to encrypt the challenge text using the configured WEP key, and send it back in another authentication request.
4. The Access Point decrypts the material, and compares it with the clear-text it had sent. Depending on the success of this comparison, the Access Point sends back a positive or negative response.

After the authentication and association, the pre-shared WEP key is also used for encrypting the data frames using RC4.

At first glance, it might seem as though Shared Key authentication is more secure than Open System authentication, since the latter offers no real authentication. However, it is quite the reverse. It is possible to derive the keystream used for the handshake by capturing the challenge frames in Shared Key authentication.^[2] Hence, it is advisable to use Open System authentication for WEP authentication, rather than Shared Key authentication. (Note that both authentication mechanisms are weak.)

Flaws

Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets.

In August 2001, Scott Fluhrer, Itsik Mantin, and Adi Shamir published a cryptanalysis of WEP that exploits the way the RC4 cipher and IV is used in WEP, resulting in a passive attack that can recover the RC4 key after eavesdropping on the network. Depending on the amount of network traffic, and thus the number of packets available for inspection, a successful key recovery could take as little as one minute. If an insufficient number of packets are being sent, there are ways for an attacker to send packets on the network and thereby stimulate reply

packets which can then be inspected to find the key. The attack was soon implemented, and automated tools have since been released. It is possible to perform the attack with a personal computer, off-the-shelf hardware and freely available software such as aircrack-ng to crack *any* WEP key in minutes.

Cam-Winget et al. (2003) surveyed a variety of shortcomings in WEP. They write "*Experiments in the field indicate that, with proper equipment, it is practical to eavesdrop on WEP-protected networks from distances of a mile or more from the target.*" They also reported two generic weaknesses:

- the use of WEP was optional, resulting in many installations never even activating it, and
- WEP did not include a key management protocol, relying instead on a single shared key among users.

In 2005, a group from the U.S. Federal Bureau of Investigation gave a demonstration where they cracked a WEP-protected network in 3 minutes using publicly available tools.^[9] Andreas Klein presented another analysis of the RC4 stream cipher. Klein showed that there are more correlations between the RC4 keystream and the key than the ones found by Fluhrer, Mantin and Shamir which can additionally be used to break WEP in WEP-like usage modes.

In 2006, Bittau, Handley, and Lackey showed^[4] that the 802.11 protocol itself can be used against WEP to enable earlier attacks that were previously thought impractical. After eavesdropping a single packet, an attacker can rapidly bootstrap to be able to transmit arbitrary data. The eavesdropped packet can then be decrypted one byte at a time (by transmitting about 128 packets per byte to decrypt) to discover the local network IP addresses. Finally, if the 802.11 network is connected to the Internet, the attacker can use 802.11 fragmentation to replay eavesdropped packets while crafting a new IP header onto them. The access point can then be used to decrypt these packets and relay them on to a buddy on the Internet, allowing real-time decryption of WEP traffic within a minute of eavesdropping the first packet.

In 2007, Erik Tews, Andrei Pychkine, and Ralf-Philipp Weinmann were able to extend Klein's 2005 attack and optimize it for usage against WEP. With the new attack^[10] it is possible to recover a 104-bit WEP key with probability 50% using only 40,000 captured packets. For 60,000 available data packets, the success probability is about 80% and for 85,000 data packets about 95%. Using active techniques like deauth and ARP re-injection, 40,000 packets can be captured in less than one minute under good conditions. The actual computation takes about 3 seconds and 3 MB of main memory on a Pentium-M 1.7 GHz and can additionally be optimized for devices with slower CPUs. The same attack can be used for 40-bit keys with an even higher success probability.

In 2008, Payment Card Industry (PCI) Security Standards Council's latest update of the Data Security Standard (DSS), prohibits the use of the WEP as part of any credit-card processing after 30 June 2010, and prohibit any new system from being installed that uses WEP after 31 March 2009. The use of WEP contributed to the T.J. Maxx parent company network invasion^[11].

Remedies

Use of encrypted tunneling protocols (e.g. IPSec, Secure Shell) can provide secure data transmission over an insecure network. However, replacements for WEP have been developed with the goal of restoring security to the wireless network itself.

802.11i (WPA and WPA2)

The recommended solution to WEP security problems is to switch to WPA2 or with older equipment the less resource intensive WPA. Either is much more secure than WEP.^[12] To add support for WPA or WPA2, some old Wi-Fi access points might need to be replaced or have their firmware upgraded. WPA was designed as an interim software-implementable solution for WEP that could forestall immediate deployment of new hardware.^[13] However, TKIP (the basis of WPA) has reached the end of its designed lifetime, and has been deprecated in the next full release of the 802.11 standard.^[14]

Implemented non-standard fixes

WEP2

This stopgap enhancement to WEP was present in some of the early 802.11i drafts. It was implementable on *some* (not all) hardware not able to handle WPA or WPA2, and extended both the IV and the key values to 128 bits.^[15] It was hoped to eliminate the duplicate IV deficiency as well as stop brute force key attacks.

After it became clear that the overall WEP algorithm was deficient (and not just the IV and key sizes) and would require even more fixes, both the WEP2 name and original algorithm were dropped. The two extended key lengths remained in what eventually became WPA's TKIP.

WEPplus

WEPplus, also known as WEP+, is a proprietary enhancement to WEP by Agere Systems (formerly a subsidiary of Lucent Technologies) that enhances WEP security by avoiding "weak IVs".^[16] It is only completely effective when WEPplus is used at *both ends* of the wireless connection. As this cannot easily be enforced, it remains a serious limitation. It is possible that successful attacks against WEPplus will eventually be found. It also does not necessarily prevent replay attacks.

Dynamic WEP

Dynamic WEP refers to the combination of 802.1x technology and the EAP.^[17] Dynamic WEP changes WEP keys dynamically. It is a vendor-specific feature provided by several vendors such as 3Com.

The dynamic change idea made it into 802.11i as part of TKIP, but not for the actual WEP algorithm.

References

- [1] *IEEE Std 802.11-1997 Information Technology- telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications* ([http://ieeexplore.ieee.org/search/freesrchabstract.jsp?arnumber=654749&isnumber=14251&punumber=5258&k2dockey=654749@ieeestds&query=\(802.11+1997\)<in>metadata&pos=0](http://ieeexplore.ieee.org/search/freesrchabstract.jsp?arnumber=654749&isnumber=14251&punumber=5258&k2dockey=654749@ieeestds&query=(802.11+1997)<in>metadata&pos=0)). 1997. .
- [2] Nikita Borisov, Ian Goldberg, David Wagner. *Intercepting Mobile Communications: The Insecurity of 802.11* (<http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>). . Retrieved 2006-09-12.
- [3] "What is a WEP key?" (<http://lirent.net/wifi/what-is-a-wep-key.html>). lirent.net. . Retrieved 2008-03-11.
- [4] Andrea Bittau, Mark Handley, Joshua Lackey. *The Final Nail in WEP's Coffin* (<http://www.cs.ucl.ac.uk/staff/M.Handley/papers/fragmentation.pdf>). . Retrieved 2008-03-16.
- [5] RSA Security (2007-06-14). "Wireless Adoption Leaps Ahead, Advanced Encryption Gains Ground in the Post-WEP Era" (http://www.rsa.com/press_release.aspx?id=8451). Press release. .
- [6] "WPA Part 2: Weak IV's" (<http://www.informit.com/guides/content.aspx?g=security&seqNum=85>). informit.com. . Retrieved 2008-03-16.
- [7] "An Inductive Chosen Plaintext Attack against WEP/WEP2" (<http://www.cs.umd.edu/~waa/attack/v3dcmnt.htm>). cs.umd.edu. . Retrieved 2008-03-16.
- [8] Fluhrer, Mantin and Shamir. *Weaknesses_in_the_Key_Scheduling_Algorithm_of_RC4* (http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf). . Retrieved 2008-03-16.
- [9] http://www.smallnetbuilder.com/index.php?option=com_content&task=view&id=24251&Itemid=100
- [10] <http://eprint.iacr.org/2007/120.pdf>
- [11] "T.J. Maxx data theft likely due to wireless 'wardriving'" (<http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=199500574>). eetimes.com. . Retrieved 2009-07-04.
- [12] "802.11b Update: Stepping Up Your WLAN Security" (<http://www.networkmagazineindia.com/200112/focus3.htm>). networkmagazineindia.com. . Retrieved 2008-03-16.
- [13] *WIRELESS NETWORK SECURITY* (http://www.proxim.com/learn/library/whitepapers/wireless_security.pdf). Proxim Wireless. . Retrieved 2008-03-16.
- [14] "802.11mb Issues List v12" (<https://mentor.ieee.org/802.11/file/08/11-08-1127-12-000m-tgmb-issues-list.xls>) (excel). 20-Jan-2009. p. CID 98. . "The use of TKIP is deprecated. The TKIP algorithm is unsuitable for the purposes of this standard"
- [15] "WEP2, Credibility Zero" (<http://www.starkrealities.com/wireless003.html>). starkrealities.com. . Retrieved 2008-03-16.

- [16] "Agere Systems is First to Solve Wireless LAN Wired Equivalent Privacy Security Issue; New Software Prevents Creation of Weak WEP Keys" (http://findarticles.com/p/articles/mi_m0EIN/is_2001_Nov_12/ai_79954213). Business Wire. 2001-11-12. . Retrieved 2008-03-16.
- [17] "Is Dynamic WEP Secure Enough enterprise solution ?" (<http://www.astrotv.co.tv/2007/11/is-dynamic-wep-secure-enough-enterprise.html>). . Retrieved 2010-12-30.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) and **Wi-Fi Protected Access II (WPA2)** are the names of security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy).^[1]

The WPA protocol implements the majority of the IEEE 802.11i standard. The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the preparation of 802.11i. Specifically, the Temporal Key Integrity Protocol (TKIP), was brought into WPA. TKIP encryption replaces WEP's small 40-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet and thus prevents collisions.^[2] TKIP could be implemented on pre-WPA wireless network interface cards that began shipping as far back as 1999 through firmware upgrades. However, since the changes required in the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA with TKIP. Researchers have since discovered a flaw in TKIP that relied on older weaknesses to retrieve the keystream from short packets to use for re-injection and spoofing.^[3]

WPA also includes a Message Integrity Check. This is designed to prevent an attacker from capturing, altering and/or resending data packets. This replaces the Cyclic Redundancy Check (CRC) that was used and implemented by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled. MIC solved these problems. MIC uses an algorithm to check the integrity of the packets, and if it does not equal, it drops the packet.^[4]

The later WPA2 certification mark indicates compliance with the full IEEE 802.11i standard. This advanced protocol will not work with some older network cards.^[5]

WPA2

WPA2 has replaced WPA; WPA2 requires testing and certification by the Wi-Fi Alliance. WPA2 implements the mandatory elements of 802.11i. In particular, it introduces CCMP, a new AES-based encryption mode with strong security.^[6] Certification began in September, 2004; from March 13, 2006, WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark.^[7]

Security & Insecurity in pre-shared key mode

Pre-shared key mode (PSK, also known as *Personal* mode) is designed for home and small office networks that don't require the complexity of an 802.1X authentication server.^[8] Each wireless network device encrypts the network traffic using a 256 bit key. This key may be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters.^[9] If ASCII characters are used, the 256 bit key is calculated by applying the PBKDF2 key derivation function to the passphrase, using the SSID as the salt and 4096 iterations of HMAC-SHA1.^[10]

Shared-key WPA remains vulnerable to password cracking attacks if users rely on a weak passphrase.^[11] ^[12] To protect against a brute force attack, a truly random passphrase of 13 characters (selected from the set of 95 permitted characters) is probably sufficient.^[13] To further protect against intrusion the network's SSID should not match any

entry in the top 1000 SSIDs^[14] as downloadable rainbow tables have been pre-generated for them and a multitude of common passwords.^[15]

In November 2008 Erik Tews and Martin Beck - researchers at two German technical universities (TU Dresden and TU Darmstadt) - uncovered a WPA weakness^[16] which relied on a previously known flaw in WEP that could be exploited only for the TKIP algorithm in WPA. The flaw can only decrypt short packets with mostly known contents, such as ARP messages. The attack requires Quality of Service (as defined in 802.11e) to be enabled, which allows packet prioritization as defined. The flaw does not lead to key recovery, but only a keystream that encrypted a particular packet, and which can be reused as many as seven times to inject arbitrary data of the same packet length to a wireless client. For example, this allows someone to inject faked ARP packets which makes the victim send packets to the open Internet. This attack was further optimised by two Japanese computer scientists Toshihiro Ohigashi and Masakatu Morii.^[17] Their attack doesn't require Quality of Service to be enabled. In October 2009, Halvorsen with others made further progress, enabling attackers to inject larger malicious packets (596 bytes, to be more specific) within approximately 18 minutes and 25 seconds.^[18] In February 2010, a new attack was found by Martin Beck that allows an attacker to decrypt all traffic towards the client. The authors say that the attack can be defeated by deactivating QoS, or by switching from TKIP to AES-based CCMP.^[19]

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

EAP extensions under WPA- and WPA2- Enterprise

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

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

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

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

Hardware support

Most newer certified Wi-Fi devices support the security protocols discussed above, out-of-the-box: compliance with this protocol has been required for a Wi-Fi certification since September 2003.^[20]

The protocol certified through Wi-Fi Alliance's WPA program (and to a lesser extent WPA2) was specifically designed to also work with wireless hardware that was produced prior to the introduction of the protocol^[5] which usually had only supported inadequate security through WEP. Many of these devices support the security protocol after a firmware upgrade. Firmware upgrades are not available for all legacy devices.

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

References

- [1] "Understanding WEP Weaknesses" (<http://eu.dummies.com/WileyCDA/how-to/content/understanding-wep-weaknesses.html>). Wiley Publishing. . Retrieved 2010-01-10.
- [2] Meyers, Mike (2004). *Managing and Troubleshooting Networks*. Network+. McGraw Hill. ISBN 978-0-07-225665-9.
- [3] "Battered, but not broken: understanding the WPA crack" (<http://arstechnica.com/articles/paedia/wpa-cracked.ars>). Ars Technica. 2008-11-06. . Retrieved 2008-11-06.
- [4] Ciampa, Mark (2006). *CWNA Guide to Wireless LANS*. Networking. Thomson.
- [5] "Wi-Fi Protected Access White Paper" (http://www.wi-fi.org/white_papers/whitepaper-042903-wpa/). *Wi-Fi Alliance*. . "WPA is both forward and backward-compatible and is designed to run on existing Wi-Fi devices as a software download."
- [6] Jonsson, Jakob. "On the Security of CTR + CBC-MAC" (<http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm-ad1.pdf>). NIST. . Retrieved 2010-05-15.
- [7] "WPA2 Security Now Mandatory for Wi-Fi CERTIFIED Products" "WPA2 Security Now Mandatory for Wi-Fi CERTIFIED Products" (http://www.wi-fi.org/pressroom_overview.php?newsid=16). *Wi-Fi Alliance*. .
- [8] "Wi-Fi Alliance: Glossary" (http://www.wi-fi.org/knowledge_center_overview.php?type=3). . Retrieved 2010-03-01.
- [9] *Each character in the pass-phrase must have an encoding in the range of 32 to 126 (decimal), inclusive.* (IEEE Std. 802.11i-2004, Annex H.4.1)
The space character is included in this range.
- [10] van Rantwijk, Joris (2006-12-06). "WPA key calculation — From passphrase to hexadecimal key" (<http://www.xs4all.nl/~tjoris/wpapsk.html>). . Retrieved 2009-01-16.
- [11] Wireball said... (2009-04-21). "Test attack WPA-PSK and WPA2-PSK by using Pyrit" (<http://techviewz.org/2009/04/test-attack-wpa-psk-and-wpa2-psk-by.html>). Techviewz.org. . Retrieved 2010-11-15.
- [12] "Securing Wireless Network" (<http://blogs.iium.edu.my/jaiz/2009/04/17/securing-wireless-network/>). ERM Blog. . Retrieved 2009-06-09.
- [13] "A key generated from a passphrase of less than about 20 characters is unlikely to deter attacks." "... against current brute-strength attacks, 96 bits [of security] SHOULD be adequate." (Weakness in Passphrase Choice in WPA Interface, by Robert Moskowitz. Retrieved March 2, 2004. (<http://wifinetnews.com/archives/002452.html>))
- [14] "Wireless Geographic Logging Engine - SSID Stats" (<http://www.wigle.net/gps/gps/main/ssidstats>). WiGLE. . Retrieved 2010-11-15.
- [15] "Church of Wifi WPA-PSK Rainbow Tables" (<http://www.renderlab.net/projects/WPA-tables/>). The Renderlab. . Retrieved 2010-11-15.
- [16] "Practical Attacks against WEP and WPA" (<http://dl.aircrack-ng.org/breakingwepandwpa.pdf>) (PDF). . Retrieved 2010-11-15.
- [17] "A Practical Message Falsification Attack on WPA" ([http://jwis2009.nsysu.edu.tw/location/paper/A Practical Message Falsification Attack on WPA.pdf](http://jwis2009.nsysu.edu.tw/location/paper/A%20Practical%20Message%20Falsification%20Attack%20on%20WPA.pdf)) (PDF). . Retrieved 2010-11-15.
- [18] Halvorsen, Finn M.; Haugen, Olav; Eian, Martin; Mjøl̂snes, Stig F. (September 30, 2009). *An Improved Attack on TKIP*. doi:10.1007/978-3-642-04766-4_9.
- [19] "Enhanced TKIP Michael Attacks" (http://download.aircrack-ng.org/wiki-files/doc/enhanced_tkip_michael.pdf) (PDF). . Retrieved 2010-11-15.
- [20] "Wi-Fi Protected Access Security Sees Strong Adoption" (http://www.wi-fi.org/pressroom_overview.php?newsid=37). *Wi-Fi Alliance Press Room*. .

External links

- Wi-Fi (http://www.dmoz.org/Computers/Data_Communications/Wireless/802.11/) at the Open Directory Project
- Wi-Fi Alliance's Interoperability Certificate page (http://certifications.wi-fi.org/wbcs_certified_products.php)
- Weakness in Passphrase Choice in WPA Interface, by Robert Moskowitz. Retrieved March 2, 2004. (<http://wifinetnews.com/archives/002452.html>)
- IEEE Std. 802.11i-2004 (<http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>)

Power over Ethernet

Power over Ethernet or **PoE** technology describes a system to pass electrical power safely, along with data, on Ethernet cabling. PoE requires category 5 cable or higher for high power levels, but can operate with category 3 cable for low power levels.^[1] Power can come from a power supply within a PoE-enabled networking device such as an Ethernet switch or can be *injected* into a cable run with a *midspan* power supply.

The original **IEEE 802.3af-2003**^[2] PoE standard provides up to 15.4 W of DC power (minimum 44 V DC and 350 mA^{[3] [4]}) to each device.^[5] Only 12.95 W is assured to be available at the powered device as some power is dissipated in the cable.^[6]



Wireless LAN access point, powered by a PoE splitter

The updated **IEEE 802.3at-2009**^[7] PoE standard also known as **PoE+** or **PoE plus**, provides up to 25.5 W of power.^[8] Some vendors have announced products that claim to comply with the 802.3at standard and offer up to 51 W of power over a single cable by utilizing all four pairs in the Cat.5 cable.^[9] Numerous non-standard schemes had been used prior to PoE standardization to provide power over Ethernet cabling. Some are still in active use.

Advantages over other integrated data and power standards

This technology is especially useful for powering IP telephones, wireless LAN access points, cameras with pan tilt and zoom (PTZ), remote Ethernet switches, embedded computers, thin clients and LCDs.

All these require more power than USB offers and very often must be powered over longer runs of cable than USB permits. In addition, PoE uses only one type of connector, an 8P8C modular connector, whereas there are numerous types of USB connectors.

PoE is presently deployed in applications where USB is unsuitable and where AC power would be inconvenient, expensive^[10] or infeasible to supply. However, even where USB or AC power could be used, PoE has several advantages over either, including the following:

- Cheaper cabling — even category 5 cable is cheaper than USB repeaters, and the task of meeting building code requirements to run AC power cable is eliminated.
- A Gigabit of data per second to every device is possible, which exceeds 2009 USB and the AC powerline networking capabilities.
- Global organizations can deploy PoE everywhere without concern for any local variance in AC power standards, outlets, plugs, or reliability.
- Direct injection from standard 48 V DC battery power arrays; this enables critical infrastructure to run more easily in outages, and make power rationing decisions centrally for all the PoE devices.
- Symmetric distribution is possible. Unlike USB and AC outlets, power can be supplied at either end of the cable or outlet. This means the location of the power source can be determined after cables and outlets are installed.

Uses for PoE

Uses for Power over Ethernet include:

- Network routers
- A mini network switch installed in distant rooms, to support a small cluster of ports from one uplink cable. (These ports on the mini-switch do not themselves provide PoE.)
- Network webcams
- Network Intercom / Paging / Public address systems and hallway speaker amplifiers
- VoIP phones
- Wall clocks in rooms and hallways, with time set using Network Time Protocol
- Wireless access points



Terminology

Power sourcing equipment

Power sourcing equipment (PSE) is a device (switch or hub for instance) that will provide power in a PoE setup. Maximum allowed continuous output power per such device in IEEE 802.3af is 15.40 W.

When the device is a switch, it's called an endspan. Otherwise, if it's an intermediary device between a non PoE capable switch and a PoE device, it's called a midspan.

Powered device

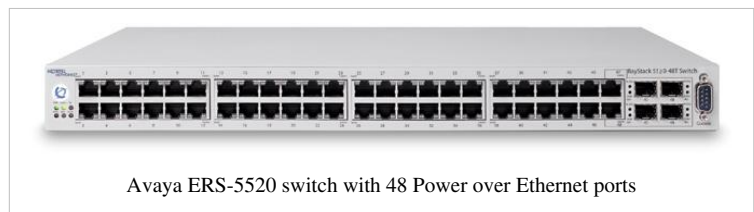
A powered device (PD) is a device powered by a PSE and thus consumes energy. Examples include wireless access points, IP Phones, and IP cameras. The IEEE 802.3af standard specifies a minimum available power of 12.95 W.

Many powered devices have another connector for an optional auxiliary power supply. If used, this gives backup power to the device if the power to the Ethernet connector is inadequate or suddenly fails.^[11]

Power management features and integration

Most advocates expect PoE to become a global longterm DC power cabling standard and replace "wall wart" converters, which cannot be easily centrally managed, waste energy, are often poorly designed, and are easily vulnerable to damage from surges and brownouts.

A combination of G.9960 networking on existing AC power lines to an outlet where a PoE router is plugged in is capable of moving a gigabit per second to every device, with minimal wiring and participating fully in both AC and DC device power demand management.



Integration with the IEEE 802.3az standard, the energy management capabilities of the combined standard are expected to be formidable. However, that integration has not yet occurred.

There are several PoE implementations, including ad-hoc techniques, but using the IEEE standard for supplying power over Ethernet is strongly recommended.^[12]

Standard implementation

Standards-based power over Ethernet is implemented following the specifications in IEEE 802.3af-2003 (which was later incorporated as clause 33 into IEEE 802.3-2005) or the 2009 update, IEEE 802.3at. A phantom power technique is used to allow the powered pairs to also carry data. This permits its use not only with 10BASE-T and 100BASE-TX, which use only two of the four pairs in the cable, but also with 1000BASE-T (gigabit Ethernet), which uses all four pairs for data transmission. This is possible because all versions of Ethernet over twisted pair cable specify differential data transmission over each pair with transformer coupling; the DC supply and load connections can be made to the transformer center-taps at each end. Each pair thus operates in common mode as one side of the DC supply, so two pairs are required to complete the circuit. The polarity of the DC supply may be inverted by crossover cables; the powered device must operate with either pair: spare pairs 4-5 and 7-8 or data pairs 1-2 and 3-6. Polarity is required on data pairs, and ambiguously implemented for spare pairs, with the use of a diode bridge.

Standard PoE parameters and comparison

Property	802.3af (802.3at Type 1)	802.3at Type 2
Power available at PD ^[13]	12.95 W	25.50 W per mode
Maximum power delivered by PSE	15.40 W	34.20 W per mode
Voltage range (at PSE)	44.0 - 57.0 V ^[14]	50.0 - 57.0 V ^[14]
Voltage range (at PD)	37.0 - 57.0 V ^[15]	42.5 - 57.0 V ^[15]
Maximum current	350 mA ^[16]	600 mA ^[16] per mode
Maximum cable resistance	20 Ω (Category 3)	12.5 Ω (Category 5)
Power management	Three power class levels negotiated at initial connection	Four power class levels negotiated at initial connection or 0.1 W steps negotiated continuously
De rating of maximum cable ambient operating temperature	None	5°C with one mode (two pairs) active, 10°C with two modes (four pairs) simultaneously active
Supported cabling	Category 3 and Category 5 ^[1]	Category 5 ^[1] [17]
Supported modes	Mode A (endspan), Mode B (midspan)	Mode A, Mode B, Mode A and Mode B operating simultaneously

Powering devices

Two modes, A and B, are available. Mode A delivers phantom power on the data pairs of 100BASE-T or 10BASE-T. Mode B delivers power on the spare pairs. PoE can also be used on 1000BASE-T Ethernet in which case, there are no spare pairs and all power is delivered using the phantom technique.

Mode A has two alternate configurations (MDI and MDI-X), using the same pairs but with different polarities. In mode A, pins 1 and 2 (pair #2 in T568B wiring) form one side of the 48 V DC, and pins 3 and 6 (pair #3 in T568B) form the other side. These are the same two pairs used for data transmission in 10BASE-T and 100BASE-TX, allowing the provision of both power and data over only two pairs in such networks. The free polarity allows PoE to accommodate for crossover cables, patch cables and auto-MDIX.

In mode B, pins 4-5 (pair #1 in both T568A and T568B) form one side of the DC supply and pins 7-8 (pair #4 in both T568A and T568B) provide the return; these are the "spare" pairs in 10BASE-T and 100BASE-TX. Mode B, therefore, requires a 4-pair cable.

The PSE, not the powered device (PD), decides whether power mode A or B shall be used. PDs that implement only Mode A or Mode B are disallowed by the standard.

The PSE can implement mode A or B or both. A PD indicates that it is standards-compliant by placing a 25 kΩ resistor between the powered pairs. A major difference between IEEE802.3af and IEEE802.3at is that while IEEE802.3af clearly precluded collocating two PD interfaces on a single RJ45 connector, IEEE802.3at changes the definition of a PD, and therefore allows two PDs collocation, one mode A and the other mode B. If the PSE detects a resistance that is too high or too low (including a short circuit), no power is applied. This protects devices that do not support PoE. An optional "power class" feature allows the PD to indicate its power requirements by changing the sense resistance at higher voltages. To stay powered, the PD must continuously use 5–10 mA for at least 60 ms with no less than 400 ms since last use or else it will be unpowered by the PSE.^[18]

There are two types of PSEs: endspans and midspans. Endspans are Ethernet switches that include the power over Ethernet transmission circuitry. Endspans are commonly called PoE switches. Midspans are power injectors that stand between a regular Ethernet switch and the powered device, injecting power without affecting the data.

Endspans are normally used on new installations or when the switch has to be replaced for other reasons (such as moving from 10/100 Mbit/s to 1 Gbit/s or adding security protocols), which makes it convenient to add the PoE capability. Midspans are used when there is no desire to replace and configure a new Ethernet switch, and only PoE needs to be added to the network.

Stages of powering up a PoE link

Stage	Action	Volts specified [V]	
		802.3af	802.3at
Detection	PSE detects if the PD has the correct signature resistance of 15 - 33 kΩ	2.7 - 10.0	
Classification	PSE detects resistor indicating power range (see below)	14.5 - 20.5	
Mark 1	Signals PSE is 802.3at capable. PD presents a 0.25 - 4 mA load.	-	7 - 10
Class 2	PSE output classification voltage again to indicate 802.3at capability	-	14.5 - 20.5
Mark 2	Signals PSE is 802.3at capable. PD presents a 0.25 - 4 mA load.	-	7 - 10
Startup	Startup voltage	> 42	> 37.2 ^[19]
Normal operation	Supply power to device	44 - 57	50 - 57 ^[19]

IEEE 802.3at capable devices are also referred to as "type 2". An 802.3at PSE may also use layer2 communication to signal 802.3at capability.^[19]

Power levels available^[20]

Class	Usage	Classification current [mA]	Power range [Watt]	Class description
0	Default	0 - 4	0.44 - 12.94	Classification unimplemented
1	Optional	9 - 12	0.44 - 3.84	Very Low power
2	Optional	17 - 20	3.84 - 6.49	Low power
3	Optional	26 - 30	6.49 - 12.95	Mid power
4	Reserved	36 - 44	12.95 - 25.50	High power

PSEs classify as Class 0^[20]

For IEEE 802.3at (type 2) devices class 4 instead of Reserved has a power range of 12.95 - 25.5 W.^[19]

Configuration via Ethernet layer 2 LLDP

LLDP-MED Advanced Power Management^[21]

TLV Header		MED Header		Extended power via MDI			
Type (7 bits)	Length (9 bits)	TIA OUI (3 octets)	Extended power via MDI subtype (1 octet)	Power type (2 bits)	Power source (2 bits)	Power priority (4 bits)	Power value (2 octets)
127	7	00-12-BB	4	PSE or PD	Normal or Backup conservation	Critical, High, Low	0 - 102.3 W in 0.1 W steps

The setup phases are as follows:

- PSE (provider) tests PD (consumer) physically using 802.3af phase class 3.
 - PSE powers up PD.
- PD sends to PSE: I'm a PD, max power = X, max power requested = X.
- PSE sends to PD: I'm a PSE, max power allowed = X.
 - PD may now use the amount of power as specified by the PSE.

The rules for this power negotiation are:

- PD shall never request more power than physical 802.3af class
- PD shall never draw more than max power advertised by PSE
- PSE may deny any PD drawing more power than max allowed by PSE
- PSE shall not reduce power allocated to PD, that is in use
- PSE may *request* reduced power, via conservation mode

[21]

Non-standard implementations

Cisco

Cisco manufactured WLAN access points and IP phones many years before there was an IEEE standard for delivering PoE. Cisco's original PoE implementation is not software upgradeable to the IEEE 802.3af standard. Cisco's original PoE equipment was capable of delivering up to 10 W per port. The amount of power to be delivered is negotiated between the endpoint and the Cisco switch based on a power value that was added to the Cisco proprietary Cisco Discovery Protocol (CDP). CDP is also responsible for dynamically communicating the Voice VLAN value from the Cisco switch to the Cisco IP Phone.

Under Cisco's pre-standard scheme, the PSE (switch) will send a Fast Link Pulse (FLP) on the transmit pair. The PD (device) connects the transmit line to the receive line via a low pass filter. And thus the PSE gets the FLP in return. And a common mode current between pair 1 and 2 will be provided resulting in 48 V DC^[22] and 6.3 W^[23] default of allocated power. The PD has then to provide Ethernet link within 5 seconds to the auto-negotiation mode switch port. A later CDP message with a type-length-value tells the PSE its final power requirement. A discontinued link pulses shuts down power.^[24]

PowerDsine

PowerDsine, now a Microsemi brand, sold midspans since 1999 with its proprietary Power over LAN solution. Several companies like Level1 , 3Com and Nortel followed PowerDsine's Power over LAN.

Notes

- [1] IEEE 802.3at-2009, clause 33.1.1c
- [2] *802.3af-2003*, June 2003
- [3] IEEE 802.3-2005, section 2, table 33-5, item 1
- [4] IEEE 802.3-2005, section 2, table 33-5, item 4
- [5] IEEE 802.3-2005, section 2, table 33-5, item 14
- [6] IEEE 802.3-2005, section 2, clause 33.3.5.2
- [7] *802.3at Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements*, September 11, 2009
- [8] "Amendment to IEEE 802.3 Standard Enhances Power Management and Increases Available Power" (http://standards.ieee.org/announcements/stdbd_approves_ieee802.3at.html). IEEE. . Retrieved 2010-06-24.
- [9] "802.3at-2009 Power over Ethernet (PoE) Plus Standard Ratified" (<http://blog.tmcnet.com/blog/tom-keating/voip/8023at-2009-power-over-ethernet-poe-plus-standard-ratified.asp>). . Retrieved 2010-06-24.
- [10] Mains wiring must often be done by qualified and/or licensed electricians for legal or insurance reasons.
- [11] National Semiconductor application note 1474: "The LM507X Family of PoE Devices: Frequently Asked Questions (FAQs)" (<http://www.national.com/an/AN/AN-1474.pdf>)
- [12] Powered Device Controller Supports Upcoming IEEE 802.3at PoE Standard, Akros Silicon AS1135 (<http://power.elecdesign.com/Articles/index.cfm?articleid=18768&StyleName=maroon>)
- [13] Most switched power supplies within the powered device will lose another 10 to 25% of the available power.
- [14] IEEE 802.3at-2009 Table 33-11
- [15] IEEE 802.3at-2009 Table 33-18
- [16] IEEE 802.3at-2009 Table 33-1
- [17] More stringent cable specification allows assumption of more current carrying capacity and lower resistance (20.0 Ohms for Category 3 versus 12.5 Ohms for Category 5).
- [18] Banish Those "Wall Warts" With Power Over Ethernet (<http://www.elecdesign.com/Articles/Index.cfm?ArticleID=5945&pg=3>)
- [19] "LTC4278 IEEE 802.3at PD with Synchronous No-Opto Flyback Controller and 12V Aux Support" (<http://cds.linear.com/docs/Datasheet/4278fa.pdf>). . 2010-01-11 cds.linear.com
- [20] IEEE 802.3-2005, section 2, table 33-3
- [21] "LLDP / LLDP-MED Proposal for PoE Plus (2006-09-15)" (<http://www.ieee802.org/1/files/public/docs2006/ab-congdon-ldp-med-8023at-0906.pdf>). . 2010-01-10
- [22] "Planning for Cisco IP Telephony > Network Infrastructure Analysis" (<http://www.ciscopress.com/articles/article.asp?p=385336&seqNum=2&rll=1>). . 2010-01-12 ciscopress.com
- [23] "Power over Ethernet on the Cisco Catalyst 6500 Series Switch" (http://www.conticomp.com/PDF/CAT6500POE_ds.pdf). . 2010-01-12 conticomp.com
- [24] "Understanding the Cisco IP Phone 10/100 Ethernet In-Line Power Detection Algorithm - Cisco Systems" (http://www.cisco.com/en/US/products/hw/phones/ps379/products_tech_note09186a00801189b5.shtml). . 2010-01-12 cisco.com

Category 5 cable uses 24 AWG conductors, which can safely carry 360 mA at 50 V according to the latest TIA ruling. The cable has eight conductors (only half of which are used for power) and therefore the absolute maximum power transmitted using direct current is $50\text{ V} \times 0.360\text{ A} \times 2 = 36\text{ W}$. Considering the voltage drop after 100 m, a PD would be able to receive 31.6 W. The additional heat generated in the wires by PoE at this current level (4.4 watts per 100 meter cable) limits the total number of cables in a bundle to be 100 cables at 45 °C, according to the TIA.

Drawbacks of IEEE 802.3af are:

- Excessive voltage with a peak at 60 V (many standard components are limited to ~30 V).
- Undefined polarity (requires a diode bridge which causes a voltage drop and require more board space and components).
- Undefined wire pairs (multiple configurations must be handled which requires more board space and components) (The diode bridge will waste 0.74 W at 25.5 W operation)

- Unexpected AC current flow due to faulty design of the PoE source, and/or power supplied to non-differential I/O signals such as RS232. The major cause of this problem is unaccounted for capacitance which can form a bridge to an AC wall source. Symptoms include electrical shock when touching the case, and failure to negotiate startup on some PoE sources, especially when non-differential I/O is connected prior to power up.

A partial solution to the input source drawbacks of IEEE 802.3af is to assume pin 4 + 5 as positive (+) and pin 7 + 8 as negative (-). This would not be standards compliant but will make PD implementation easier and not damage anything. Any incompatibilities with IEEE 802.3af will only result in an unpowered device.

Another solution is to use an existing IEEE 802.3af compliant power supply chip, adapting its sample designs to your specific needs. The chip will handle negotiation, slow startup, multiple auxiliary sources, and possibly provide additional protection in the form of automatic shutdown. If possible use the fully isolated design, especially if there is exposed metal on the outer case. The drawback can be a high component count.

PoE compatible 8P8C connectors are available with internal magnetics, input diodes, minor capacitors, and LED indicators incorporated into the package. These can help reduce component count. Be careful when placing them anywhere but at the edge of a circuit board, as most are designed to support a dangling cable. If the cable has a boot protecting the end, it can press against the circuit board and produce an intermittent connection.

The 0.74 W waste in the diode bridge, above, assumes the use of standard rectifier diodes. If Schottky diodes are used, the waste will be half that much. In either case, the waste is much less than the losses in the DC-DC converter that must be used to convert the power to the low voltages used in the PD logic circuits.

802.3af Standards A and B

PINS on Switch	10/100 DC on Spares (mode B)	10/100 Mixed DC & Data (mode A)	1000 (1 Gigabit) DC & Bi-Data
Pin 1	Rx +	Rx + DC +	TxRx A + DC +
Pin 2	Rx -	Rx - DC +	TxRx A - DC +
Pin 3	Tx +	Tx + DC -	TxRx B + DC -
Pin 4	DC +	unused	TxRx C +
Pin 5	DC +	unused	TxRx C -
Pin 6	Tx -	Tx - DC -	TxRx B - DC -
Pin 7	DC -	unused	TxRx D +
Pin 8	DC -	unused	TxRx D -

Another modification is to limit voltage from the PSE to 30 V and thus enable the use of standard components. But this may destroy the PD if it is connected to a PSE that isn't modified to keep the voltage low enough. It also limits the amount of power that can be used.

When converting an existing ethernet design to accept PoE, verify that the input isolation transformer is rated to carry PoE currents.

See also

- Network switch, connects network nodes with independent pipes (efficient).
- Category 5 cable
- Power line communication, data communication over mains electricity.
- Switched-mode power supply, efficient electrical power conversion.
- ITU-T G.hn, a standard that provides a way to create a high-speed (up to 1 Gigabit/s) Local area network using existing home wiring (power lines, phone lines and coaxial cables).
- Phantom power, long established standard technique to power microphones.
- HomePlug Powerline Alliance, an industry trade group on datacommunication over mains electricity.

References

External links

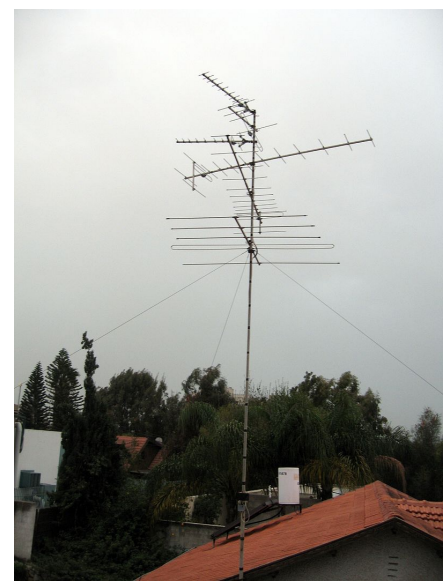
- [ieee802.org](http://standards.ieee.org/getieee802/802.3.html): Download the IEEE 802.3 standards (<http://standards.ieee.org/getieee802/802.3.html>)
- [ieee802.org](http://www.ieee802.org/3/af/): IEEE 802.3af Task Force (<http://www.ieee802.org/3/af/>)
- [ieee802.org](http://www.ieee802.org/3/at/): IEEE 802.3at Task Force (<http://www.ieee802.org/3/at/>)
- [altair.org](http://www.altair.org/labnotes_POE.html): Power Over Ethernet (http://www.altair.org/labnotes_POE.html)
- [poweroverethernet.com](http://www.poweroverethernet.com/): PoE portal (<http://www.poweroverethernet.com/>)

Antenna (radio)

An **antenna** (or **aerial**) is a transducer that transmits or receives electromagnetic waves. In other words, antennas convert electromagnetic radiation into electric current, or vice versa. Antennas generally deal in the transmission and reception of radio waves, and are a necessary part of all radio equipment. Antennas are used in systems such as radio and television broadcasting, point-to-point radio communication, wireless LAN, cell phones, radar, and spacecraft communication. Antennas are most commonly employed in air or outer space, but can also be operated under water or even through soil and rock at certain frequencies for short distances.

Physically, an antenna is an arrangement of one or more conductors, usually called *elements* in this context. In transmission, an alternating current is created in the elements by applying a voltage at the antenna terminals, causing the elements to radiate an electromagnetic field. In reception, the inverse occurs: an electromagnetic field from another source induces an alternating current in the elements and a corresponding voltage at the antenna's terminals. Some receiving antennas (such as parabolic and horn types) incorporate shaped reflective surfaces to collect the radio waves striking them and direct or focus them onto the actual conductive elements.

Some of the first rudimentary antennas were built in 1888 by Heinrich Hertz (1857–1894) in his pioneering experiments to prove the existence of electromagnetic waves predicted by the theory of James Clerk Maxwell. Hertz placed the emitter dipole in the focal point of a parabolic reflector. He published his work and installation drawings



Television antennas in Israel. These six antennas are of a common type called a Yagi-Uda antenna, widely used at VHF and UHF frequencies.

in *Annalen der Physik und Chemie* (vol. 36, 1889).

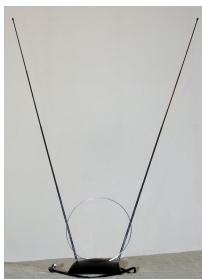
Terminology

The words *antenna* (plural: *antennas*^[1]) and *aerial* are used interchangeably; but usually a rigid metallic structure is termed an antenna and a wire format is called an aerial. In the United Kingdom and other British English speaking areas the term aerial is more common, even for rigid types. The noun *aerial* is occasionally written with a diaeresis mark—*aërial*—in recognition of the original spelling of the adjective *aërial* from which the noun is derived.

The origin of the word *antenna* relative to wireless apparatus is attributed to Guglielmo Marconi. In 1895, while testing early radio apparatuses in the Swiss Alps at Salvan, Switzerland in the Mont Blanc region, Marconi experimented with early wireless equipment. A 2.5 meter long pole, along which was carried a wire, was used as a radiating and receiving aerial element. In Italian a tent pole is known as *l'antenna centrale*, and the pole with a wire alongside it used as an aerial was simply called *l'antenna*. Until then wireless radiating transmitting and receiving elements were known simply as aerals or terminals. Marconi's use of the word *antenna* (Italian for *pole*) would become a popular term for what today is uniformly known as the *antenna*.^[2]

A Hertzian or half-wave dipole antenna is a set of terminals that does not require the presence of a ground for its operation. A Marconi, Tesla, or quarter-wave monopole antenna is grounded.^[3] A loaded antenna is an active antenna having an elongated portion of appreciable electrical length and having additional inductance or capacitance directly in series or shunt with the elongated portion so as to modify the standing wave pattern existing along the portion or to change the effective electrical length of the portion. An antenna grounding structure is a structure for establishing a reference potential level for operating the active antenna. It can be any structure closely associated with (or acting as) the ground which is connected to the terminal of the signal receiver or source opposing the active antenna terminal.

In colloquial usage, the word *antenna* may refer broadly to an entire assembly including support structure, enclosure (if any), etc. in addition to the purely functional components.



"Rabbit ears" dipole antenna for television reception



Cell phone base station antennas



Parabolic antenna for communicating with spacecraft, Canberra, Australia



Yagi antenna used for mobile military communications station, Dresden, Germany, 1955



"Super Turnstile" type transmitting antenna for VHF low band television broadcasting station, Germany.



Folded dipole antenna



Large Yagi antenna used by amateur radio hobbyist



A vertical mast radiator, Chapel Hill, North Carolina

Overview

Antennas have practical uses for the transmission and reception of radio frequency signals such as radio and television. In air, those signals travel very quickly and with a very low transmission loss. The signals are absorbed when moving through more conductive materials, such as concrete walls or rock. When encountering an interface, the waves are partially reflected and partially transmitted through.

A common antenna is a vertical rod a quarter of a wavelength long. Such antennas are simple in construction, usually inexpensive, and both radiate in and receive from all horizontal directions (omnidirectional). One limitation of this antenna is that it does not radiate or receive in the direction in which the rod points. This region is called the antenna blind cone or null.

There are two fundamental types of antenna directional patterns, which, with reference to a specific two dimensional plane (usually horizontal [parallel to the ground] or vertical [perpendicular to the ground]), are either:

1. Omni-directional (radiates equally in all directions), such as a vertical rod (in the horizontal plane) or
2. Directional (radiates more in one direction than in the other).

In colloquial usage "omnidirectional" usually refers to all horizontal directions with reception above and below the antenna being reduced in favor of better reception (and thus range) near the horizon. A "directional" antenna usually refers to one focusing a narrow beam in a single specific direction such as a telescope or satellite dish, or, at least, focusing in a sector such as a 120° horizontal fan pattern in the case of a panel antenna at a cell site.

All antennas radiate some energy in all directions in free space but careful construction results in substantial transmission of energy in a preferred direction and negligible energy radiated in other directions. By adding additional *elements* (such as rods, loops or plates) and carefully arranging their length, spacing, and orientation, an antenna with desired directional properties can be created.

An antenna array is two or more simple antennas combined to produce a specific directional radiation pattern. In common usage an array is composed of active elements, such as a linear array of parallel dipoles fed as a "broadside array". A slightly different feed method could cause this same array of dipoles to radiate as an "end-fire array". Antenna arrays may be built up from any basic antenna type, such as dipoles, loops or slots.

The directionality of the array is due to the spatial relationships and the electrical feed relationships between individual antennas. Usually all of the elements are active (electrically fed) as in the log-periodic dipole array which offers modest gain and broad bandwidth and is traditionally used for television reception. Alternatively, a superficially similar dipole array, the Yagi-Uda Antenna (often abbreviated to "Yagi"), has only one active dipole

element in a chain of parasitic dipole elements, and a very different performance with high gain over a narrow bandwidth.

An active element is electrically connected to the antenna terminals leading to the receiver or transmitter, as opposed to a parasitic element that modifies the antenna pattern without being connected directly. The active element(s) couple energy between the electromagnetic wave and the antenna terminals, thus any functioning antenna has at least one active element. A careful arrangement of parasitic elements, such as rods or coils, can improve the radiation pattern of the active element(s). Directors and reflectors are common parasitic elements.

An antenna lead-in is the medium, for example, a transmission line or feed line for conveying the signal energy between the signal source or receiver and the antenna. The antenna feed refers to the components between the antenna and an amplifier.

An antenna counterpoise is a structure of conductive material most closely associated with ground that may be insulated from or capacitively coupled to the natural ground. It aids in the function of the natural ground, particularly where variations (or limitations) of the characteristics of the natural ground interfere with its proper function. Such structures are usually connected to the terminal of a receiver or source opposite to the antenna terminal.

An antenna component is a portion of the antenna performing a distinct function and limited for use in an antenna, as for example, a reflector, director, or active antenna.

An electromagnetic wave refractor is a structure which is shaped or positioned to delay or accelerate transmitted electromagnetic waves, passing through such structure, an amount which varies over the wave front. The refractor alters the direction of propagation of the waves emitted from the structure with respect to the waves impinging on the structure. It can alternatively bring the wave to a focus or alter the wave front in other ways, such as to convert a spherical wave front to a planar wave front (or vice-versa). The velocity of the waves radiated have a component which is in the same direction (director) or in the opposite direction (reflector) as that of the velocity of the impinging wave.

A *director* is a parasitic element, usually a metallic conductive structure, which re-radiates into free space impinging electromagnetic radiation coming from or going to the active antenna, the velocity of the re-radiated wave having a component in the direction of the velocity of the impinging wave.

A reflector is a parasitic element, usually a metallic conductive structure (e.g., screen, rod or plate), which re-radiates back into free space impinging electromagnetic radiation coming from or going to the active antenna. The velocity of the returned wave has a component in a direction opposite to the direction of the velocity of the impinging wave. The reflector modifies the radiation of the active antenna.

An antenna coupling network is a passive network (which may be any combination of a resistive, inductive or capacitive circuit(s)) for transmitting the signal energy between the active antenna and a source (or receiver) of such signal energy.

Reciprocity

It is a fundamental property of antennas that the characteristics of an antenna described in the next section, such as gain, radiation pattern, impedance, bandwidth, resonant frequency and polarization, are the same whether the antenna is transmitting or receiving. For example, the "*receiving pattern*" (sensitivity as a function of direction) of an antenna when used for reception is identical to the radiation pattern of the antenna when it is *driven* and functions as a radiator. This is a consequence of the reciprocity theorem of electromagnetics. Therefore in discussions of antenna properties no distinction is usually made between receiving and transmitting terminology, and the antenna can be viewed as either transmitting or receiving, whichever is more convenient.

A necessary condition for the above reciprocity property is that the materials in the antenna and transmission medium are linear and reciprocal. *Reciprocal* (or *bilateral*) means that the material has the same response to an electric or magnetic field, or a current, in one direction, as it has to the field or current in the opposite direction. Most

materials used in antennas meet these conditions, but some microwave antennas use high-tech components such as isolators and circulators, made of nonreciprocal materials such as ferrite or garnet. These can be used to give the antenna a different behavior on receiving than it has on transmitting, which can be useful in applications like radar.

Parameters

There are several critical parameters affecting an antenna's performance that can be adjusted during the design process. These are resonant frequency, impedance, gain, aperture or radiation pattern, polarization, efficiency and bandwidth. Transmit antennas may also have a maximum power rating, and receive antennas differ in their noise rejection properties. All of these parameters can be measured through various means.

Resonant frequency

Many types of antenna are tuned to work at one particular frequency, and are effective only over a range of frequencies centered on this frequency, called the resonant frequency. These are called *resonant antennas*. The antenna acts as an electrical resonator. When driven at its resonant frequency, large standing waves of voltage and current are excited in the antenna elements. These large currents and voltages radiate intense electromagnetic waves, so the power radiated by the antenna is maximum at the resonant frequency.

In antennas made of thin linear conductive elements, the length of the driven element(s) determines the resonant frequency. To be resonant, the length of a driven element should typically be either half or a quarter of the wavelength at that frequency; these are called half-wave and quarter-wave antennas. The length referred to is not the physical length, but the electrical length of the element, which is the physical length divided by the velocity factor (the ratio of the speed of wave propagation in the wire to c_0 , the speed of light in a vacuum). Antennas are usually also resonant at multiples (harmonics) of the lowest resonant frequency.

Some antenna designs have multiple resonant frequencies, and some are relatively effective over a very broad range of frequencies. or bandwidth. One commonly known type of wide band antenna is the logarithmic or log-periodic antenna.

The resonant frequency also affects the impedance of the antenna. At resonance, the equivalent circuit of an antenna is a pure resistance, with no reactive component. At frequencies other than the resonant frequencies, the antenna has capacitance or inductance as well as resistance. An antenna can be made resonant at other frequencies besides its natural resonant frequency by compensating for these reactances by adding a loading coil or capacitor in series with it. Other properties of an antenna change with frequency, in particular the radiation pattern, so the antenna's operating frequency may be considerably different from the resonant frequency to optimize other important parameters.

Gain

Gain is a parameter which measures the degree of directivity of the antenna's radiation pattern. An antenna with a low gain emits radiation with about the same power in all directions, whereas a high-gain antenna will preferentially radiate in particular directions. Specifically, the *antenna gain*, *directive gain*, or *power gain* of an antenna is defined as the ratio of the intensity (power per unit surface) radiated by the antenna in the direction of its maximum output, at an arbitrary distance, divided by the intensity radiated at the same distance by a hypothetical isotropic antenna.

The gain of an antenna is a passive phenomenon - power is not added by the antenna, but simply redistributed to provide more radiated power in a certain direction than would be transmitted by an isotropic antenna. An antenna designer must take into account the application for the antenna when determining the gain. High-gain antennas have the advantage of longer range and better signal quality, but must be aimed carefully in a particular direction. Low-gain antennas have shorter range, but the orientation of the antenna is relatively inconsequential. For example, a dish antenna on a spacecraft is a high-gain device that must be pointed at the planet to be effective, whereas a typical

Wi-Fi antenna in a laptop computer is low-gain, and as long as the base station is within range, the antenna can be in any orientation in space. It makes sense to improve horizontal range at the expense of reception above or below the antenna. Thus most antennas labelled "omnidirectional" really have some gain.^[4]

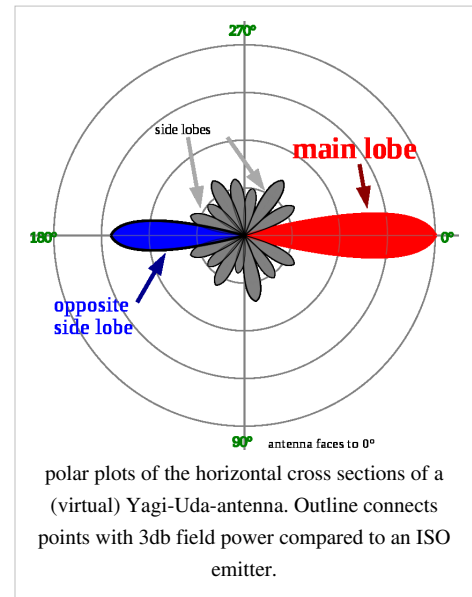
In practice, the half-wave dipole is taken as a reference instead of the isotropic radiator. The gain is then given in **dBd** (decibels over **dipole**):

NOTE: **0 dBd = 2.15 dBi**. It is vital in expressing gain values that the reference point be included. Failure to do so can lead to confusion and error.

Radiation pattern

The radiation pattern of an antenna is the geometric pattern of the relative field strengths of the field emitted by the antenna. For the ideal isotropic antenna, this would be a sphere. For a typical dipole, this would be a toroid. The radiation pattern of an antenna is typically represented by a three dimensional graph, or polar plots of the horizontal and vertical cross sections.

The radio waves emitted by different parts of an antenna typically interfere, causing maxima of radiation at some angles where the radio waves arrive in phase, and zero radiation at other angles where the radio waves arrive out of phase. So the radiation of most antennas shows a pattern of maxima or "*lobes*" at various angles. In a directional antenna designed to project radio waves in a particular direction, the lobe in that direction is larger than the others and is called the "*main lobe*". The other lobes represent unwanted radiation and are called "*sidelobes*". The axis through the main lobe is called the "*principle axis*" or "*boresight axis*".



Impedance

As an electro-magnetic wave travels through the different parts of the antenna system (radio, feed line, antenna, free space) it may encounter differences in impedance (E/H, V/I, etc.). At each interface, depending on the impedance match, some fraction of the wave's energy will reflect back to the source,^[5] forming a standing wave in the feed line. The ratio of maximum power to minimum power in the wave can be measured and is called the standing wave ratio (**SWR**). A SWR of 1:1 is ideal. A SWR of 1.5:1 is considered to be marginally acceptable in low power applications where power loss is more critical, although an SWR as high as 6:1 may still be usable with the right equipment. Minimizing impedance differences at each interface (impedance matching) will reduce SWR and maximize power transfer through each part of the antenna system.

Complex impedance of an antenna is related to the electrical length of the antenna at the wavelength in use. The impedance of an antenna can be matched to the feed line and radio by adjusting the impedance of the feed line, using the feed line as an impedance transformer. More commonly, the impedance is adjusted at the load (see below) with an antenna tuner, a balun, a matching transformer, matching networks composed of inductors and capacitors, or matching sections such as the gamma match.

Efficiency

Efficiency is the ratio of power actually radiated to the power put into the antenna terminals. A dummy load may have an SWR of 1:1 but an efficiency of 0, as it absorbs all power and radiates heat but very little RF energy, showing that SWR alone is not an effective measure of an antenna's efficiency. Radiation in an antenna is caused by radiation resistance which can only be measured as part of total resistance including loss resistance. Loss resistance usually results in heat generation rather than radiation, and reduces efficiency. Mathematically, efficiency is calculated as radiation resistance divided by total resistance.

Bandwidth

The *bandwidth* of an antenna is the range of frequencies over which it is effective, usually centered on the resonant frequency. The bandwidth of an antenna may be increased by several techniques, including using thicker wires, replacing wires with *cages* to simulate a thicker wire, tapering antenna components (like in a feed horn), and combining multiple antennas into a single assembly (array) and allowing the natural impedance of suitable inductive RF filter traps to select the correct antenna. All these attempts to increase bandwidth by adding capacitance to the surface area have a detrimental effect on efficiency by reducing the Q factor. They also have an adverse effect on the rejection of unwanted harmonics, on both received and transmitted signal frequencies. Small antennas are usually preferred for convenience, but there is a fundamental limit relating bandwidth, size and efficiency.

Polarization

The *polarization* of an antenna is the orientation of the electric field (E-plane) of the radio wave with respect to the Earth's surface and is determined by the physical structure of the antenna and by its orientation. It has nothing in common with antenna directionality terms: "horizontal", "vertical" and "circular". Thus, a simple straight wire antenna will have one polarization when mounted vertically, and a different polarization when mounted horizontally. "Electromagnetic wave polarization filters" are structures which can be employed to act directly on the electromagnetic wave to filter out wave energy of an undesired polarization and to pass wave energy of a desired polarization.

Reflections generally affect polarization. For radio waves the most important reflector is the ionosphere - signals which reflect from it will have their polarization changed unpredictably. For signals which are reflected by the ionosphere, polarization cannot be relied upon. For line-of-sight communications for which polarization can be relied upon, it can make a large difference in signal quality to have the transmitter and receiver using the same polarization; many tens of dB difference are commonly seen and this is more than enough to make the difference between reasonable communication and a broken link.

Polarization is largely predictable from antenna construction but, especially in directional antennas, the polarization of side lobes can be quite different from that of the main propagation lobe. For radio antennas, polarization corresponds to the orientation of the radiating element in an antenna. A vertical omnidirectional WiFi antenna will have vertical polarization (the most common type). An exception is a class of elongated waveguide antennas in which vertically placed antennas are horizontally polarized. Many commercial antennas are marked as to the polarization of their emitted signals.

Polarization is the sum of the E-plane orientations over time projected onto an imaginary plane perpendicular to the direction of motion of the radio wave. In the most general case, polarization is elliptical, meaning that the polarization of the radio waves varies over time. Two special cases are linear polarization (the ellipse collapses into a line) and circular polarization (in which the two axes of the ellipse are equal). In linear polarization the antenna compels the electric field of the emitted radio wave to a particular orientation. Depending on the orientation of the antenna mounting, the usual linear cases are horizontal and vertical polarization. In circular polarization, the antenna continuously varies the electric field of the radio wave through all possible values of its orientation with regard to the Earth's surface. Circular polarizations, like elliptical ones, are classified as right-hand polarized or left-hand

polarized using a "thumb in the direction of the propagation" rule. Optical researchers use the same rule of thumb, but pointing it in the direction of the emitter, not in the direction of propagation, and so are opposite to radio engineers' use.

In practice, regardless of confusing terminology, it is important that linearly polarized antennas be matched, lest the received signal strength be greatly reduced. So horizontal should be used with horizontal and vertical with vertical. Intermediate matchings will lose some signal strength, but not as much as a complete mismatch. Transmitters mounted on vehicles with large motional freedom commonly use circularly polarized antennas so that there will never be a complete mismatch with signals from other sources.

Transmission and reception

All of the antenna parameters are expressed in terms of a transmission antenna, but are identically applicable to a receiving antenna, due to reciprocity. Impedance, however, is not applied in an obvious way; for impedance, the impedance at the load (where the power is consumed) is most critical. For a transmitting antenna, this is the antenna itself. For a receiving antenna, this is at the (radio) receiver rather than at the antenna. Tuning is done by adjusting the length of an electrically long linear antenna to alter the electrical resonance of the antenna.

Antenna tuning is done by adjusting an inductance or capacitance combined with the active antenna (but distinct and separate from the active antenna). The inductance or capacitance provides the reactance which combines with the inherent reactance of the active antenna to establish a resonance in a circuit including the active antenna. The established resonance being at a frequency other than the natural electrical resonant frequency of the active antenna. Adjustment of the inductance or capacitance changes this resonance.

Antennas used for transmission have a maximum power rating, beyond which heating, arcing or sparking may occur in the components, which may cause them to be damaged or destroyed. Raising this maximum power rating usually requires larger and heavier components, which may require larger and heavier supporting structures. This is a concern only for transmitting antennas, as the power received by an antenna rarely exceeds the microwatt range.

Antennas designed specifically for reception might be optimized for noise rejection capabilities. An *antenna shield* is a conductive or low reluctance structure (such as a wire, plate or grid) which is adapted to be placed in the vicinity of an antenna to reduce, as by dissipation through a resistance or by conduction to ground, undesired electromagnetic radiation, or electric or magnetic fields, which are directed toward the active antenna from an external source or which emanate from the active antenna. Other methods to optimize for noise rejection can be done by selecting a narrow bandwidth so that noise from other frequencies is rejected, or selecting a specific radiation pattern to reject noise from a specific direction, or by selecting a polarization different from the noise polarization, or by selecting an antenna that favors either the electric or magnetic field.

For instance, an antenna to be used for reception of low frequencies (below about ten megahertz) will be subject to both man-made noise from motors and other machinery, and from natural sources such as lightning. Successfully rejecting these forms of noise is an important antenna feature. A small coil of wire with many turns is more able to reject such noise than a vertical antenna. However, the vertical will radiate much more effectively on transmit, where extraneous signals are not a concern.

Basic antenna models

There are many variations of antennas. Below are a few basic models. More can be found in Category:Radio frequency antenna types.

- The isotropic radiator is a purely theoretical antenna that radiates equally in all directions. It is considered to be a point in space with no dimensions and no mass. This antenna cannot physically exist, but is useful as a theoretical model for comparison with all other antennas. Most antennas' gains are measured with reference to an isotropic radiator, and are rated in dBi (decibels with respect to an isotropic radiator).
- The dipole antenna is simply two wires pointed in opposite directions arranged either horizontally or vertically, with one end of each wire connected to the radio and the other end hanging free in space. Since this is the simplest practical antenna, it is also used as a reference model for other antennas; gain with respect to a dipole is labeled as dBd. Generally, the dipole is considered to be omnidirectional in the plane perpendicular to the axis of the antenna, but it has deep nulls in the directions of the axis. Variations of the dipole include the folded dipole, the half wave antenna, the ground plane antenna, the whip, and the J-pole.
- The Yagi-Uda antenna is a directional variation of the dipole with parasitic elements added which are functionality similar to adding a reflector and lenses (directors) to focus a filament light bulb.
- The random wire antenna is simply a very long (at least one quarter wavelength) wire with one end connected to the radio and the other in free space, arranged in any way most convenient for the space available. Folding will reduce effectiveness and make theoretical analysis extremely difficult. (The added length helps more than the folding typically hurts.) Typically, a random wire antenna will also require an antenna tuner, as it might have a random impedance that varies non-linearly with frequency.
- The horn is used where high gain is needed, the wavelength is short (microwave) and space is not an issue. Horns can be narrow band or wide band, depending on their shape. A horn can be built for any frequency, but horns for lower frequencies are typically impractical. Horns are also frequently used as reference antennas.
- The parabolic antenna consists of an active element at the focus of a parabolic reflector to reflect the waves into a plane wave. Like the horn it is used for high gain, microwave applications, such as satellite dishes.
- The patch antenna consists mainly of a square conductor mounted over a groundplane. Another example of a planar antenna is the tapered slot antenna (TSA), as the Vivaldi-antenna.



Typical US multiband TV antenna (aerial)

Practical antennas

Although any circuit can radiate if driven with a signal of high enough frequency, most practical antennas are specially designed to radiate efficiently at a particular frequency. An example of an inefficient antenna is the simple Hertzian dipole antenna, which radiates over wide range of frequencies and is useful for its small size. A more efficient variation of this is the half-wave dipole, which radiates with high efficiency when the signal wavelength is twice the electrical length of the antenna.

One of the goals of antenna design is to minimize the reactance of the device so that it appears as a resistive load. An "antenna



Very common "rabbit ears" set-top antenna

inherent reactance" includes not only the distributed reactance of the active antenna but also the natural reactance due to its location and surroundings (as for example, the capacity relation inherent in the position of the active antenna relative to ground). Reactance diverts energy into the reactive field, which causes unwanted currents that heat the antenna and associated wiring, thereby wasting energy without contributing to the radiated output. Reactance can be eliminated by operating the antenna at its resonant frequency, when its capacitive and inductive reactances are equal and opposite, resulting in a net zero reactive current. If this is not possible, compensating inductors or capacitors can instead be added to the antenna to cancel its reactance as far as the source is concerned.

Once the reactance has been eliminated, what remains is a pure resistance, which is the sum of two parts: the ohmic resistance of the conductors, and the radiation resistance. Power absorbed by the ohmic resistance becomes waste heat, and that absorbed by the radiation resistance becomes radiated electromagnetic energy. The greater the ratio of radiation resistance to ohmic resistance, the more efficient the antenna.

Effect of ground

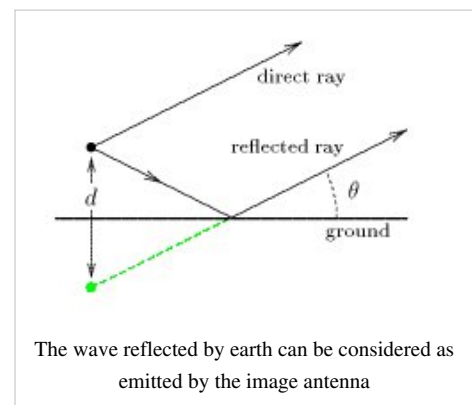
Antennas are typically used in an environment where other objects are present that may have an effect on their performance. Height above ground has a very significant effect on the radiation pattern of some antenna types.

At frequencies used in antennas, the ground behaves mainly as a dielectric. The conductivity of ground at these frequencies is negligible. When an electromagnetic wave arrives at the surface of an object, two waves are created: one enters the dielectric and the other is reflected. If the object is a conductor, the transmitted wave is negligible and the reflected wave has almost the same amplitude as the incident one. When the object is a dielectric, the fraction reflected depends (among others things) on the angle of incidence. When the angle of incidence is small (that is, the wave arrives almost perpendicularly) most of the energy traverses the surface and very little is reflected. When the angle of incidence is near 90° (grazing incidence) almost all the wave is reflected.

Most of the electromagnetic waves emitted by an antenna to the ground below the antenna at moderate (say $< 60^\circ$) angles of incidence enter the earth and are absorbed (lost). But waves emitted to the ground at grazing angles, far from the antenna, are almost totally reflected. At grazing angles, the ground behaves as a mirror. Quality of reflection depends on the nature of the surface. When the irregularities of the surface are smaller than the wavelength reflection is good.

This means that the receptor "sees" the real antenna and, under the ground, the image of the antenna reflected by the ground. If the ground has irregularities, the image will appear fuzzy.

If the receiver is placed at some height above the ground, waves reflected by ground will travel a little longer distance to arrive to the receiver than direct waves. The distance will be the same only if the receiver is close to ground.



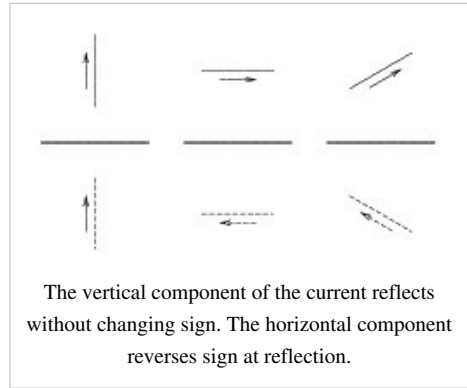
In the drawing at right, we have drawn the angle θ far bigger than in reality. Distance between the antenna and its image is d .

The situation is a bit more complex because the reflection of electromagnetic waves depends on the polarization of the incident wave. As the refractive index of the ground (average value $\simeq 2$) is bigger than the refractive index of the air ($\simeq 1$), the direction of the component of the electric field parallel to the ground inverts at the reflection. This is equivalent to a phase shift of π radians or 180° . The vertical component of the electric field reflects without changing direction. This sign inversion of the parallel component and the non-inversion of the perpendicular

component would also happen if the ground were a good electrical conductor.

This means that a receiving antenna "sees" the image antenna with the current in the same direction if the antenna is vertical or with the current inverted if the antenna is horizontal.

For a vertical polarized emission antenna the far electric field of the electromagnetic wave produced by the direct ray plus the reflected ray is:



$$|E_{\perp}| = 2 |E_{\theta_1}| \left| \cos \left(\frac{kd}{2} \sin \theta \right) \right|$$

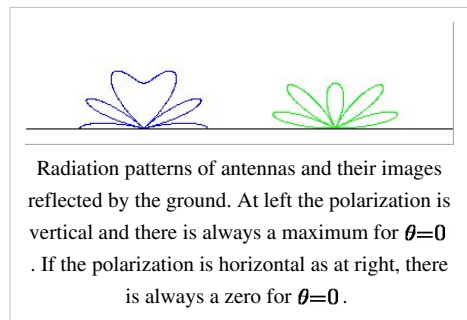
The sign inversion for the parallel field case just changes a cosine to a sine:

$$|E_{\parallel}| = 2 |E_{\theta_1}| \left| \sin \left(\frac{kd}{2} \sin \theta \right) \right|$$

In these two equations:

- E_{θ_1} is the electrical field radiated by the antenna if there were no ground.
- $k = \frac{2\pi}{\lambda}$ is the wave number.
- λ is the wave length.
- d is the distance between antenna and its image (twice the height of the center of the antenna).

For emitting and receiving antenna situated near the ground (in a building or on a mast) far from each other, distances traveled by direct and reflected rays are nearly the same. There is no induced phase shift. If the emission is polarized vertically the two fields (direct and reflected) add and there is maximum of received signal. If the emission is polarized horizontally the two signals subtracts and the received signal is minimum. This is depicted in the image at right. In the case of vertical polarization, there is always a maximum at earth level (left pattern). For horizontal polarization, there is always a minimum at earth level. Note that in these drawings the ground is considered as a perfect mirror, even for low angles of incidence. In these drawings the distance between the antenna and its image is just a few wavelengths. For greater distances, the number of lobes increases.



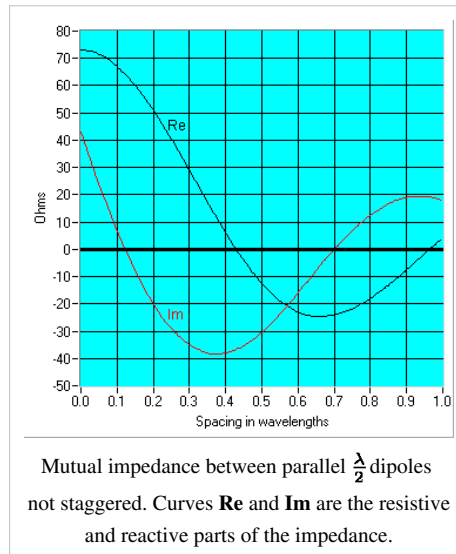
Note that the situation is different—and more complex—if reflections in the ionosphere occur. This happens over very long distances (thousands of kilometers). There is not a direct ray but several reflected rays that add with different phase shifts.

This is the reason why almost all public address radio emissions have vertical polarization. As public users are near ground, horizontal polarized emissions would be poorly received. Observe household and automobile radio receivers. They all have vertical antennas or horizontal ferrite antennas for vertical polarized emissions. In cases where the receiving antenna must work in any position, as in mobile phones, the emitter and receivers in base stations use circular polarized electromagnetic waves.

Classical (analog) television emissions are an exception. They are almost always horizontally polarized, because the presence of buildings makes it unlikely that a good emitter antenna image will appear. However, these same buildings reflect the electromagnetic waves and can create ghost images. Using horizontal polarization, reflections are attenuated because of the low reflection of electromagnetic waves whose magnetic field is parallel to the dielectric surface near the Brewster's angle. Vertically polarized analog television has been used in some rural areas.

In digital terrestrial television reflections are less obtrusive, due to the inherent robustness of digital signalling and built-in error correction.

Mutual impedance and interaction between antennas



Current circulating in any antenna induces currents in all others. One can postulate a **mutual impedance** Z_{12} between two antennas that has the same significance as the $j\omega M$ in ordinary coupled inductors. The mutual impedance Z_{12} between two antennas is defined as:

$$Z_{12} = \frac{v_2}{i_1}$$

where i_1 is the current flowing in antenna 1 and v_2 is the voltage that would have to be applied to antenna 2—with antenna 1 removed—to produce the current in the antenna 2 that was produced by antenna 1.

From this definition, the currents and voltages applied in a set of coupled antennas are:

$$\begin{aligned} v_1 &= i_1 Z_{11} + i_2 Z_{12} + \cdots + i_n Z_{1n} \\ v_2 &= i_1 Z_{21} + i_2 Z_{22} + \cdots + i_n Z_{2n} \\ &\vdots \\ v_n &= i_1 Z_{n1} + i_2 Z_{n2} + \cdots + i_n Z_{nn} \end{aligned}$$

where:

- v_i is the voltage applied to the antenna i
- Z_{ii} is the impedance of antenna i
- Z_{ij} is the mutual impedance between antennas i and j

Note that, as is the case for mutual inductances,

$$Z_{ij} = Z_{ji}$$

This is a consequence of Lorentz reciprocity. If some of the elements are not fed (there is a short circuit instead a feeder cable), as is the case in television antennas (Yagi-Uda antennas), the corresponding v_i are zero. Those elements are called parasitic elements. Parasitic elements are unpowered elements that either reflect or absorb and reradiate RF energy.

In some geometrical settings, the mutual impedance between antennas can be zero. This is the case for crossed dipoles used in circular polarization antennas.

Antenna gallery

Antennas and antenna arrays



A Yagi-Uda beam antenna.



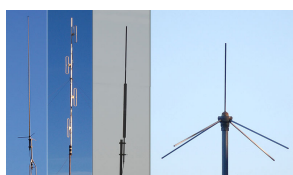
A multi-band rotary directional antenna for amateur radio use.



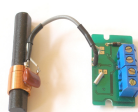
Rooftop TV antenna. It is actually three Yagi antennas. The longest elements are for the low band, while the medium and short elements are for the high and UHF band.



A terrestrial microwave radio antenna array.



Examples of US 136-174 MHz base station antennas.



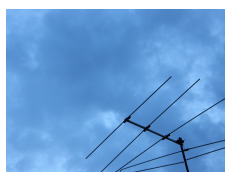
Low cost LF time signal receiver, antenna (left) and receiver (right).



Rotatable log-periodic array for VHF and UHF.



Shortwave antennas in Delano, California.



An old VHF-band Yagi-type television antenna.



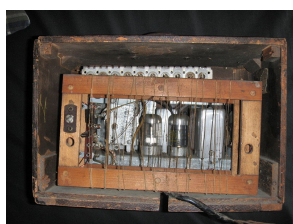
A T2FD broadband antenna, covering the 5-30MHz band.



A US multiband "aerial" TV antenna.



"Rabbit ears" antenna



AM loop antenna

Antennas and supporting structures



A building rooftop supporting numerous dish and sectored mobile telecommunications antennas (Doncaster, Victoria, Australia).



A water tower in Palmerston, Northern Territory with radio broadcasting and communications antennas.

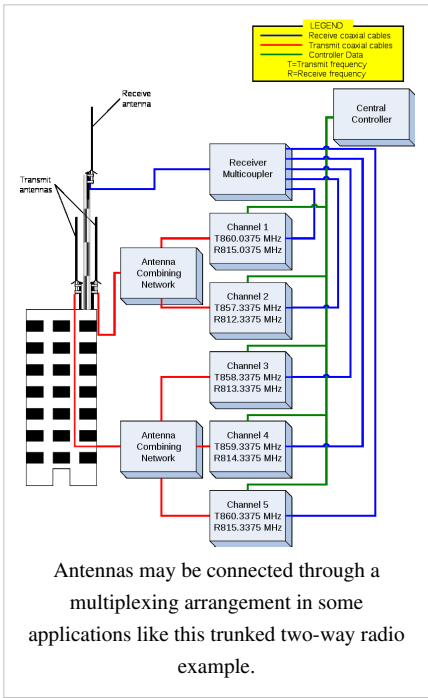


A three-sector telephone site in Mexico City.

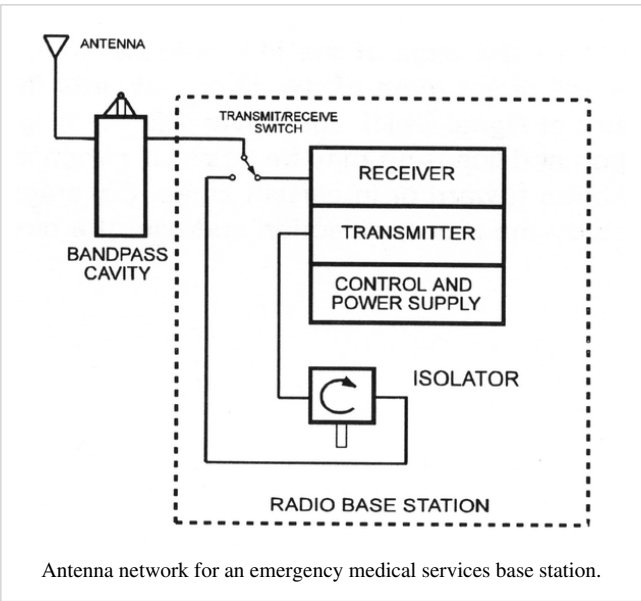


Telephone site concealed as a palm tree.

Diagrams as part of a system



Antennas may be connected through a multiplexing arrangement in some applications like this trunked two-way radio example.



Antenna network for an emergency medical services base station.

Notes

- [1] In the context of engineering and physics, the plural of *antenna* is *antennas*, and it has been this way since about 1950 (or earlier), when a cornerstone textbook in this field, *Antennas*, was published by John D. Kraus of the Ohio State University. Besides the title, Dr. Kraus noted this in a footnote on the first page of his book. Insects may have "antennae", but this form is not used in the context of electronics.
- [2] "*Salvan: Cradle of Wireless, How Marconi Conducted Early Wireless Experiments in the Swiss Alps*", Fred Gardiol & Yves Fournier, *Microwave Journal*, February 2006, pp. 124-136.
- [3] Tesla said during the development of radio that "*One of the terminals of the source would be connected to Earth [as a electric ground connection ...] the other to an insulated body of large surface*". For more information, see "*On Light and Other High Frequency Phenomena* (<http://www.tfcbooks.com/tesla/1893-02-24.htm>)". Delivered before the Franklin Institute, Philadelphia, February 1893, and before the National Electric Light Association, St. Louis, Missouri, March 1893.
- [4] "Guide to Wi-Fi Wireless Network Antenna Selection." (<http://networkbits.net/wireless-printing/wireless-network-antenna-guide/>). NetworkBits.net. . Retrieved April 8, 2008.
- [5] Impedance is caused by the same physics as refractive index in optics, although impedance effects are typically one dimensional, where effects of refractive index is three dimensional.

References

General references

- Antenna Theory (3rd edition), by C. Balanis, Wiley, 2005, ISBN 0-471-66782-X;
- Antenna Theory and Design (2nd edition), by W. Stutzman and G. Thiele, Wiley, 1997, ISBN 0-471-02590-9;
- Antennas (3rd edition), by J. Kraus and R. Marhefka, McGraw-Hill, 2001, ISBN 0-072-32103-2;
- Antennenbuch, by Karl Rothammel, publ. Franck'sche Verlagshandlung Stuttgart, 1991, ISBN 3-440-05853-0; other editions (<http://www.worldcat.org/oclc/65969707?tab=editions>) (in German)
- Antennas for portable Devices (<http://www1.i2r.a-star.edu.sg/~chenzn>), Zhi Ning Chen (edited), John Wiley & Sons in March 2007
- Broadband Planar Antennas: Design and Applications, Zhi Ning Chen and M. Y. W. Chia, John Wiley & Sons in February 2006
- The ARRL Antenna Book (15th edition), ARRL, 1988, ISBN 0-87259-207-5

"Practical antenna" references

- *Antenna Theory* [antenna-theory.com](http://www.antenna-theory.com) (<http://www.antenna-theory.com>)
- *Patch Antenna: From Simulation to Realization* EM Talk (http://www.emtalk.com/mwt_mpa.htm)
- *Why an Antenna Radiates* at ARRL (<http://www.arrl.org/tis/info/whyanradiates.html>)
- *Why Antennas Radiate*, Stuart G. Downs, WY6EE ([http://www.arrl.org/files/file/QEX Binaries/0105downs.pdf](http://www.arrl.org/files/file/QEX%20Binaries/0105downs.pdf)) (PDF)
- *Understanding electromagnetic fields and antenna radiation takes (almost) no math*, Ron Schmitt, EDN Magazine, March 2 2000 (<http://www.classicstela.com/download/emfields.pdf>) (PDF)
- Tests of FM/VHF receiving antennas. (<http://www.aerialsandtv.com/fmanddabradio.html#FMandDABaerialTests>)
- <http://www.tvantennasperth.com.au/Diyantennas.html> : "Antenna Gain"

Theory and simulations

- EM Talk, " Microstrip Patch Antenna (http://www.emtalk.com/tut_1.htm)", (Theory and simulation of microstrip patch antenna)
- " Online Calculations and Conversions (<http://www.jampro.com/index.php?page=technical-documents-and-calculators>)" Formulas for simulating and optimizing Antenna specs and placement
- " Microwave Antenna Design Calculator (<http://www.q-par.com/capabilities/software/microwave-antenna-design-calculator>)" Provides quick estimation of antenna size required for a given gain and frequency. 3 dB and 10 dB beamwidths are also derived; the calculator additionally gives the far-field range required for a given antenna.
- Sophocles J. Orfanidis, " Electromagnetic Waves and Antennas (<http://www.ece.rutgers.edu/~orfanidi/ewa/>)", Rutgers University (20 PDF Chaps. Basic theory, definitions and reference)
- Hans Lohninger, "Learning by Simulations: Physics: Coupled Radiators (http://www.vias.org/simulations/simusoftware_twoaerials.html)". [vias.org](http://www.vias.org), 2005. (ed. Interactive simulation of two coupled antennas)
- NEC Lab (<http://www.ingenierias.ugto.mx/profesores/sledesma/documentos/index.htm>) - NEC Lab is a tool that uses Numerical Electromagnetics Code and Artificial Intelligence to design and simulate antennas.
- Justin Smith " Aerials (<http://www.aerialsandtv.com/aerials.html>)". A.T.V (Aerials and Television), 2009. (ed. Article on the (basic) theory and use of FM, DAB & TV aerials)
- Antennas Research Group, " Virtual (Reality) Antennas (<http://www.antennas.gr>)". Democritus University of Thrace, 2005.
- "Support > Knowledgebase > RF Basics > Antennas / Cables > dBi vs. dBd detail (<http://www.maxstream.net/helpdesk/article-27>)". MaxStream, Inc., 2005. (ed. How to measure antenna gain)
- Yagis and Log Periodics, Astrosurf article. (<http://www.astrosurf.com/luxorion/qs1-antenna4.htm>)
- Raines, J. K., "Virtual Outer Conductor for Linear Antennas," Microwave Journal, Vol. 52, No. 1, January, 2009, pp. 76–86
- Tests of FM/VHF receiving antennas. (<http://www.aerialsandtv.com/fmanddabradio.html#FMandDABaerialTests>)

Effect of ground references

- Electronic Radio and Engineering. F.E. Terman. McGraw-Hill
- Lectures on physics. Feynman, Leighton and Sands. Addison-Wesley
- Classical Electricity and Magnetism. W. Panofsky and M. Phillips. Addison-Wesley

Patents and USPTO

- CLASS 343 (<http://www.uspto.gov/go/classification/uspc343/defs343.htm>), Communication: Radio Wave Antenna

Further reading

- Antennas for Base Stations in Wireless Communications, edited by Zhi Ning Chen and Kwai-Man Luk, McGraw-Hill Companies, Inc, USA in May 2009

Article Sources and Contributors

Comparison of mobile phone standards *Source:* http://en.wikipedia.org/w/index.php?oldid=403676863 *Contributors:* -def, Achangeisasgoodasa, Avneesh rupal, CaribDigitita, ClementSeveillac, Comatose51, CosineKitty, DocWatson42, Download, FayssalF, Fishtron, Fresheneesz, Gnewf, Gvkinal, Hmwith, Jidanni, Kalleboo, Kozuch, Lightmouse, MMuzammils, MSTCrow, Mange01, Mariersteve, Marks, Mathiastck, Mdwyer, Mojodaddy, Momo san, Moxfyre, Mukkakukaku, Nakumi, Phroggy, Phyrus, RHaworth, Richard Kervin, Sandox, Seoidau, Sigma902, Steppres, Tomi T Ahonen, Towel401, Unforgettableid, Vegaswikian, W17aml, 81 anonymous edits

3G *Source:* http://en.wikipedia.org/w/index.php?oldid=405215108 *Contributors:* 121a0012, Itephania, 2D, A bit iffy, ABF, Ab1, Abce2, Abrech, Achromatic, Adamdiant, Adpenaranda, Aeonx, AgarwalSumeet, Aitias, Akshay2212, AlephGamma, Alexius08, Aliceokello, Allanrod, Allkindsofthings, Allseen, Amarhindustani, Andreaskem, Andres, Andreworkney, Andros 1337, Animum, Arastep, Article editor, Arunprabu.v, Ary29, Asaliyev, Audrius u, Avoided, Awesomepothi, Baloo rch, Barras, Bbx, Behind The Wall Of Sleep, Beland, Ben kenobi 00, BenFrantzDale, Bijee, Binyamin Goldstein, Blaisorblade, Blake-, Blanchardb, Bluezy, Bobblewik, Bobet, Bonadea, Bongwarrior, Boothy443, Bpangti, Breakeydown, Brianski, Bsoft, Bugnot, Bunnyhop11, Cacophony, CambridgeBayWeather, Camitommy, Can't sleep, clown will eat me, Cctan-daphanelg, Cdman882, Ceros, Cfaerber, Chancheelam, Chaojoker, ChigoZ, Chrisbolt, Christopher Mann McKay, Chuck Marean, Chuckwits, Cihan, Courcelles, Courtarro, Crakktot, Ctrw, Cuppa, DARTH SIDIOUS 2, Daften, Dan100, Dancter, DanielDeibler, Danielcohn, Dansk14, Dantis, Darth Panda, Davewho2, Dawnseeker2000, DeadEyeArrow, Debpratim.ghosh, Debroglie, Denilsen, DerHexer, Dicklyon, Digfareenough, Digisus, DiiCinta, Dikteren, DocWatson42, DonBronson, Doublex120, Download, Dpareit, Drizzd, DuffDudeX1, ESkog, Earth, Edcolins, Edknol, Elassin, Elavendran, EliasAlucard, EmirA, Enochlau, Eprb123, Erianna, Erotml, Erunestian, Esurnir, Ethridgela, Euchiasmus, Evdo, Evil Monkey, Falcon8765, Fanatix, Ferdinand Pienaar, Flashywordz, Fleetfuhl, FrYGuY, Freakofnurture, FrummerThanThou, Fudoreaper, Fui in terra aliena, Funandtrvl, Fuzheado, Fæ, GJDR, Gail, Galoubet, Gerbon689, Gggh, Gh5046, Ghildiaysumit, Ginsengbomb, Giraffedata, Gja822, GoLLoMboje, Gogo Dodo, Golbez, Goodvac, Grafen, Graymornings, GregA, Gurchzilla, H3llbringer, Hadal, Hadiyana, HaeB, HairY Dude, Hanacy, Haresh06, Harryzilber, Harshthegreat89, Heartnseoul, Heman, Hoosteen5, Hornlitz, Hu12, Hurmata, IRP, IReceivedDeathThreats, IceKarma, Igveinfo, Immunize, Impi, Insanity Incarnate, InternetMeme, IntrigueBlue, Ixfdd64, J Crow, J.delanoy, JVz, Jab843, Jack999999, Jagged 85, Jaizanuvar, James.pole, James086, Jamessungjin.kim, Jarsyl, Jasongolod, Jatra, JavierMC, Jcw69, Jean15paul, Jeepday, Jeff G., Jeffq, Jiang, Jigen III, Jmlinden7, Incraton, Joal ban Kluaane, Joe18, Joes8888, John1, JohnTechnologist, JonHarder, Jonpaulusa, Jortheo, Joycloete, Jpatokal, Julesd, Kalanzit, Kamath.nakul, Kanthamohan, Kbh3rd, Kdriver, Kimchi.sg, KirrVlad, Klimov, Knowledge lover1123, KnowledgeOfSelf, Kozuch, Krymson, Ksarawar, Kurumban, L0L, Laager, Le Fou, Leafyplant, LeaveSleaves, LeviathinXII, LiDaobing, Lightmouse, Lilac Soul, Lord of the Pit, Loti, Lucy1981, MMuzammils, Mac, Mackeriv, Mafmafmaf, Mange01, Marnues, Mat-C, Matdrones, Materialscientist, Mathiastck, Maxis ftw, Mercury McKinnon, Mesquita, Mets501, Mfactor, Midway, Mikeo, Mindmatrix, Minesweeper, Mojodaddy, Monaarora84, MonoAV, Mortense, Morton.lin, Morwen, Mosh1111, Mowgli, Mswake, Muhandes, Munawarmuniruae, Mysid, N0YKG, Naerli, NawlinWiki, Nelson00, Newone, Nibuud, Nigel XX, Nirala nagar, Nisselua, Nixeaegle, Noctibus, Nolibur, Nono64, Noodlenut, Nubiatedch, Ocaasi, Odie5533, Ochofucius, Oldiesmann, Oli Filth, OneP6t18, Oneliuss, Padgeman, Pahari Sahib, Panscient, Pantosys, Phamma, Pdcok, Peter.C, Petiatil, Pgan002, Pharaoh of the Wizards, Phoenix-forgotten, Photoo, Pikiwin, Pinethicket, Piz d'Es-Cha, Pizzadeliveryboy, Pmicel, Prashanthns, Prateekchanda, Pretzels, Probrell, Pvsadev, Radagast83, Radiojon, Radiosband, RainbowOfLight, Rat144, Ravenperch, Raymondwin, Rbarpar, Ricky81682, Rjme656, Rjwilmsi, Robert K S, Rockysmile11, RoySmith, Rrburke, RuED, RuM, Rwalters, Ryuch, SJ, Saddy Dumbington, Sagale, Saimhe, Sajalkdas, Salamurai, Samdlaw, Sanmele, Sceptre, SchmuckyTheCat, Sciriune, Secretlondon, Sedathut, Sexymann48, Sgb22, Shaktiyadav, Shamespwns, Sharp11, Sheki nitk, Shenme, Shiro jdn, Shirulashem, Siddhant, Silvestre Zabala, Simone, Skaterdan323, Slammer111, Snigbrook, Sole Soul, Solipsis, SpLoT, Springclean, Squallwc, Stephan Leeds, Stephenb, Strandist, Supertouch, Synchrite, T0ky0, THEN WHO WAS PHONE?, TJJFV, Tekosyete, Telecomwave, TellWeb, TexasDawg, The Thing That Should Not Be, Thingg, Tillmo, Timewatcher, Tobixen, Togo, Tomi T Ahonen, Tommy2010, Towel401, Toytoy, Tpradbury, Tracer9999, Tregoweth, Trevyn, Triona, TrumpetPlayer, Tsange, Turian, Ugur Basak, Utcursch, ValC, Vanished user 34958, Vbs, Vec, Vegaswikian, Verdatum, Versus22, VictorianMutant, Violetriga, Vipinhari, Viriditas, WATP, Waterfox, Wavelength, Wdwd, Webshared, Wernher, Whereisjim, Wideangle, Wikiliki, Wikitumnus, Wikizen, Wildrider99, Wjfox2005, Worldedixor, WriterHound, Yamla, Yoenit, Yuckfok, Zakia4, Zanol, Zernovoi, Zigger, ZimZalaBim, ZooFari, Zorxd, Zuanzuanfuu, Zzuuzz, 1212 anonymous edits

CDMA2000 *Source:* http://en.wikipedia.org/w/index.php?oldid=405315487 *Contributors:* Ablabla459, Adaryanto, Alohawolf, Andros 1337, Ario28, Armando82, Asankakr, Aughtandzero, Avik pram, Axylight, Bdragon, Beland, Berencicity, Betacommand, Bgurg, Bluezy, Bobblewik, Breno, Cdc, Chengli.liu, Cipz, Cmgross, Crimsonedage34, Crystallina, Deelan006, Drjmb, DropDeadGorgias, Dudyk al, DuncanHill, DylanW, Editore99, Elume, Email4mobile, Engineerism, Eurolite x3, Firsfron, Fudoreaper, Fuzheado, Gdn, GeneralBelly, Goofrider, Hadal, Haruyasha, Helixblue, Henri de Solages, Hongooi, Imcdnzl, InternetMeme, Intgr, Jabz10, James.pole, Jensbn, Jesse Viviano, Jewel96, Jhdaly, Jmoz2989, Joaopaulo1511, John Chamberlain, JonHarder, Jonverve, Joviman, Jpatokal, Jusjih, JustinRossi, KJRehberg, Karn, Kauczuk, Khalid hassani, Kinema, KnightRider, Kooky, Kozuch, Ksn, Kyng, Lappack, Lesswrie, LeviStrauss, LilHelpa, Markalex, MichaelWheeler, Mikefzhu, Mojodaddy, Mozzerati, Musically ut, Nisselua, Nkcm, NuclearWinner, Omiazad, Owt, Petri Krohn, PhilHibbs, Porttikivi, Protean, Qst, RHaworth, Rdschwarz, RedWolf, Ren0, Requestion, Rjairam, Rohan Jayasekera, Sakimori, Sauralf, Sewebster, Shankarcs, Skyfire, Smileglance, StradivariusTV, Supaklailert, Swid, Tfine80, The Fifth Horseman, Thunderbird2, Trialsanderrors, Umbrau44, Vespristiano, Vishyvoice, VoxLuna, Wdwd, Woohokitty, WriterHound, Xxxxx, Yosh3000, Zagothal, Zigger, Zygmunt lozinski, 387 anonymous edits

3GPP Long Term Evolution *Source:* http://en.wikipedia.org/w/index.php?oldid=404807464 *Contributors:* 1983px, 81120906713, Adamr81, Adrianski, Afiler, Aintneo, Akshays, Alakh.jai, Alexander Chervov, Alexandre.2.beaudry, Alexkon, Altaphon, Andros 1337, Ashokec, Avamsik, Balajai280283, Basangbur, Bctwriter, Bender235, Benignbala, Bin22, Boffbo, Brendabum, Brian2wood, Brotheryu, Bssc81, Camw, Can't sleep, clown will eat me, Capstar12, Cfeet77, Chmyr, Chowbok, Chris the speller, Chris01720, Conti, Crati, Cycloneopp, DaMan92, Daithibaru, Dalyswe, Damian Yerrick, Darin-0, David Haslam, David Levy, Dawnseeker2000, Deineka, Dipankar biswas, DmitryKo, Doris Meier, Dorsacato, Dwonak, DylanW, EXonyte, Editore99, Egmontaz, Ehugne, Eikoseidell, Elisabeth Hillman, Ensconsed, Envelopetracker, Epameinondas, Escottf, Excirial, Fbiots, Firetwerk, Fishbert, Flexar, Fstorno, Fudoreaper, Gaius Cornelius, Gcfreeland, Georgematewiki, Gerti W, GoLLoMboje, Goingstuckey, GregA, Gsarwa, Guspaz, Guy Harris, Hgmyung, Hijklmno, ICanAlwaysChangeThisLater, Iansanderson, Impala2009, InternetMeme, Iolaire, Isheden, Isoman00, JHUnterJ, JMiall, Jakeroot, Jamessungjin.kim, Jb 007clone, JefeMxltli, Jim.henderson, Jlf, Jmgonzalez, Jni, Joconnor, John Broughton, Johnnyjagger, Jpat34721, Jspaid, Jswin123, JustinRossi, Kanags, Kbrose, Kevinmon, KirbyRandolf, Konst1977, Kozuch, Kushal one, Kyng, Letireur, Lightmouse, Lisa Andersson, Lonniev, Lohart, Louisarogers, LukeTheSpook, M2Ys4U, MC-CDMA, MMuzammils, Mafeu, Maikel, Mange01, Manop, Marv moskowitz, Maryhit, Matthew, Mblumber, Merf64, Metageek, MichaelVernonDavis, Miguelameida, Mills00013, Mindmatrix, Mojodaddy, Mortense, MrOllie, Mrwojo, Muhandes, Muhdunahmad, Mwaibsen, Mwanner, Mwoleben, Mynetworks, Nelson50, Nick in syd, Nicknmr, Nikpapag, NoJackhorkheimer, Ohnoitsjamie, Oli Filth, Oliyoung, Omegatron, Paradoxian, Paultt, Phatom87, ProtocolOH, Psgimon, QueueNut, Rajjivs, Ranjithsutari, Remind me never, Retroneo, Rich Farmbrough, Rick7425, Rjwilmsi, Ronz, Rupert baines, Saini613, Sajalkdas, Santiperez, Scatter98, Schwijker, Scrapking, Secator, Semiautomata, SidP, Siddhant, Smnc, Solphusion, Soyguapa, SpK, Spiral5800, Spotticus, Squiggleslash, St3vo, Stefoun, Sunflowermalta, Swellesley, TRosenbaum, TY-214, Tali, Thanthalas39, TheAllSeeingEye, TheBigZzz, Toomooomba, Tuxa, Uvb, Vega702, Vernapp, Vishal Singhal, Vocaro, Wdfarmer, Wikiborg, Wirelessgal, Wksam, Wikiborg, Xaltoton, Yellowdesk, ZacBowling, 410 anonymous edits

Router *Source:* http://en.wikipedia.org/w/index.php?oldid=405673941 *Contributors:* 128.107.253.xxx, 16@r, 1wofblake, 4.35.185.xxx, 4twenty42o, A8UDI, AKMask, AdamWeeden, Adamantios, Adamn, Aditya, AdjustShift, Adoniscik, Aecis, Aeusoes1, Afed, Ahoerstermeier, Ahyl, Ajo Mama, Akc9000, Alan Liefthing, Aldie, Alex Smotrov, AlexFerrara, Alexandropolis, Algebra, Algocu, Alimaq9, Altimolc, Altoniske, Alvin-cs, Alyssapvr, Amire80, Andy102990, Angr, Anonymi, Antandrus, Anthonyjameswood, Arch dede, Arnon Chaffin, Atchius, Avoided, BMB, Barnea, Bbukh, Bcat, Bebenko, Ben D., BenAveling, Benemin, Bernard S. Jansen, Betbest1, Bevo, BigChicken, Bishonen, Blood reaper, BlueH2O, Bobo192, Boing! said Zebedee, BorgHunter, Boscobiscotti, Brandon, Brendan Moody, Brianboonstra, Brianga, Bryan Derksen, BrydoF1989, Bunnyhop11, CWii, Cactus.man, Camw, Can't sleep, clown will eat me, Canterbury Tail, Capricorn42, CardinalDan, CaribDigitita, Carlwिकारl, Catbar, Causa sui, Chachoo, Cburnett, CecilVard, Chexum, ChilipalmerIII, Chlodwig, Chun-hian, Chuq, Clemente, Cobi, Colonna, Cometstyles, Conversion script, Cpl Syx, Crakktot, CroweIO, DARTH SIDIOUS 2, Damian Yerrick, Daniel.Cardenas, Darth Panda, David0811, DavidCiani, DeadEyeArrow, Deagle AP, Deepak365, Delirium, Demicx, Dennis, DerHexer, Desuz, Dgies, Dinko13, Discospinster, Dmt018, DocWatson42, Dpm64, Drhex, Dtrebbien, Eclipssettaja, Edokter, El C, Emote, EmporerD, English Fox, Enviroboy, Eprb123, Eric Shalov, Ethereal Dragon, Excirial, Extols, Extransit, F15x28, Fabricationary, Face, Facts707, Falcon8765, Favonion, Ferkelparade, Finereach, Firebee, Flewis, Francis E Williams, Frap, Furrykef, Fuzheado, Fvw, Fyyer, GB fan, GSSAGE7, Galoubet, Gareth Jones, Gascreed, Gazwald, Gcirafrisi, Geek2003, Geimas5, Gidonb, Giftlite, Gjp23, Glenn, Goat-see, Gogo Dodo, Goodnightmush, Gracenotes, Graeme Bartlett, Graham87, Green451, Gtg204y, Gwernol, Gökhan, Hadal, Hairmare, Ham Pastrami, Harwardedotcom, HarlandQPitt, Hashir tasleem, Heckerowitzz, Hd83, Heavy1974, Herambal1, Hfzeto, Hibana, Hm2k, Honta, Hsmith254, Humannetwork, Hut 8.5, IRP, IRT.BMT.IND, Ian Lynch, lanmacm, Ilario, Imran, Insanity Incarnate, Ireneshusband, Iridescent, Ironholds, Isatre, Itai, J Di, J.delanoy, JForget, JPilborough, JTN, Jacheem.m.eqbal, Jackrabbt2, James086, Jared Preston, Jasonfward, Jaxl, JdeJ, Jec, Jhdaly, JidGom, Jim.henderson, Jinlye, Jjron, Jkn, Jodi.a.schneider, JoeOnSunset, JohnT, JonHarder, Jrash, K Watson1984, K4DSP, Kakeru, Kaszeta, Kbolino, Kgfeischmann, Kgrg, Kingghost, Kizor, Kku, Klemen Kocjancic, Komap, Kremit, Kukini, Kuru, Kwamikagami, L00pLaUzXxX, LachlanA, Leandrops, LeaveSleaves, Leeb, Leodmacleod, Lepidus16, Lerdthenerd, Liftarn, Lightmouse, LightningMultiCom, LilHelpa, Lilac Soul, Little Mountain 5, LittleBenW, Livrocanea, Lloyd Wood, LonelyBeacon, LouScheffer, Love manjeet kumar singh, Lowzeewee, Luna Santin, Luo, Luxomni, MER-C, Mac, Mackensen, Magioladitis, Marek69, Markharris, Masonprof, Mateo SA, Mattgirling, Matthew Martin11, Matusz, Mav, Mboverload, Meegs, Memset, Mgoerner, Miaow Miaow, Micahhiggs, Michael Devore, Michael Hardy, Middeladid, Mike1024, Mills, Minna Sora no Shita, Mintleaf, Mipadi, Mmerex, Mo0, Mohitsport, Monkeyman, Moonie0079, Moratinz, Moulding, Mrx374325732, Mschlindwein, Mushroom, Mxn, Mygerardromance, Nakon, NaranKPatel, Natkeeran, Nbarth, NerdyScienceDude, Nethgirb, Netkinetic, Neuro, Neverquick, Ngriffeth, Nick, Niteowlneis, Njh, Nmacu, Nn123645, No Guru, NonobisSolum, Npss, Nubiatech, Nww mag, Octahedron80, Odie5533, Oli Filth, Omega187, Omicronpersei8, OrgasGrl, PJTraill, Palsmarbort, Papadopa, Paul Koning, Pbb, Pchov, Pedant17, Penosa, Petrasmom, Phil Holmes, Philip Trueman, PhilipMW, Phynicen, Piano non troppo, Pianodude363, Pinethicket, Polly, Possum, Potter831, Pradeep pn, Pradeepdesign, Prolixium, Protonk, Quinxorin, RTC, Raano, Raul654, Readro, RebelzGang, Rebroad, Retodon8, RexNL, Rhanbury, Rick Sidwell, Ricky@36, Rjwilmsi, Roberts83, Robertvan1, Robthebob, Rohithrakall, Rollier, RonSigPi, Rrjanbiah, S-n-ushakov, SJP, Sakhalinf, Scootey, Secretlondon, Seraphimblade, Shadowjams, Shahid789, Shanedidona, Shanes, Sharon gngt, Shervinafshar, Shortynugget, Shyamal, SilentC, Simetrical, SimonMackay, SirGrant, Skipperdd, Slp1, Smalljim, Smappy, Sonicforest, Sorintopex, SpaceFlight89, Specs112, SpuriousQ, Sridev, Staka, Stephenb, Sternagel, Steveboy90, SummonerMarc, SunSw0rd, Tabasco01, Team4Technologies, TechNotch, Tedickey, Tekinfo, Telecomwisdom, The Anome, The Thing That Should Not Be, TheDwoo, TheJ2, Thornomad, Thorpe, Tide rolls, Timberlake, Tiinucherian, Titoxd, Tobycat,

Tollund man, Tomas skare, Tomgreeny, Tommcce7, Tommy2010, Tony1, Topdeck, Travisyoung, Triwbe, Tumbledry, TwistOfCain, Tylerdmace, Typhoonchaser, Tyrenius, UU, Uncle Dick, Unfree, Vanka5, Vassili Nikolaev, Vegaswikian, Verbatim9, Vhiskas, Via strass, Vijaykcm, Vishalsaran, Vishnava, Vjardin, Voicrouter, Voidxor, Vorthax, Vvarkey, W Nowicki, Wagers, Waxiemarie, Wernher, Western Pines, Wideangle, WikiFew, WikiLeon, WillMak050389, Willie the Walrein, WinTakeAll, Winkydink, Wlgrin, Wtmitchell, Wtshymanski, X42bn6, Xmp, Xtreme.msen, Xyzy288, YUL89YYZ, Yamamoto Ichiro, Yath, Yelyos, Yendor1958, Yennathan, ZacBowling, Zachb90e, Zeroshell, Zpb52, Zwirello, 1104 anonymous edits

Machine-to-Machine *Source:* http://en.wikipedia.org/w/index.php?oldid=399991608 *Contributors:* A Nobody, Affleb, Affiliat, Alecv, Austinmills, Bjoertvedt, Bsandg, Byron.appelt, CL, Crispnmuncher, DanielPenfield, Dbrennan17, Drbreznjev, Ezuk, Flowerpotman, George100, Gixbrown, Gogo Dodo, Gwernol, Hu12, Ignorance is strength, Internetofthings, Isida1028, Jcarterwil, JoeBiron, JoeSmack, Justindrew, Kjlweis, Kozuch, Kuru, M2M, Machfest, MariaSantella, Mgwai, MrOllie, NickShoe, OlYeller21, Oleg Alexandrov, Paws222, PeterSymonds, Pie Man 360, Pikaco, Reficelcor, Ridernyc, Rjwilmsi, Rmorillo, RoyKok, Saturnine42, Sbisolo, SidP, Silver seren, Stevage, Stoneygirl45, Sushant gupta, Swwhitehead, TastyPoutine, Thierry37 2, Timothy Andux-Jones, Vchava, Wavelength, 106 anonymous edits

Input/output *Source:* http://en.wikipedia.org/w/index.php?oldid=405081736 *Contributors:* 16@r, ABF, Ahoerstemeier, Aidan W, Ale jrb, Alecv, AlexanderPar, Algotime, Andy16666, Anonymous4367, Anuang, Apokrif, Atreyu42, AxG, B4hand, Badseed, Bento00, BlueSquadronRaven, Blueraspberry, Bobianite, Bornhj, Bryan Derksen, COMPATT, Calmer Waters, CanisRufus, Conversion script, Courcelles, Csigabi, Cuperdon, DXBari, Daemorris, Dave6, Dawewild, DavidLevinson, Dawnseeker2000, DragonHawk, Drmies, EagleFan, Eprb123, Ewlyahoocom, Excirial, FatalError, Fritzpoll, Furrykef, Fvw, Gardar Rurak, Goodoldpolonius, Goodoldpolonius2, Goodvac, Graham87, Greenrd, Grika, Gurch, Guy M, Hadal, Hairy Dude, Happysailor, HarisM, Helixblue, Hellisp, Hemanshu, Heron, Hut 8.5, Ignacioerico, Ithateblazing, Iridescent, Isnow, Ixf64, Ja 62, Jbattersby, Jj137, Jnc, Jumpytoo, Jusdafax, Kanonkas, Karl-Henner, Kathryn NicDhàna, Kbdank71, Kesla, Khargas, Knowledge Seeker, Kusunose, Kyz, Lambiam, Lee Daniel Crocker, LeeDanielCrocker, Liberatus, Little Mountain 5, Manway, McBrayn, Mdebet, MeganMc08, Merlion444, Mintleaf, Mirror Vax, MsHyde, Mudlock, Mwtoews, N-Man, NapoliRoma, Neilc, NevilleDNZ, Nivix, Nixdorf, Noah Salzman, Oda Mari, OrgasGirl, Orion11M87, Patrick, PdDemeter, Polluks, Polonium, Pseudomonas, Public Menace, Pussyhole, QASIMARA, Quoxplusone, RedWolf, Redconfetti, Rencas, Rhrad, Richdiesal, Rjstott, Rjwilmsi, Rlove, Rtdrury, Saintuser, Saric, Sciturne, Seaphoto, Siroxo, Sligocki, SoSaysChappy, Sonnyjim 06, Stephenb, Suruena, Tagishsimon, Tatterfly, Tbhotch, Tempodivalse, The Rogue Penguin, Thehotelambush, Tobias Bergemann, Tommy2010, Tompsci, Tpk5010, Twaring, TutterMouse, TuukkaH, Useight, V4nd4l king, Vipulcvyas, Voyagerfan5761, Waycool27, Wmahan, Ykh Wong, ZenerV, Zhernovoi, Zzuuzz, 325 anonymous edits

RS-232 *Source:* http://en.wikipedia.org/w/index.php?oldid=405649839 *Contributors:* 209.75.42.xxx, 64.180.177.xxx, AJim, Abisys, Acather96, Adoniscik, Aldie, Ali@gwc.org.uk, Allen Moore, An-chan, Andrew Hampe, Arch dude, Aronzak, Atlant, Ato basehore, Austinmurphy, AxelBoldt, Bajsejohannes, Baylink, Bert490, Bevo, Bobblewik, Bollinger, Bon21, Bongwarrior, Bovineone, Breakpoint, Brouhaha, Bryan Derksen, Buddhikaeport, CWenger, Caerwine, CanOfWorms, Captain Segfault, Captainspizzo, Charivari, Chrike, Christopher Parham, ClementSeveillac, Closeapple, Colonies Chris, Conversion script, Crispnmuncher, Crissov, Djeffo, DanMS, Danhash, Davandron, Dave Yost, Dekisugi, Delirium, Deor, DmitTrix, Dmlmax, Dmsar, Druirool, Ed Brey, Ed g2s, Efalk, Egil, Electron18, Electron9, Engineerism, Evicse, Exosort, Extrantist, Face, Fahidka, Femto, Ferkelparade, Fingew, Fixxed, Flydpnktrn, Frap, Gazpacho, Gcbirzan, Gimmietrow, Glenn, Gogo Dodo, Hatched3, Hawklord, Hcberkowitz, Heron, Hit.kansagra, Hopp, Hpa, IanOsgood, IlyaHaykinson, Imroy, Inter, Itai, J Clear, JLD, Jason One, Jaktns, Jcmaco, Jeh, Jheald, Jonbowen234, Jonsg, Jonverve, Jroddi, Justfred, Keilana, Koavf, Krótki, Ksero, Kthbn, KyferEz, L Kensington, Lambiam, Liftam, Lightmouse, Linkmimer, Lio, Luna Santin, Lunawill, Maarten1980, Maldobster, Malcolm Farmer, Mange01, Markthemas, Maury Markowitz, McCulley, Mikeblas, Miketwo, Mild Bill Hiccup, Mipadi, Miquanranger03, Mmxx, Mobius, Mortense, NHRHS2010, Nasa-verve, Neil.steiner, Nekkensj, Ngorham, Nicolaasuni, Nixdorf, Nmnogueira, Oparidae, Orlolan88, Overdoer949, Paddu, PaterMcFly, Paul Foxworthy, Petr Kopáč, Petri Krohn, Plugwash, Pointillist, Poppafuze, Pplshero54, Phurmes, RTC, Reddi, Requestion, Reswobslc, Rgraham nz, Rich Farmbrough, Rick Sidwell, Rjwilmsi, Robinhw, Ronaldsmith, Rowine719, Rror, S Roper, SEREGA784, SGBailey, Sam Hovevar, Samuel Tardieu, Smeirow, SchmuckyTheCat, Scott McNay, Shaddack, Shadowjams, Sigmundg, Signal7, SixSix, Snafflekid, Someguy1221, SpaceFlight89, SparhawkWiki, Spitfire, Spoxox, SreekumarC, SummitWulf, Sweetie Rose, The Yowser, The imp, Theo177, Theresa knott, Thunderboltz, Tim Starling, Tkbwik, Tokachu, TomViza, Tongtang, Tony esopi patra, Toolnut, Topory, Tothwolf, Towel401, Tsaavik, Uncle Milty, Underdog, Useight, Utcursch, Uzume, Vertago1, Vihljun, Vrenator, Weevil, WeißNix, West London Dweller, WillFarrell, Wipe, Wmahan, Wtshymanski, Xenonice, Yonkie, Zoicon5, 503 anonymous edits

RS-422 *Source:* http://en.wikipedia.org/w/index.php?oldid=400361964 *Contributors:* Andrew sh, Anthony Bradbury, Bobblewik, Brolin Empey, CanisRufus, CesarB, Crm123, David Gerard, Dennis, DirkHelgemo, Dorftrottel, Dysprosia, Fahidka, Femto, Fightin' Phillie, Garzo, Ged UK, Haikupoet, Hongooi, Hpa, Iridescent, ISNOW, J Clear, J Crow, Jerome Charles Potts, Joeyhagedorn, Jonverve, Khrose, Kslicch, Linkminer, M7, Markus Kuhn, Mboverload, Nelson50, Rjwilmsi, Robinhw, Ronaldsmith, Sciams, Shaddack, SimonP, Skarg, Template namespace initialisation script, Thaas00, Unyoyega, Wtshymanski, Xezbeth, Yuriybrisk, 42 anonymous edits

EIA-485 *Source:* http://en.wikipedia.org/w/index.php?oldid=403655219 *Contributors:* 4k05, Adamarthurryan, AlexBadea, Andrew sh, Armistej, Arteille, Back ache, Birdy1982, Bon21, CanisRufus, Charlierichmond, CiudadanoGlobal, Cst17, Cybercluster, DMahalko, Dbrunner, Dekisugi, Deor, Deville, Dicklyon, Dmlmax, Electron18, Electron9, EncMstr, Fahidka, Femto, Fleminra, Fox, Frap, Frappucino, Fratrep, Freetoetheeworld, Funvill, Gene Nygaard, Gogo Dodo, Gri6507, Homo stannous, I2so4, Intchanter, Isnow, J.delanoy, Joel Saks, Jonverve, Jzap, Kevin, Kristen Eriksen, Lectorar, Lightmouse, LinkTiger, Littleman TAMU, M7, MagicBobert, Marianoceowski, MaxSem, MementoVivere, Mjuarez, Mortense, Nelson50, Petr Matas, Pyrrhus16, Radiojon, Rhdv, RonWessels, Ronaldsmith, Ronaldvd, SEREGA784, Sfxtd, Shaddack, SlayerK, Smack, Thaas00, The Tarnz, UtherSRG, Vanuan, ViperSnake151, Voidxor, Wdfarmer, Wsmarz, Wtshymanski, 132 anonymous edits

Modbus *Source:* http://en.wikipedia.org/w/index.php?oldid=405575384 *Contributors:* 7, Aarontpeterson, Alshain01, Batman2000, Begoon, Bert490, Bertus, Billymac00, Bobblewik, Btilm, CA1.R, Calitech, Calton, CanOfWorms, Ceallachan, CharlesWemyss, Chungyan5, Cp2020, Crucone, Cyberparam in, Dareces, Darwin30dec, Dicklyon, Dogaroon, Eadric, Electron9, Fahidka, Failanas, Faught, Femto, Frau Holle, Frau K, Funvill, Gadget1700, Glenn, Gorhas, Goy Harris, Hongooi, Hooperbloob, Hu12, InntegrationExpert, Iridescent, Jimwelch, Jmundo, Jt, Komantian, Kuttipapu, LynnLise, Matsuz, Modbus.ug, Morpheios Melas, Nasa-verve, Nathalie Erin, Nelson50, Ninokurtaj, One half 3544, PKlammer, Pswriter, Rajenduchowels, Remuel, Schastain, Sega381, SoManySpammers, Spalding, T. Canens, Thaas00, Thomas Larsen, Tmwusa1, Trussilver, UnitedStatesian, Waffleguy4, Wtshymanski, XandroZ, Xareu bs, Xsolarwindx, Zaphodikus, Важнов Алексей Геннадьевич, 157 anonyms edits

Virtual private network *Source:* http://en.wikipedia.org/w/index.php?oldid=405604196 *Contributors:* (:, 1984, 2005, 33rogers, ARTamb, Aaron north, Abune, Adi4094, Aditya, Aeon17x, Agaffin, Alansohn, Aldie, AlexeyN, Allstarecho, Alphawave, Alvestrand, Americaninseoul, AndreasJS, Andrewpmk, Angelbo, Anirvan, Anon lynx, Anthony Appleyard, Apankrat, Apothecia, Armando82, Art LaPella, Ashwin ambekar, Ausinha, Az1568, Azadk, Barek, Barek-public, Bbbone, Ben 9876, BenAveling, Bevo, Bewildebeast, BiT, BirdValiant, Bishopolis, Blacklogic, Blonkm, BlueJaeger, Boardista, Bobo192, Borgx, Bovineone, Brainix, Brandon, Braviojk, Brwawe, Bryan Derksen, Bswilson, CWenger, CYD, Can't sleep, clown will eat me, Carbuncle, Cfleisch, CharlotteWebb, Chenghui, Chris400, Chrisbolt, Chrisch, Chupacabras, Cleared as filed, ClementSeveillac, Closedmouth, Cometstyles, Cr0w, Crazytaes8, Cwofsheep, DKEdwards, Danno uk, David H Braun (1964), David Martland, David Woodward, Davidoff, Decltype, Deeahbz, Deice, Deli nk, Delldot, DerHexer, Dgtsyb, Diabolo-D3, Discospinster, Dlg2006, Dmktg, Dmol, Dpottor, DrFausty, Drable, DreamGuy, Drugonot, Dlugosz, E. Ripley, EagleOne, EdTrist, Edcolins, Eenu, Efa, ElTopo, Elinrubby, Emmatheartist, EoGuy, Eprb123, Escape Orbit, Eubene, Evansda, Everyking, Evicse, Extraordinary, FACHI, FJPB, Falcon8765, Fancy seve, Fangufu, Fingavia, Ftsloom, Fuday-sunday, Fijal, Fleminra, Flockmeal, Foggy Morning, Fosterbt, Foxb, Fuzheado, GSK, Gardar Rurak, Gascreed, Gaurav.khatiri, Gershwinrb, Gkstyle, Glenn, Godsmoke, Gracefool, Gracenotes, GraemeL, Ground Zero, Hadal, Haemo, Hal 2001, Hcberkowitz, Hellisp, Heron, HisSpaceResearch, Humannetwork, Hyakugei, Iannacm, Iceb, Ieopo, Informedbacker, Inkling, Intgr, Invenio, Ironman5247, Isilanes, IvanStepaniuk, Izwalito, J'raxis, J.delanoy, JGXenite, JHunterJ, JNW, Ja 62, Jaan513, Jacksk, Jadam576, Jairo lopez, Jazappi, Jcap11n, JidGom, Jim.henderson, Jino123, Jlavapoze, Jleedev, Jmundo, JoeSmack, John Vandenberg, John254, Johnuniqu, JonHarder, Jonomacrones, Joshk, Joy, Jrapo, Jrgetsin, Juliancolton, K-secure, Kaaveh Ahangar, Karlzt, Kateshortforbop, Kbrose, Kevinzhouyan, Khag7, Kielvon, Kikbguy, Kimchi.sg, Kku, KnowledgeOfSelf, Kurt Jansson, Kuru, Kvg, L Kensington, LOL, Leafyplant, LeaveLeaves, Les boys, LetMeLookItUp, Lightmouse, LindArlaud, Lucabwe, Ludovic.ferre, Luna Santin, M. B., Jr., MCB, MER-C, MFNickster, Ma8thew, Majorly, Manop, MarcoTolo, Mashouri, Matt Crypto, MattTM, MattieTK, Maxgrin, Me.rs, MeToo, Mercury543210, Mhking, Michaelas10, Mike Rosoft, Mindmatrix, Ministry of Truth, Minna Sora no Shita, Mkidson, Mmermex, Mohsen Basirat, Monkeyman, Movingonup, Mr.Clown, Mxn, Nacnud22032, Nardixsempe, Natalie Erin, Nealmbc, Negruilo, Neolain, Netmotion1234, Niffweed17, Nklatt, Noah Salzman, Novastorm, Nqtrng, Ntsimp, Nubiatech, Nuno Tavares, Nurg, Nuttycoconut, Octahedron80, Oheconfucius, Oli Filth, Omicronperseid8, Ottawa4ever, OverlordQ, Pascualv, Paulehoffman, Pauli133, Pearle, Peteinterpol, Peter M Dodge, Phantom87, Philomathoholic, Phr, Pinchomic, PlatHome, Plyd, Pmcn, Pokrajac, PositiveNetworks, Prari, PuerExMachina, Quarl, R'n'B, R. S. Shaw, RFightmaster, RHaworth, Raano, Rafigordon, RainbowOfLight, Ray Dassen, RayAYang, Razorflame, Rearden9, RedHillian, Redlazer, Rees11, Regancy42, Res221firestar, Rgore, Rhobite, Rich45, Rjwilmsi, Rnneman, Robert Brockway, Rocketron5, Saimhe, Scarpy, Checky4, Scott.somohano, SecurityManager, Selah28, Sgarson, Shadowjams, Shandon, Shelley Adams, Shijiree88, Shimgray, ShorelineVA, Sijokjose, SilentAshes, Sintesia, Skarebo, Skier Dude, SmartGuy, Smartchain, Smithkkj, Snaxe920, Snowolf, SpaceFlight89, SqueakBox, Sunny2who, Superpixelpro, Sydbaret74, Szquirrel, THEN WHO WAS PHONE?, Tahren B, Talinus, TastyPoutine, Tech editor007, TehPhil, Thatguyflint, Thaurisil, The Anome, The Thing That Should Not Be, TheBilly, TheNeutroniumAlchemist, ThePromenader, Therefore, Tide rolls, Timurx, Tivedshambo, Tiroche, Tobias Bergemann, Tom Foley, Tomlee1968, Tommy2010, TonyUK, Torqueing, Trailbum, Tryggvia, Tsloum, Tuxa, Tuxcrafter, Unixer, Utcursch, Vanderedecken, Vanisheduser12345, Veinor, Vicarious, Vicky2020, Visiting1, Vjardin, W.F.Galway, WEJohnston, WakingLili, Wavelength, WebHamster, Webster21, Whaa?, Wik, Wiki 101, Wikievil666, Williambolely, Wimt, Winchelsea, Wknigh94, Wodkreso, Ww, Xpclient, YUL89YYZ, Yama, Yamamoto Ichiro, YordanGeorgiev, Youssefsan, ZeroOne, Zeroshell, Ziabhat, Zzuuzz, 1128 anonymous edits

Layer 2 Tunneling Protocol *Source:* http://en.wikipedia.org/w/index.php?oldid=405455058 *Contributors:* A5b, Aaronbrick, Andareed, Anon lynx, Apyule, Borgx, CecilWard, CiaPan, Cibu, Cryptic, Cwofsheep, Daedalus01, Dispenser, Dmeranda, Enjoia4586, Evil saltine, Ferdinand Pienaar, Fontoponto, Free4948445, Frencheigh, Gogo Dodo, Hono sepanta, IlyaHaykinson, Infoarmor, JHunterJ, JTN, John Cardinal, K3rb, Kbrose, Kinema, Matieux, Mdmkolbe, Mendaliv, Metaclassing, Mmtmtmt, Moocha, MrJones, MrOllie, Muhandes, Muruga86, Mwaisberg, Nate Silva, Nealc, NescioNomen, Oblivious, Ohnoitsjamie, Peyre, PlatHome, Sietse Snel, Spearhead, Srbauer, Stephan Leeds, The Anome, TheAnarcart, Unyoyega, Vjardin, Walkerhamilton, Web-Crawling Stickler, Wrs1864, Xpclient, Yaronf, Ylem, Ynhockey, ^demon, 109 anonymous edits

Network address translation *Source:* http://en.wikipedia.org/w/index.php?oldid=405419131 *Contributors:* (:, 65.29.90.xxx, Aapo Laitinen, Aelantha, Aitias, Ajo Mama, Alan U. Kennington, Alansohn, Aldie, Alex Smotrov, Alex.atkins, Alex.zeffertt, Alexhixon, AlistairMcMillan, Althena, Altnr8r, Andrew Hampe, Andrewpmk, Andrewridell12, Angela, Ap, ArsénierDeGallium, John

Ashwin, Asymmetric, Balajisarithi, Bbpen, Benoit rigaut, Bevo, Bos-Herz edit acct, Brion VIBBER, Brynosaurus, Cate, Cbarbry, Cburnett, CesarB, Cheung1303, Chowbok, Conversion script, Copewood, Cotoco, Crazycomputers, Crispmmurder, CrucifiedChrist, CyberSkull, D235, DARTH SIDIOUS 2, Daf, DanielEng, Daveg1k, Daveofthenewcity, Dawnsseeker2000, Dcoetzee, DevastatorIIC, Dgtsyb, DiGiT, DisillusionedBitterAndKnackered, Droob, Drpxiie, Drumzandspace2000, Dspradau, Dysprosia, EH74DK, Ecolins, Eddy264, Edward, Eelsdon, Eloquent, Ergy, Everyking, Evil Monkey, Excirial, Fenix*NBK*, Fresheneesz, Gareth Owen, Gary King, Garyvdm, Giftlite, Giraffedata, Glenn, Goatasaur, Golbez, GorillaWarfare, Gracefool, Graham87, Grimmfarmer, Guiltyspark, Guitargod2323, Hairy Dude, HarlandQPitt, Harrymcfoogs, Hcberkowitz, Helix84, Hovden, Icairns, Imcdnzl, Indrian, Iranway, Ivan Pozdeev, Ivan.Lt, J.delanoy, JTN, Jan Kunder, Jengelh, Jcz9999, JidGom, Jokerspuppet, JonDePlume, JonHarder, Jondel, Jonshea, Josh Parris, Joshf, Joy, Jpbowen, Jsxn, Just Another Dan, KD5TVI, Karada, Karstbj, Kbdank71, Kbrose, Kenyon, Keycard, Kglfeischmann, Kristof vt, Kwi, Kzollman, Leuk he, LiDaobing, Lightdarkness, LittleOldMe, M gol, MARQUIS111, MER-C, Magnus Manske, Mallow40, Maltest, Mannafredo, Manop, Marchash, MarcoTolo, Mav, Mditto, Mercury543210, Mindmatrix, Mintguy, Misza13, Mmmeg, Murjek, Mygerardromance, Naniwako, Nazli, Nealmbc, Nilmerg, Niemiew, Nixdorf, Nubiatch, Nurg, Nyttend, Oalbacha, Oystein, PPBlais, Para, Pash, Pde, Pdelong, Peyre, Parham87, Phenry, Philadams, Philbert2.71828, Piano non troppo, PierreAbbat, Pinkadelica, Plugwash, Pmsyzz, Psychocim, Quarl, Rabarberski, Ramsey585, Rchandra, Rebecca, RedWolf, Rick Sidwell, Rmrftar, Rohithakral, Ross Fraser, Rrburke, Rushotoshankar, Ryan Roos, SF007, SQL, SalineBrain, SaulPerdomo, Smehta, Seikku Kaita, Shahid789, Shirimasen, Shiro jdn, Sideswipe091976, Siipikarja, Simetrical, Simon South, SimonEast, Slackerhobo, Smalljim, SoWhy, Sollosonic, Steelmans1980, Stephan Leeds, Stephenb, Steven Zhang, Sujirou, Svetovid, Syndicate, Taestell, Tagishsimon, TakuyaMurata, Teles, The Anome, The Inedible Bulk, Tiddly Tom, Tide rolls, Tobias Bergemann, Tommy2010, TonyHagale, Tresiden, Tristanb, Tverbeek, Twilsonb, UncleBubba, Urhixidur, VanishingUser, Wernher, Wiki alf, Wimbykit, Winterheart, WithGLEE, WojPob, Wolf0403, Wolfkeeper, Wolfrack, Wrs1864, Xpanzion, Yk4ever, YordanGeorgiev, Zap Rowsdower, Zhlmnc, Zondor, Zundark, 530 anonymous edits

Wi-Fi *Source:* <http://en.wikipedia.org/w/index.php?oldid=405513816> *Contributors:* -Majestic-, 12dstirng, 16@r, 19.158, 19.7, 2over0, 802geek, A Softer Answer, A8UDI, A930913, ABF, AEMoreira042281, AGruntsJaggon, AL SAM, AWoodland, Aamrod, Aapo Laitinen, Abstract Idiot, Abune, Acebulf, ActiveExpression, Adacnews, Adashiel, Addihockey10, Addshore, AeonSAFE, Ahoerstemeier, Ajarmateir, Ajaysreedharan, Akerans, Alain r, Alan Liefing, Alansohn, Albedo, Albert109, Aldie, AlexF, AlexTiefing, Alexander UA, Alexius08, AlexiusHoratius, Algoco, AlstairMcMillan, AllanHainey, Allen Moore, Altermike, Alyssa hoeffel, Amars, Amorow, AndersTR, Andrei Stroe, Andrew Maiman, Andy, Andriou52345, Andriou5jth, Andywmm9, Anna Lincoln, Anonymous anonymous, Antonojo, Anttilk, Ardrolat, Aremith, Arichnad, Armando82, Armynable, ArnoldReinhold, Arvindn, Asterion, Astral, Auric, Aushina, Aveekbh, Awostrack, Awpsys, Baka tori, Barek, BarretBonden, BartBenjamin, Bartman007, Baseball Bugs, Bawolff, Beavel, BelAir Networks Wireless Mesh, Beland, Belmond, Ben1220, Benhutchings, Beno1000, Berkut, Bevo, Bfigura's puppy, Big Brother 1984, Bigbluefish, Bilbobee, BillC, Billywhack, Binkowski, Biscuitin, Blackdragon1157, Blackjewishfag, Blackroo1967, Blair Bonnett, Blooperfoob, Bluefoxicy, CzarB, D, Bnordlund, Bobblewik, Bobo192, Bonadea, Bornhj, Bozonz, Bratch, Brazil4Linux, Bremerenator, Briandjohnson, Brianga, Brillow, Broadband118, Brons, Brookneck, Btilm, BuddhaDharma, Bullzeze, Burnte, Bxmpls, C.Crane, C0nanPayne, C3k, CAJ, CGorman, CRH3 EMU, CUSENZA Mario, Cabalamat, Calilil, Calabraxthis, Caliga10, Callidior, Calmer Wescn, Caltas, Caltrop, Cambrant, Can't sleep, clown will eat me, CanisRufus, Capricorn42, CardinalDan, Carter, Carterdiggis, Casito, Cavanagh12345, Cbruno, Celtus, Charivari, Charles Moss, Charles Nguyen, Charm, Chaser, Chcknwnm, Chealer, Cheeseemonger, Chendy, Chitrapa, Chomperhead, Chowbok, Chris 73, Chris Q, Chrisji, Christin varghese, Circus, Classicrockfan42, ClementSeveillac, Click23, Clipdude, Closeapple, Closedmouth, Cmdrjameson, cnKALTDS, Coasterlover1994, CobraBK, Cocaquy, Coffee, Coffin, Colenso, ColinHogben, Cometstyles, Compellingelegance, Corevette, Corvus cornix, Courcelles, Cpl Syx, Crag, Crazycomputers, Crazyviolinist, Crimsoundestroyer, Crissow, Cruiserjmc, Cryout, Cshay, Cswilly, Cy21, CyberSkull, Cyrius, CZarB, D, DAJF, DARTH SIDIOUS 2, Dan Fuhr, Dancrags, DanielCardenas, DanielTahar, Dank, Dannyilm, Dark Shikari, Dark jedi requiem, Darkmaster2004, Darkwind, DARTHraider, DaveBurstein, Daven200520, Davhorn, DavidCary, Davidjk, Davidmack, Dawnsseeker2000, DeVoteDz, DeadEyeArrow, Debresser, Delirium, Dendodge, DerHexer, Dieseldrinker, Dilane, Dilettante99, Dirkbh, Discospinster, DistopiaSPM, Djcapelis, Djg2006, Djkurtz, Dlohcierikm, Dmccarty, Dmchyla, Dochoat, Dogman15, Domeail, Doniogo, DopefishJustin, Doyley, Dposse, Dredracap, Dreadstar, Drewzhrodague, Dust Filter, Dylan Lake, Dystopianray, Dzubint, E Wing, ESKog, EagleEye96, Earthlyreason, Eatsaq, Ecamdog, Eclectek, Ed Cormany, Ed g2s, Ecolins, Editor at Large, Eggnock, Ehn, Ejrs, Elasant, Elberle, Electro94, Electron9, Elvey, Em978, Enauspeaker, Enviroboy, Epachamo, Epr123, Eptin, Erencexor, Eric Kvaalen, Eric Wester, Eric-Wester, Ericyu, Eskalin, Everyking, Evic, Excirial, Exit13, FF2010, Falcon9x5, Falopalump, FastLizard4, Favonian, Fbarton, Feedmecereal, Feureau, Fieldday-sunday, Fifieldt, Figueroaedgar, FilippoSidoti, Fireaxe888, Fiskbullar, Fitch, Fleisher, Fleminga, Flowerportman, Fonzenze, Fosnez, Fox, Fractal3, Freeddomknight, Freewol, Frencheigh, FreplySpang, Frigator, Ftblfn33, Fubar Obfusco, Funandtrvl, Fuzheado, GNUtoo, GRAHAMUK, Gabbe, Gadfium, Gaius Cornelius, Galifardeu, Garion96, Gavinatkinson, Gazpacho, Gd001, General Wesc, Genestr, Giftlite, Gilbertfien, Gilgamesh, Gilliam, Gimmetrow, Glenn, Godfather xie, Gojomo, Gokusandwich, Golbez, Golfandme, Gomm, Goodvac, Gorank4, GozzoMan, Grafen, Grandfeller, Grandor, Greghe, Gregrethlyh, Grim4593, Ground Zero, Groxx, Guaka, Gulliveig, Gurch, Gutzmer, Guy Harris, Guycarmeli, Gwalarn, Gxti, Gyll, Gyrfreter, H2g2bob, Hackfreewifi, Hadal, HaeB, Hagrinass, Hairy Dude, Halfbreath, Hankwang, Hanseichbaum, Haoie, Happinessiseasy, Happysailor, HarisM, Hawaiiiboy99, Hede2000, Hedgehoglet, Helix84, Heman, HenkeB, HeraIaphrodite, Heron, HexaChord, Hh001, HiddenInPlainSight, Hillcrest, Holierthanhou, Holo16, Homerjay, Ht1848, Hu12, HybridBoy, Hydrargyrum, Hydroxides, I already forgot, INKubusse, IRP, IReceivedSelfThreats, Iainelder, IceKarma, Iliptii, Immunize, Impulse9, Inbamkumar86, Inkybutton, Inter16, Into The Fray, Intractable, Iridescent, Itai, Itusg15q4user, Ixsf64, Izzysanime, J.delanoy, JD554, JFreeman, JLaTondre, JOSamsung, JPMcGrath, Jafeluv, Jakohn, James Galloway, JamesAM, JamesBWatson, Jamesontai, Jamyskis, Jandalhandler, Janizary, Jaryth000, Jason Recliner, Esq., Jason Stormchild, Jauricchio, Jawavazard, Jaxsonj, JayW, Jayharish, Jbowdenhm, Jc4p, Jeff G., Jeffrey Mall, Jehochman, JeremyA, Jerome Charles Potts, Jesse Viviano, Jh51681, Jhenderson777, Jim.henderson, Jngraham, Jjensen347, Jj1544, Jlmerrill, Jmlk17, Jnavas, JoGusto, JoanneB, John Mash, John254, JohnCD, JohnCub, Jon787, JonHarder, Jondel, Joseph Solis in Australia, Jossysayir, Joy, Joycloete, Jp78450, Jpatokal, Jtalledo, Juanscott, Jukeboxlord, Juliano, Justinko, Jw21, Jwissick, KD5TVI, KGasso, Kantmorie, Kautoorikrishna9, Kbrose, KeesCook, Keilana, KelleyCook, Key19, Kevin chen2003, Kevinlie10, Kfluck, Kgpoinath, Kikadeek, Kimiko, Kimvr, Kingboyk, Kingpin13, Kixy, Klingoncoyboy4, KnowledgeOfSelf, Koman90, Kostisl, Kotra, Kozuch, Krellis, Kuru, Kvg, Kwamikagami, Kynn, Kzll, Labboy, Landroo, Larry laptop, Laudaka, Lawnchair, Lawrence Cohen, Le Fou, LeaveSleeves, Leendert, Leif, LeoDV, Lexor, Liam.winder@bozii.net, Liao, Lightmouse, Lights, Lilac Soul, Linkspamremover, Lino Mastrodomenico, Lisatwo, Little Professor Stonecold, Little-man, Liyang, LizardJr8, Llort, Logictheo, LordHector, LordOfor, Lucano, Luci Sador, Luis007cruz, Luk, M5, M7, MARQUIS111, MCB, MER-C, MLauba, MSTCrow, Mac, MacIaine, Madd the sane, Magister Mathematicae, Mahendra, Mailer diablo, Mammad2002, Markaci, Markrd, Markpeak, Martinhayes, Matt Whyndinham, Mazerin07, Mboverload, Mbw227, McSly, Mckenzie1995, Mcmarmatt, Me Three, Meco, MedicineMen, Meekywiki, Mehrunes Dagon, Melah Hashamaim, MennoMan, Merlion444, Metaclassing, Mgnbar, Mia.bo, Michael Hardy, Michael93555, MichaelMaggs, Microsoft, Mike Moreton, Mike.lifeguard, MikeFenney, Mikemoral, Mindmatrix, Miranda, Miremare, Mirko.fidisk.fv, Mistemunivtor, Mjmarcus, Mkzz, Mmdoogie, Moarmudkipzulz, MollyMistress, Modulatium, Mollykate82, Momo san, Monaarora84, Monkeyman, Monochnotos, Monoku, Moreati, Mornegil, Mortense, Morthmolvna, Mowgli, Mrmiscellaneous, Mshahbaig, Msm20032003, Mtonkin, Mumia-w-18, Mushroom, Muzzle, Mwanner, Mygerardromance, Namenad, Nankeyman, Nappymonster, Nasa-verve, Nbarth, Ncmvocalist, Ndyguy, Nealcardwell, NellieBli, Nelson50, NeoChaosX, Nerminbarman, Networkingguy, NeuroJanis, Niemeyerstein en, Night Gyr, NilOlaf, Nixdorf, Noah Salzman, Noctibus, Nopetro, Notedgrant, Novalis, Nowcrash, Npss, Nsaa, Nux, Octahedron80, Ohnoitsjamie, Oldr4ver, Omegatron, Omhafaicio, Omicronperse8, Otivaale, Oxymoron83, Oystein, Oszeden, P Carn, Pacific1982, Paddu, PamD, Parrotheadmjb, Parsmutaf, ParticleMan, Patrick, Patrick Fisse, Paistuart, Paul Weaver, Paulshanks, Peak, Pekaje, Pelago, PeregrineAY, Peter, Peter McGinley, Peterl, Petrb, Petri Krohn, Peyre, Phatom87, Phi beta, Phil-welch, PhilKnight, Phil Truman, Phelegat, Photo, Photocopier, Phreakuency, Piano non troppo, Pie4all88, Pieleric, Piet Delpot, Pimfig, PinkPig, PipZandahalf, PleaseInsertGirder, PoTi, Pokipsy76, Pol098, Polaralex, Porschedriver403, Preslethe, PrestonH, Primary0, ProhibitOnions, Project2501a, Pt, Public Menace, Puggs, Pujanmalla, Puneet.kasera, Quantpole, Qui lche, Quintote, QuiteUnusual, Qutezuce, R6144, RDolivaw, RHaworth, Radagast, Radiant chains, RadioActive, Raj bhinde, Rannpháirtí anathind, Raxian, Ray Radlein, Raysonho, Raywil, Rcassidy, Rce-revo, Reach Out to the Truth, Rearden9, Recognizance, Reconsider the static, Recurring9, Rees11, Regara MKII, Reisio, Renewal36, RenniePet, Requestion, Res2216firestar, Retired username, Retodon8, Rewt, Rfc1394, Rhobite, Riddlem, Ribread2, Rich257, Richwales, Riddz17, Ripetom, Risk one, Riskariandita, Rjanag, Rjhatl, Rjwilmsi, Rkopplin, Rmallins, Robartin, Robert Cassidy, Robertvan1, Robo56, RockOfVictory, Rogerbrent, Romanski, RoseTech, Roybadami, Rror, Rsrikanth05, RufusThorne, Rumping, RupertMillard, Russoc4, Ryan Postlethwaite, RyanCross, S.kollmor, S.K., S.ferguson, SEWilco, SMC, SPANGER BANGER, STGM, Saikiri, Sailor iain, Salyt!, Sam Hovecar, Sean Korn, Sandeepreddyus, Sandstein, Sangol23, Saxtoncrys, Saxtonrob, Sbenton, Smeirow, Shurpeudencan, Sceptre, Scholia, SciCorrector, Skirkklan, Scurless, Seadood90, Seajay, Sean Reynolds, Sean2074, Seancoady, Seans Potato Business, Seaphoto, Searchme, Secfan, Seikku Kaita, Seqsea, Sesu Prime, Setveen, Sevenneed, Shanafme, Shandris, Shinpah1, Shirik, Shorty114, Shunt010, Sikon, Silverxxx, Silvery, Simm, SimonP, Simonn, SineWave, Sixteen Left, Sijupadhay, Skatebiker, Skategem, Skierpage, Skor, Slon02, Slowking Man, Smailis, Smalljim, Smoke, Snori, Snowolf, Soap, Socrates2008, Sodapop89, Sonam.bhutta, SonicBlue, Soumyasch, Souseiseki42, SpacedOut, Spearhead, Speck-Made, Spitfire19, Spooke, SpuriousQ, Sraraja, Sbrorlongan, Strikeit, Ssd, Ssri1983, Stangaa, Star Trek Man, StaticGull, Stephan Leeds, Stephen, Stephenb, Stevenj, Stickee, Styrofoam1994, Sunray, SuperDude115, Superborsuk, Superway25, SusanLesch, Susvolans, Suwa, Svetovid, Swizman, T callahan, T h e m a v e r i c k, Tabledhot, Tainter, TakuyaMurata, Taralsoni, TastyPoutine, Tbxexile, Tcnv, Teapeat, Teddybearspicnic, Teixant, Tekinera, Teles, Texaswebcsoot, Texture, Tfi, The Belgain, The Bryce, The Rambling Man, The Thing That Should Not Be, The Utterly Annoying Pedant, The undertow, The wub, TheGWO, TheLiberalTruth, TheRealFennShysa, TheTito, Thentukiran, Theymos, Thiago R Ramos, Thingg, Think outside the box, Think smith, ThrashedParanoid, Thunderbrand, Tide rolls, TigerShark, Tim1988, Timbatron, Tiptoety, Tjrana0, Tntnbnlt, Tobiaslw, Toccatafugue, Tohd8B0haiithuGh1, Tokachu, Tom.k, Tommy2010, Tony Sidaway, Tony1, Topazg, Tpbardbury, Tree Biting Conspiracy, Tri400, Trusilver, Tsange, Ttiotsw, Tucker001, TucsonDavid, Twang, Twocs, Twp, Tyler, Uu, Ultraman2008, Umerqureshi, Unprovoked, Useight, Utopianfiat, Valfontis, Valley2city, Vedantn, Vegaswikian, Veledan, Verbal, Versageek, Versus22, Vgautham 91, Viajero, Vicarious, Viktor Laszlo, VodkaJazz, Vossman, Vrenator, Waggars, Walloon, Wandab12, Warwickcaddie, WatermelonPotion, Watkinsclass67, Wavelength, Wdfarmer, Webwizard, Wehe, Wellithy, Wendell, Wep, Wereon, White Cat, Whitepap, Wifiveverywhere2007, Wickerize, Wikipedia314, Wikikuser104, Wikizeta2, William Avery, WilliamH, Wimt, Wingspant, Wizardist, Wknight94, Wog7777, Wolfkeeper, Wormeyman, Wrrr, Wskish, Ww, Wysprgr2005, XSSX, Xmnemonic, Xtefan, Xtifr, Yosri, Your wasted elf, Yuhong, ZKPilot, Zack Holly Venturi, Zarherif, Zeroshell, Zgreycocat, Zzuuz, ॠॠॠॠ, 滑天下之大稽, 2522 anonymous edits

Service set (802.11 network) *Source:* <http://en.wikipedia.org/w/index.php?oldid=403612171> *Contributors:* AB, AThing, Abuseemore, AlphaPyro, Arifhidayat, Beej, Bluemoose, Bongwarrior, Busyzz, Dawnsseeker2000, DuLithog, Edetic, Fuzzykiller, Gaunt, Geoffadams, Guy Harris, Hadrianheugh, Helixblue, Homestarmy, J0nokun, Jesse Viviano, Jvinius, KelleyCook, LOL, Lee Carre, Marokwitz, Marshall.Mills, Mattdm, Mike Moreton, Milan Keršlager, Nikrow, Nixdorf, Nvowell, Od Mishehu, OverlordQ, Oxymoron83, PGWG, Para, Quiggles, Radagast83, Rparle, SLP.Viper.YearX, Saxifrage, Simm, Spoon!, TG2, TheMissileSilo, Tlroche, Toftutwitch11, Xanzibbar, Xavid, Yaseenahmed, 95 anonymous edits

Wireless access point *Source:* <http://en.wikipedia.org/w/index.php?oldid=402233243> *Contributors:* Ahoerstemeier, Alan Rockefeller, Alansohn, Alla tedesca, ArnoldReinhold, Asdaqamin, Asfarer, Azaciacorp, Backstabb, Bazciscor, BenFrantzDale, Bennybp, Bfigura's puppy, Bigglescat, Bobblewik, Boston, Brianski, Brousch, Btornado, Callidior, Can't sleep, clown will eat me, Celineey, Chasingsof, Chongkian, ClarkR8, Clcketyclack, CosineKitty, Cwolfofsheep, DadMachine, Davepark, David.Mestel, Dawnsseeker2000, Deathphoenix, Dicklyon, Djssao, Donpizette26, Dori, Dr Madvibe, DropDeadGorgias, Duy Huu Nguyen, Editore99, Efeg, Ejabberd, ElKevbo, Frecklefoot, Funkendub, Gail, Gamera2, Geekosaurus, Giftlite, Gilliam, Gimboid13, Glenn, GreyCat, HarisM, Hdcomm, Hecktorzr, Heimstern, Hgilbert, Illythr, Ivansanchez, JYi, Jeepday, Jeff G., Jim.henderson, Jlmerrill, Jnavas, Jobeard, JonHarder, Joseph Solis in Australia, JosephWatkins, Justin Johnson, KaiAdin, Kcrao, KelleyCook, Kingsley16, KnightRider, Knudottor, Kozuch, Lawelmor, Lzur, Mac, Macic7, Malachias111, Mange011, Mathiastck, Miami33139, JosephWatkins, Justin Johnson, KaiAdin, Kcrao, KelleyCook, Kingsley16, KnightRider, Knudottor, Kozuch, Lawelmor, Lzur, Mac, Macic7, Malachias111, Mange011, Mathiastck, Miami33139,

MichaelAhlers, Mike Peel, Mim37204, Mintleaf, Mmmeg, Mozkill, Mtzweil, Mulad, Nagy, Neile, Nelson50, No1lakersfan, Nposs, Ohnoitsjamie, Okaven, Oli Filth, Palffy, Palthainon, Patriociogarcia57, Patrick, Pavarolar, Pedant17, Petri Krohn, Peyre, Platypus222, Pnm, PrologFan, Puggs, Qoqnous, Quest for Truth, RedWolf, Redline84, Rewt, Ronz, Runtime, Sa.vakilian, Sean Reynolds, Seraphimblade, Sickmate, Silvery, Smaug123, SonicSam, Splash, Squilibob, Themrpotatohead, Timwi, Tntdj, Tobixen, Tonkie67, Triona, UU, Ultramandk, ValC, Versus22, Waldir, Weihao.chiu, Western Pines, Xp54321, Zeltak, Zvar, Царя Крауц, 281 anonymous edits

Wired Equivalent Privacy *Source:* <http://en.wikipedia.org/w/index.php?oldid=404986898> *Contributors:* ADVENT Gray, Addshore, Alansohn, AlistairMcMillan, Andrewpwmk, ArnoldReinhold, Arnon Chaffin, Arsenalboi18, Asfarer, Asocall, Azimout, B*4, BenjaminGittins, Benrick, Betatruly, BilCat, Bobo192, Bradgib, BumbaBaby, Burnte, CanadianLinuxUser, Carlsor, Chairman Kaga, ChangChienFu, Charles Gaudette, Cincydude55, CIPHERgoth, Cntrucking, David Gerard, Davidgothberg, Dawnseeker2000, Deckernico, DerHexer, Dimitris74, Dogcow, Dr.queso, Ds13, Dzubint, Eckesicle, ErrantX, EvanCarroll, Evice, Fabian.a, Fox, Frysalebald, GB fan, GT40, Geekamallo, Gekkonaut, GerardM, Gibbocool, Gogo Dodo, Hadal, Hashar, Hellisp, Hokie92, Imran, InGearX, Intr, Isidore, Iwick, JDG, Jaizovic, Jamelan, Jesse Viviano, Jjalocha, Jnavas, Jon787, Jumping cheese, Kadin2048, Kcrao, KelleyCook, Kenyon, Khym Chanur, Kyleomalley, LeaveSleaves, Lee Carre, Loadmaster, Luna Santin, Lzur, Matt Crypto, Mblumber, Mhandley, Michael Hardy, Mmernex, Mschlindwein, Muhandes, MureninC, Mystaker1, NetRoller 3D, Nikita Borisov, Ninjai, Nocrej, Ntsimp, Oli Filth, Omegatron, Pearle, Peyre, Phillipbeynon, Photographerguy, Pkemma, Plugwash, Primary0, Quarl, Raed abu farha, RandallZ, Requestion, Roadrunner, Robartin, Rusl, Ryker, ScottDavis, Scriptedfate, Securiger, Shmget, SiseraRose, Slakr, Spymanut, Stannered, Superm401, The Inedible Bulk, TheBilly, TheProject, Theymos, Thief12, Tim Peterson, Tommy2010, Tomstensrod, Trusilver, Tsv55, Ubiqu, Van helsing, Vipinhari, Vlad, WWC, WatchAndObserve, Wik, Wiki Wikardo, Wknight94, Wrs1864, Ww, Xenium, Yaronf, Zerbey, 245 anonymous edits

Wi-Fi Protected Access *Source:* <http://en.wikipedia.org/w/index.php?oldid=405463742> *Contributors:* Adrian M. H., Agiorgio, Akella, Akerkhof, Alanhwi, AlistairMcMillan, AnthonyQBachler, Arifsaha, ArnoldReinhold, Asfarer, AtOMICNebula, Bartavelle, Basil.bourque, Bbrownp, Bender235, Buggerlugz, Callidior, CanisRufus, Chris Roy, Crcsmnky, Cynical, Dawnseeker2000, Deor, Devourer09, Dimawik, Direvus, Dzubint, Dzx, Egh0st, Elektron, Evgeni Sergeev, FJPB, Falcon8765, Flurry, FrankT, Frankie1969, Frysalebald, Gahrns, Gail, Glennf, Gma3-NJITWILL, Grafen, Hardincj, Hellisp, Hsan22, Hughcharlesparker, Husky, Ian Page, Imran, Int21h, IronGargoyle, Jackfork, Jaizanu, Jamelan, Jasyynash2, Jeffq, Jesse Viviano, Jnavas, Jonathan Drain, Jtir, KYSoH, Karenjc, Karlh21, KelleyCook, Kravietz, L33th4x0rguy, Lavenderbunny, Leotohill, Lightmouse, Loisel, Lzur, M4gnum0n, MER-C, MadmanNova, Manly0102, MarS, Matt Crypto, Mauls, MiG, Micah hainline, Microfrost, Mindmatrix, Mkilly, Mmernex, Mout, Mr. Zarniwoop, MrStalker, Mrdarrett, Navstar, Nbahn, Ndemarco, Neile, NetRoller 3D, Netrapt, Nile, Paddu, Panarchy, Pessi, Peter m, Peterdx, Peyre, Phantom87, Phil Boswell, Philip Trueman, Pinkadelica, Pixelperfect777, Plrk, Pmaccabe, Ppelteti, PrologFan, Qutorial, RLTAEdit, Ray andrew, Rebelrsr, RenniePet, Requestion, Roadrunner, Robartn, Robmv, Ronjhones, Rrusiejr, Runtime, ScottDavis, Scrdcow, Seajay, Segfault87, Seraven2007, SigiTM, Sleske, SlubGlub, Strafepelon2, SvenGodo, Tabletop, Thingg, Tide rolls, Tohd8BohathuGh1, Topbanana, Trenton11tgs, Tryptamine dreamer, Twistor96, Unimaginative Username, Vanhoefm, Vegaswikian, Versus22, Vespriestiano, Vitz-RS, Vrenator, WinTakeAll, WindowsNT, Winterst, Wlanmac, Writermomique, Wrs1864, Wtmitchell, Xcentaur, Xizhi.zhu, Yaronf, Ykhwong, Zé da Silva, 326 anonymous edits

Power over Ethernet *Source:* <http://en.wikipedia.org/w/index.php?oldid=404687493> *Contributors:* Adam Trogon, Adam850, Ali@gwc.org.uk, Antilived, Armando82, BW95, Bifter121, Bihoek, Bilboq, Biot, Btilm, Cartque, Cheti, Coelacan, ColinATL, Cyril.holweck, Danifel, Dan1999, Dawnseeker2000, Dfallon, Dicklyon, Dkhydema, Dmbaty, Domaskuo, Doomed498, Dustinblack, ESKog, Echoray, Edward, Egolnik, Electron9, Eptalon, Eraserhead1, Erebus555, Fgscsm, Fleminra, ForthOK, Fragglet, Gavron, Gene Nygaard, Giftlite, Glenn, Glrx, Gregmg, HenrikOlsen, IW4, Idleguy, Imroy, Indefatigable, Itusg15q4user, JLD, Javawizard, Jimz, Jnk, John Vandenberg, Karn, KelleyCook, Kvng, Lee Carre, Lohray, MLD7865 Auto, Marcincak, Markus b, Mattgirling, Mboverload, Megya, Meros, Mindmatrix, Monedula, Morpheios Melas, Mtdorov 69, Muchness, Mugman, Nasa-verve, Neile, Nelson50, Niteowlneils, Nmarus, Ohados, Orpheus, PassportDude, Pengo, Pias93, Piper8, Plugwash, Poccil, Requestion, Reswobslc, Rhobite, Rhombus, Ricci75, Rick Sidwell, Rjmunro, Rjwilmsi, Splintax, Testbells, Texture, Thaas00, The Thing That Should Not Be, Tntdj, Tompw, Towel401, UU, Usemyname3times, VSWR99, Vman049, Voidxor, Wgcrafty, Xchbla423, YUL89YYZ, Zodon, Zuzy, 227 anonymous edits

Antenna (radio) *Source:* <http://en.wikipedia.org/w/index.php?oldid=404649898> *Contributors:* A. B., Aarchiba, Abhivyakti s, Aceman2000, Acimatti, Adamantios, Addshore, Adrian, Adziura, Ai4ijoe, Alanacheng, Algocu, AltairPayne, Altenmann, Andre Engels, Andrewjuren, Angr, AngryParsley, Anonym1ty, Anthony Appleyard, Archanamiya, Arnero, Arteitle, Asrghashiojadrhr, AugPi, Auntof6, BD2412, Bernd in Japan, Betacommand, Bidgee, Blackjack3, Blainster, Bobo192, Bonzo, Borqx, Brandon, Brandon.irwin, Broadcastrtransmitter, Bryan Derksen, Bsskchaitanya, Catslash, Chetvorno, Christopher Parham, Cimon Avaro, Clarkefreak, Clubjuggle, CosineKitty, Crisis, Cybercobra, Cybermetic, Cyrius, DV8 2XL, DWatson, Dan Parnell, Daniel Christensen, Daniel.Cardenas, Dante Alighieri, Darguz Parsilvan, David Jordan, David R. Ingham, Dawnseeker2000, Deljr, Den.chang@rogers.com, Deor, Digitat, Dleather, Dogcow, Doradus, Dougher, Drys, Ekconklin, Emoboy2, Enochlau, EscapeVelocity, Euchiasmus, Ewlyahocoom, Ezeu, Francis E Williams, Fresheneesz, GLPeterson, GRAHAMUK, GaeusOctavius, Gaius Cornelius, Gary King, Gassaver, Gene Nygaard, George100, GetsEclectic, Glenn, GoingBatty, Graeme Bartlett, Greenrd, Haham hanuka, HereToHelp, Heron, Hertzian, Hickorybark, Hooperbloob, Horsten, IPSOS, Intr, It1224, JA.Davidson, Jamesgjf, Jc3s5h, Jcbarr, Jddriessen, Jdiyef, JesseW, Jim.henderson, Jjensen347, Jmrowland, John of Reading, JohnOwens, JohnTechnologist, Johnnymartins, Johnor, Joy, Jpgordon, Jugni, Juhachi, Julesd, JurginG, JustinSmith, Jyri1, KD5TVI, Kaimbridge, Kamenlitchev, Karl gregory jones, Kcordina, Keesiewonder, KeithH, KelleyCook, Kevin Rector, Kevmitch, Kgr, Kharker, Kingturtle, Kostisl, Kotoviski, Kristian Ovaska, Kymacpherson, LMB, LPFR, LQ, Lethe, Light current, Liquidcable, Loren.wilton, LorenzoB, Loul, Lukeseed, Mac, Mako098765, Matthias Holger, Mauls, Mazarin07, Meisam, Michael Hardy, Mifter, Migo, Mikeblas, Moggie2002, Mondebleu, Mouchoir le Souris, MrRK, NOYKG, N5iln, NameThatWorks, Nedim Ardoğa, Networkingguy, NeutralLang, Nicholasrs, Nobodyinpart, Norm mit, Nuggetboy, Ohnoitsjamie, Ominae, Onco p53, Pete463251, Peter Harriman, Pezant, PhantomS, Pixel :-), Pol098, Quantumobserver, R'n'B, RDT2, RTG, RadioFan, Ransu, Razimantv, Read-write-services, Red Winged Duck, Reddi, Rememberway, Requestion, Rheostatik, RickK, Rmrfrstar, Rob.desbois, RobertG, Rogerbrent, Sauerfmj, Scrabbler, Searchme, Sergioledesma, Shadowjams, ShelfSkewed, SiobhanHansa, Smndalila, Snafflekid, Spamhog, SparhawkWiki, SpeedyGonsales, SpuriousQ, Sreeram bh, Srleffler, Ssd, Stannered, Stephan Leeds, Stepp-Wulf, Steve Quinn, Steve carlson, Stevenj, SunCreator, Sv1xv, The Original Wildbear, TheGerm, Thunderchild, Tim Starling, Timo Honkasalo, Timothy Truckle, Tivedshambo, Tizio, Tusfa, TomCat4680, Tony Sidaway, Un chien andalous, Unyoeyga, Vanessaekewitz, Vegaswikian, Vegaswikian1, Voyajer, W.F.Galway, WO2, Warut, Waveguy, Wavelength, Whpq, Wikieditoroftoday, Wjbeaty, Wmahan, Wolfkeeper, Wolfmankurd, Woohookitty, Wskish, Ww, Yaf, Zoicon5, Zoohouse, しまでん, 大西洋鯨, 435 anonymous edits

Image Sources, Licenses and Contributors

Image:Cellphone-subscribers-by-technology.svg *Source:* <http://en.wikipedia.org/w/index.php?title=File:Cellphone-subscribers-by-technology.svg> *License:* Public Domain *Contributors:* User:Sbsky

File:3G With USB cable.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:3G_With_USB_cable.jpg *License:* Creative Commons Attribution 2.0 *Contributors:* Julien Min GONG

File:Ciscosystemsrouteratcern.jpg *Source:* <http://en.wikipedia.org/w/index.php?title=File:Ciscosystemsrouteratcern.jpg> *License:* GNU Free Documentation License *Contributors:* Coolcaesar

File:Juniper srx210 front view.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Juniper_srx210_front_view.jpg *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:MarcPG

File:Computernetwork.png *Source:* <http://en.wikipedia.org/w/index.php?title=File:Computernetwork.png> *License:* Public Domain *Contributors:* User:Joshap

File:Switch.JPG *Source:* <http://en.wikipedia.org/w/index.php?title=File:Switch.JPG> *License:* Public Domain *Contributors:* Original uploader was RedEagle at en.wikibooks

File:Adsl connections.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Adsl_connections.jpg *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Asim18

File:Leonard-Kleinrock-and-IMP1.png *Source:* <http://en.wikipedia.org/w/index.php?title=File:Leonard-Kleinrock-and-IMP1.png> *License:* Public Domain *Contributors:* Leonard Kleinrock

File:ERS-8600.JPG *Source:* <http://en.wikipedia.org/w/index.php?title=File:ERS-8600.JPG> *License:* GNU Free Documentation License *Contributors:* Original uploader was PassportDude at en.wikipedia

File:Linksys WRT54GL.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Linksys_WRT54GL.jpg *License:* Public Domain *Contributors:* User:J4ckzor

File:OpenWRT 8.09.1 LuCI screenshot.png *Source:* http://en.wikipedia.org/w/index.php?title=File:OpenWRT_8.09.1_LuCI_screenshot.png *License:* GNU General Public License *Contributors:* User:Moxfyre

Image:RS232 PCI-E.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:RS232_PCI-E.jpg *License:* Public Domain *Contributors:* Original uploader was Towel401 at en.wikipedia. Later version(s) were uploaded by Kbh3rd at en.wikipedia.

Image:Rs232 oscilloscope trace.svg *Source:* http://en.wikipedia.org/w/index.php?title=File:Rs232_oscilloscope_trace.svg *License:* Creative Commons Sharealike 1.0 *Contributors:* User:Ktnbn, User:Samuel Tardieu

Image:RS-485 3 wire connection.png *Source:* http://en.wikipedia.org/w/index.php?title=File:RS-485_3_wire_connection.png *License:* Public Domain *Contributors:* User:gri6507

Image:RS-485 waveform.svg *Source:* http://en.wikipedia.org/w/index.php?title=File:RS-485_waveform.svg *License:* GNU Free Documentation License *Contributors:* Rhdv, Royvegard

File:Virtual Private Network overview.svg *Source:* http://en.wikipedia.org/w/index.php?title=File:Virtual_Private_Network_overview.svg *License:* GNU Free Documentation License *Contributors:* Ludovic.ferre

Image:l2tp pkt exchg.PNG *Source:* http://en.wikipedia.org/w/index.php?title=File:L2tp_pkt_exchg.PNG *License:* Public Domain *Contributors:* Muruga86

Image:Full Cone NAT.svg *Source:* http://en.wikipedia.org/w/index.php?title=File:Full_Cone_NAT.svg *License:* Creative Commons Attribution-Sharealike 2.5 *Contributors:* Christoph Sommer

Image:Restricted Cone NAT.svg *Source:* http://en.wikipedia.org/w/index.php?title=File:Restricted_Cone_NAT.svg *License:* Creative Commons Attribution-Sharealike 2.5 *Contributors:* Christoph Sommer

Image:Port Restricted Cone NAT.svg *Source:* http://en.wikipedia.org/w/index.php?title=File:Port_Restricted_Cone_NAT.svg *License:* Creative Commons Attribution-Sharealike 2.5 *Contributors:* Christoph Sommer

Image:Symmetric NAT.svg *Source:* http://en.wikipedia.org/w/index.php?title=File:Symmetric_NAT.svg *License:* Creative Commons Attribution-Sharealike 2.5 *Contributors:* Christoph Sommer

File:Wi-Fi Logo.svg *Source:* http://en.wikipedia.org/w/index.php?title=File:Wi-Fi_Logo.svg *License:* unknown *Contributors:* AEMoreira042281, Austin512, Koman90, Tbhotch, 3 anonymous edits

File:WIFI Amp Setup.JPG *Source:* http://en.wikipedia.org/w/index.php?title=File:WIFI_Amp_Setup.JPG *License:* Public Domain *Contributors:* Fosnez, Kozuch, 1 anonymous edits

File:Metro Wireless Node.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Metro_Wireless_Node.jpg *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Robo56

File:Toronto WiFi.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Toronto_WiFi.jpg *License:* Creative Commons Attribution 2.0 *Contributors:* Marc Lostracco

File:WiFi-detector.jpg *Source:* <http://en.wikipedia.org/w/index.php?title=File:WiFi-detector.jpg> *License:* Public Domain *Contributors:* User:Raysonho

File:Wimax.svg *Source:* <http://en.wikipedia.org/w/index.php?title=File:Wimax.svg> *License:* GNU General Public License *Contributors:* User:Benjamin M. A'Lee

File:RouterBoard 112 with U.FL-RSMA pigtail and R52 miniPCI Wi-Fi card.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:RouterBoard_112_with_U.FL-RSMA_pigtail_and_R52_miniPCI_Wi-Fi_card.jpg *License:* GNU Free Documentation License *Contributors:* User:Kozuch

File:3GN .jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:3GN_.jpg *License:* Public Domain *Contributors:* Original uploader was Rewt at en.wikipedia

File:Wireless adaptor USB.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Wireless_adaptor_USB.jpg *License:* Creative Commons Attribution 3.0 *Contributors:* Ben Ben, Silverxxx, 1 anonymous edits

File:Ezurio wism2 small.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Ezurio_wism2_small.jpg *License:* GNU Free Documentation License *Contributors:* Photoo, 4 anonymous edits

Image:Industrial wireless access point.JPG *Source:* http://en.wikipedia.org/w/index.php?title=File:Industrial_wireless_access_point.JPG *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Celineyy

Image:Linksys WAP54G.JPG *Source:* http://en.wikipedia.org/w/index.php?title=File:Linksys_WAP54G.JPG *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Macic7, 1 anonymous edits

Image:RouterBoard 112 with U.FL-RSMA pigtail and R52 miniPCI Wi-Fi card.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:RouterBoard_112_with_U.FL-RSMA_pigtail_and_R52_miniPCI_Wi-Fi_card.jpg *License:* GNU Free Documentation License *Contributors:* User:Kozuch

Image:Wep-crypt-alt.svg *Source:* <http://en.wikipedia.org/w/index.php?title=File:Wep-crypt-alt.svg> *License:* GNU Free Documentation License *Contributors:* User:Stannered

File:PoE Access Point v2.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:PoE_Access_Point_v2.jpg *License:* Public Domain *Contributors:* myself

File:1140E-7.JPG *Source:* <http://en.wikipedia.org/w/index.php?title=File:1140E-7.JPG> *License:* Creative Commons Attribution-Sharealike 2.5 *Contributors:* User:James38

File:5520-24-POE.JPG *Source:* <http://en.wikipedia.org/w/index.php?title=File:5520-24-POE.JPG> *License:* unknown *Contributors:* Darth Panda, PassportDude, Shell Kinney, 3 anonymous edits

File:Antenna.jpg *Source:* <http://en.wikipedia.org/w/index.php?title=File:Antenna.jpg> *License:* Creative Commons Attribution 2.5 *Contributors:* User:Yonatanh

File:Rabbit-ears dipole antenna with UHF loop 20090204.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Rabbit-ears_dipole_antenna_with_UHF_loop_20090204.jpg *License:* Creative Commons Attribution 2.5 *Contributors:* User:Carnildo

File:6 sector site in CDMA.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:6_sector_site_in_CDMA.jpg *License:* Public Domain *Contributors:* hardikvasa

File:Canberra Deep Dish Communications Complex - GPN-2000-000502.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Canberra_Deep_Dish_Communications_Complex_-_GPN-2000-000502.jpg *License:* Public Domain *Contributors:* NASA

File:Bundesarchiv Bild 183-29802-0001, MTS Strehla, Bezirk Dresden, Ukw-Sprechfunk.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Bundesarchiv_Bild_183-29802-0001_MTS_Strehla_Bezirk_Dresden_Ukw-Sprechfunk.jpg *License:* Public Domain *Contributors:* Braun

File:Superturnstile Tx Muehlacker.JPG *Source:* http://en.wikipedia.org/w/index.php?title=File:Superturnstile_Tx_Muehlacker.JPG *License:* Creative Commons Attribution-Sharealike 2.5 *Contributors:* Hans-Peter Scholz, Birkenfeld (Enzkreis), Germany

File:Folded dipole.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Folded_dipole.jpg *License:* Creative Commons Attribution 3.0 *Contributors:* User:Bidgee

File:Antenna visalia california.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Antenna_visalia_california.jpg *License:* Creative Commons Attribution 2.5 *Contributors:* User:Kotoviski

File:2008-07-28 Mast radiator.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:2008-07-28_Mast_radiator.jpg *License:* GNU Free Documentation License *Contributors:* User:Specious

Image:Sidelobes en.svg *Source:* http://en.wikipedia.org/w/index.php?title=File:Sidelobes_en.svg *License:* GNU Free Documentation License *Contributors:* Santosga, Timothy Truckle

File:TV Aerial.jpg *Source:* <http://en.wikipedia.org/w/index.php?title=File:TV Aerial.jpg> *License:* Public Domain *Contributors:* User:Daniel Christensen

File:old rabbit ears.JPG *Source:* http://en.wikipedia.org/w/index.php?title=File:Old_rabbit_ears.JPG *License:* Creative Commons Attribution 3.0 *Contributors:* User:Daniel Christensen

File:A6-1EN.jpg *Source:* <http://en.wikipedia.org/w/index.php?title=File:A6-1EN.jpg> *License:* GNU Free Documentation License *Contributors:* LP, Santosga

File:A6-2.jpg *Source:* <http://en.wikipedia.org/w/index.php?title=File:A6-2.jpg> *License:* GNU Free Documentation License *Contributors:* Anonymous Dissident, Inductiveloat, LP, Santosga, 1 anonymous edits

File:A6-4.jpg *Source:* <http://en.wikipedia.org/w/index.php?title=File:A6-4.jpg> *License:* GNU Free Documentation License *Contributors:* LP, Santosga, 1 anonymous edits

File:Zij-en.png *Source:* <http://en.wikipedia.org/w/index.php?title=File:Zij-en.png> *License:* GNU Free Documentation License *Contributors:* Alejo2083, LP, 1 anonymous edits

Image:Montreal-tower-top.thumb2.jpg *Source:* <http://en.wikipedia.org/w/index.php?title=File:Montreal-tower-top.thumb2.jpg> *License:* Public Domain *Contributors:* Original uploader was Aarchiba at en.wikipedia

Image:Antenna d44ac.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Antenna_d44ac.jpg *License:* Creative Commons Attribution-Sharealike 2.5 *Contributors:* Adamantios, HenkVD, Kotoviski, Liftarn, Siebrand, Stepa, Waldir

Image:Television Antenna.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Television_Antenna.jpg *License:* Creative Commons Attribution-Sharealike 2.5 *Contributors:* Andreas -horn- Hornig, Conti, Daniel Christensen, Enochlau, Jerome Charles Potts

Image:Space diversity.gif *Source:* http://en.wikipedia.org/w/index.php?title=File:Space_diversity.gif *License:* GNU Free Documentation License *Contributors:* David Jordan, Jim.henderson

File:136 to 174 MHz base station antennas.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:136_to_174_MHz_base_station_antennas.jpg *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* w:en:David JordanDavid Jordan on English Wikipedia

Image:Low cost DCF77 receiver.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Low_cost_DCF77_receiver.jpg *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Jaho

Image:VHF UHF LP-antenna.JPG *Source:* http://en.wikipedia.org/w/index.php?title=File:VHF_UHF_LP-antenna.JPG *License:* Attribution *Contributors:* User:Sv1xv

Image:Delano VOA.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Delano_VOA.jpg *License:* Public Domain *Contributors:* User:Akitoki7

Image:OldTV Antenna.JPG *Source:* <http://en.wikipedia.org/w/index.php?title=File:OldTV Antenna.JPG> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Sreerambh

Image:T2FD_Antenna.png *Source:* http://en.wikipedia.org/w/index.php?title=File:T2FD_Antenna.png *License:* Public Domain *Contributors:* User:Spamhog

File:Aerial antenna.JPG *Source:* http://en.wikipedia.org/w/index.php?title=File:Aerial_antenna.JPG *License:* Creative Commons Attribution 3.0 *Contributors:* User:Daniel Christensen

File:Old rabbit ears.JPG *Source:* http://en.wikipedia.org/w/index.php?title=File:Old_rabbit_ears.JPG *License:* Creative Commons Attribution 3.0 *Contributors:* User:Daniel Christensen

File:Philco am loop.jpg *Source:* http://en.wikipedia.org/w/index.php?title=File:Philco_am_loop.jpg *License:* Creative Commons Attribution 3.0 *Contributors:* User:Daniel Christensen

Image:Doncastertower.JPG *Source:* <http://en.wikipedia.org/w/index.php?title=File:Doncastertower.JPG> *License:* unknown *Contributors:* Original uploader was Skyscraper297 at en.wikipedia

File:Palmerston-water-tank.jpg *Source:* <http://en.wikipedia.org/w/index.php?title=File:Palmerston-water-tank.jpg> *License:* Creative Commons Attribution 3.0 *Contributors:* User:Bidgee

Image:base_station_mexico-city.JPG *Source:* http://en.wikipedia.org/w/index.php?title=File:Base_station_mexico-city.JPG *License:* Public Domain *Contributors:* Pptudela

Image:PalmCellTower.jpg *Source:* <http://en.wikipedia.org/w/index.php?title=File:PalmCellTower.jpg> *License:* Public Domain *Contributors:* User:Minnaert

Image:Trunked 5ch central control.svg *Source:* http://en.wikipedia.org/w/index.php?title=File:Trunked_5ch_central_control.svg *License:* GNU Free Documentation License *Contributors:* User:Stannered

Image:Base station antenna network.png *Source:* http://en.wikipedia.org/w/index.php?title=File:Base_station_antenna_network.png *License:* Public Domain *Contributors:* Original uploader was David Jordan at en.wikipedia. Later version(s) were uploaded by MashrurR at en.wikipedia.

License

Creative Commons Attribution-Share Alike 3.0 Unported
<http://creativecommons.org/licenses/by-sa/3.0/>
