IEEE 802.11

From Wikipedia, the free encyclopedia

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands. They are created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997, and has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. While each amendment is officially revoked when it is incorporated in the latest version of the standard, the corporate world tends to market to the revisions because they concisely denote capabilities of their products. As a result, in the market place, each revision tends to become its own standard.

Contents

The Linksys WRT54G contains a router with an 802.11b/g radio (common in the early 2000s) and two antennas

General description

The 802.11 family consists of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. 802.11-1997 was the first wireless networking standard in the family, but 802.11b was the first widely accepted one, followed by 802.11a, 802.11g, 802.11n, and 802.11ac. Other standards in the family (c–f, h, j) are service amendments that are used to extend the current scope of the existing standard, which may also include corrections to a previous specification.[1]

802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 of the U.S. Federal Communications Commission Rules and Regulations. Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwave ovens, cordless telephones, and Bluetooth devices. 802.11b and 802.11g control their interference and susceptibility to interference by using direct-sequence spread spectrum (DSSS) and orthogonal frequency-division multiplexing (OFDM) signaling methods, respectively. 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz ISM frequency band offering only three non-overlapping channels, where other adjacent channels overlap—see list of WLAN channels. Better or worse performance with higher or lower frequencies (channels) may be realized, depending on the environment.

The segment of the radio frequency spectrum used by 802.11 varies between countries. In the US, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations. Frequencies used by channels one through six of 802.11b and 802.11g fall within the 2.4 GHz amateur radio band. Licensed amateur radio operators may operate 802.11b/g devices under Part 97 of the FCC Rules and Regulations, allowing increased power output but not commercial content or encryption.[2]

History

802.11 technology has its origins in a 1985 ruling by the U.S. Federal Communications Commission that released the ISM band for unlicensed use.[3]

In 1991 NCR Corporation/AT&T (now Alcatel-Lucent and LSI Corporation) invented a precursor to 802.11 in Nieuwegein, The Netherlands. The inventors initially intended to use the technology for cashier systems. The first wireless products were brought to the market under the name WaveLAN with raw data rates of 1 Mbit/s and 2 Mbit/s.

Vic Hayes, who held the chair of IEEE 802.11 for 10 years, and has been called the "father of Wi-Fi", was involved in designing the initial 802.11b and 802.11a standards within the IEEE.[4]

In 1999, the Wi-Fi Alliance was formed as a trade association to hold the Wi-Fi trademark under which most products are sold.[5]

Protocol

802.11 network PHY standards										
802.11 protocol	Release date[6]	Frequency	Bandwidth	Stream data rate[7]	Allowable MIMO streams	Modulation	Approximate range			
							Indoor		Outdoor	
		(GHz)	(MHz)	(Mbit/s)			(m)	(ft)	(m)	(ft)
802.11-1997	Jun 1997	2.4	22	1, 2	N/A	DSSS, FHSS	20	66	100	330
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	35	115	120	390
		3.7[A]					—	—	5,000	16,000[A]
b	Sep 1999	2.4	22	1, 2, 5.5, 11	N/A	DSSS	35	115	140	460
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	38	125	140	460
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 [B] (6.5, 13, 19.5, 26, 39, 52, 58.5, 65) [C]	4	OFDM	70	230	250	820[8]
			40	15, 30, 45, 60, 90, 120, 135, 150 [B] (13.5, 27, 40.5, 54, 81, 108, 121.5, 135) [C]			70	230	250	820[8]
ac	Dec 2013	5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3 [B] (6.5, 13, 19.5, 26, 39, 52, 58.5, 65, 78, 86.7) [C]	8		35	115[9]		
			40	15, 30, 45, 60, 90, 120, 135, 150, 180, 200 [B] (13.5, 27, 40.5, 54, 81, 108, 121.5, 135, 162, 180) [C]			35	115[9]		
			80	32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3 [B] (29.2, 58.5, 87.8, 117, 175.5, 234, 263.2, 292.5, 351, 390) [C]			35	115[9]		
			160	65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 [B] (58.5, 117, 175.5, 234, 351, 468, 702, 780) [C]			35	115[9]		
ad	Dec 2012	60	2,160	Up to 6,912 (6.75 Gbit/s) [10]	N/A	OFDM, single carrier, low-power single carrier	60	200	100	300
ah	Est. 2016[6]	0.9								
aj	Est. 2016[6]	45/60								
ax	Est. 2019[6]	2.4/5				MIMO-OFDM				
ay	2017	60	8000	Up to 100,000 (100 Gbit/s)	4	OFDM, single carrier,	60	200	1000	3000

- **A1 A2** IEEE 802.11y-2008 extended operation of 802.11a to the licensed 3.7 GHz band. Increased power limits allow a range up to 5,000 m. As of 2009, it is only being licensed in the United States by the FCC.
- **B1 B2 B3 B4 B5 B6** Assumes short guard interval (SGI) enabled.
- **C1 C2 C3 C4 C5 C6** Assumes short guard interval (SGI) disabled.

802.11-1997 (802.11 legacy)

The original version of the standard IEEE 802.11 was released in 1997 and clarified in 1999, but is today obsolete. It specified two net bit rates of 1 or 2 megabits per second (Mbit/s), plus forward error correction code. It specified three alternative physical layer technologies: diffuse infrared operating at 1 Mbit/s; frequency-hopping spread spectrum operating at 1 Mbit/s or 2 Mbit/s; and direct-sequence spread spectrum operating at 1 Mbit/s or 2 Mbit/s. The latter two radio technologies used microwave transmission over the Industrial Scientific Medical frequency band at 2.4 GHz. Some earlier WLAN technologies used lower frequencies, such as the U.S. 900 MHz ISM band.

Legacy 802.11 with direct-sequence spread spectrum was rapidly supplanted and popularized by 802.11b.

802.11a (OFDM waveform)

Originally described as clause 17 of the 1999 specification, the OFDM waveform at 5.8 GHz is now defined in clause 18 of the 2012 specification, and provides protocols that allow transmission and reception of data at rates of 1.5 to 54 Mbit/s. It has seen widespread worldwide implementation, particularly within the corporate workspace. While the original amendment is no longer valid, the term *802.11a* is still used by wireless access point (cards and routers) manufacturers to describe interoperability of their systems at 5.8 GHz, 54 Mbit/s.

The 802.11a standard uses the same data link layer protocol and frame format as the original standard, but an OFDM based air interface (physical layer). It operates in the 5 GHz band with a maximum net data rate of 54 Mbit/s, plus error correction code, which yields realistic net achievable throughput in the mid-20 Mbit/s.[11]

Since the 2.4 GHz band is heavily used to the point of being crowded, using the relatively unused 5 GHz band gives 802.11a a significant advantage. However, this high carrier frequency also brings a disadvantage: the effective overall range of 802.11a is less than that of 802.11b/g. In theory, 802.11a signals are absorbed more readily by walls and other solid objects in their path due to their smaller wavelength, and, as a result, cannot penetrate as far as those of 802.11b. In practice, 802.11b typically has a higher range at low speeds (802.11b will reduce speed to 5.5 Mbit/s or even 1 Mbit/s at low signal strengths). 802.11a also suffers from interference,[12] but locally there may be fewer signals to interfere with, resulting in less interference and better throughput.

802.11b

The 802.11b standard has a maximum raw data rate of 11 Mbit/s, and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard. The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

Devices using 802.11b experience interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include microwave ovens, Bluetooth devices, baby monitors, cordless telephones, and some amateur radio equipment.

802.11g

In June 2003, a third modulation standard was ratified: 802.11g. This works in the 2.4 GHz band (like 802.11b), but uses the same OFDM based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput.[13] 802.11g hardware is fully backward compatible with 802.11b hardware, and therefore is encumbered with legacy issues that reduce throughput by ~21% when compared to 802.11a.

The then-proposed 802.11g standard was rapidly adopted in the market starting in January 2003, well before ratification, due to the desire for higher data rates as well as to reductions in manufacturing costs. By summer 2003, most dual-band 802.11a/b products became dual-band/tri-mode, supporting a and b/g in a single mobile adapter card or access point. Details of making b and g work well together occupied much of the lingering technical process; in an 802.11g network, however, activity of an 802.11b participant will reduce the data rate of the overall 802.11g network.

Like 802.11b, 802.11g devices suffer interference from other products operating in the 2.4 GHz band, for example wireless keyboards.

802.11-2007

In 2003, task group TGma was authorized to "roll up" many of the amendments to the 1999 version of the 802.11 standard. REVma or 802.11ma, as it was called, created a single document that merged 8 amendments (802.11a, b, d, e, g, h, i, j) with the base standard. Upon approval on March 8, 2007, 802.11REVma was renamed to the then-current base standard **IEEE 802.11-2007**.[14]

802.11n

802.11n is an amendment that improves upon the previous 802.11 standards by adding multiple-input multiple-output antennas (MIMO). 802.11n operates on both the 2.4 GHz and the lesser-used 5 GHz bands. Support for 5 GHz bands is optional. It operates at a maximum net data rate from 54 Mbit/s to 600 Mbit/s. The IEEE has approved the amendment, and it was published in October 2009.[15][16] Prior to the final ratification, enterprises were already migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal.

802.11-2012

In 2007, task group TGmb was authorized to "roll up" many of the amendments to the 2007 version of the 802.11 standard. REVmb or 802.11mb, as it was called, created a single document that merged ten amendments (802.11k, r, y, n, w, p, z, v, u, s) with the 2007 base standard. In addition much cleanup was done, including a reordering of many of the clauses.[17] Upon publication on March 29, 2012, the new standard was referred to as **IEEE 802.11-2012**.

802.11ac

IEEE 802.11ac-2013 is an amendment to IEEE 802.11, published in December 2013, that builds on 802.11n.[18] Changes compared to 802.11n include wider channels (80 or 160 MHz versus 40 MHz) in the 5 GHz band, more spatial streams (up to eight versus four), higher-order modulation (up to 256-QAM vs. 64-QAM), and the addition of Multi-user MIMO (MU-MIMO). As of October 2013, high-end implementations support 80 MHz channels, three spatial streams, and 256-QAM, yielding a data rate of up to 433.3 Mbit/s per spatial stream, 1300 Mbit/s total, in 80 MHz channels in the 5 GHz band.[19] Vendors have announced plans to release so-called "Wave 2" devices with support for 160 MHz channels, four spatial streams, and MU-MIMO in 2014 and 2015.[20][21][22]

802.11ad

IEEE 802.11ad is an amendment that defines a new physical layer for 802.11 networks to operate in the 60 GHz millimeter wave spectrum. This frequency band has significantly different propagation characteristics than the 2.4 GHz and 5 GHz bands where Wi-Fi networks operate. Products implementing the 802.11ad standard are being brought to market under the WiGig brand name. The certification program is now being developed by the Wi-Fi Alliance instead of the now defunct WiGig Alliance.[23] The peak transmission rate of 802.11ad is 7 Gbit/s.[24]

The first product is set to be released in 2016.[25]

802.11af

IEEE 802.11af, also referred to as "White-Fi" and "Super Wi-Fi",[26] is an amendment, approved in February 2014, that allows WLAN operation in TV white space spectrum in the VHF and UHF bands between 54 and 790 MHz.[27][28] It uses cognitive radio technology to transmit on unused TV channels, with the standard taking measures to limit interference for primary users, such as analog TV, digital TV, and wireless microphones.[28] Access points and stations determine their position using a satellite positioning system such as GPS, and use the Internet to query a geolocation database (GDB) provided by a regional regulatory agency to discover what frequency channels are available for use at a given time and position.[28] The physical layer uses OFDM and is based on 802.11ac.[29] The propagation path loss as well as the attenuation by materials such as brick and concrete is lower in the UHF and VHF bands than in the 2.4 and 5 GHz bands, which increases the possible range.[28] The frequency channels are 6 to 8 MHz wide, depending on the regulatory domain.[28] Up to four channels may be bonded in either one or two contiguous blocks.[28] MIMO operation is possible with up to four streams used for either space–time block code (STBC) or multi-user (MU) operation.[28] The achievable data rate per spatial stream is 26.7 Mbit/s for 6 and 7 MHz channels, and 35.6 Mbit/s for 8 MHz channels.[30] With four spatial streams and four bonded channels, the maximum data rate is 426.7 Mbit/s for 6 and 7 MHz channels and 568.9 Mbit/s for 8 MHz channels.[30]

802.11ah

IEEE 802.11ah defines a WLAN system operating at sub 1 GHz license-exempt bands, with final approval slated for March 2016.[27][31] Due to the favorable propagation characteristics of the low frequency spectra, 802.11ah can provide improved transmission range compared with the conventional 802.11 WLANs operating in the 2.4 GHz and 5 GHz bands. 802.11ah can be used for various purposes including large scale sensor networks,[32] extended range hotspot, and outdoor Wi-Fi for cellular traffic offloading, whereas the available bandwidth is relatively narrow.

802.11ai

IEEE 802.11ai is an amendment to the 802.11 standard that will add new mechanisms for a faster initial link setup time.[33]

802.11aj

IEEE 802.11aj is a rebanding of 802.11ad for use in the 45 GHz unlicensed spectrum available in some regions of the world (specifically China).[33]

802.11aq

IEEE 802.11aq is an amendment to the 802.11 standard that will enable pre-association discovery of services. This extends some of the mechanisms in 802.11u that enabled device discovery to further discover the services running on a device, or provided by a network.[33]

802.11ax

IEEE 802.11ax is the successor to 802.11ac, and will increase the efficiency of WLAN networks. Currently at a very early stage of development this project has the goal of providing 4x the throughput of 802.11ac.[34]

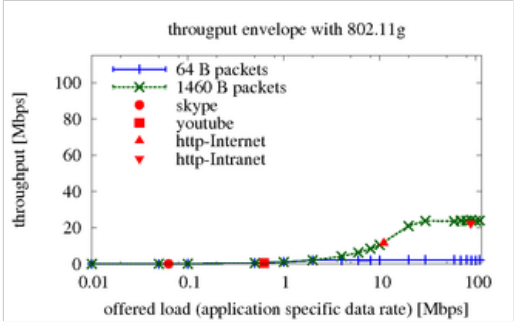
802.11ay

IEEE 802.11ay is a standard that is being developed. It is an amendment that defines a new physical layer for 802.11 networks to operate in the 60 GHz millimeter wave spectrum. It will be an extension of the existing 11ad, aimed to extend the throughput, range and use-cases. The main use-cases include: indoor operation, out-door back-haul and short range communications. The peak transmission rate of 802.11ay is 20 Gbit/s.[35] The main extensions include: channel bonding (2, 3 and 4), MIMO and higher modulation schemes.

Common misunderstandings about achievable throughput

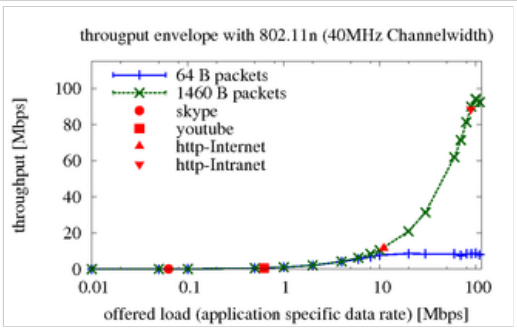
Across all variations of 802.11, maximum achievable throughputs are given either based on measurements under ideal conditions or in the layer-2 data rates. This, however, does not apply to typical deployments in which data is being transferred between two endpoints, of which at least one is typically connected to a wired infrastructure and the other endpoint is connected to an infrastructure via a wireless link.

This means that, typically, data frames pass an 802.11 (WLAN) medium, and are being converted to 802.3 (Ethernet) or vice versa. Due to the difference in the frame (header) lengths of these two media, the application's packet size determines the speed of the data transfer. This means applications that use small packets (e.g., VoIP) create dataflows with high-overhead traffic (i.e., a low goodput). Other factors that contribute to the overall application data rate are the speed with which the application transmits the packets (i.e., the data rate) and, of course, the energy with which the wireless signal is received. The latter is determined by distance and by the configured output power of the communicating devices.[36][37]



Graphical representation of Wi-Fi application specific (UDP) performance envelope 2.4 GHz band, with 802.11g

The same references apply to the attached graphs that show measurements of UDP throughput. Each represents an average (UDP) throughput (please note that the error bars are there, but barely visible due to the small variation) of 25 measurements. Each is with a specific packet size (small or large) and with a specific data rate (10 kbit/s – 100 Mbit/s). Markers for traffic profiles of common applications are included as well. Please note, this text and measurements do not cover packet errors, but information about this can be found at the references above.

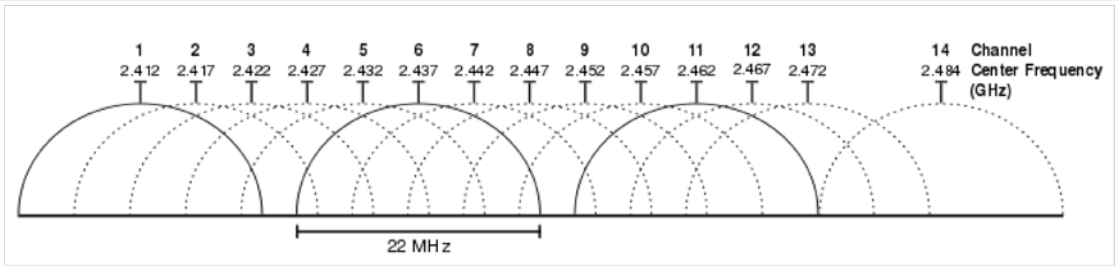


Graphical representation of Wi-Fi application specific (UDP) performance envelope 2.4 GHz band, with 802.11n with 40MHz

Channels and frequencies

802.11b, 802.11g, and 802.11n-2.4 utilize the 2.400–2.500 GHz spectrum, one of the ISM bands. 802.11a and 802.11n use the more heavily regulated 4.915–5.825 GHz band. These are commonly referred to as the "2.4 GHz and 5 GHz bands" in most sales literature. Each spectrum is sub-divided into *channels* with a center frequency and bandwidth, analogous to the way radio and TV broadcast bands are sub-divided.

The 2.4 GHz band is divided into 14 channels spaced 5 MHz apart, beginning with channel 1, which is centered on 2.412 GHz. The latter channels have additional restrictions or are unavailable for use in some regulatory domains.



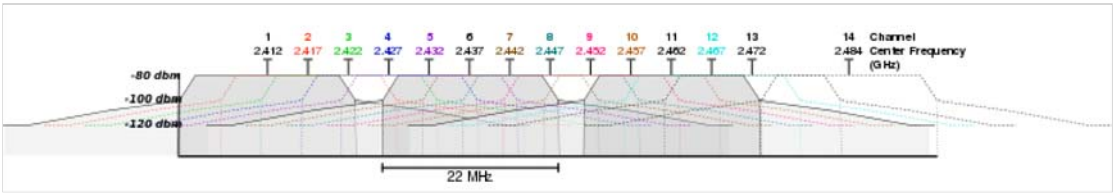
Graphical representation of Wi-Fi channels in the 2.4 GHz band

The channel numbering of the 5.725–5.875 GHz spectrum is less intuitive due to the differences in regulations between countries. These are discussed in greater detail on the list of WLAN channels.

Channel spacing within the 2.4 GHz band

In addition to specifying the channel centre frequency, 802.11 also specifies (in Clause 17) a spectral mask defining the permitted power distribution across each channel. The mask requires the signal be attenuated a minimum of 20 dB from its peak amplitude at ±11 MHz from the centre frequency, the point at which a channel is effectively 22 MHz wide. One consequence is that stations can use only every fourth or fifth channel without overlap.

Availability of channels is regulated by country, constrained in part by how each country allocates radio spectrum to various services. At one extreme, Japan permits the use of all 14 channels for 802.11b, and 1–13 for 802.11g/n-2.4. Other countries such as Spain initially allowed only channels 10 and 11, and France allowed only 10, 11, 12, and 13; however, they now allow channels 1 through 13.[38][39] North America and some Central and South American countries allow only 1 through 11.



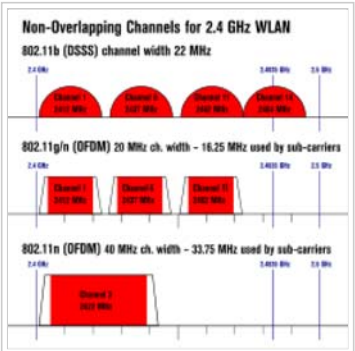
Spectral masks for 802.11g channels 1–14 in the 2.4 GHz band

Since the spectral mask defines only power output restrictions up to ±11 MHz from the center frequency to be attenuated by −50 dBr, it is often assumed that the energy of the channel extends no further than these limits. It is more correct to say that, given the separation between channels, the overlapping signal on any channel should be sufficiently attenuated to minimally interfere with a transmitter on any other channel. Due to the near-far problem a transmitter can impact (desense) a receiver on a "non-overlapping" channel, but only if it is close to the victim receiver (within a meter) or operating above allowed power levels.

Confusion often arises over the amount of channel separation required between transmitting devices. 802.11b was based on DSSS modulation and utilized a channel bandwidth of 22 MHz, resulting in *three* "non-overlapping" channels (1, 6, and 11). 802.11g was based on OFDM modulation and utilized a channel bandwidth of 20 MHz. This occasionally leads to the belief that *four* "non-overlapping" channels (1, 5, 9, and 13) exist under 802.11g, although this is not the case as per 17.4.6.3 Channel Numbering of operating channels of the IEEE Std 802.11 (2012), which states "In a multiple cell network topology, overlapping and/or adjacent cells using different channels can operate simultaneously without interference if the distance between the center frequencies is at least 25 MHz."[40] and section 18.3.9.3 and Figure 18-13.

This does not mean that the technical overlap of the channels recommends the non-use of overlapping channels. The amount of interference seen on a configuration using channels 1, 5, 9, and 13 can have very small difference from a three-channel configuration,[41] and in the paper entitled "Effect of adjacent-channel interference in IEEE 802.11 WLANs" by Villegas this is also demonstrated.[42]

Although the statement that channels 1, 5, 9, and 13 are "non-overlapping" is limited to spacing or product density, the concept has some merit in limited circumstances. Special care must be taken to adequately space AP cells, since overlap between the channels may cause unacceptable degradation of signal quality and throughput.[43] If more advanced equipment such as spectral analyzers are available, overlapping channels may be used under certain circumstances. This way, more channels are available.[42]



802.11 non-overlapping channels for 2.4GHz. Covers 802.11b,g,n

Regulatory domains and legal compliance

IEEE uses the phrase *regdomain* to refer to a legal regulatory region. Different countries define different levels of allowable transmitter power, time that a channel can be occupied, and different available channels.[44] Domain codes are specified for the United States, Canada, ETSI (Europe), Spain, France, Japan, and China.

Most Wi-Fi certified devices default to *regdomain* 0, which means least common denominator settings, i.e., the device will not transmit at a power above the allowable power in any nation, nor will it use frequencies that are not permitted in any nation.

The *regdomain* setting is often made difficult or impossible to change so that the end users do not conflict with local regulatory agencies such as the United States' Federal Communications Commission.

Layer 2 – Datagrams

The datagrams are called *frames*. Current 802.11 standards specify frame types for use in transmission of data as well as management and control of wireless links.

Frames are divided into very specific and standardized sections. Each frame consists of a **MAC header**, **payload**, and **frame check sequence** (FCS). Some frames may not have a payload.

The first two bytes of the MAC header form a frame control field specifying the form and function of the frame. This frame control field is subdivided into the following sub-fields:

- **Protocol Version:** Two bits representing the protocol version. Currently used protocol version is zero. Other values are reserved for future use.
- **Type:** Two bits identifying the type of WLAN frame. Control, Data, and Management are various frame types defined in IEEE 802.11.
- **Subtype:** Four bits providing additional discrimination between frames. Type and Sub Type together to identify the exact frame.
- **ToDS** and **FromDS:** Each is one bit in size. They indicate whether a data frame is headed for a distribution system. Control and management frames set these values to zero. All the data frames will have one of these bits set. However communication within an Independent Basic Service Set (IBSS) network always set these bits to zero.
- **More Fragments:** The More Fragments bit is set when a packet is divided into multiple frames for transmission. Every frame except the last frame of a packet will have this bit set.
- **Retry:** Sometimes frames require retransmission, and for this there is a Retry bit that is set to one when a frame is resent. This aids in the

elimination of duplicate frames.
- **Power Management:** This bit indicates the power management state of the sender after the completion of a frame exchange. Access points are required to manage the connection, and will never set the power-saver bit.
- **More Data:** The More Data bit is used to buffer frames received in a distributed system. The access point uses this bit to facilitate stations in power-saver mode. It indicates that at least one frame is available, and addresses all stations connected.
- **Protected Frame:** The Protected Frame bit is set to one if the frame body is encrypted by a protection mechanism such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or Wi-FI Protected Access II (WPA2).
- **Order:** This bit is set only when the "strict ordering" delivery method is employed. Frames and fragments are not always sent in order as it causes a transmission performance penalty.

The next two bytes are reserved for the Duration ID field. This field can take one of three forms: Duration, Contention-Free Period (CFP), and Association ID (AID).

An 802.11 frame can have up to four address fields. Each field can carry a MAC address. Address 1 is the receiver, Address 2 is the transmitter, Address 3 is used for filtering purposes by the receiver.

The remaining fields of the header are:

- The Sequence Control field is a two-byte section used for identifying message order as well as eliminating duplicate frames. The first 4 bits are used for the fragmentation number, and the last 12 bits are the sequence number.
- An optional two-byte Quality of Service control field that was added with 802.11e.

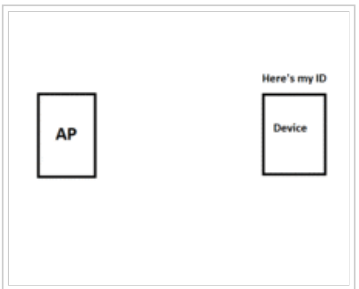
The payload or frame body field is variable in size, from 0 to 2304 bytes plus any overhead from security encapsulation, and contains information from higher layers.

The Frame Check Sequence (FCS) is the last four bytes in the standard 802.11 frame. Often referred to as the Cyclic Redundancy Check (CRC), it allows for integrity check of retrieved frames. As frames are about to be sent, the FCS is calculated and appended. When a station receives a frame, it can calculate the FCS of the frame and compare it to the one received. If they match, it is assumed that the frame was not distorted during transmission.[45]

Management frames

Management frames allow for the maintenance of communication. Some common 802.11 subtypes include:

- Authentication frame: 802.11 authentication begins with the Wireless network interface card (WNIC) sending an authentication frame to the access point containing its identity. With an open system authentication, the WNIC sends only a single authentication frame, and the access point responds with an authentication frame of its own indicating acceptance or rejection. With shared key authentication, after the WNIC sends its initial authentication request it will receive an authentication frame from the access point containing challenge text. The WNIC sends an authentication frame containing the encrypted version of the challenge text to the access point. The access point ensures the text was encrypted with the correct key by decrypting it with its own key. The result of this process determines the WNIC's authentication status.
- Association request frame: Sent from a station it enables the access point to allocate resources and synchronize. The frame carries information about the WNIC, including supported data rates and the SSID of the network the station wishes to associate with. If the request is accepted, the access point reserves memory and establishes an association ID for the WNIC.
- Association response frame: Sent from an access point to a station containing the acceptance or rejection to an association request. If it is an acceptance, the frame will contain information such an association ID and supported data rates.
- Beacon frame: Sent periodically from an access point to announce its presence and provide the SSID, and other parameters for WNICs within range.
- Deauthentication frame: Sent from a station wishing to terminate connection from another station.
- Disassociation frame: Sent from a station wishing to terminate connection. It's an elegant way to allow the access point to relinquish memory allocation and remove the WNIC from the association table.
- Probe request frame: Sent from a station when it requires information from another station.
- Probe response frame: Sent from an access point containing capability information, supported data rates, etc., after receiving a probe request frame.
- Reassociation request frame: A WNIC sends a reassociation request when it drops from range of the currently associated access point and finds another access point with a stronger signal. The new access point coordinates the forwarding of any information that may still be contained in the buffer of the previous access point.
- Reassociation response frame: Sent from an access point containing the acceptance or rejection to a WNIC reassociation request frame. The frame includes information required for association such as the association ID and supported data rates.



Illustrated authentication method

Information Elements

2. In terms of ICT, an **Information Element** (IE) is a part of management frames in the IEEE 802.11 wireless LAN protocol. IEs are a device's way to transfer descriptive information about itself inside management frames. There are usually several IEs inside each such frame, and each is built of TLVs mostly defined outside the basic IEEE 802.11 specification.

The common structure of an IE is as follows:

```
← 1 → ← 1 →  ←      3      →  ←  1-252  →
+-------+------+-------------+------------+
| Type |Length|      OUI      |    Data    |
+-------+------+-------------+------------+
```

Whereas the OUI (organizationally unique identifier) is used only when necessary to the protocol being used, and the data field holds the TLVs relevant to that IE.

Control frames

Control frames facilitate in the exchange of data frames between stations. Some common 802.11 control frames include:

- Acknowledgement (ACK) frame: After receiving a data frame, the receiving station will send an ACK frame to the sending station if no errors are found. If the sending station doesn't receive an ACK frame within a predetermined period of time, the sending station will resend the frame.
- Request to Send (RTS) frame: The RTS and CTS frames provide an optional collision reduction scheme for access points with hidden stations. A station sends a RTS frame as the first step in a two-way handshake required before sending data frames.
- Clear to Send (CTS) frame: A station responds to an RTS frame with a CTS frame. It provides clearance for the requesting station to send a data frame. The CTS provides collision control management by including a time value for which all other stations are to hold off transmission while the requesting station transmits.

Data frames

Data frames carry packets from web pages, files, etc. within the body.[46] The body begins with an IEEE 802.2 header, with the Destination Service Access Point (DSAP) specifying the protocol; however, if the DSAP is hex AA, the 802.2 header is followed by a Subnetwork Access Protocol (SNAP) header, with the Organizationally Unique Identifier (OUI) and protocol ID (PID) fields specifying the protocol. If the OUI is all zeroes, the protocol ID field is an EtherType value.[47] Almost all 802.11 data frames use 802.2 and SNAP headers, and most use an OUI of 00:00:00 and an EtherType value.

Standards and amendments

Within the IEEE 802.11 Working Group,[27] the following IEEE Standards Association Standard and Amendments exist:

- IEEE 802.11-1997: The WLAN standard was originally 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and infrared (IR) standard (1997), all the others listed below are Amendments to this standard, except for Recommended Practices 802.11F and 802.11T.
- IEEE 802.11a: 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b: Enhancements to 802.11 to support 5.5 Mbit/s and 11 Mbit/s (1999)
- IEEE 802.11c: Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d: International (country-to-country) roaming extensions (2001)
- IEEE 802.11e: Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11F: Inter-Access Point Protocol (2003) Withdrawn February 2006
- IEEE 802.11g: 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h: Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i: Enhanced security (2004)
- IEEE 802.11j: Extensions for Japan (2004)
- IEEE 802.11-2007: A new release of the standard that includes amendments a, b, d, e, g, h, i, and j. (July 2007)
- IEEE 802.11k: Radio resource measurement enhancements (2008)
- IEEE 802.11n: Higher-throughput improvements using MIMO (multiple-input, multiple-output antennas) (September 2009)
- IEEE 802.11p: WAVE—Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (July 2010)
- IEEE 802.11r: Fast BSS transition (FT) (2008)
- IEEE 802.11s: Mesh Networking, Extended Service Set (ESS) (July 2011)
- IEEE 802.11T: Wireless Performance Prediction (WPP)—test methods and metrics Recommendation cancelled
- IEEE 802.11u: Improvements related to HotSpots and 3rd-party authorization of clients, e.g., cellular network offload (February 2011)
- IEEE 802.11v: Wireless network management (February 2011)
- IEEE 802.11w: Protected Management Frames (September 2009)
- IEEE 802.11y: 3650–3700 MHz Operation in the U.S. (2008)
- IEEE 802.11z: Extensions to Direct Link Setup (DLS) (September 2010)
- IEEE 802.11-2012: A new release of the standard that includes amendments k, n, p, r, s, u, v, w, y, and z (March 2012)
- IEEE 802.11aa: Robust streaming of Audio Video Transport Streams (June 2012)
- IEEE 802.11ac: Very High Throughput <6 GHz;[48] potential improvements over 802.11n: better modulation scheme (expected ~10% throughput increase), wider channels (estimate in future time 80 to 160 MHz), multi user MIMO;[49] (December 2013)
- IEEE 802.11ad: Very High Throughput 60 GHz (December 2012) — see WiGig
- IEEE 802.11ae: Prioritization of Management Frames (March 2012)
- IEEE 802.11af: TV Whitespace (February 2014)

In process

- IEEE 802.11mc: Roll-up of 802.11-2012 with the aa, ac, ad, ae & af amendments to be published as 802.11-2016 *(~ March 2016)*

- IEEE 802.11ah: Sub 1 GHz license exempt operation (e.g., sensor network, smart metering) *(~ March 2016)*
- IEEE 802.11ai: Fast Initial Link Setup *(~ November 2015)*
- IEEE 802.11aj: China Millimeter Wave *(~ June 2016)*
- IEEE 802.11ak: General Links *(~ May 2016)*
- IEEE 802.11aq: Pre-association Discovery *(~ July 2016)*
- IEEE 802.11ax: High Efficiency WLAN *(~ May 2018)*
- IEEE 802.11ay: Enhancements for Ultra High Throughput in and around the 60 GHz Band *(~ TBD)*
- IEEE 802.11az: Next Generation Positioning *(~ TBD)*

802.11F and 802.11T are recommended practices rather than standards, and are capitalized as such.

802.11m is used for standard maintenance. 802.11ma was completed for 802.11-2007, 802.11mb was completed for 802.11-2012, and 802.11mc is working towards publishing 802.11-2016.

Standard vs. amendment

Both the terms "standard" and "amendment" are used when referring to the different variants of IEEE standards.[50]

As far as the IEEE Standards Association is concerned, there is only one current standard; it is denoted by IEEE 802.11 followed by the date that it was published. IEEE 802.11-2012 is the only version currently in publication. The standard is updated by means of amendments. Amendments are created by task groups (TG). Both the task group and their finished document are denoted by 802.11 followed by a non-capitalized letter, for example, IEEE 802.11a and IEEE 802.11b. Updating 802.11 is the responsibility of task group m. In order to create a new version, TGm combines the previous version of the standard and all published amendments. TGm also provides clarification and interpretation to industry on published documents. New versions of the **IEEE 802.11** were published in 1999, 2007, and 2012. The next is expected in 2016.[51]

Nomenclature

Various terms in 802.11 are used to specify aspects of wireless local-area networking operation, and may be unfamiliar to some readers.

For example, Time Unit (usually abbreviated TU) is used to indicate a unit of time equal to 1024 microseconds. Numerous time constants are defined in terms of TU (rather than the nearly equal millisecond).

Also the term "Portal" is used to describe an entity that is similar to an 802.1H bridge. A Portal provides access to the WLAN by non-802.11 LAN STAs.

Community networks

With the proliferation of cable modems and DSL, there is an ever-increasing market of people who wish to establish small networks in their homes to share their broadband Internet connection.

Many hotspot or free networks frequently allow anyone within range, including passersby outside, to connect to the Internet. There are also efforts by volunteer groups to establish wireless community networks to provide free wireless connectivity to the public.

Security

In 2001, a group from the University of California, Berkeley presented a paper describing weaknesses in the 802.11 Wired Equivalent Privacy (WEP) security mechanism defined in the original standard; they were followed by Fluhrer, Mantin, and Shamir's paper titled "Weaknesses in the Key Scheduling Algorithm of RC4". Not long after, Adam Stubblefield and AT&T publicly announced the first verification of the attack. In the attack, they were able to intercept transmissions and gain unauthorized access to wireless networks.

The IEEE set up a dedicated task group to create a replacement security solution, 802.11i (previously this work was handled as part of a broader 802.11e effort to enhance the MAC layer). The Wi-Fi Alliance announced an interim specification called Wi-Fi Protected Access (WPA) based on a subset of the then current IEEE 802.11i draft. These started to appear in products in mid-2003. IEEE 802.11i (also known as WPA2) itself was ratified in June 2004, and uses the Advanced Encryption Standard AES, instead of RC4, which was used in WEP. The modern recommended encryption for the home/consumer space is WPA2 (AES Pre-Shared Key), and for the enterprise space is WPA2 along with a RADIUS authentication server (or another type of authentication server) and a strong authentication method such as EAP-TLS.

In January 2005, the IEEE set up yet another task group "w" to protect management and broadcast frames, which previously were sent unsecured. Its standard was published in 2009.[52]

In December 2011, a security flaw was revealed that affects some wireless routers with a specific implementation of the optional Wi-Fi Protected Setup (WPS) feature. While WPS is not a part of 802.11, the flaw allows a remote attacker to recover the WPS PIN and, with it, the router's 802.11i password in a few hours.[53][54]

In late 2014 Apple announced that its iOS 8 mobile operating system would scramble MAC addresses[55] during the pre-association stage to thwart retail footfall tracking made possible by the regular transmission of uniquely identifiable probe requests.

Non-standard 802.11 extensions and equipment

Many companies implement wireless networking equipment with non-IEEE standard 802.11 extensions either by implementing proprietary or draft features. These changes may lead to incompatibilities between these extensions.

See also

- Comparison of wireless data standards
- OFDM system comparison table
- Ultra-wideband
- Wi-Fi operating system support
- Wibree or Bluetooth low energy
- Wireless Gigabit Alliance – also known as WiGig
- Fujitsu Ltd. v. Netgear Inc.
- Wireless USB – another wireless protocol primarily designed for shorter-range applications
- TU (time unit)

References

- "IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" (PDF). (2012 revision). IEEE-SA. 5 April 2012. doi:10.1109/IEEESTD.2012.6178212.
- "IEEE 802.11k-2008—Amendment 1: Radio Resource Measurement of Wireless LANs" (PDF). IEEE-SA. 12 June 2008. doi:10.1109/IEEESTD.2008.4544755.
- "IEEE 802.11r-2008—Amendment 2: Fast Basic Service Set (BSS) Transition" (PDF). IEEE-SA. 15 July 2008. doi:10.1109/IEEESTD.2008.4573292.
- "IEEE 802.11y-2008—Amendment 3: 3650–3700 MHz Operation in USA" (PDF). IEEE-SA. 6 November 2008. doi:10.1109/IEEESTD.2008.4669928.

Footnotes

1. "IEEE-SA Standards Board Operations Manual". IEEE-SA. Retrieved 2015-09-13.
2. "ARRLWeb: Part 97 - Amateur Radio Service". American Radio Relay League. Retrieved 2010-09-27.
3. Wolter Lemstra , Vic Hayes , John Groenewegen , *The Innovation Journey of Wi-Fi: The Road To Global Success*, Cambridge University Press, 2010, ISBN 0-521-19971-9
4. http://news.cnet.com/1200-1070-975460.html
5. "Wi-Fi Alliance: Organization". *Official industry association web site*. Retrieved August 23, 2011.
6. "Official IEEE 802.11 working group project timelines". June 2, 2014. Retrieved 2014-06-03.
7. "Wi-Fi CERTIFIED n: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi® Networks" (registration required). *Wi-Fi Alliance*. September 2009.
8. "802.11n Delivers Better Range". *Wi-Fi Planet*. 2007-05-31.
9. "IEEE 802.11ac: What Does it Mean for Test?" (PDF). *LitePoint*. October 2013.
10. "WiGig and IEEE 802.11ad For Multi-Gigabyte-Per-Second WPAN and WLAN" (PDF). Tensorcom Inc.
11. http://www.oreillynet.com/wireless/2003/08/08/wireless_throughput.html
12. Angelakis, V.; Papadakis, S.; Siris, V.A.; Traganitis, A. (March 2011). "Adjacent channel interference in 802.11a is harmful: Testbed validation of a simple quantification model". *Communications Magazine* (IEEE) **49** (3): 160–166. doi:10.1109/MCOM.2011.5723815. ISSN 0163-6804
13. *Wireless Networking in the Developing World: A practical guide to planning and building low-cost telecommunications infrastructure* (PDF) (2nd ed.). Hacker Friendly LLC. 2007. p. 425. page 14
14. IEEE 802.11-2007
15. "IEEE-SA - News & Events". Standards.ieee.org. Retrieved 2012-05-24.
16. "IEEE 802.11n-2009—Amendment 5: Enhancements for Higher Throughput". IEEE-SA. 29 October 2009. doi:10.1109/IEEESTD.2009.5307322.
17. "Why did 802.11-2012 renumber clauses?". Matthew Gast, Aerohive Networks. Retrieved 2012-11-17.
18. Kelly, Vivian (2014-01-07). "New IEEE 802.11ac™ Specification Driven by Evolving Market Need for Higher, Multi-User Throughput in Wireless LANs". IEEE. Retrieved 2014-01-11.
19. Higgins, Tim (2013-10-08). "AC1900: Innovation or 3D Wi-Fi?". SmallNetBuilder. Retrieved 2013-12-31.
20. Hachman, Mark (2014-01-05). "Quantenna chipset to anchor speedy first 'Wave 2' Asus router". PCWorld. Retrieved 2014-01-11.
21. Gilby, Christian (2012-12-02). "What Wave of 802.11ac is Right for You?". Aruba Networks. Retrieved 2014-01-11.
22. Rubino, Bill (2013-05-07). "Cisco will ride the 802.11ac Wave2". Cisco Systems. Retrieved 2014-01-11.
23. Kevin Fitchard. "Wi-Fi Alliance gobbles up WiGig; plans to certify devices this year". Retrieved 8 January 2016.
24. "IEEE Standard Association - IEEE Get Program" (PDF). Retrieved 8 January 2016.
25. Zach Epstein (January 6, 2016). "Meet the router that will make your home Wi-Fi network 3 times faster". Boy Genius Report.
26. Lekomtcev, Demain; Maršálek, Roman (June 2012). "Comparison of 802.11af and 802.22 standards – physical layer and cognitive functionality". elektrorevue. Retrieved 2013-12-29.
27. "Official IEEE 802.11 working group project timelines". 2011-12-11. Retrieved 2011-12-11.
28. Flores, Adriana B.; Guerra, Ryan E.; Knightly, Edward W.; Ecclesine, Peter; Pandey, Santosh (October 2013). "IEEE 802.11af: A Standard for TV White Space Spectrum Sharing" (PDF). IEEE. Retrieved 2013-12-29.
29. Dongguk Lim (2013-05-23). "TVWS Regulation and Standardization (IEEE 802.11af)" (PDF). Retrieved 2013-12-29.
30. Lee, Wookbong; Kwak, Jin-Sam; Kafle, Padam; Tingleff, Jens; Yucek, Tevfik; Porat, Ron; Erceg, Vinko; Lan, Zhou; Harada, Hiroshi (2012-07-10). "TGaf PHY proposal". IEEE P802.11. Retrieved 2013-12-29.
31. "P802.11ah Project Authorization Request" (PDF). IEEE. 2010-09-30. Retrieved 2014-02-11.
32. Churchill, Sam (2013-08-30). "802.11ah: WiFi Standard for 900MHz". dailywireless.org. Retrieved 2014-02-11.
33. "IEEE 802.11, The Working Group Setting the Standards for Wireless LANs". Retrieved 8 January 2016.
34. https://mentor.ieee.org/802.11/dcn/14/11-14-0165-01-0hew-802-11-hew-sg-proposed-par.docx

35. "P802.11ay" (PDF). IEEE. p. 1. Retrieved 19 August 2015. "This amendment defines standardized modifications to both the IEEE 802.11 physical layers (PHY) and the IEEE 802.11 medium access control layer (MAC) that enables at least one mode of operation capable of supporting a maximum throughput of at least 20 gigabits per second (measured at the MAC data service access point), while maintaining or improving the power efficiency per station."
36. "Towards Energy-Awareness in Managing Wireless LAN Applications". IEEE/IFIP NOMS 2012: IEEE/IFIP Network Operations and Management Symposium. Retrieved 2014-08-11.
37. "Application Level Energy and Performance Measurements in a Wireless LAN". The 2011 IEEE/ACM International Conference on Green Computing and Communications. Retrieved 2014-08-11.
38. "Cuadro nacional de Atribución de Frecuencias CNAF". Secretaría de Estado de Telecomunicaciones. Archived from the original on 2008-02-13. Retrieved 2008-03-05.
39. "Evolution du régime d'autorisation pour les RLAN" (PDF). French Telecommunications Regulation Authority (ART). Retrieved 2008-10-26.
40. "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" (PDF). Retrieved 2013-12-05.
41. "Choosing the clearest channels for WiFi... continued". Retrieved 2013-12-05.
42. Garcia Villegas, E.; et al. (2007). *Effect of adjacent-channel interference in IEEE 802.11 WLANs* (PDF). CrownCom 2007. ICST & IEEE.
43. "Channel Deployment Issues for 2.4 GHz 802.11 WLANs". Cisco Systems, Inc. Retrieved 2007-02-07.
44. IEEE Standard 802.11-2007 page 531
45. "802.11 Technical Section". Retrieved 2008-12-15.
46. "Understanding 802.11 Frame Types". Retrieved 2008-12-14.
47. Olivier Bonaventure. "Computer Networking : Principles, Protocols and Practice". Retrieved 2012-07-09.
48. "IEEE P802.11 - TASK GROUP AC". IEEE. November 2009. Retrieved 2009-12-13.
49. Fleishman, Glenn (December 7, 2009). "The future of WiFi: gigabit speeds and beyond". Ars Technica. Retrieved 2009-12-13.
50. "MU-MIMO MAC Protocols for Wireless Local Area Networks: A Survey". *IEEE Communications Surveys & Tutorials* (IEEE) **PP** (99). December 4, 2014. doi:10.1109/COMST.2014.2377373.
51. "IEEE 802.11, The Working Group Setting the Standards for Wireless LANs". Retrieved 8 January 2016.
52. Jesse Walker, Chair (May 2009). "Status of Project IEEE 802.11 Task Group w: Protected Management Frames". Retrieved August 23, 2011.
53. http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf
54. http://www.kb.cert.org/vuls/id/723755 US CERT Vulnerability Note VU#723755
55. "iOS 8 strikes an unexpected blow against location tracking".

External links

- IEEE 802.11 working group (http://www.ieee802.org/11/)
- Official timelines of 802.11 standards from IEEE (http://www.ieee802.org/11/Reports/802.11_Timelines.htm)
- List of all Wi-Fi Chipset Vendors (https://wikidevi.com/wiki/List_of_Wi-Fi_Chipset_Vendors) – Including historical timeline of mergers and acquisitions

Categories: Channel access methods | IEEE 802.11 | 1997 introductions | Wireless networking standards | Local area networks

---