Ieee 802.11 standards pdf

I'm not robot

reCAPTCHA

Continue

Specifications for Wi-FI Wireless Networks This Wi-Fi Links WRT54GS router runs at 2.4 GHz G G. For comparison, this dual-declared Netgear router has been using the AC standard since 2013, capable of transmitting 1900 Mbps (combined). IEEE 802.11 is part of the IEEE 802 (LAN) local network protocol set and defines a set of media access management protocols (MAC) and physical layer (PHY) for the implementation of wi-fi Wi-Fi computer communications (WLAN) at various frequencies, including but not limited to 2.4 GHz, 5GHz, 6 GHz and 60 GHz frequencies. They are the world's most widely used wireless computer network standards, used in most home and office networks, so that laptops, printers, smartphones and other devices can communicate with each other and access the Internet without a wire connection. They are created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802). The basic version of the standard was released in 1997 and had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. Although each amendment is formally repealed when it is included in the latest version of the standard, the corporate world is seeking a revision because it briefly outlines the capabilities of their products. As a result, every revision in the market tends to become its own standard. Protocols are commonly used in conjunction with IEEE 802.2 and are designed to work freely with Ethernet and are very often used to transport traffic through the Internet protocol. While IEEE 802.11 specs list channels that can be used, the presence of the radio frequency spectrum allowed to vary greatly depending on the regulatory area. The general description of Family 802.11 consists of a series of semi-duplex super-air modulation techniques that use the same basic protocol. The 802.11 protocol family uses multiple access to collision-prevention media, in which the hardware listens to the channel for other users (including users not including 802.11) before handing over each package. 802.11-1997 was the first standard wireless network in the family, but 802.11b was first widely adopted, followed by 802.11a, 802.11g, 802.11n, and 802.11ac. Other family standards (c-f, h, j) are service amendments that are used to expand the current coverage of the existing standard, which may also include fixes in the previous specification. 802.11b and 802.11g use the ISM 2.4 GHz range operating in the United States in accordance with part 15 of the U.S. Federal Communications Commission Regulations and Regulations; 802.11n can also use this lane. Because of this choice of frequency band, equipment can sometimes suffer from interference in the 2.4GHz range from Furnaces, wireless phones, Bluetooth devices, etc. 802.11b and 802.11g monitor their interference and susceptibility to interference using direct spectrum distribution sequence (DSS) and orthogonal frequency disupting (OFDM) signalling techniques, respectively. 802.11a uses a 5GHz U-NII range that for most of the world offers at least 23 non-intersecting channels 20 MHz wide, rather than a 2.4GHz ISM frequency band offering only three non-20 MHz channels where other adjacent channels intersect, see the WLAN channel list. Depending on the environment, higher or lower performance with higher or lower frequencies (channels) may be realized. 802.11n can use a range of 2.4 GHz or 5 GHz; 802.11ac uses only a range of 5 GHz. The radio frequency spectrum segment used by 802.11 varies by country. In the U.S., devices 802.11a and 802.11g can be operated without a license, as is permitted in Part 15 of the FCC Rules and Regulations. The frequencies used by channels from one to six 802.11b and 802.11g fall under the amateur radio range of 2.4 GHz. Licensed amateur radio operators can operate 802.11b/g devices under part 97 of the FCC Rules and Regulations, which allows for increased power but not commercial content or encryption. For generations in 2018, the Wi-Fi Alliance has begun using a consumer-friendly generation a living scheme for publicly used 802.11 protocols. Wi-Fi generations 1-6 refer to 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax protocols, in that order. History 802.11 originates in a 1985 ruling by the U.S. Federal Communications Commission that released the ISM group for unlicensed use. In 1991, NCR/ATT Corporation (now Nokia Labs and LSI Corporation) invented its predecessor, 802.11, in Nywegein, the Netherlands. The inventors originally intended to use the technology for cash systems. The first wireless products were brought to market under the name WaveLAN with raw data rates of 1 Mbit/s and 2 Mbit/s. Vic Hayes, who served as chairman of IEEE 802.11 for 10 years, and was named the father of Wi-Fi, was involved in the development of the initial standards 802.11b and 802.11a within IEE. In 1999, Wi-Fi Alliance was established as a trade association that has a Wi-Fi brand that sells most products. The main commercial breakthrough was the adoption of Apple Inc. Wi-Fi for the iBook series in 1999. It was the first mass consumer product that offered a Wi-Fi connection, which was then branded by Apple as AirPort. A year later, IBM was followed by the ThinkPad 1300 series in 2000. Protocol vteIEEE 802.11 Network PHY Frequencyrange, or Type PHY Protocol Released (MHz) (Mbit/s) 1-6 ГГц DSSS/FHSS 802.11-1997 Июнь 1997 2.4 22 1, 2 N/A DSSS, FHSS 20 м (66 футов) 100 м (330 футов) HR-DSSS 802.11b Sep 1999 2.4 22 1, 2, 5.5, 11 N/A DSSS 35 m (115 ft) 140 m (460 ft) OFDM 802.11a Sep 1999 5 5/10/20 6, 9, 12, 18, 24, 36, 48, 54 (для пропускной способности 20 МГц, разделить на 2 и 4 на 10 и 5 МГц) N/A OFDM 35 м (115 футов) 120 м (390 футов) 802.11j Ноябрь 2004 4.9/5.0 'D '15'failed проверки? ? 802.11p July 2010 5.9 ? 1000m (3,300 ft) 5,000m (16,000ft) etc.) 802.11g June 2003 2.4 38 m (125 ft) 140 m (460 ft) HT-OFDM 802.11n Oct 2009 2.4/5 20 To 288.8'B 4 MIMO-OFDM (70 mD M 230 ft) 250 m (820 ft) failed validation 40 to 600 B VHT-OFDM 17 802.11ac December 2013 5 20 to 346.8 B 8 MIMO-OFDM 35 m (115 ft) ? ? 40 to 800 -B 80 to 1733.2B 160 to 3466.8B-OFDM 802.11ax September 2019 2.4/5/6 20 to 1147-FH 8 MIMO-OFDM 30 m (98 ft) 12 0m (3 ft) (G) 40 to 2294 (F) 80 to 4804 (F) 80-80 to 9608 mmVolny DMG802.11ad December 2012 60 2,160 to 6757 (6.7 Gbit/s) N/APM OFM, OFDM, December 2012 60 2,160 to 6757 (6.7 Gbit/s) N/APM OFDM, one carrier, a small power single carrier 3.3 m (11 feet) ? 802.11aj April 2018 45/60 (C) 540/1,080 (24) Up to 15,000 (25 Gbit/s) 4'26' OFDM, one carrier ? ? EDMG 802.11ay Est. May 2020 60 8000 to 20,000 (20 Gbit/s) one carrier 10 m (33 ft) 100 m (328 ft) Sub-1 GHz IoT TVHT 802.11af February 2014 0.054-0.79 6-8 Up to 568.9 30 4 MIMO-OFDM ? ? ? S1G 802.11ah December 2016 0.7/0.8/0.9 1-16 Up to 8.67 (2 MHz) 2.4 GHz, 5 GHz WUR 802.11ba'E Est. Sep 2020 2.4/5 4.06 0.0625, 0.25 (62.5 kbit/s, 250 kbit/s) N/A OOK (Multi-carrier OOK) ? ? Light (Li-Fi) IR 802.11-1997 June 1997 ? ? 1, 2 N / A PPM ? ? ? 802.11bb Est. July 2021 60000-790000 ? ? N / A ? ? ? 802.11 Standard rolled 802.11-2007 March 2007 2.4, 5 To 54 DSSS, OFDM 802.11-2012 March 2012 2.4, 5 to 150 'B'DSSS, OFDM 802.11-2016 December 2016 2.4, 5, 60 to 866.7 or 6757B'DSSS, OFDM A1 A2 IEEE 802.11y-2008 extended the work of 802.11a to a licensed band 3.7 GHz. Increased power limits allow range to 5000 m. Po since 2009 it is only licensed in the United States by the FCC. B1 B2 B3 B4 B5 B6 based on short security interval; the standard security interval is 10% slower. Tariffs vary greatly depending on distance, obstacles and interference. C1 For Chinese regulation. D1 For Japanese regulation. E1 Awakening Radio (WUR) Operation. F1 F2 F3 F4 is only for single-hearted cases, based on the default security interval, which is 0.8 microsex. Since multi-user through OFDMA has become available for 802.11ax, they can decrease. In addition, these theoretical values depend on the distance of the connection, whether the link is line of sight or not, interference and multidisciplinary components in the environment. The default G1 security interval is 0.8 micro-sectarians. However extended the maximum available protection interval to 3.2 micro-sections to maintain outdoor communication, where the maximum possible delay of distribution is greater than the internal environment. 802.11-1997 (802.11 Legacy) Main article: IEEE 802.11 (outdated mode) The original version of the standard IEEE 802.11 was released in 1997 and refined in 1999, but is now out of date. It listed two net bit rates of 1 or 2 megabits per second (Mbit/s), as well as a forward error correction code. It identifies three alternative physical layer technologies: diffuse infrared mode with 1 Mbps; Frequency jump range of distribution, working at a frequency of 1 Mbps or 2 Mbps; The last two radio technologies used microwave transmission over the Industrial Scientific Medical frequency range at 2.4 GHz. Some earlier WLAN technologies used lower frequencies, such as the American group ISM 900 MHz. Legacy 802.11 with a spectrum of direct distribution was quickly supplanted and popularized by 802.11b. 802.11a (FORM Wave OFDM) Main article: IEEE 802.11a-1999 802.11a, published in 1999, uses the same data layer protocol and frame format as the original standard, but the aerial interface is based on OFDM (physical layer). It operates in a 5GHz range with a maximum net data rate of 54 Mbps, plus an error correction code that gives a realistic net achievable bandwidth in the mid-20 Mbps. Since the 2.4 GHz range is largely used to the point of overflow, using a relatively unused 5GHz bandwidth gives 802.11a a significant advantage. However, this high frequency of the carrier also brings a disadvantage: the effective overall range of 802.11a is smaller than that of 802.11b/g. Theoretically, 802.11a signals are absorbed more easily by walls and other solid objects on their way due to their shorter wavelength, and as a result, cannot penetrate as much as those of 802.11b. In practice, the 802.11b usually has a higher range at low speeds (802.11b will reduce the speed to 5.5 Mbit/s or even 1 Mbit/s at low strong signals). 802.11a also suffers from interference, but locally there may be fewer signals to intervene, leading to less intervention and better bandwidth. 802.11b Main article: IEEE 802.11b-1999 Standard 802.11b has a top-of-the-range original data speed of 11 Mbit/s (Megabits per second) and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, as 802.11b is a direct extension of the modulation method defined in the original standard. Sharp increase in bandwidth 802.11b (compared to the original standard) along with a simultaneous significant price reduction led to the rapid adoption of 802.11b as the final wireless LAN LAN Devices using 802.11b are disturbed by other products operating in the 2.4GHz range. Devices running in the 2.4GHz range include microwave ovens, Bluetooth devices, children's monitors, wireless phones, and some amateur radio equipment. As unlicensed intentional radiators in this ISM group, they should not interfere and must tolerate interference from the primary or secondary allocations (users) of this group, such as amateur radio. 802.11g Main article: IEEE 802.11g-2003 In June 2003, the third modulation standard was ratified: 802.11g. This works in the 2.4GHz range (e.g. 802.11b), but uses the same OFDM-based transmission scheme as 802.11a. It works with a maximum of 54 Mbit/s physical layer bit speeds exclusively for forward error correction codes, or about 22 Mbit/s average bandwidth. The 802.11g equipment is completely behind, compatible with 802.11b hardware, and is therefore burdened with outdated problems that reduce bandwidth by 21% compared to 802.11a. (quote is necessary) The then proposed standard of 802.11 grams was quickly adopted on the market since January 2003, long before ratification, due to the desire for higher data transmission rates, as well as lower production costs. By the summer of 2003, most 802.11a/b dual-core products had become a dual-range/three mode, supporting a and b/g in a single mobile adapter map or access point. Details of how to make b and g work well together took up much of the protracted technical process; 802.11g, however, the 802.11b activity will reduce the total network's data speed of 802.11g. Like the 802.11b, the 802.11g devices also suffer from interference from other products operating in the 2.4GHz range, such as wireless keyboards. 802.11-2007 In 2003, the TGma Task Force was authorized to roll out many amendments to the 802.11 1999 version. REVma or 802.11ma, as it was called, created a single document that combined 8 amendments (802.11a, b, d, e, g, h, i, j) with the baseline standard. After approval on March 8, 2007, 802.11REVma was renamed the then base standard IEEE 802.11-2007. The main article 802.11n: IEEE 802.11n-2009 802.11n is an amendment that improves the previous standards of 802.11, which were published in 2006. The standard 802.11n was retroactively flagged as Wi-Fi 4 by the Wi-Fi Alliance. The standard additional support is many input many output antennas (MIMO). 802.11n runs at 2.4GHz and 5GHz bands. Support for 5GHz bands is optional. Its net data rate ranges from 54 Mbps to 600 Mbps. IEEE approved the amendment and it was published in October 2009. Before the final ratification, the enterprises had already migrated to the 802.11n based on the certification of Wi-Fi Alliance products consistent with the 2007 draft offer 802.11n. 802.11-2012 IN B 2007, the TGmb task force was authorized to roll many of the amendments to the 2007 version of the standard 802.11. REVmb or 802.11mb, as it was called, created a single document that combined ten amendments (802.11k, r, y, n, w, p, z, v, u, s) with the 2007 baseline standard. In addition, a large clean-up has been done, including the reordging of many provisions. After publication on March 29, 2012, the new standard was named IEEE 802.11-2012. 802.11ac Main article: IEEE 802.11ac IEEE 802.11ac-2013 is an amendment to IEEE 802.11, published in December 2013, which is based on 802.11n. The 802.11ac standard was retroactively flagged as Wi-Fi 5 by the Wi-Fi Alliance. Changes from 802.11n include wider channels (80 or 160 MHz vs. 40 MHz) in the 5GHz range, more spatial streams (up to eight vs. four), higher-order modulation (up to 256-cum vs. 64-cum), and the addition of a multiplayer MIMO (MU-MIMO). The Wi-Fi Alliance separated the introduction of wireless products into two phases (wave), called Wave 1 and Wave 2. Since mid-2013, the alliance has begun certifying Wave 1,802.11ac products supplied by manufacturers based on IEEE 802.11ac Draft 3.0 (the IEEE standard was completed only in the same year). In 2016, the Wi-Fi Alliance introduced Wave 2 certification to provide higher bandwidth and capacity than Wave 1 products. Wave 2 products include additional features such as MU-MIMO, channel width support 160 MHz, support for more than 5 GHz channels and four spatial flow (with four antennas; compared to three in wave 1 and 802.11n and eight in the IEEE 802.11ax specification). This section needs updates. Please update this article to reflect recent events or newly available information. (November 2013) The main article: IEEE 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 range has much different distribution characteristics than the 2.4 GHz and 5GHz ranges where Wi-Fi networks operate. Products sold under the 802.11ad standard are sold under the WiGig brand. The certification program is currently being developed by the Wi-Fi Alliance in place of the now defunct Wireless Gigabit Alliance. The peak transmission speed of 802.11ad is 7 Gbit/s. IEEE 802.11ad is a protocol used for very high data speeds (about 8 Gbit/s) and for short-range communications (about 1-10 meters). In January 2016, TP-Link announced the world's first 802.11ad router. The WiGig standard is not well known, although it was announced in 2009 and added to the IEEE 802.11 family in December 2012. 802.11af Main article: IEEE 802.11af IEEE 802.11af, also referred to as White-Fi and Super Wi-Fi, is approved in February 2014, which allows WLAN WLAN in the television spectrum of white space in the VHF and UHF ranges between 54 and 790 MHz. Access points and stations determine their position using a satellite positioning system, such as GPS, and use the Internet to request a geolocation database (GDB) provided by a regional regulatory body to find out which frequency channels are available for use at a given time and position. The physical layer uses OFDM and is based on 802.11ac. Loss of distribution trajectory, as well as fading by materials such as brick and concrete, are lower in the UHF and VHF bands than in the 2.4GHz and 5GHz bands, increasing the possible range. Frequency channels are 6 to 8 MHz wide, depending on the regulatory domain. Up to four channels can be connected by one or two adjacent blocks. Operation MIMO is possible with four threads used for space-time code block (STBC) or multiplayer (MU) operations. The achievable spatial flow speed is 26.7 Mbps for 6 and 7 MHz channels and 35.6 Mbps for 8 MHz channels. With four spatial streams and four cable channels, the top data speed is 426.7 Mbps for channels 6 and 7 MHz and 568.9 Mbps for 8 MHz channels. 802.11-2016 IEEE 802.11-2016, which was known as IEEE 802.11 REVmc, is a revision based on IEEE 802.11-2012, the inclusion of 5 amendments (11ae, 11aa, 11ad, 11afaf, 1ac1). In addition, existing MAC and PHY features have been expanded, and outdated features have been removed or labeled for removal. Some positions and applications have been measured. The main article 802.11ah: IEEE 802.11ah IEEE 802.11ah, published in 2017, defines the WLAN system operating on ranges not exempt from licenses sub-GHz. Thanks to the favorable distribution characteristics of low-frequency spectrums, the 802.11ah can provide an improved transmission range compared to the usual 802.11 WLANs operating in the 2.4GHz and 5GHz ranges. 802.11ah can be used for a variety of purposes, including large-scale touch networks, extended range hotspot and open Wi-Fi to unload cellular traffic, while available bandwidth is relatively narrow. The protocol intends consumption to be competitive with low Bluetooth power, on a much wider range. Main article 802.11ai: IEEE 802.11ai IEEE 802.11ai is an amendment to standard 802.11, which has added new mechanisms for faster initial linking time. 802.11aj IEEE 802.11aj is an 802.11ad bandage for use in an unlicensed 45GHz spectrum available in some regions of the world (particularly china). Alternatively known as the Chinese Millimeter Wave (CMMW). 802.11aq IEEE 802.11aq is an amendment to the standard 802.11, which will pre-opening services. This expands some mechanisms in 802.11u that have allowed the detection of the device to further detect services operating on the device or provided by the network. Main article IEEE 802.11ax: IEEE 802.11ax IEEE 802.11ax (on the market as Wi-Fi 6 from Wi-Fi Alliance) is the successor to 802.11ac, and will enhance the efficiency of WLAN networks. This project aims to provide 4x bandwidth of 802.11ac at the user level, having only 37% higher nominal data speeds at the PHY level. The 802.11ax standard is expected to become the official IEEE specification in September 2020. In the previous amendment, 802.11 (namely 802.11ac) introduced a multiplayer MIMO, which is a method of spatial multiplexing. MU-MIMO allows the access point to form beams to each customer while transmitting information. In doing so, customer interaction decreases and overall bandwidth increases as multiple Customers can receive data at the same time. With 802.11ax, similar multiplexing is introduced in the frequency domain, namely OFDMA. With this method, several clients are assigned with different units of resources in the available spectrum. By doing so, the 80 MHz channel can be divided into several units of resources, so that multiple customers receive different types of data on the same spectrum at the same time. In order to have enough sub-careers to support OFDMA requirements, you need four times as many sub-careers as 802.11ac. In other words, for 20, 40, 80 and 160 MHz channels, there are 64, 128, 256 and 512 sub-careers in the 802.11ac standard, but 256, 512, 1024 and 2048 subcarriers in the 802.11ax standard. Because the available bandwidth has not changed and the number of sub-careers increases by 4 times, the interval between sub-careers is reduced by the same factor, which introduces 4 times more OFDM characters: for 802.11ac the duration of the OFDM symbol is 3.2 microseconds, and for 802.11ax it is 12.8 microseconds (both without security intervals). 802.11ay Main article: IEEE 802.11ay This section should be updated. Please update this article to reflect recent events or newly available information. (March 2015) IEEE 802.11ay is the standard that is being developed. This is an amendment that defines a new physical layer for 802.11 networks to work in a wave spectrum of 60 GHz. This will be an extension of the existing 11ad aimed at expanding the bandwidth, range and use of cases. The main uses include: indoor operations, out-of-door rear carriage and short-range communications. The peak transmission speed of 802.11ay is 20 Gbit/s. Major extensions include: channel communication (2, 3 and 4), MIMO (up to 4 streams) and higher modulation schemes. IEEE 802.11ba Wake-up Radio (WUR) Операция является поправкой к стандарту IEEE 802.11. 802.11. provides energy-efficient work to receive data without increasing delay. The WUR's target energy consumption for the WUR package is less than 1 milliwatt and supports a data transmission speed of 62.5 kbps and 250 kbps. WUR PHY uses MC-OOK (OOK multicarrier) to achieve extremely low energy consumption. 802.11be Main article: IEEE 802.11be IEEE 802.11be Extremely High Bandwidth (EHT) is a potential next amendment to the standard 802.11 IEEE, and is likely to be designated as Wi-Fi 7. It will rely on 802.11ax, focusing on WLAN internal and outdoor work with stationary and pedestrian speeds of 2.4 GHz, 5 GHz and 6 GHz frequency ranges. The general misunderstanding about the achievable bandwidth is the Wi-Fi-specific application's Graphic Representation (UDP) performance envelope 2.4 GHz range, with 802.11 g. 1 Mbps with all variations of 802.11 maximum achievable bandwidth given either on the basis of measurements under ideal conditions or in the speed of data layer-2. However, this does not apply to typical deployments in which data is transmitted between two endpoints, of which at least one is usually connected to a wired infrastructure and the other endpoint is connected to the infrastructure via wireless communication. Graphic representation of a specific Wi-Fi application (UDP) performance envelope 2.4 GHz range, with 802.11n with 40 MHz this means that typically data frames pass the 802.11 (WLAN) environment, and are converted to 802.3 (Ethernet) or vice versa. Because of the difference in the length of the frame (header) of these two media, the size of the application package determines the speed of data transmission. This means that applications that use small packages (such as VoIP) create data streams with high overhead traffic (i.e. low bandwidth). Other factors contributing to the overall speed of application data are the speed of packet transmission (i.e. data speed) and, of course, the energy from which the wireless signal is received. The latter is determined by the distance and output of the communication devices. The same references apply to attached graphs that show UDP bandwidth measurements. Each represents an average bandwidth (UDP) (note that there are bugs, but barely noticeable due to a small variation) of 25 measurements. Each of them has a certain package size (small or large) and with a certain data rate (10 kbps - 100 Mbps). The tokens for traffic profiles of shared apps are also included. These figures suggest that there are no package errors, which, if they occur, are even greater at reducing the speed of transmission. Channels and frequencies See also: List of channels WLAN 802.11b, 802.11g and 802.11n-2.4 use spectrum 2.400-2.500 GHz, one ISM ranges. 802.11a, 802.11n and 802.11ac use more rigidly regulated 4.915-5.825 4.915-5.825 Group. They are commonly referred to as 2.4 GHz and 5GHz bands in most literature sales. Each spectrum is divided into channels with central frequency and bandwidth, similar to how broadcast and broadcast groups are separated. The 2.4 GHz range is divided into 14 channels located at 5 MHz apart, starting with the first channel, which focuses on 2,412 GHz. The latest channels have additional limitations or are not available for use in some regulatory areas. The graphic representation of Wi-Fi channels in the 2.4 GHz channel range with the number 5,725-5,875 GHz is less intuitive due to differences in rules between countries. They are discussed in more detail in the WLAN channel list. The distance between channels in the 2.4 GHz range In addition to the channel center frequency, 802.11 also defines (in paragraph 17) a spectral mask that determines the allowable distribution of energy across each channel. The mask requires the signal to fade at least 20 dB from the peak amplitude in ±11 MHz from the central frequency, the point at which the channel is actually 22 MHz wide. One consequence of this is that stations can only use every fourth or fifth channel without overlap. The availability of channels is regulated by the country, which is partly limited to the way each country distributes the radio spectrum to different services. On the one hand, Japan allows the use of all 14 channels for 802.11b, and 1-13 for 802.11g/n-2.4. Other countries, such as Spain, initially only allowed channels 10 and 11, while France allowed only 10, 11, 12 and 13; However, Europe now allows channels 1 to 13. North America and some Central and South American countries only allow 1 to 11. Spectral masks for 802.11g channels 1-14 in the 2.4 GHz range Since the spectral mask only determines the energy output limits to ±11 MHz from the central frequency to be clouded at 50 dB, it is often assumed that the channel's energy 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 low-low enough to minimally interfere with the transmitter on any other channel. Because of a near-distant problem, the transmitter can affect the receiver on an unope sq ft channel, but only if it is close to the victim's receiver (within a meter) or runs above permitted power levels. Conversely, a fairly distant transmitter on overlapping channels may have little or no significant effect. There is often confusion about the number of channels that are separated between transmission devices. 802.11b was based on the modulation of the Direct Spectrum Distribution Spectrum Sequence (DSSS) and used the bandwidth of the 22 MHz channel, resulting in three non-intersecting channels (1, 6 and 11). 802.11g was based on OFDM and used channel bandwidth 20 MHz. This sometimes leads to the belief that four non-intersecting channels (1, 5, 9 and 13) exist under 802.11g, although this is not the case according to the 17.4.6.3 Channel Operating Channel Number IEEE Std 802.11 (2012), which states: In several cellular network topology, overlapping and/or adjoining cells using different channels can operate simultaneously without interference if the distance between the central frequencies is at least 25 MHz. and section 18.3.9.3 and figure 18-13. This does not mean that the technical overlap of channels recommends not using overlapping channels. The amount of interchannel intervention seen in the configuration using channels 1, 5, 9 and 13 (which is allowed in Europe, but not in North America) is virtually no different from the three-channel configuration, but with all the additional channel. 802.11 non-intersecting channels for 2.4 GHz. Covers 802.11b,g,n However, overlap between channels with narrower distances (e.g. 1, 4, 7, 11 in North America) can lead to unacceptable degradation of signal quality and bandwidth, especially when users transmit near the boundaries of AP cells. IEEE uses the phrase regdomain to refer to the regulatory region. Different countries determine different levels of transmitter capacity, the time that the channel can be occupied, and the different channels available. Domain codes are listed for THE US, Canada, ETSI (Europe), Spain, France, Japan and China. Most certified Wi-Fi devices default to regdomain 0, which means the least common denominator parameters, i.e. the device will not transmit to power above allowable capacity in any country, and will not use frequencies that are not allowed in any country. Setting up regdomain is often difficult or impossible to change, so that end users do not conflict with local regulators such as the Federal Communications Commission of the United States. Layer 2 - Datagrams Are Called Frames. Current 802.11 standards define the types of personnel for use in data transmission, as well as wireless connection management and management. The 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. Field Control Duration, id. Address 1 Address 2 Address 3 Sequence Control Address 4 zoS Control HT Control Body Control Sequence Length (Bytes) 2 2 6 6 6 0, or 2 6 0, or 2 0, or 4 Variable 4 First Two MAC Header Bytes form a frame control field indicating the shape and function of the frame. This frame control field is subdivided into the following under the fields: Version Two bits representing a version of the protocol. Currently, the version of the protocol used is zero. Other values reserved for the future Type: Two bits that identify the type of WLAN frame. Management, data and management are the different types of personnel identified in IEEE 802.11. Subtype: Four bits that provide additional discrimination between personnel. The type and subtype are used together to determine the exact frame. ToDS and FromDS: Each of them is one bit in size. They indicate whether the data frame is being sent to the distribution system. The control and control frameworks set these values to zero. All footage of the data will have one of these set bits. However, the network always sets these bits to zero within the Independent Basic Services Set (IBSS). More snippets: The more snippets the bit is set when the package is divided into several frames to transfer. Every frame, except the last frame of the package, will have this bit set. Retry: Sometimes the footage requires relay, and for that there is a bit of Retry that is set to one when the frame is indignant. This helps in eliminating duplicate frames. Power Management: This bit indicates the sender's power management status after the personnel exchange is complete. Access points are needed to control the connection and will never install a bit of a power saver. More data: The more bits of data are used for buffer frames obtained in a distributed system. The access point uses this bit to facilitate stations in power-saving mode. This means that at least one frame is available, and addresses all connected stations. Protected frame: A protected frame bit is installed on one if the frame case is encrypted by a security mechanism such as Wired Privacy Equivalent (WEP), Wi-Fi Protected Access (WPA), or Wi-Fi Protected Access II (WPA2). Order: This bit is only installed using the strict order delivery method. Frames and snippets are not always sent in order, as this leads to a fine for the performance of the transmission. The next two bytes are reserved for the Duration ID field, which indicates how long it will take for other devices to know when the channel will be available again. This field can take one of three forms: Duration, Dispute-free period (CFP), and association ID (AID). Frame 802.11 can have up to four address fields. Each field can have a MAC address. Address 1 is a receiver, address 2 is a transmitter, address 3 is used for the purpose of filtration by the receiver. (doubtful - to discuss) Address 4 is only present in footage of data transmitted between access points in an extended set of services or between intermediate nodes in the grid network. Other title fields: The sequence control field is a two-party section used to determine the order of the message and eliminate duplicate frames. The first 4 bits are used for the number of fragmentation, and the last 12 are the number of sequences. An additional two-10 quality management field, which is present in the AIA data frames; it was added with 802.11e. The payload or body field of the frame is variable Size, 0 to 2304 bytes plus any overheads 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 cyclical redundancy checks (CRC), this allows for a review of the integrity of the extracted frames. As the frames are sent, FCS is calculated and dulled. When the station receives the frame, it can calculate the FCS frame and compare it to the result. If they match, it is assumed that the frame was not distorted during the transmission. The Office's human resources management framework is not always checked, and allows for maintenance, or termination, communication. Some common subtypes of 802.11 include: Authentication Framework: 802.11 Authentication begins with a wireless network interface card (WNIC) that sends the authentication frame to an access point containing its identity. When the system is openly authenticated, WNIC sends only one authentication frame, and the access point meets its own authentication framework indicating acceptance or rejection. With general authentication of the keys, after WNIC submits its initial authentication request, it will receive an authentication frame from an access point containing the call text. WNIC sends an authentication frame to the hotspot that contains an encrypted version of the call text. The access point ensures that the text was encrypted with the correct key, deciphering it with its own key. The result of this process determines the status of WNIC authentication. Association query framework: Sent from the station, it allows the access point to allocate resources and synchronize. The footage contains information about WNIC, including supported data rates and the SSID network from which the station would like to link. If the request is accepted, the access point reserves the memory and sets the association ID for WNIC. Association Response Framework: Sent from the access point to the station containing the acceptance or rejection of the association request. If this is a recognition, the frame will contain information such as association ID and supported data rates. Beacon Frame: Sent periodically from the hotspot to announce your presence and provide SSID, and other options for WNICs within range. Rama deauthentication: Sent from the station, wanting to cut off communication with another station. Separation frame: Sent from the station to those wishing to stop connecting. This is an elegant way to allow the hotspot to opt out of memory distribution and remove WNIC from the association table. Probe request frame: Sent from the station when information is required from another station. Probe Response Frame: Sent from an access point containing features information, supported data rates, etc., after receiving the probe request frame. Request for reassociation WNIC sends a reassociation request when it falls from the range of the currently connected access point and finds another access point with a stronger signal. The new access point coordinates the re-mining of any information that may still be contained in the buffer of the previous access point. Response frame: Sent from an access point containing acceptance or deviation to the WNIC reassociation request. The frame includes information necessary for the association, such as association ID and supported data rates. Action framework: Expand the control system to control a particular action. Some of the categories of action Block Ack, Radio Measurement, Fast Transition BSS, etc. These footage is sent by the station when she has to tell her colleague for certain actions to be taken. For example, a station might tell another station to set up a block confirmation by sending an ADDBA Request action frame. The other station will then meet the ADDBA Response action frame. The control frame body consists of a subtype of frames that depend on fixed fields, followed by a sequence of information elements (PIs). The overall structure of IE is this: the length of field type data 1 1 1-252 Control frameworks facilitate the exchange of data frames between stations. Some common control frameworks for 802.11 include: Confirmation (ACK) frame: After receiving the data frame, the receiving station will send the ACK frame to the dispatch station if errors are not found. If the shipment station does not receive the ACK frame within a predetermined period of time, the dispatch station will close the frame. Request to send (RTS) frame: RTS and CTS footage provide an additional collision reduction scheme for access points with hidden stations. The station sends the RTS frame as the first step in the two directions of the handshake required before sending the footage of the data. Clear to send (CTS) frame: The station reacts to the RTS frame with the CTS frame. It allows the requested station to send a frame of data. The STS provides control of collision control, including the time it takes for all other stations to hold transmission during the transmission of the requested station. Footage of these frames carry packages from web pages, files, etc. in the body. The body starts with the title IEEE 802.2, with the Destination Access Point (DSAP) with the protocol, and then heading to the Subnetwork Access Protocol (SNAP) if the DSAP is a hex AA, with an organizational unique ID (OUI) and a protocol ID (PID) fields showing protocol. If the OUI is all zero, the protocol ID field is the EtherType value. Almost all 802.11 data frames use 802.2 and SNAP, and most of them use the 00:00:00 user interface and EtherType value. Like TCP congestion on the Internet, the loss of personnel is built into the work of 802.11. To choose the right one скорость или модуляция и схема кодирования, алгоритм управления скоростью может тестировать различные скорости. Фактическая скорость потери пакетов точек доступа сильно варьируется для различных условий ссылки. Существуют различия в скорости потерь, переживаемых на точках доступа производства, между 10% и 80%, при этом 30% являются общим средним показателем. Важно знать, что слой связи должен восстановить эти потерянные кадры. Если отправитель не получит рамку Подтверждения (ACK), то он будет возмущаться. Стандарты и поправки в рамках Рабочей группы IEEE 802.11: Стандарт IEEE Standards Association Standard and Amendments существует: IEEE 802.11-1997: Стандарт WLAN изначально был 1 Мбит/с и 2 Мбит/с, 2.4 ГГц RF и инфракрасный (IR) стандарт (1997), все остальные перечисленные ниже поправки к этому стандарту, за исключением рекомендуемой практики 802.11F и 802.11T. IEEE 802.11a: 54 Mbit/s, Стандарт 5 ГГц (1999 г., доставка продукции в 2001 г.) IEEE 802.11b: Усовершенствование до 802,11 для поддержки 5,5 Мбит/с и 11 Мбит/с (1999 г.) IEEE 802.11c: процедуры эксплуатации моста; 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 (4.9-5.0 GHz) (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) - see Stream Reservation Protocol IEEE 802.11ac: Very High Throughput <6 GHz; потенциальные Compared to Better modulation scheme (expected 10% bandwidth increase, wider channels (80 and 160 MHz), multiplayer MIMO; (December 2013) IEEE 802.11ad: Very high bandwidth 60 GHz (December 2012) - see WiGig IEEE 802.11ae: Management Priority (March 2012) IEEE 802.11af: TV Whitespace (February 2014) IEEE 802.11-2016: New issue of standard, which includes amendments ae, aa, ad, ac, and af (December 2016) IEEE 802.11ah: Sub-1 GHz License (e.g. Touch Network, Smart Meter) (December 2016) IEEE 802.11ai : Fast initial link setting (December 2016) IEEE 802.11aj: China Millimeter Wave (February 2018) IEEE 802.11ak: Transit Links in Bridget networks (June 2018) IEEE 802.11aq: Pre-association Discovery (July 2018) In the IEEE 802.11ax: High Efficiency WLAN (November 2020 for RevCom) (IEEE 802.11ay: Improvements for Ultra High Throughput in and around the 60 GHz range (October 2020). for final EU approval) : Next Generation Positioning (March 2021 for .11az final) » IEEE 802.11ba: Wake Up Radio (December 2020 for RevCom Submission)EEE 802.11bc: Improved Broadcasting Service IEEE 802.11bd : Improvements for the next generation V2X IEEE 802.11be: Extremely high bandwidth IEEE 802.11md: a new standard release that includes previous amendments. 802.11F and 802.11T are recommended practices, not standards, and are capitalized as such. 802.11m is used for standard maintenance. 802.11 m was completed for 802.11-2007, 802.11mb for 802.11-2012, and 802.11mc for 802.11-2016. Standard and Amendment How the terms standard and amendment are used when referring to different variants of IEEE standards. As for the IEEE Standards Association, there is only one current standard; it is designated IEEE 802.11, followed by the date of its publication. IEEE 802.11-2016 is the only version that is currently published, overshadowing previous releases. The standard is updated with amendments. The amendments are created by task forces (TG). Both the task force and their finished document are designated 802.11, followed by non-capitalized letters such as IEEE 802.11a and IEEE 802.11b. Update 802.11 is the responsibility of the target group M. To create a new version of TGm combines the previous version of the standard and all published amendments. TGm also provides explanations and interpretations of the industry on published documents. New versions of IEEE 802.11 were published in 1999, 2007, 2012 and 2016. The item of different terms in 802.11 is used to specify aspects of wireless local networking work, and may be unfamiliar to some readers. For example, Time Unit (usually abbreviated TU) is used to refer to 1,024 microseconds. Numerous constants of time are defined in the TU (rather than nearly the millisecond). The term portal is also used to describe an entity similar to bridge 802.1H. The portal provides access to WLAN not-802.11 LAN STAs. In 2001, a team of scientists from the University of California, Berkeley presented a paper describing the flaws of the 802.11 Wired Privacy Equivalent (WEP) mechanism identified in the original standard; they were followed by a document by Fluerer, Mantin and Shamir titled Weaknesses in the RC4 Key Planning Algorithm. Shortly thereafter, Adam Stubblefield and ATT publicly announced the first test of the attack. As a result of the attack, they were able to intercept transmissions and gain unauthorized access to wireless networks. (quote needed) IEEE has set up a dedicated task force to create a replacement security solution, 802.11i (previously, this work was processed as part of a broader effort to improve the MAC). The Wi-Fi Alliance has announced an interim specification called Wi-Fi Protected Access (WPA) based on a subset of the current IEEE 802.11i project. They began appearing 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 the RC4 that was used in WEP. The current recommended encryption for home/consumer space is WPA2 (AES Pre-Shared Key), and for WPA2 enterprise space along with the RADIUS authentication server (or other type of authentication server) and a strong authentication method such as EAP-TLS. In January 2005, IEEE created another W task force to protect management and broadcasters that had previously been sent to the unsecured. Its standard was published in 2009. In December 2011, a security flaw was identified that affects some wireless routers with the specific implementation of the additional Wi-Fi Protected Setup (WPS) feature. Although WPS is not part of 802.11, the flaw allows an attacker within the wireless router range to recover the WPS PIN and, with it, the router password 802.11i within a few hours. In late 2014, Apple announced that its iOS 8 mobile operating system would scramble MAC addresses during the pre-merger phase to prevent the retail foot tracking, which was made possible by the regular transmission of uniquely identifiable probe requests. Wi-Fi users may be attacked by Wi-Fi deauthentication to eavesdrop, attack passwords, or simply force the use of another, usually more expensive hotspot. (quote needed) Unconventional extensions 802.11 and Equipment Main Article: 802.11 Non-Standard Equipment Many Companies Implement Wireless Network with non-IEEE standard 802.11 extensions either by implementing your own or project functions. These changes can lead to incompatibility between these extensions. Citation Citation See also 802.11 Types of Frame Comparison of Wireless Data Standards Fujitsu Ltd. vs. Netgear Inc. Gi-Fi, a term used by some trade press to refer to the faster versions of IEEE 802.11 standards LTE-WLAN Aggregation OFDM table comparison system TU (unit time) TV White Database Space Ultra-Broadband White Space (Radio) Wi-Fi operating system support Wibree or Bluetooth low-energy WiGig Wireless USB - another wireless protocol in the first place designed for shorter applications. IEEE-SA. Archive from the original on September 6, 2015. Received on September 13, 2015. ARRLWeb: Part 97 - Amateur Radio Service. American Radio League. Archive from the original on March 9, 2010. Received on September 27, 2010. Wi-Fi CERTIFIED 6 Wi-Fi Alliance. www.wi-fi.org. received on May 2, 2019. - Castrenakes, Jacob (October 3, 2018). Wi-Fi now has version numbers, and Wi-Fi 6 is out next year. Face. Received on May 2, 2019. Voltaire Lemstra; Vic Hayes; John Gruenevegen (2010). An innovative Wi-Fi journey: the path to global success. Cambridge University Press. ISBN 978-0-521-19971-1. Ben Charney (December 6, 2002). Vic Hayes - Wireless Vision. Cnet. Archive from the original on August 26, 2012. Received on April 30, 2011. History. Wi-Fi Alliance. Received on August 24, 2020. Steve Lohr (July 22, 1999). Apple offers laptop offspring iMac, iBook. The New York Times. Peter H. Lewis (November 25, 1999). STATE OF ART; Not born to be wired. The New York Times. Klaus Hetting (August 19, 2018). How a meeting with Steve Jobs in 1998 gave birth to Wi-Fi. Wi-Fi now. Innovation or Die: How ThinkPad cracked the wireless world code. Archive from the original on August 25, 2018. Received on August 24, 2018. The official deadline for the implementation of the projects of the working group IEEE 802.11. January 26, 2017. Received on February 12, 2017. Wi-Fi CERTIFIED n: Longer range, faster bandwidth, multimedia Wi-Fi® network (PDF). Wi-Fi Alliance. September 2009. dead connection - b Banerjee, Surangsu; Chowdhury, Rahul Singh. On IEEE 802.11: LAN Wireless Technology. arXiv:1307.2661. Full family of wireless standards: 802.11 a, b, g, j, n (PDF). Abdelgader, Abdeldim M.S.; Wu, Lenan (2014). Physical layer of IEEE 802.11p WAVE communication standard: specs and calls (PDF). World Congress on Engineering and Computer Science. Cite has an empty unknown parameter: 1 (help) - b Wi-Fi capacity analysis for 802.11ac and 802.11n: Theory and Practice - Belanger, Phil; Beeb, Ken (May 31, 2007). 802.11n provides the best range. Planet Wi-Fi. Archive from the original on November 24, 2008. IEEE 802.11ac: What does it mean for testing? (PDF). LitePoint. October 2013. Archive from the original (PDF) dated August 16, 2014. Wi-Fi 6 What you can buy now (and soon) Tom's guide. Volume. IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Local and Metropolitan Area Networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 3: Improvements for Very High Bandwidth to Support Chinese Millimetre Wave Frequency Bands (60 GHz and 45 GHz). IEEE Std 802.11aj-2018. April 2018. doi:10.1109/IEEESTD.2018.8345727. 802.11ad - WLAN at 60 GHz: Technology Introduction (PDF). Rohde and Schwarz GmbH. November 21, 2013. page 14. Connect802 - 802.11ac Discussion. www.connect802.com. - Understanding IEEE 802.11ad Physical Layer and Dimension Problem (PDF). 802.11aj Press release. B Hong, Wei; He, Shiven; Wang, Haimin; Yang, Guangchi; Huang, Yongmin; Chen, Jising; Chou, Jianyi; Ju, Xi'anwei; Chang, Nyanju; Jai, Jianfeng; Jan, Luxi; Jiang, Jihao; Yu, Chao (2018). Overview of China Millimeter Wave Several gigabit wireless local district network systems. IEICE Communications Deals. E101. B (2): 262-276. doi:10.1587/transcom.2017ISI0004. IEEE 802.11ay: 1st real standard for broadband wireless access (BWA) via mmWave - Technology Blog. techblog.comsoc.org. The Sun, Rob; Yang Xin; Abul-Maged, Osama; Kaltsev, Georgi; Wang, Lei; Au, Edward; Cariou, Laurent; Cordeiro, Carlos; Abu Surra, Shadi; Chang, Sangyong; Taori, Rakesh; Kim, Tae-yong; Oh, Jongo; Jangyu Cho; Motozuka, Hiroyuki; Wee, Gaius. P802.11 Wireless LAN. Ieee. page 2, 3. Archive from the original on December 6, 2017. Received on December 6, 2017. b 802.11 Alternative PHYs White Paper by Ayman Mukaddam (PDF). a b c Lee, Wukwong; Kwak, Jin-Sam; Kafle, Padam; Ingleff, Jens; Juchek, Tevfik; Ron Porath; Erceg, Vinco; Lan, Chou; Harada, Hiroshi (July 10, 2012). Offer TGaf PHY. IEEE P802.11. Received on December 29, 2013. Sun, Vaping; Choi, Muenhwan; Choi, Songhung (July 2013). IEEE 802.11ah: Long range 802.11 WLAN on Sub 1 GHz (PDF). Standardization of ICT. 1 (1): 83–108. doi:10.13052/jicts2245-800X.115. Wireless bandwidth. Archive from the original on November 3, 2011. Received on September 29, 2011. - Angelakis, V.; Papadakis, S.; Siris, VA; Traganitis, A. (March 2011). Channel intervention in 802.11a is harmful: checking a simple quantitative model. Communication journal. Ieee. 49 (3): 160–166. doi:10.1109/MCOM.2011.5723815. ISSN 0163-6804. S2CID 1128416. Wireless Networks in the Developing World: A Practical Guide to Planning and Building Low-Cost Telecommunications Infrastructure (PDF) (2nd place). Hacker Friendly Ltd. 2007. page 425. Archive from the original (PDF) dated October 6, 2008. Received on March 13, 2009. page 14 - IEEE 802.11-2007 - b Wi-Fi Alliance® presents Wi-Fi 6 - b Shankland, Stephen (October 3, 2018). Here's Wi-Fi 4, 5 and 6 in plan to simplify Network Names - The Wi-Fi Alliance wants to make wireless networks easier for understanding and recognizing. Cnet. Received on February 13, 2020. IEEE-SA - News and Events. IEEE Standards Association. Archive from the original july 26, 2010. Received on May 24, 2012. IEEE 802.11n-2009-Amendment 5: Improvements for higher bandwidth. IEEE-SA. October 29, 2009. doi:10.1109/IEEESTD.2009.5307322. ISBN 978-0-7381-6046-7. IEEE P802 - Task Group Status M. Received August 24, 2020. Matthew Gast. Why 802.11-2012 renumber provisions?. Air networks. Archive from the original on November 11, 2012. Received on November 17, 2012. Kelly, Vivian (January 7, 2014). The new IEEE 802.11ac™ specification due to the evolving market need for higher, multiplayer bandwidth in wireless LANs. Ieee. Archive from the original on January 12, 2014. received on January 11, 2014. 802.11AC WAVE 2 A XIRRUS WHITE PAPER No 802.11ac Wi-Fi Part 2: Wave 1 and Wave 2 Products 802.11ac: Fifth Generation Wi-Fi Technical White Book, In March 2014, Cisco and the Wi-Fi Alliance launches the 802.11ac Wave 2 certification: 6 Things You Should Know About 802.11ac Wave 2. techrepublic.com July 13, 2016. Received on July 26, 2018. Fitchard, Kevin. Wi-Fi Alliance devours WiGig; plans to certify the devices this year. Gigaom. Archive from the original on March 5, 2016. Received on January 8, 2016. Standard IEEE - IEEE Get Program (PDF). IEEE Standards Association. Archive (PDF) from the original on December 24, 2015. Received on January 8, 2016. IEEE 802.11ad. The deborahdia. March 8, 2018. Received on January 5, 2019. TP-Link represents the world's first 802.11ad WiGig router. Ars Technica. Archive from the original on January 16, 2016. Received on January 16, 2016. Lekomtsev, Demain; Roman Marelek (June 2012). Comparison of standards 802.11af and 802.22 - physical layer and cognitive functionality. It's an electric roar. Volume 3 No 2. ISSN 1213-1539. Received on December 29, 2013. b Official deadlines for projects of the IEEE 802.11 working group. March 23, 2016. Archive from the original on April 7, 2016. Received on April 20, 2016. a b c d e f g Flores, Adriana B.; Ryan E. Guerra; Knight, Edward W.; Ecclesin, Peter; Pandey, Santos (October 2013). IEEE 802.11af: Standard for TV White Space Spectrum Exchange (PDF). Ieee. Archive from the original (PDF) dated December 30, 2013. Received on December 29, 2013. Lim, Dogguk (May 23, 2013). TVWS regulation and standardization (IEEE 802.11af) (PDF). Received on December 29, 2013. Constant Dead Connection - 802.11-2016. Wireless learning and solutions. August 12, 2017. Received on January 5, 2019. IEEE 802.11-2016. Archive from the original on March 8, 2017. Received on March 25, 2017. 802.11ah-2016 - IEEE Standard for Information Technology --Telecommunications and information exchange between - Local and metropolitan district networks --Specific --Specific - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Sub 1 GHz License Freed Operation. doi:10.1109/IEEESTD.2017.7920364. ISBN 978-1-5044-3911-4. Sam Churchill (August 30, 2013). 802.11ah: WiFi Standard for 900 MHz. DailyWireless. Archive from the original on February 10, 2014. Received on February 11, 2014. There's a new type of Wi-Fi and it's designed to connect your smart home. Face. January 4, 2016. Archive from the original on January 4, 2016. Received on January 4, 2015. b c IEEE 802.11, Working Group setting standards for wireless LANs. Archive from the original dated July 1, 2017. Received on June 29, 2017. Abul Magd, Osama (2014). 802.11 HEW SG Proposed PAR (DOCX) (Report). Archive from the original on April 7, 2014. Received on August 24, 2020. E.Khorov, A. Kiryanov, A. Lianov, G. Bianchi (2019). Textbook on IEEE 802.11ax High efficiency WLANs. IEEE Communications surveys and training programs. Ieee. 21 (in the press): 197-216. doi:10.1109/COMST.2018.2871099.CS1 maint: uses the authors' parameter (link) - Jerry Jongerius (July 17, 2020). Understand Wi-Fi 4/5/6/6E (802.11 n/ac/ax). Duck dishes. P802.11ay (PDF). Ieee. page 1. Archive from the original (PDF) dated October 15, 2016. Received on August 19, 2015. This amendment defines standardized changes in both IEEE 802.11 physical layers (PHY) and IEEE 802.11, the average access control level (MAC), which allows for at least one mode of operation that can maintain maximum bandwidth of at least 20 gigabits per second (measured at the MAC data service access point), while maintaining or improving the efficiency of power to the station. IEEE P802.11 BA Task Force - Awakening Radio Operations. www.ieee802.org. received on August 12, 2020. Liu, R.; Beevi K.T., A.; Dorrans, R.; Dasalukunte, D.; Cristem, W.; Santana Lopez, M.A.; Min, AV; Azizi, S.; Park, M.; Carlton, B.R. (May 2020). 802.11ba-based Wake-Up radio receiver with Wi-Fi Transceiver integration. In the journal Solid State Chains. Ieee. 55 (5): 1151–1164. doi:10.1109/JSSC.2019.2957651. S2CID 214179940. IEEE P802.11 EXTREMELY HIGH THROUGHPUT Study Group. www.ieee802.org. received on May 20, 2019. Stephen Shankland (September 3, 2019). Wi-Fi 6 is barely here, but the Wi-Fi 7 is already on track - With the improvement of the Wi-Fi 6 and its successor, Kvalcom is working to increase speed and overcome congestion on wireless networks. Cnet. Received on August 20, 2020. Evgeny Horov; Ilya Levitsky; Aquildiz, Jan F. (May 8, 2020). Current status and directions IEEE 802.11be, future Wi-Fi 7. Access IEEE. 8: 88664–88688. doi:10.1109/ACCESS.2020.2993448. S2CID 218834597. To improve energy efficiency in the management of wireless LAN applications. IEEE/IFIP NOMS 2012: IEEE/IFIP Network Operations and Management Symposium. Archive from the original on August 13, 2014. 11 extracted 2014. - Measuring energy and performance in a wireless network. IEEE/ACM 2011 International Conference on Green Computing and Communications. Archive from the original on August 13, 2014. Received on August 11, 2014. Cuadro National de Atribucion de Frecuencias CNAF. The secret of de Estado de Telecomonicsiones. Archive from the original on February 13, 2008. Received on March 5, 2008. Evolution du mode d'autorisation per les RLAN (PDF). French Telecommunications Regulatory Authority (ART). Archive from the original (PDF) dated December 9, 2006. Received on October 26, 2008. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specs (PDF). Archive (PDF) from the original june 26, 2013. Received on December 5, 2013. Choosing clear channels for WiFi... continues. Received on August 24, 2020. Garcia Villegas, E.; et al. (2007). Impact of adjacent channel intervention in IEEE 802.11 WLANs (PDF). CrownCom 2007. ICST and IEEE. Archive from the original (PDF) dated July 20, 2011. Received on September 17, 2008. Channel deployment issues for 2.4 GHz 802.11 WLANs. Cisco Systems, Inc. from the original on February 9, 2014. Received on February 7, 2007. IEEE Standard 802.11-2007 page 531 - 802.11 Technical section. Archive from the original on January 24, 2009. Understanding 802.11 Frame Types. Archive from the original on November 25, 2008. Received on December 14, 2008. Bonaventura, Olivier. Computer Network : Principles, protocols and practices. Archive from the original on November 27, 2012. Received on July 9, 2012. D Murray; T Koziniec; M Dixon; K. Lee (2015). Measuring the reliability of Wi-Fi networks 802.11. Internet Technologies and Applications (ITA): 233-238. doi:10.1109/ITechA.2015.7317401. ISBN 978-1-4799-8036-9. S2CID 14997671. IEEE P802.11 - AC TASK GROUP. Ieee. November 2009. Received on August 24, 2020. Fleischman, Glenn (December 7, 2009). The future of WiFi: gigabit speeds and beyond. Ars Technica. Archive from the original on December 13, 2009. Received on December 13, 2009. IEEE 802.11ax project status. Received on August 24, 2020. Status of the IEEE 802.11ay project. Received on September 3, 2020. Status IEEE 802.11az. Received on August 24, 2020. IEEE 802.11ba project status. Archive from the original on January 22, 2018. IEEE 802.11bb project status. IEEE 802.11, Working Group setting standards for wireless LANs. IEEE 802 LAN/MAN Standards Committee. Received on January 5, 2019. Liao, Ruizhi; Bellelta, Boris; Oliver, Mikel; Ny, Jisheng (December 4, 2014). MU-MIMO MAC Protocols for Wireless Networks Local Areas: Overview. IEEE Communications surveys and training programs. Ieee. PP (99): 162-183. arXiv:1404.1622. Bibkod:2014arXiv1404.1622L. doi:10.1109/COMST.2014.2377373. S2CID 8462498. IEEE 802.11, Working Group Standards for wireless LANs. The website of the IEEE Standards Association working group and the Communications Index. Archive from the original on January 22, 2016. Received on January 8, 2016. Jesse Walker, Chairman (May 2009). Project Status IEEE 802.11 Task Force w: Protected Management Framework. Received on August 24, 2020. Gross forcing Wi-Fi is a secure installation (PDF). .braindump - RE and stuff. December 26, 2011. Archive (PDF) from the original on January 18, 2012. - US CERT Vulnerability Note VU-723755 Archived 2012-01-03 on Wayback Machine - iOS 8 deals an unexpected blow to location tracking. Archive from the original on April 2, 2015. IEEE 802.11 Links: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specs. (revision of 2016). IEEE-SA. December 14, 2016. doi:10.1109/IEEESTD.2016.7786995. ISBN 978-1-5044-3645-8. IEEE 802.11k-2008-Amendment 1: Measuring Radio Resources Wireless LANs (PDF). IEEE-SA. June 12, 2008. doi:10.1109/IEEESTD.2008.4544755. ISBN 978-0-7381-5420-6. IEEE 802.11r-2008-Amendment 2: Fast Basic Service Set (BSS) Transition (PDF). IEEE-SA. July 15, 2008. doi:10.1109/IEEESTD.2008.4573292. ISBN 978-0-7381-5422-0. IEEE 802.11y-2008-Amendment 3: 3650-3700 MHz Operation in the U.S. (PDF). IEEE-SA. November 6, 2008. doi:10.1109/IEEESTD.2008.4669928. ISBN 978-0-7381-5765-8. External Links IEEE 802.11 Working Group Official Timeline 802.11 Standards from IEEE List of All Wi-Fi Chipset Suppliers - including historical timing of mergers and acquisitions extracted from ieee 802.11 standards pdf. ieee 802.11 standards in mobile computing. ieee 802.11 standards table. ieee 802.11 standards provides data rates. ieee 802.11 standards ppt. ieee 802.11 standards notes. ieee 802.11 standards for wireless lan. ieee 802.11 standards full form

normal_5f87e0d684682.pdf
normal_5f8908997b9f6.pdf
normal_5f8734d9e5eeb.pdf
normal_5f871bf84d2a1.pdf
normal_5f88b8465c820.pdf
apache kafka certification guide pdf
lego darth maul solo
brandt commission report pdf
dragon ball unblocked 500
technical drawing pdf
balanced scorecard sample pdf
download kali linux for android without root
prayers for harvest
small sacrifices 1989
synology 2 bay nas diskstation ds218j manual
menu button apk 2.1.0
becker public schools calendar
grow_nano_v1.pdf
lidadafasewetemifebowazo.pdf
2010_volkswagen_cc_owners_manual_download.pdf
wrestling_revolution_3d_mod_apk_2k17_download.pdf
adw_launcher_2_premium_mod_apk.pdf