I'm human

IEEE 802.11 Wi-Fi networks are the most widely used wireless networks globally, connecting devices like laptops and smartphones through routers. The standard specifies medium access control (MAC) and physical layer (PHY) protocols for implementing WLAN computer communication. It's part of the IEEE 802 set of local area network (LAN) technical standards. The first version was released in 1997, with subsequent amendments providing a basis for wireless network products using the Wi-Fi brand. The standard uses various frequencies, including 2.4 GHz, 5 GHz, and 6 GHz frequency bands. IEEE 802.11 is used in most home and office networks to allow devices to communicate with each other and access the Internet without wires. It's also a basis for vehicle-based communication networks. The protocols are designed to interwork seamlessly with Ethernet and often carry Internet Protocol traffic. The Wi-Fi generations have evolved over time, with new standards being released periodically. These include 802.11n (2009), 802.11ac (2013), 802.11ax (2021), and upcoming releases like 802.11be (2024) and 802.11bn (2028). 802.11 is a family of wireless networking standards that have evolved over time to improve performance and capacity. The first standard in this family, 802.11-1997, laid the groundwork for future revisions, which include 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac, and 802.11ax. Service amendments to these standards allow for extensions of their scope without requiring new equipment. The 2.4-GHz band is used by many 802.11b, g, and n devices in the United States, while 802.11a operates on the 5 GHz U-NII band. This choice can lead to interference issues with microwave ovens, cordless telephones, and Bluetooth devices. To mitigate this, 802.11b/g use direct-sequence spread spectrum, while 802.11a employs orthogonal frequency-division multiplexing. The availability of channels in the 5 GHz U-NII band offers more options for operators, with at least 23 non-overlapping channels available. However, performance can vary depending on environmental conditions. In contrast, 802.11n and 802.11ax devices use either the 2.4 GHz or 5 GHz bands, while 802.11ac operates exclusively on the 5 GHz band. The spectrum used by 802.11 varies between countries, with some frequencies falling within amateur radio bands. Historically, the development of Wi-Fi has been driven by technological advancements and regulatory changes. The U.S. Federal Communications Commission released the ISM band in 1985 for unlicensed use, paving the way for the first wireless products, such as WaveLAN. Vic Hayes played a key role in designing the original 802.11 standard, which later evolved into Wi-Fi. The development of Wi-Fi standards began in the late 1990s when engineers approached the IEEE (Institute of Electrical and Electronics Engineers) to create a standard for wireless networking. In 1999, the Wi-Fi Alliance was formed to promote the use of Wi-Fi technology and to hold the trademark for Wi-Fi-enabled products. The first commercial breakthrough came in 1999 with Apple's adoption of Wi-Fi for its iBook laptops, which featured AirPort network connectivity. This was followed by IBM's ThinkPad 1300 series in 2000. Since then, several new Wi-Fi standards have been introduced, each offering improved performance and capabilities. These include: * 802.11b (1999): Offered data rates of up to 11 Mbps * 802.11a (1999): Provided faster data transfer speeds of up to 54 Mbps * 802.11g (2003): Introduced data rates of up to 54 Mbps in the 2.4 GHz frequency band * 802.11n (2009): Offered improved performance with data rates of up to 600 Mbps and multiple input, multiple output (MIMO) technology * 802.11ac (2013): Provided even faster speeds of up to 1.3 Gbps in the 5 GHz frequency band * 802.11ax (2020): Introduced new features such as orthogonal frequency-division multiple access (OFDMA) and multi-user MIMO for improved performance Future standards, including 802.11be (Wi-Fi 7), are expected to offer even faster speeds and more advanced capabilities. Note that I have removed some of the technical details from the original text to make it easier to understand. If you would like me to include those details as well, please let me know! Li-Fi and VLC/OWC standards have undergone changes over the years. The IEEE 802.11bb standard is expected to be released in December 2023 for frequencies between 800-1000 nm with speeds of up to 9.6 Gbit/s using O-OFDM technology. The older IR[A] (IrDA) standard, released in June 1997, operated at 850-900 nm with limited capabilities. The 802.11 Standard has undergone several rollups over the years, including the 802.11-2007 and 802.11-2012 standards which increased speeds to up to 54 Mbit/s and 150 Mbit/s respectively. The 802.11me standard is expected to be released in September 2024 for frequencies of 2.4 GHz, 5 GHz, 6 GHz, and 60 GHz with speeds of up to 9608 or 303336 Mbit/s using DSSS and OFDM technologies. Some legacy standards include IEEE 802.11-1997, which specified two net bit rates of 1 or 2 megabits per second (Mbit/s) and was rapidly supplanted by the 802.11b standard. The 802.11a-1999 standard, released in 1999, operates in the 5 GHz band with a maximum net data rate of 54 Mbit/s. The IEEE 802.11y-2008 extended the operation of 802.11a to the licensed 3.7 GHz band, allowing for increased power limits and a range of up to 5,000 meters. 802.11a is utilized extensively due to its use of the relatively unused 5 GHz band, providing a significant advantage over 802.11b/g. However, this higher carrier frequency also presents drawbacks: 802.11a signals are more readily absorbed by walls and other solid objects in their path, resulting in shorter ranges. In contrast, 802.11b generally exhibits longer ranges at lower speeds, although its performance diminishes when signal strengths are weak. 802.11a is also susceptible to interference, yet locally, there may be fewer signals interfering with it, leading to better throughput. The 802.11b standard boasts a maximum raw data rate of 11 Mbit/s and utilizes the same media access method as the original standard. Its products emerged in early 2000 due to the direct extension of the modulation technique defined in the original standard. A notable drawback of 802.11b devices is their susceptibility to interference from other products operating in the 2.4 GHz band, such as microwave ovens and cordless telephones. The introduction of 802.11g in June 2003 marked a significant development, operating within the same 2.4 GHz band as 802.11b but utilizing an OFDM-based transmission scheme similar to 802.11a. While it offers higher data rates, its performance is slightly reduced compared to 802.11a. IEEE 802.11 standards evolution and improvements The 60 GHz frequency band differs significantly from the more commonly used 2.4 GHz and 5 GHz Wi-Fi bands in terms of propagation characteristics. Products that implement the 802.11ad standard are branded as WiGig and undergo certification through the Wi-Fi Alliance's program. The peak data transfer rate for 802.11ad is a staggering 7 Gbit/s, while its primary function lies in facilitating extremely high data rates (around 8 Gbit/s) and short-range communication (approximately 1–10 meters). TP-Link made history by releasing the world's first 802.11ad router in January 2016. However, a distinct standard exists for operating WLANs within TV white space spectrum in VHF and UHF bands between 54 and 790 MHz - IEEE 802.11af or "White-Fi" and "Super Wi-Fi". This amendment, approved in February 2014, uses cognitive radio technology to transmit on unused TV channels while limiting interference for primary users like analog TV, digital TV, and wireless microphones. Access points and stations can determine their position using GPS, then query a geolocation database (GDB) provided by regional regulatory agencies to discover available frequency channels based on time and location. The physical layer of IEEE 802.11af is based on OFDM and utilizes 802.11ac as its foundation. This leads to lower propagation path loss and material attenuation in UHF and VHF bands compared to the more commonly used frequencies, thereby increasing possible range. Frequency channels for IEEE 802.11af are between 6 to 8 MHz wide, depending on regulatory domains, with up to four channels that can be bonded into either one or two contiguous blocks. MIMO operation is feasible with up to four streams used for space–time block code (STBC) or multi-user (MU) operation, leading to significant data rate enhancements. The IEEE 802.11ax standard, also known as Wi-Fi 6, offers significant improvements over its predecessor, 802.11ac, with a focus on dense environments such as corporate offices and residential apartments. IEEE 802.11 standards continue to evolve, with recent advancements like MIMO (up to four streams) and higher modulation schemes enabling ranges of 300-500 meters.[82] The IEEE 802.11ba Wake-up Radio (WUR) Operation amendment prioritizes energy-efficient data reception without compromising latency.[83] WUR packets can be received at a power consumption of less than one milliwatt, supporting data rates of 62.5 kbit/s and 250 kbit/s.[84] The IEEE 802.11bb standard utilizes infrared light for communication.[85] In the pipeline is IEEE 802.11be Extremely High Throughput (EHT), which will likely be designated as Wi-Fi 7, focusing on indoor and outdoor WLAN operation with stationary and pedestrian speeds in the 2.4 GHz, 5 GHz, and 6 GHz frequency bands.[86][87][88] Graphical representations show the performance envelopes for various IEEE 802.11 standards, including 802.11g and 802.11n, highlighting the differences in data transfer rates between these protocols. In typical deployments, maximum achievable throughputs are not representative of real-world scenarios, where data is transferred between two endpoints, with at least one endpoint connected to a wired infrastructure and the other via wireless link. This means that frame lengths and packet sizes play crucial roles in determining data transfer speeds. Other factors influencing application data rates include transmission speed, wireless signal reception energy, distance, and configured output power of communicating devices.[89][90] The ISM bands used by Wi-Fi technologies such as 802.11a, n, and ac fall within the 4.915–5.825 GHz range. This band is commonly referred to as the "2.4 GHz and 5 GHz bands." Each spectrum is divided into channels with a center frequency and bandwidth, similar to how radio and TV broadcast bands are structured. The 2.4 GHz band consists of 14 channels, spaced 5 MHz apart, starting from channel 1, which is centered on 2.412 GHz. Channels 11-14 have additional restrictions or are unavailable in certain regulatory domains. The channel numbering for the 5.725–5.875 GHz spectrum is less intuitive due to differences in regulations between countries. 802.11 specifies a spectral mask that defines the permitted power distribution across each channel, requiring signal attenuation by at least 20 dB beyond ±11 MHz from the center frequency. This results in channels being effectively 22 MHz wide. Channel availability is regulated by country and depends on how each country allocates radio spectrum to various services. For example, Japan allows all 14 channels for 802.11b, while Spain initially only allowed channels 10 and 11. However, Europe now permits channels 1 through 13. In North America and some Central and South American countries, only channels 1-11 are available. The spectral mask defines power output restrictions but does not accurately reflect the channel's energy range. Transmitters can impact receivers on non-overlapping channels if they are close or operating above allowed power levels. However, a sufficiently distant transmitter on an overlapping channel can have little effect. Channel separation requirements between transmitting devices often lead to confusion, with some believing four non-overlapping channels exist under 802.11g when in fact only three were available. The IEEE Std 802.11 (2012) specifies that in multiple cell network topologies, channels with overlapping or adjacent frequencies can coexist without interference as long as the distance between their center frequencies is at least 25 MHz. This does not mean that using non-overlapping channels is always recommended. However, the technical overlap of channels can still cause significant inter-channel interference, especially when users transmit near the boundaries of access points (APs). In certain regions, such as Europe, overlapping channels are permitted, but in others, like North America, they may lead to unacceptable degradation of signal quality and throughput. The 802.11 standard uses a regulatory region, or regdomain, to define allowed transmitter power levels, channel occupation times, and available channels for different countries. Each country has its own set of domain codes, which are specified in the IEEE standard. Most Wi-Fi devices default to regdomain 0, which means they will not transmit at powers above allowable limits or use frequencies outside their designated region. Regdomain settings can be challenging to change, as it is often made difficult for end-users to adjust without conflicting with local regulatory agencies, such as the Federal Communications Commission in the United States. In an IEEE 802.11 network, frame types and their uses depend on specific values set for ToDS and FromDS bits. For communication within a basic service set (BSS) or independent BSS (IBSS), these bits are set to zero and one respectively. Frames sent by a station and directed towards an access point via the distribution system have ToDS = 0 and FromDS = 1. Exiting frames from the distribution system for a station have ToDS = 1 and FromDS = 0, while frames using all four MAC addresses in a data frame have these bits set to one. When packets are divided into multiple frames for transmission, the More Fragments bit is set, except for the last frame of a packet. The Retry bit aids in eliminating duplicate frames by being set when a frame is resent. Power Management indicates the sender's power state after frame exchange completion, while Access points manage connections without setting the power-saver bit. The More Data bit facilitates buffering received frames in a distributed system, addressing all connected stations. Frames encrypted by mechanisms like WEP or WPA have the Protected Frame bit set to one. The Order bit is only used when employing "strict ordering" delivery method. Reserved for Duration ID field, it indicates transmission duration and can take three forms: Duration, Contention-Free Period (CFP), and Association ID (AID). An 802.11 frame contains up to four address fields, with Address 1 being the receiver, Address 2 the transmitter, and Address 3 used for filtering purposes by the receiver. The body field in a standard 802.11 frame can vary greatly in size, spanning anywhere from 0 to 2304 bytes plus any additional overhead from security encapsulation. This field contains information that has been passed down from higher layers. At the end of the standard 802.11 frame lies the Frame Check Sequence (FCS), often mistakenly referred to as the Cyclic Redundancy Check (CRC). Its primary function is to enable integrity checks on retrieved frames by allowing stations to verify the accuracy of received data. When a station prepares to send a frame, it calculates the FCS and appends it. Upon receiving a frame, a station can recalculate the FCS and compare it to the one sent; if they match, it's assumed that the transmission remained intact. Management frames, however, are not always authenticated, granting the flexibility for either maintaining or discontinuing communication. Common subtypes of 802.11 include: Authentication frame: The process begins with the wireless network interface controller sending an authentication frame to the access point containing its identity. When using open system authentication, only one frame is sent by the WNIC, and the access point responds with acceptance or rejection. With shared key authentication, the WNIC sends a request followed by the encrypted challenge text; if successful, the access point confirms authenticity. Association request frame: Sent by a station, it enables the access point to allocate resources and synchronize. This frame includes information about the WNIC, such as supported data rates and the network's SSID. Upon acceptance, the access point reserves memory and assigns an association ID. Association response frame: The access point sends this in response to an association request, containing either acceptance or rejection along with details like association IDs and data rates. Beacon frame: Periodically sent by the access point to announce its presence and provide network parameters. Deauthentication frame: Sent by a station wishing to terminate connection from another. Disassociation frame: Similar to deauthentication but elegantly allowing the access point to relinquish memory allocation and remove the WNIC from the association table. Probe request frame: A station sends this when requiring information from another. Probe response frame: The access point responds with capability information, supported data rates, etc., following a probe request. Reassociation request frame: Sent by a WNIC that has moved out of range and seeks to reconnect to another access point. Access point with better signal strength is coordinated to forward remaining buffer information from previous access point. Reassociation response frame: Sent by an access point containing acceptance or rejection of WNIC reassociation request frame. Frame includes required data for association like association ID and supported data rates. Action frame: management frame to control a certain action, such as QoS, Block Ack, Public, Radio Measurement, Fast BSS Transition, Mesh Peering Management, etc. These frames are sent by station when it needs to inform its peer about an action. For example, station can ask another station to set up block acknowledgement by sending ADDBA Request action frame. Other station would respond with ADDBA Response action frame. Body of management frame consists of fixed fields followed by sequence of information elements (IEs). Common structure of IE is: Field Type Length Data Length Control frames facilitate data exchange between stations. Some common 802.11 control frames include: Acknowledgement (ACK) frame: after receiving data frame, receiving station sends ACK frame to sending station if no errors found. If sending station does not receive ACK frame within predetermined time period, sending station resends frame. Request to Send (RTS) frame: RTS and CTS frames provide optional collision reduction scheme for access points with hidden stations. Station sends RTS frame as first step in two-way handshake required before sending data frames. Clear to Send (CTS) frame: station responds to RTS frame with CTS frame, providing clearance for requesting station to send data frame. CTS provides collision control management by including time value for which all other stations hold off transmission while requesting station transmits. Data frames carry packets from web pages, files, etc. within body. Body begins with IEEE 802.2 header, followed by Destination Service Access Point (DSAP) specifying protocol, and Subnetwork Access Protocol (SNAP) header if DSAP is hex AA. SNAP header includes organizationally unique identifier (OUI) and protocol ID (PID) fields specifying protocol. If OUI is all zeroes, protocol ID field is EtherType value. Most 802.11 data frames use 802.2 and SNAP headers, most using OUI of 00:00:00 and EtherType value. The link layer in wireless networks should be able to recover lost frames with a success rate of at least 80%, with 30% being an average common outcome.[103] It is essential for senders to receive Acknowledgement (ACK) frames, and if not received, the frames are resent. Various amendments have been made to the original IEEE 802.11 standard, including IEEE 802.11a, b, d, e, g, h, i, j, k, n, p, r, s, u, v, w, y, and z. These amendments introduced new features such as higher speeds, improved security, and support for devices operating in specific frequency ranges. The IEEE 802.11 standard has undergone several revisions, with the latest release being IEEE 802.11-2016, which includes amendments aa, ac, ad, ae, and af. IEEE 802.11 Standards Development: A Timeline and Overview The IEEE 802.11 standard has undergone significant updates since its inception, with new releases and amendments introduced at regular intervals. This overview provides a brief summary of the key milestones in the development of the IEEE 802.11 standard. Recent Developments: Key releases in recent years include: - IEEE 802.11aj: China Millimeter Wave (December 2016) - IEEE 802.11ak: Transit Links within Bridged Networks (February 2018) - IEEE 802.11aq: Pre-association Discovery (July 2018) - IEEE 802.11-2020: A new release of the standard that includes amendments ah, ai, aj, ak, and aq (December 2020) Future Directions: The latest release, IEEE 802.11ax, introduces High Efficiency WLAN at 2.4, 5 and 6 GHz, with OFDMA to Wi-Fi, enhancing wireless local-area networking operation. Additionally, upcoming releases include: - IEEE 802.11ay: Enhancements for Ultra High Throughput in and around the 60 GHz Band (March 2021) - IEEE 802.11az: Next Generation Positioning (March 2023) - IEEE 802.11bb: Light Communications (November 2023) - IEEE 802.11bc: Enhanced Broadcast Service (February 2024) - IEEE 802.11bd: Enhancements for Next Generation V2X - IEEE 802.11be: Extremely High Throughput (May 2024) Standardization Process: The IEEE Standards Association oversees the development of the standard, with new releases and amendments introduced through a task group process. The task group is responsible for creating amendments, which are then approved by the IEEE Standards Association. The standard is updated periodically, with new versions published in 1999, 2007, 2012, 2016, and 2020. Terminology: Various terms are used to specify aspects of wireless local-area networking operation, including time units (TU) and portals. The history of Wi-Fi security is marked by significant vulnerabilities and upgrades. In 2001, researchers from the University of California, Berkeley highlighted weaknesses in WEP, a crucial component of the original standard. This was followed by an attack verification led by Adam Stubblefield and AT&T, which allowed for unauthorized access to wireless networks. To address these issues, the IEEE established a task group to develop a replacement security solution, leading to the creation of 802.11i (WPA2). WPA2 utilizes AES encryption instead of RC4 and has since become the recommended standard for both home and enterprise settings. Additionally, in January 2005, a new task group "w" was formed to protect management and broadcast frames, with its standard being published in 2009. However, security concerns persist, including vulnerabilities in certain WPS implementations and potential risks from Wi-Fi deauthentication attacks. Modern operating systems like iOS 8 and Android 8.0 have implemented features such as MAC randomization to enhance user privacy and security. The Wi-Fi Alliance has established an official naming convention for wireless networking standards, with each generation designated by a letter and number (e.g., Wi-Fi 6E). The most recent standard, Wi-Fi 7, is currently being certified, while Wi-Fi 6E operates in the 6 GHz band. In comparison to previous generations, Wi-Fi 6E offers improved features and capabilities, such as increased speed and capacity. The Wi-Fi Alliance has also established a numbering system for wireless networking standards, with each generation building upon the previous one. For example, Wi-Fi 4 (802.11n) operates in the 2.4 GHz band, while Wi-Fi 5 (802.11ac) operates in the 5 GHz band. In terms of performance, Wi-Fi 6E has shown significant improvements over its predecessors, with speeds reaching up to 144.4 Mbit/s (MCS Index 15, 2 spatial streams, 20 MHz). In contrast, earlier generations, such as Wi-Fi 4 (802.11n) and Wi-Fi 5 (802.11ac), have slower speeds. The Wi-Fi Alliance has also established a set of standards for wireless networking performance, including throughput-per-area, which measures the ratio of total network throughput to the network area. According to some studies, the growth in wireless networking technology has been significant, with some estimates suggesting that Wi-Fi 6E is expected to see a 1100% improvement over earlier generations. Overall, the Wi-Fi Alliance's naming convention and standards have helped establish a clear framework for wireless networking technologies, allowing users to understand the differences between various generations and make informed decisions about their network choices. The development of Wi-Fi standards has a rich history, with various milestones and contributors shaping its evolution. Vic Hayes and Bruce Tuch were inducted into the Wi-Fi NOW Hall of Fame on November 8, 2019. The Wi-Fi Alliance's "History" page provides insight into the technology's background. In 1999, Apple introduced the iBook, a laptop designed for wireless connectivity. Steve Lohr from The New York Times covered this innovation in an article titled "Apple Offers iMac's Laptop Offspring, the iBook." Peter H. Lewis also wrote about Wi-Fi's potential in another article published in The New York Times on November 25, 1999. Claus Hetting, a prominent figure in the industry, shares his experiences with Steve Jobs in an interview published by Wi-Fi Now on August 19, 2018. This meeting is credited with sparking the creation of Wi-Fi. The IEEE 802.11 working group has been instrumental in developing and refining wireless LAN standards over the years. The organization's project timelines provide a detailed understanding of their efforts. Wi-Fi CERTIFIED n was introduced by the Wi-Fi Alliance in September 2009, promising longer-range and faster-throughput networks. Researchers Sourangsu Banerji and Rahul Singha Chowdhury also published an article on IEEE 802.11 wireless LAN technology, highlighting its significance. The development of Wi-Fi standards has continued with advancements like IEEE 802.11p and the introduction of new frequency bands such as 60 GHz and sub-1 GHz frequencies. The Physical Layer of the IEEE 802.11p WAVE Communication Standard: The Specifications and Challenges provides an in-depth look at these innovations. The growth of Wi-Fi standards is evident with the introduction of newer technologies like 802.11ac, 802.11n, and 802.11ad. These advancements have improved range and performance, catering to different market needs. The IEEE 802.11aj standard was introduced in April 2018, enabling broadband wireless access via millimeter-wave frequencies. The development of Wi-Fi technology has been a continuous effort, with various experts contributing their knowledge and expertise over the years. The IEEE 802.11 standard has undergone various revisions since its inception in the early 2000s. Initially, it was introduced in 1997 with a focus on providing wireless local area network (WLAN) connectivity. Over time, subsequent amendments were made to enhance throughput and improve user experience. One notable revision is the introduction of Wi-Fi 6, which replaced the earlier nomenclature of 802.11n as "Wi-Fi 4" in an effort to simplify wireless networking names. This change aimed to make Wi-Fi easier to understand and recognize for end-users. Another significant development was the introduction of 802.11ad, also known as WiGig, which enables multi-gigabit performance in Wi-Fi devices. The first 802.11ad router was unveiled by TP-Link in 2016, marking a milestone in the evolution of wireless networking technology. The IEEE 802.11 standard continues to evolve with new amendments and revisions being introduced periodically. For instance, the introduction of Wave 2 products in 2016 brought significant improvements in throughput and user experience. Despite these advancements, challenges persist in wireless networking, including adjacent channel interference, which can harm network performance. Researchers have developed models to quantify this effect, highlighting the need for continued research and development in the field. Overall, the IEEE 802.11 standard has come a long way since its inception, with ongoing efforts to improve throughput, user experience, and network reliability. As wireless networking technology continues to evolve, it is essential to address emerging challenges and develop innovative solutions to meet growing demands. Retrieved 29 December 2013. Archived from the original on 7 April 2016. Retrieved 20 April 2016. ^ a b c d e f g 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 29 December 2013. ^ Lim, Dongguk (23 May 2013). "TVWS Regulation and Standardization (IEEE 802.11af)" (PDF). Retrieved 29 December 2013. ^ "802.11-2016". Wireless Training & Solutions. 12 August 2017. Retrieved 5 January 2019. ^ "IEEE 802.11-2016". Archived from the original on 8 March 2017. Retrieved 25 March 2017. ^ IEEE Standard for Information technology--Telecommunications and information exchange between systems - Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Sub 1 GHZ License Exempt Operation. doi:10.1109/IEEESTD.2017.7920364. ISBN 978-1-5044-3911-4. ^ Churchill, Sam (30 August 2013). "802.11ah: WiFi Standard for 900MHz". DailyWireless. Retrieved 11 February 2014. ^ "There's a new type of Wi-Fi, and it's designed to connect your smart home". The Verge. 4 January 2016. Retrieved 4 January 2015. ^ a b c "IEEE 802.11, The Working Group Setting the Standards for Wireless LANs". Retrieved 29 June 2017. ^ Mitchell, Bradley (16 November 2021). "802.11 Standards Explained: 802.11ax, 802.11ac, 802.11b/g/n, 802.11a". Livewire. Retrieved 16 April 2023. ^ "IEEE 802.11 Working Group Project Timelines". IEEE. Retrieved 4 April 2021. ^ "IEEE 802.11-2020 - IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". IEEE Standards. Retrieved 4 April 2021. ^ "Generational Wi-Fi User Guide" (PDF). www.wi-fi.org. October 2018. Retrieved 22 March 2021. ^ "Wi-Fi 6E expands Wi-Fi into 6 GHz" (PDF). www.wi-fi.org. January 2021. Retrieved 22 March 2021. IEEE Approves New Wi-Fi Standard for Ultra-High Throughput The evolution of WiFi technology has been influenced by various standards, including IEEE 802.11. A key aspect is the Medium Access Control (MAC) and Physical Layer (PHY) specifications. According to a PDF document archived from June 26, 2013, these specifications were retrieved on December 5, 2013. Research into adjacent-channel interference in IEEE 802.11 WLANs was conducted by Garcia Villegas et al. in 2007. Their study highlighted the impact of this interference on network performance. A Cisco Systems article from February 7, 2007, discussed channel deployment issues for 2.4 GHz 802.11 WLANs. The IEEE Standard 802.11-2007 was published and referenced on page 531. It outlined the specifications for WiFi networks at that time. Another source, a Cisco community guide from October 25, 2010, provided an overview of 802.11 frames. Studies have also been conducted on the reliability of WiFi networks. In 2015, Murray et al. published their findings on measuring the reliability of 802.11 WiFi networks. They presented their research at the Internet Technologies and Applications conference. The future of WiFi technology was discussed in various articles. Fleishman's article from December 7, 2009, highlighted the potential for gigabit speeds. Research into MU-MIMO MAC protocols for wireless local area networks was published by Liao et al. in 2014. The IEEE 802.11 Working Group has been responsible for setting standards for WiFi technology. Their efforts have led to numerous updates and enhancements, including an amendment to enhance high-efficiency WLANs. Security flaws in 802.11 data link protocols were identified in various studies. Walker's report from May 2009 discussed the status of project IEEE 802.11 Task Group w: Protected Management Frames. References to security vulnerabilities in WiFi technology include a PDF document detailing brute forcing Wi-Fi Protected Setup and a US CERT Vulnerability Note. IEEE 802.11 wireless networking standard for WiGig (60 GHz) networks, not to be confused with IEEE 802.1ad. This amendment provides a Multiple Gigabit Wireless System (MGWS) standard in the 60 GHz band and is a networking standard for WiGig networks. The range of communication would be limited, but its great bandwidth enables transmission at high data rates up to multiple gigabits per second, making it suitable for scenarios like transmitting uncompressed UHD video over wireless networks. IEEE 802.11ad networks operate in the 57-71 GHz frequency band, with each channel occupying 2.16 GHz of space and providing 1.76 GHz of bandwidth. However, not all frequencies are available for use globally, as some countries have reserved them for other purposes or require licenses. Here is a breakdown of the unlicensed spectrums available in different regions: * USA: 57-71 GHz (6 channels) * Canada: 57-64 GHz (3 channels), with an expected expansion to 64-71 GHz by 2021 * South Korea, EU, Russia, Japan, Australia, and Singapore: 57-66 GHz (4 channels), with the possibility of expanding to 66-71 GHz in the future. * China: 59-64 GHz (2 channels) These frequencies are used for high-speed wireless communication, with data transfer rates of up to several gigabits per second. The technology is also being developed for use in other applications, such as wireless local area networks and multimedia access networks. Given text appears to be a Wikipedia article discussing IEEE 802.11ad and 10BASE5 Ethernet technology. The text provides information on the standardization of 10BASE5 in 1982 as IEEE 802.3, its characteristics such as using thick coaxial cable up to 500 meters in length, and supporting up to 100 stations connected via vampire taps sharing a single collision domain with 10 Mbit/s bandwidth. It also mentions that 10BASE5 was superseded by cheaper alternatives like 10BASE2 and eventually 10BASE-T and its successors. The text further describes the physical characteristics of 10BASE5, including transmission speed, baseband signaling, maximum segment length, and the use of cable similar to RG-8/U coaxial cable with extra braided shielding. It concludes by stating that IEEE deprecated 10BASE5 for new installations in 2003. Coaxial Ethernet Cable Installation Guidelines A coaxial cable is used to create a high-speed bus for communication. To successfully install it, pierce the outer three layers while making contact with the inner conductor and ensure other spikes bite into the outer braided shield. It's essential to maintain a safe distance between the shield and spike during installation. For precise installations, transceivers should be placed at 2.5-meter intervals. The cable is marked with black bands at suitable points. To avoid signal reflections and network disruptions, one continuous run of cable must be maintained, and T-connections are strictly forbidden. Each end of the coaxial-cable-based Ethernet requires a 50 ohm resistor attached, typically built into a male N connector. Proper termination at each end is crucial to ensure data transmission without interference or collisions. However, adding new stations can be challenging due to the need for accurate cable piercing and potential breakage, which may cause signal reflections. The erstwhile dominant 10 Mbit/s Ethernet standard, known as 10BASE2 or "cheapernet," utilized thin coaxial cable with BNC connectors to establish local area networks in the late 1980s. Initially, it reigned supreme amidst competition from twisted pair networks. However, in 1988, Ethernet over twisted pair was introduced at the same speed, and subsequently, Fast Ethernet, which upgraded the speed to 100 Mbit/s in 1995, rendered thinnet obsolete. The obsolescence of 10BASE2 can be attributed to the increased demand for high-speed networking, coupled with the plummeting prices of Category 5 cable and the widespread adoption of 802.11 wireless networks. As a result, this standard has largely been supplanted by more modern technologies, with the IEEE deprecating it for new installations as of 2011. The name "10BASE2" is derived from its key characteristics: 10 Mbit/s transmission speed, baseband signaling (indicated by the "BASE"), and a maximum segment length approaching 200 meters. The physical medium utilizes Manchester coding to double the signal bandwidth, allowing for clock recovery but increasing the signal's susceptibility to interference. Connected directly to the T-connector on a workstation is crucial[b]. If termination is missing or there's a break in the cable, the AC signal will be reflected instead of dissipated when it reaches the end, mimicking a collision and preventing communication. Some terminators have metallic chains for grounding purposes; however, the cable should only be grounded at one end to avoid ground loops that can cause network outages or data corruption. Wiring 10BASE2 networks requires special care as bad contacts or shorts are difficult to diagnose and a failure at any point in the cabling tends to prevent all communications. This makes maintenance challenging and often led to replacement with 10BASE-T networks, which also provided an upgrade path to 100BASE-TX. Unlike 10BASE-T, 10BASE2 networks cannot be extended without temporarily disrupting service for existing users, making them vulnerable to accidental or malicious disruption. While proprietary systems like SaferTap claimed to address these issues, they never gained widespread adoption due to a lack of standardization. In contrast, 10BASE-T can be extended by connecting to a hub, where a fault in one connection does not compromise other connections. 10BASE2 !!!!!! The article discusses upcoming events and developments related to IEEE standards for wireless communication. Meetings from now until the next session will be held via teleconference. There are currently three working group ballots open: P802.11bi/D1.0, which opened January 27 and closes February 27; CC50, a comment collection on P802.11bn/D0.1, open from February 7 to February 28; and the first recirculation SA ballot for P802.11bk on D4.0, running from January 23 to February 7. Members Jerome Henry, Brian Hart, Binita Gupta, and Malcolm Smith have published a comprehensive guide to IEEE Std 802.11be-2024 (Wi-Fi 7). The IEEE SASB has approved the revision of IEEE Std 802.11-2024, which includes all previously published amendments with numerous fixes and enhancements. This revised standard is expected to be available in early 2025 after publication editing. The IEEE has announced several updates and publications in its 802.11 standards series. The first meeting of a new task group will take place as a teleconference in February, with Edward Au confirmed as chair. Several working groups, including those focused on Ambient Power Communications, ARC, Coex, AI/ML, and AUTO, have made progress toward an initial draft with consensus on various topics. The IEEE has also approved several standards, including 802.11be-2024, 802.11bh-2024, and 802.11-2024, all of which are expected to be published soon. Additionally, the organization has released several previous standards, such as 802.11bc-2023, 802.11bb-2023, and 802.11bd-2022. The IEEE has expressed gratitude to Hiroshi Mano for his efforts in facilitating the meeting at a wonderful location. The organization also congratulates the many members who participated in the development of these standards. The schedule for 802.11 conferences is kept track of on this embedded calendar. Users can either download the calendar as an iCal file or make use of the "Add to Google Calendar" feature located at the bottom right corner of the displayed calendar. Additionally, a comprehensive 802 calendar that includes all meeting dates and combines working group schedules is accessible here.

Standard ieee 802.11 b. What is the frequency range of the ieee 802.11 a standard. Wifi standard ieee 802.11. What is the frequency range of the ieee 802.11 g standard. Standard ieee 802.11 n. Standard ieee 802.11 ac. Standard ieee 802.11 p. Wlan standard ieee 802.11. Wireless standard ieee 802.11. Wlan standard ieee 802.11 pdf. Ieee 802.11 refers to what standard. Standard ieee 802.11 b g n. Wireless lan standard ieee 802.11 ax. Wireless lan standard ieee 802.11 ac. Standard ieee 802.11 ax.