# WIFI – IEEE 802.11 a/b/g/n/ac/ax

Nu ska vi ta en djupdykning i de olika standarder som finns kring WiFi, men för att kunna göra det på ett någorlunda metodiskt sätt ska vi börja med att titta på vilka det är som skrivit standarderna: Standardnamnen för alla trådlösa nätverkstekniker heter något med IEEE 802.11. Men vad säger oss egentligen det standardnamnet?

IEEE – Institute of Electrical and Electronics Engineers är en i sammanhanget mycket gammal standardiseringsorganisation (***IEEE har sin hemvist i USA och är en icke-vinstorienterad organisation, bildad 1963 genom sammanslagning av två tidigare elektrotekniska organisationer: AIEE (American Institute of Electrical Engineers***) ***med rötter från 1884, och det några decennier yngre IRE (Institute of Radio Engineers, 1912 - 1963). som finns i USA. De är fokuserade på standarder kring t.ex. elsäkerhet, telefon- och datanät etc.***

IEEE 802 är IEEE:s grupp som jobbar med att ta fram standarder för LAN (Local Area Networks) och MAN (Metropolitan Area Networks). De vanligaste standarderna under 802 är ethernet (802.3) och WLAN (802.11).

## IEEE 802.11 Trådlöst LAN (WLAN)

Ej att förväxla med VLAN.

Trådlöst LAN eller WLAN (av engelskans Wireless Local Area Network) är ett samlingsnamn för olika typer av trådlösa lokala datornätverk. För att förhindra sammanblandning med VLAN bör termen ”Trådlöst LAN” användas, eller det mer specifika Wi-Fi.

Den vanligaste typen är IEEE 802.11a/b/g/n/ac/ax-familjen som bland annat kan användas för att koppla ihop en central accesspunkt (AP) med klienter i form av datorer, IP-telefoner, handdatorer, smarta mobiltelefoner, mediaspelare och annan utrustning i kontors- eller hemmiljö.

Trådlösa LAN använder sig av teknologi baserad på radio eller mikrovågor (vid radio-LAN), och förr även infraröda vågor, för att kommunicera med andra enheter inom en begränsad radie. På senare år har LED-teknik (Light Emitting Diods) gjort att man också försökt med optiska signaler från dessa (alltså mänskligt noterbart ljus). Denna teknik har emellertid aldrig riktigt ”slagit” pga det problem för arbetsmiljön som ”flimrigt ljus” kan orsaka – och att bygga in tekniken – t.ex. bakom takplattor på ett kontorsnät är mångdubbelt dyrare än själva accesstekniken.

Radio-LAN ger användaren möjligheten att röra sig fritt inom detta område och fortfarande vara ansluten till nätverket. Radio-LAN har på senare tid blivit mer och mer populär bland annat på grund av den låga investeringskostnaden jämfört med trådbundet LAN, IR-teknik eller olika ljus-tekniker.

De standarder som idag används för radio-LAN ger tillgång på upp till 300 Mbit/s i delad överföringshastighet (beroende på router och mottagare), det vill säga hastigheten delas av samtliga klienter i nätverket.

### Historik

Norman Abramson - en professor vid University of Hawaii utvecklade världens första trådlösa nätverk för datakommunikation, ALOHAnet, med hjälp av billiga radioapparater. Systemet gick ut på att sju datorer placerades ut på fyra öar för att kommunicera med den centrala datorn på Oahu utan att använda telefonlinjer. Just ALOHAnet brukar användas som exempel på ett trådlöst MAN. IEEE 802.11 började alltså sitt arbete med trådlösa MAN, för att sedan – alltmer – inrikta sig mot trådlösa LAN,

### Olika typer av trådlöst LAN (Alternativ till WiFi)

HomeRF - Data över DECT (Digital Enhanced Cordless Telecommunication - ”Sladdlösa telefoner”)

**Bonuslänk:** What is DECT? <https://youtu.be/Qqawd9zk20Y>

HiperLAN - Europeisk IEEE 802.11-konkurrent.

**Bonuslänk:** What is HiPeRLAN? (HiPerformanceRadioLAN)? <https://youtu.be/L9nqBZrhtYo>

OpenAIR

## WiFi – historik:

I början av 1990-talet uppfanns en mängd saker, som skulle kunna komma att bli använda i WiFi-sammanhang av olika rymdforskare i Australien. Bl.a. ett chip som kan översätta optiska spektrum till radiosignaler (och vice versa). Till en början tänktes chipet användas för att underlätta bildanalys av bilder från ett radioteleskop, men då det visade sig vara för överarbetat för det ändamålet vid det tillfället kom det inte till användning i den applikationen vid det tillfället.

Tekniken som chipet använder och som sedan kommit att användas i wifi kommer av att andra australiska forskare kom på att principen för frekvensmodulering skulle kunna användas i radiobaserade nätverk – framförallt mellan laptops, som på den här tiden började bli allt vanligare. Idén var att om man hade en sladdlös – batteridriven – dator att kunna bära med sig överallt – varför skulle man behöva koppla in den med en sladd i nätverket?

Idén om trådlös kommunikation – inom LAN – var född. Trådlös kommunikation hade tidigare framförallt använts i WAN (Wide Area Network) och i MAN-sammanhang och någon riktigt bra teknik för att koppla upp datorer i lokala nätverk fanns inte.

Då man började utveckla WLAN-teknik hade vanliga, kabelbundna, traditionellt byggda LAN bandbredder på normalt 10 Mbps och den siffran fick stå som ”mål” för när man utvecklade WLAN-standarderna. Man ville ha samma nätprestanda ”bärbart” som man skulle ha ”i kabeln”.

Sättet att nå dit var just genom tekniken med frekvensmodulering där frekvensen kan omkodas i ”spektrum” och inom dessa signallera på ”flera kanaler samtidigt” när signalen återtolkades. Det gjorde att den första standarden för WLAN var en standard om 11Mbps som gick på 5GHz-nätet. Våglängden visade sig emellertid vara för kort – varför räckvidden blev något för kort för att kunna användas praktiskt. Den första komersiellt användbara standarden blev därför en standard med 2.4GHz-frekvensband, men med lägre räckvidd.

Medialänk: “The history of Wifi” <https://youtu.be/esA9YhdgvIg>

## Frekvensbanden och dess fördelar och nackdelar:

2.4 GHz har längre räckvidd, då mikrovågorna/radiovågornas våglängd helt enkelt är längre. De ”studsar” så att säga längre ut från antennen och du får längre räckvidd – och en signal som i många fall är mer ”stabil” än högre frekvenser, då det kommer till enklare hinder som tunna väggar och andra saker som kan ”stå i vägen” mellan sändare och mottagare.

Men – på 1990-talet fanns många saker som strålade ut andra signaler – just i 2.4 GHz-spektrumet – då detta var oreglerat i lag att använda. Tillverkare gjorde trådlösa ringklockor, ”baby monitors”, övervakningskameror och tillochmed lät microvågsugnar ha en rundstrålning som var godkänd just kring 2.4 GHz. Risken för ”interferrans” – alltså störande signaler – är betydligt större i 2.4 GHz-spektrumet.

5 GHz-frekvenserna har betydligt kortare räckvidd (med sändare av samma effekt) – men tillåter då man har fler ”signallerbara svängningar” givetvis högre bandbredd. Risken för Interferrans är också betydligt lägre – eftersom få andra saker i vardagen använder samma frekvensband att sinallera på.

Men – signalen blir ”svagare” och då våglängden är kortare kommer den ”lättare att studsa” mot objekt som står i vägen (som väggar) än en signal med längre våglängd. Det gör att man nästan måste ha ”optisk sikt” mellan sändare och mottagare, och att avståndet är (mycket) kort – ibland så kort som bara några meter.

## ”Dual band”

Ibland pratas det om att trådlös nätverksutrustning har stöd för ”dual band” – att kunna användas på både 2.4 GHz och på 5GHz – något som egentligen är en sanning med viss modifikation. Många standarder för WiFi är skrivna för att hanteras \_antingen\_ på 2.4 GHz-bandet \_eller\_ på 5 GHz. Däremot kan utrustningen: ”basstationen”, ”accesspunkten”, ”routern” eller vad det nu är kunna använda flera WiFi-standarder. Ibland kan denna vara bestyckad både med fler antenner och/eller fler processorer – där en antenn och/eller processor på kortet kan köra en standard för WiFi var.

Medialänk: Dual band. 2.4 GHz and 5 GHz: <https://youtu.be/J_bf_KE5llQ>

## Standarder är bra – det är därför det finns så manga!

En full lista av använda WiFi-standarder skulle kunna se ut såhär: 802.11a, 802.11b, 802.11g, 802.11n (Wi-Fi 4), 802.11h, 802.11i, 802.11-2007, 802.11-2012, 802.11ac (Wi-Fi 5), 802.11ad, 802.11af, 802.11-2016, 802.11ah, 802.11ai, 802.11aj, 802.11aq, 802.11ax (Wi-Fi 6), 802.11ay (Wi-Fi6-E)

Det ger att det är väldigt många sorters WiFi-standarder att hålla reda på. Flera av standarderna har dessutom flera olika namn för samma standard! För att förenkla har man försökt att flera gånger namnge standarderna med mer lättbegripliga namn än ”IEEE 802.11[bokstäver]” och 2018 började man att titta på att ”klumpa ihop standarder” av ungefär samma tidsålder för att se vilken ”generation” av WiFi standarden beskriver. 802.11a och 802.11b kan – faktiskt bägge - sägas tillhöra ”generation 1 och 2”. Stardarnerna 802.11g blir ”generation 3” och 802.11n räknas som ”generation 4” tillsammans med en massa andra standarder som utvecklas fram t.o.m 2012. 802.11ac kommer i den vevan, och med så pass mycket ny funktionalitet att de standarder som kommer sedan samtliga brukar kallas ”generation 5”. 802.11ax (Som kom 2018/2019) och efterföljande standarder brukar kallas ”generation 6” och för något år sedan kom utbyggnad för de standarderna i 802.11ay. De utbyggnaderna i funktionaliteten brukar emellertid inte sägas rättfärdiga ett nytt generationsnummer utan man brukar kalla nya standarder efter 802.11ax för ”Generation 6 – Extended” eller ”WiFi6E”.

Före generation 4 fanns egentligen ingen bakåtkompabilitet. Generation 1 och 2- nät använde helt olika teknik (frekvensspann, moduleringsteknik, bandbredd etc.). Generation 3-nät var bakåtkompatibla med 802.11b men inte med 802.11a etc.) Det är egentligen inte förrän vi får den fjärde generationens nät som man har tekniken med ”dual band” och kan vara bakåtkompatibla till alla standarder.

Krångligt? Ja – det är det.

Men enkelt kan sägas att 802.11b – den ursprungliga WiFi-standarden är ”WiFi1” och att vi nu i praktiken kör femte och sjätte generationens WiFi – WiFi5 och WiFi6.

Den första generationens WiFi-nät hade en bandbredd på bara 2 Mbps – medan den sjätte generationens WiFi har teoretiskt en bandbredd på upp till 6 Gbps – alltså (teoretiskt) tretusen gånger fler!

Medialänk – kolla in Explained: WiFi 802.11 a/b/g/n/ac <https://youtu.be/txueGsf92Ts>

Och för att jämföra IEEE 802.11ac och 802.11ax (WiFi6 vs WiFi6E) <https://youtu.be/hG6UrVhEJkM>

## Säkerhetsproblem - ”Snyltning”

Ett okrypterat nätverk kan i allmänhet användas eller avlyssnas av vem som helst inom hörbarhetsområdet. Accesspunkten har oftast ingen möjlighet att skilja mellan legitima och icke-legitima användare på sådana nät eller nät utan lösenord eller kryptografisk nyckel. Att använda sådana nät (eller nät med otillräcklig kryptering) utan tillstånd kallas snyltning. Vanligen används NAT på privatpersoners intranät, och snyltares nätverkstrafik kommer då utåt att se ut att komma från samma dator som de legitima användarnas trafik.

Det är också vanligt att medvetet lämna sitt trådlösa nät öppet att användas av andra som tillfälligt behöver en Internet-anslutning.

## Kryptering och andra skydd

För att skydda sig mot snyltning och andra typer av intrång, tillämpas olika typer av skydd. Det vanligaste är att man krypterar nätverket. Det finns olika typer av krypteringsmetoder, de vanligaste är WEP, WPA och WPA2. WPA och WPA2 är nyare och bättre standarder, men WEP-krypteringen existerar fortfarande p.g.a. att många accesspunkter inte stöder något annat.

Det finns även andra sätt att skydda sitt trådlösa nätverk från intrång, till dessa hör MAC-adressbegränsning, MAC-filtrering och att stänga av SSID-broadcast. Dessa skydd bör bara användas som komplement till kryptering då de är mycket lätta att komma förbi och deras huvudsakliga uppgift är att stänga ute oavsiktlig användning. Snyltare kommer förbi dem ändå genom att bland annat använda spoofing. Att stänga av SSID-broadcast ger egentligen inget skydd alls eftersom SSIDet fortfarande finns i all trafik på det aktuella WLAN:et.

Vidare referenser.

<https://en.wikipedia.org/wiki/Wi-Fi>

Bonuslänkar:

Wifi - Evolution and trends 2021 <https://www.youtube.com/watch?v=e4URFC70g3A>