

TRÅDLØSE NETTVERK - WLAN

Vi har i dette "faget" konsentrert oss om trådløse hjemmenettverk. Mye er felles med et bedriftsnettverk, men sikkerhetsnivået er (og bør) være mye høyere enn på et privat hjemmenettverk. Noe av det som omtales nedenfor vil også være relevant for en bedrift, men ikke alene. Det bør alltid kombineres med "kraftigere sikkerhetsløsninger". Del to av faget er en [stikkordsliste](#), som går litt dypere på en del begreper.

Hva er et trådløst nettverk?

Definisjonen på et trådløst nettverk er: *En infrastruktur som gjør det mulig å koble en eller flere enheter (datamaskiner, printere, spillekonsoller etc) sammen eller til f. eks Internet uten bruk av en fysisk tilkobling i form av en kabel.*

Et trådløst nettverk gir deg muligheten til å koble så mange datamaskiner du vil sammen til internett, og gir deg muligheten til å sitte å surfe eller jobbe i hagen, i stua eller hvor du nå måtte ønske å sitte, så lenge du er innenfor rekkevidden av nettet. Et trådløst nettverk kalles ofte et [WLAN](#).

Historisk sett kom trådløse lokalnett på banen for å løse problemet med nettverk mellom datamaskiner i områder der det var vanskelig eller umulig å kable. Verneverdige bygninger og lagersystem er to eksempler på slike bygninger. I 1990 ble den amerikanske gruppa IEEE 802.11 (Institute of Electrical and Electronic Engineers) dannet, med utspring i dataverden, og hadde som mål å lage standarder for WLAN. Den første standarden (av en lang rekke) var IEE 802.11, deretter kom [IEE 802.11a](#) og [IEE 802.11b](#) i 1999 og hadde en overføringshastighet på 11 Mbit/s. Da startet den "trådløse boomen".

Hvor stor er rekkevidden?

Det er flere faktorer som vil påvirke rekkevidden til et trådløst nettverk

- Styrken på signalene som sendes fra aksesspunktet/router
- Styrken på signalene som sendes fra det trådløse nettverkskortet
- Graden av fri sikt fra datamaskin til aksesspunkt
- Typen av hindringer i veien
- Været (dersom "strekket" går utendørs)

Signalene som sendes i trådløse datanett er radiobølger (ofte 2,4 GHz), og dermed sårbare for det samme som disse, Dette betyr i klartekst fysiske hindringer som vegger og tak. Normalt vil ikke trevegger være noen hindring for signalene, men erfaring tilsier at spesielt vått treverk begrenser rekkevidden. Massive konstruksjoner av betong og mur er imidlertid verre når det gjelder rekkevidde. Mikrobølgeovner kan også forstyrre signalene.

Utendørs vil man oppleve at regn, sludd, snøvær og tåke kan redusere signalstyrken.

En tommefingerregel er at rekkevidden utendørs er ca. 150-200 meter, mens innendørs går signalene ca. 20 meter gjennom vegger og tak.

Et ekstern antenne vil øke rekkevidden, men husk at du da som oftest må ha en slik antenne i "hver ende", altså både på basestasjonen og på datamaskinen. (Det finnes faktisk også basestasjoner som har flere antenner, så kalte mimo (multiple in - multiple out) som gjør at rekkevidden økes uten at maskinen trenger ekstra antenne). Et annet alternativ for å øke rekkevidden er å sette opp en basestasjon til, men det må da kables opp til denne. Setter man kun opp en repeater holder det at denne tilkobles strøm.

Hvordan virker et trådløst nettverk?

For at datamaskiner skal kunne kommunisere med et trådløst nettverk trengs et trådløst nettverkskort. Disse finnes både for stasjonære og bærbare maskiner, men er selvfølgelig mest aktuelle for bærbare maskiner. En del nyere bærbare maskiner har også dette innebygget. Det trådløse nettverkskortet (ofte kalt WLAN kort) er utstyrt med en antenne slik at det kan kommunisere med basestasjonen. Basestasjonen kalles ofte et aksesspunkt (kommer mer om det senere), og denne er tilkoblet det fysiske nettverket gjennom en nettverkskabel. Nettverkskabelens oppgave er å viderefordre signalene mellom det trådløse nettverkskortet og det fysiske nettet. Basestasjonen kan behandle signaler fra mange trådløse nettverkskort samtidig.

Hvorfor bruke et trådløst nettverk?

Hovedårsaken til at man benytter et trådløst nettverk er å slippe å være fysisk bundet. Ved hjelp av trådløs aksess er man fortsatt mobil (dog innenfor nettverkets rekkevidde) samtidig som man er tilkoblet nettverket. Ved bruk av flere aksesspunkter, vil det trådløse nettverkskortet i maskinen hele tiden kommunisere med den basestasjonen som har sterkest signalstyrke. Overgangen mellom disse skal være sømløs og skje automatisk.

En av fordelene ved WLAN nett er at man reduserer vedlikeholdet betraktelig. Det kan være svært kostbart å opprettholde standarden på et kablet nettverk med kabler og veggpunkter etc. Samtidig er det langt enklere å sette opp midlertidige/nye løsninger (gjester, nye medarbeidere etc). Oppsett av aksesspunkt er imidlertid ganske enkelt, så det kan de fleste få til. Dette beskrives nærmere nedenfor.

Utstyrskrav

For å få installert et trådløst nettverk trenger du et [aksesspunkt](#) eller en [ruter](#) og en eller flere datamaskiner med trådløse nettverkskort. Det kan også være hensiktsmessig å anskaffe en [svitsj](#) eller [hub](#). Her anbefaler vi en svitsj, da den er mer "intelligent" enn en hub. Et trådløst nettverk egner seg best om du har bredbånd. Ofte følger det med en ruter fra bredbåndsløseleverandøren når du bestiller bredbånd. Dersom dette er tilfelle bør du sette på et aksesspunkt med evt. en svitsj. Har du ingen ruter, må du gå til anskaffelse av en, den kobles direkte på [WAN](#)-utgangen ("bylinjesiden"). Det er også mulig å koble en ruter bak en ruter, men dette skaper ofte problemer. Hvordan du eventuelt løser disse, kommer vi tilbake til. Husk at ruterens som kommer fra bredbåndsløseleverandøren ofte kun har en utgang.

Vær oppmerksom på at det finnes kombinerte enheter, som inneholder både ruter, aksesspunkt og en svitsj (som oftest med 4 utganger for kabeltilkobling av inntil 4 pc'er). Må du kjøpe en ruter anbefales en slik kombinert løsning. En ruter har også ofte en innebygd brannvegg (firewall). De fire inngangene er ofte merket [LAN](#). I tillegg er det også en port merket [WAN](#), det er her du kobler til boksen fra bredbåndsløseleverandøren.

Dersom du tidligere har hatt en stasjonær pc direkte tilkoblet boksen fra bredbåndsselskapet med en nettverkskabel, så kobler du denne i fra, og isteden kobler WAN-porten på ruterens til boksen fra bredbåndsselskapet. Deretter kobler du en nettverkskabel mellom den stasjonære pc'en og en av LAN-portene på ruterens/svitsjen.

Oppsett av trådløst nettverk

Nedenfor kommer en skrittvis beskrivelse av hvordan du setter opp et trådløst nettverk.

- Koble til det trådløse aksesspunktet/ruterens til bredbåndslinjen (se ovenfor)
- Sjekk at PC'ene du skal tilkoble har trådløst nettverkskort. En del bærbare maskiner har dette innebygget. Har den ikke det, må det settes inn et eksternt kort.
- Noen ruterleverandører leverer med en programvare som må installeres, og som benyttes for oppsett av ruter. Men det kan også være tilfelle at du for oppgitt en [IP-adresse](#) som må skrives inn i adressefeltet på leseren din. Du kommer da direkte inn på

innstillingene i ruterer, og du kan her sette opp nettverket.

- I oppsettet legger du inn de vanligste innstillingene. Det viktigste er å gi nettverket et navn, og velge en nøkkel eller passord for kryptering og tilgangskontroll til det trådløse nettverket. Vi kommer nærmere tilbake til det senere.
- Når alt dette er lagt inn, så starter du ruterer på nytt, og nettverket skal nå være oppe.
- Skru deretter på PC, aktiver det trådløse nettverkskortet, og dette søker etter tilgjengelige nett. Når "ditt" nettverk er funnet, legger du inn navnet og passordet du lagde under ruteroppsettet. Og vips så er alt klart.

Sikkerhet

Det å sikre en trådløst nettverk er meget viktig. Det finnes flere måter å sikre nettverket på. Vi har valgt å presentere en løsning som er tilstrekkelig god for de aller fleste **hjemmenettverk, samt en løsning for de litt mer paranoide (men fortsatt hjemmenettverk/små bedrifter)** Vi sikrer da muligheten for at andre maskiner kan benytte seg av det trådløse nettverket, f.eks i boligblokker der flere leiligheter kan være dekket av en basestasjon. Disse sikkerhetsanstaltningene vil ikke beskytte mot virus eller hackerangrep. For å unngå dette må man ha antivirus og brannmur. Dette er ikke tema i dette "faget". Det er faktisk straffbart å koble seg til andres ubeskyttede nettverk, og det har en strafferamme på inntil 6 mnd. Noen av rådene for sikkerhet gjelder begge "løsninger"

Løsning 1 (for de fleste av oss til hjemmebruk):

1. Skift navn på **SSID** (navnet på hjemmenettet). Kall det f.eks "hjemme", bruk aldri navnet ditt eller adressen. Alle som søker etter tilgjengelige nett vil få opp det valgte navnet.
2. Skift standard passord på ruter
3. Sjekk ut om det er andre nettverk i nærheten (hvis ja, vurder pkt. 5 en ekstra gang)
4. Aktiver **WEP**-kryptering på 64 eller 128 bits (128 er sikrere). Dette er en kode som må tastes inn ved pålogging. Naboer kan se nettverket, men siden han ikke kjenner koden, kan han/hun ikke logge seg på. Får du besøk som du ønsker å gi tilgang til nettet, må koden oppgis. Koden kan imidlertid lett endres i etterkant.

Alternativt/tillegg til pkt. 4

4. Aktiver **MAC** filtrering. Du taster inn din unike MAC adresse inn i ruterer, og ruterer kjenner den når du logger deg på. Ingen andre enn du slipper gjennom.
5. Vurder å sette ned hastigheten slik at signalene ikke når så langt.

Løsning 2 (forsatt for hjemmebruk, men for de litt mer avanserte):

1. Skru av kringkasting av SSID

Aksesspunkter (basestasjoner) identifiserer vanligvis seg selv ved å sende ut sin SSID. Da kan for eksempel Windows XP automatisk konfigurere trådløskortet i PC'en slik at det kan koble seg til nettverket. Dersom man skrur av utsendelse av SSID blir det mye vanskeligere for uvedkommende. I et nettverk som skal være åpent tilgjengelig, for eksempel på et offentlig sted, er det nødvendig å sende SSID. (SSID blir likevel sendt når legitime brukere kobler seg til («association»)). Det finnes også spesial software som analyserer WLAN-trafikk (f.eks. «AirMagnet» eller «AiroPeek»), og med slike er det mulig å få tak i SSID. Men med stor sannsynlighet vil da uærlige prøve å finne andre nettverk.

2. Bruk statiske IP-adresser

Svært mange benytter dynamisk tildeling av IP-adresser ([DHCP](#)) når maskiner kobler seg til trådløstnett. Problemet med dette er at denne protokollen ikke skiller mellom "lovlige" og andre brukere. Med korrekt SSID kan enhver maskin få tildelt en IP-adresse og bli en legitim node i nettverket. Dersom DHCP er skrudd av og "lovlige" brukere er tildelt faste IP-adresser, blir det mye vanskeligere for inntrengere å få tak i en gyldig IP-adresse. Faste IP-adresser blir imidlertid fort u håndterlig i store nettverk, men kan være et nyttig tiltak i nett med begrenset antall brukere. (Ved hjelp av avlytting av nettverkstrafikk («sniffing») kan en inntrenger finne ut hvilke IP-adresser som er i bruk. Dermed kan han gjette hvilket adresseområde som brukes og prøve IP-adresser innenfor området.)

3. Skru på WEP eller WPA

WEP-algoritmen skal beskytte datapakker i trådløse nett mot avlytting og uønsket endring. Imidlertid har algoritmen svakheter. Det er dermed mulig å forsere krypteringen. Det finnes programvare tilgjengelig på Internet («AirSnort») som gjør slike analyser, basert på noen timers sniffing av krypterte pakker, men dette krever en god del tid, og de aller fleste inntrengere vil bli utestengt. Dersom du ikke har svært verdifulle og/eller sensitive data på nettverket er det neppe grunn til å bekymre seg for denne type angrep.

Nyere trådløst utstyr (< 2 år) støtter stort sett [WPA](#)-algoritmen, som er vesentlig vanskeligere å forsere. En utvidelse av 802.11-standarden (802.11i) som benytter AES (Advanced Encryption Algorithm) var klar i 2004. Utstyr basert på denne standarden vil i praksis være immune mot forsering av selve krypteringen.

4. Installer personlige brannmurer

Mange bærbare PC-er inneholder store mengder sensitive data. Det er viktig å ta høyde for at bærbare maskiner med trådløskort kan bli benyttet i andre trådløse nettverk enn «hjemmenettet». Maskiner må ha egen beskyttelse og må ikke være avhengig av perimetersikring o.l. Dersom for eksempel fildeling er slått på, kan enhver bruker på et trådløst nett (for eksempel på en flyplass) få tilgang til filer på den lokale disken. Vi snakker da her om en "ekstra" brannmur, i tillegg til den som ofte befinner seg i ruter. Benyttes Windows XP, har denne en innebygget brannmur i SP2 (Service Pack 2)

5. Unngå unødig spredning av radiosignaler

En basestasjon har meget begrenset rekkevidde hvis den skal aksesserer av et standard WLAN-kort som sitter i bærbare PC-er. Imidlertid er det forholdsvis enkelt å lage billige antenner som gjør det mulig å plukke opp signaler fra bestemte basestasjoner på betydelig større avstand. Tenk gjennom plassering av antenner, slik at de i minst mulig grad dekker områder utenfor eiers kontroll, slik som parkeringsplasser, andre bygninger og offentlige steder. Dette gjør det også vanskeligere for angripere å gjennomføre "jamming" av signaler eller andre typer tjenestenektingsangrep

Stråling

Vi mennesker er opptatt av om stråling vil være helseskadelig. Et WLAN nett vil naturlig nok avgir stråling. Frekvensen som brukes er 2,4 GHz. Radiobølgene som sendes ut fra basestasjonen er mikroskopiske, og det er ikke påvist noen risiko for helsefare. Til sammenlikning vil en mobiltelefon stråle opptil 100 ganger mer enn et trådløst nettverk, og mobiltelefonen holder vi jo inntil hodet flere ganger om dagen.

Hvorfor har vi ikke bare trådløse nettverk?

Årsaken er at det selvfølgelig også er noen ulemper forbundet med WLAN nett. Først og fremst er det hastigheten i et trådløst nettverk betydelig lavere enn i et fysisk nettverk. Vi kan se forskjeller på inntil 5 - 10 ganger høyere hastighet i en trådbundet nett sammenliknet med et trådløst. I tillegg er den hastigheten man i praksis opplever avhengig av bl.a. fri sikt og atmosfæriske forhold. Dersom et aksesspunkt betjener mange brukere samtidig, vil hver enkelt bruker oppleve redusert

hastighet. Muligheten for mobilitet veier ikke alltid tungt nok til at innføring av trådløst nett blir hensiktsmessig. Et fysisk nettverk er også sikrere fordi man må ha fysisk kontakt med et nettverk for å kunne bli tilkoblet.

Andre tips

Nedenfor her har vi samlet en del "temaer" som ikke faller inn under punktene ovenfor.

Skrivere

Ønskes det å ha en skriver i nettverket anbefales en nettverksskriver. Har man imidlertid kun en "vanlig" skriver, vil denne også kunne tilkobles. Det må da deles ut rettigheter via den PC'en som skriveren står tilkoblet. Denne PC'en må også alltid være påslått for at skriveren skal virke. Det finnes også rutere og trådløse enheter med printerport, og da er jo saken løst.

Ruter etter ruter

Ønskes det å ha to rutere "etter hverandre" vil ikke alltid dette fungere bra. (Årsaken til to rutere etter hverandre kan være bredbåndsleverandør leverer en ruter med kun en port, og ingen WLAN funksjonalitet. Ideelt sett vil et aksesspunkt da være det beste, men har man en ruter kan denne benyttes.) Dersom du får problemer med å få en slik løsning til å fungere, gå inn i oppsettet på ruterens (den siste) og slå av [DHCP](#) (altså ruterfunksjonen).

Hot spots

En hot spot er "offentlig" WLAN sone, hvor det koster penger å logge seg på. Enhver kan i utgangspunktet skaffe seg en hot spot, og vi finner disse som oftest på kafeer, flyplasser, bibliotek etc. Det finnes flere løsninger, men i hovedtrekk inneholder disse et trådløst aksesspunkt, med innebygget avregning av forbruk og brukerkontroll, i tillegg til en kompakt skriver. Skriveren skriver kvitteringer med brukernavn, passord og informasjon om forbruk. En del av disse "boksene" krever ingen PC, men kobles direkte på bredbåndstilkoblingen. Dermed blir brukergrensesnittet meget enkelt, og det kreves ingen spesialkompetanse for å betjene slike hot spots.

WI-FI

Wi-Fi (Wireless Fidelity) er et stempel (godkjenning) som gis trådløst utstyr av organisasjonen [Wi-Fi Alliance](#). Wi-Fi oppfattes nå mer og mer synonymt med trådløst nettverk som følger standarden IEE 802.11. Wi-Fi stemplede produkter garanterer interoperabilitet mellom de forskjellige produsenter.

Tilbake

Kilde: De fleste dataleverandørers hjemmeside, Telenor, Bredbåndsleverandører, Teknisk Ukeblad, Nettverk og Kabling.

Ord og uttrykk

DHCP

DHCP (Dynamic Host Configuration Protocol) er en måte å dele ut IP-adresser på automatisk. Som nevnt tidligere er IP-adressen det som unikt identifiserer en maskin på et nettverk, slik at trafikk kan komme riktig frem og tilbake. Det er DHCP-tjenesten som gjør at du stort sett kan plukke nettverksledningen i datamaskinen, og forvente å komme rett på nett uten å taste inn noen tall eller adresser.

Slik DHCP normalt virker er at en rekke adresser er avsatt til å dynamisk deles ut til de maskiner som til enhver tid er koblet til et nettverk. Hvis maskinen er koblet fra nettet i flere dager vil adressen som var tildelt kunne bli delt ut til andre, derfor vil det variere hvilken adresse en maskin har over tid, selv om man ikke fysisk flytter på maskinen.

En HUB kan lettest kalles en "dum" [svitsj](#). Direkte oversatt betyr ordet HUB et nav (sentrum i et hjul). En hub er den enheten som befinner seg i sentrum av et stjerneformet nettverk. I Ethernet-sammenheng er en hub - eller konsentrator - en enhet som videresender signalene mellom datamaskiner i nettet.

IP-Adresse

En IP-adresse (Internet Protocol) er adressen til en datamaskin som er tilkoblet internet. Den består av 32 sifre fordelt på fire grupper som skilles med punktum. IP-adressen gjør det mulig kommunisere med en unik datamaskin i nettet, og den oppgis i all kommunikasjon. Hver av de fire gruppene er representert med et nummer mellom 0 og 255. Disse tallene oversettes av datamaskinen til de alfabetiske navnene på nettstedene (f. eks www.elektronikkforbundet.no).

IP-adressen gjør det også mulig å returnere eller svare på all informasjon man mottar over nettet. Slik kan en server sende den etterspurte nettsiden til rett datamaskin.

Dette er eksempel på en IP-adresse: 213.236.223.61

LAN

LAN (Local Area Network) er et lokalnett for datakommunikasjon. Nettsegment for datakommunikasjon lokalt i en bedrift eller et hjem. LAN er typisk begrenset til noen tusen meter, kapasitet internt fra noen titalls Mbit/s og opp til noen Gbit/s. Det kan benyttes flere teknologier. Med et LAN kan PC'er, arbeidsstasjoner og servere jobbe sammen og dele ressurser som programvare, lagringsenheter og skrivere.

Router

En router (eller ruter på norsk) er en enhet som styrer internett trafikken ved å overføre informasjon (pakker) fra et lokalnett (LAN) til et annet ved hjelp av såkalte ruter-tabeller. Disse tabellene er tildels meget kompliserte lister over hvem som befinner seg hvor i nettet, og hvilken vei informasjonen bør overføres for å nå den rette maskinen. Ruterer holder seg informert om tilgjengelige veier gjennom nettet og om de rådene trafikkforhold for å finne den mest kostnadseffektive rute for informasjonen.

Enkelt fortalt sier vi ofte at en ruter fordeler internett-linja mellom flere datamaskiner.

~~SSID~~

SSID (Service Set Identifier) er identiteten eller navnet til et trådløst lokalnett.

~~Svitsj~~

En svitsj er en enhet som fordeler nett-trafikken til riktig(e) adressat(er) og bare til dem. En svitsj har som regel 1 inngang og flere u ganger. På utgangene kobles de respektive PC eller aksesspunkt. Mange rutere og aksesspunkt har innebygde svitsjer. Utgangene på en svitsj kalles porter, og vi omtaler de som f.eks "8-porters svitsjer". Det finnes små svitsjer for hjemmebruk med 4 eller 8 porter, mens større svitsjer (som ofte rack monteres) kan f.eks ha 24 porter.

Det finnes forskjellige typer svitsjer, f.eks. IP-svitsjer, ATM-svitsjer og Ethernet svitsjer.

~~WAN~~

WAN (Wide Area Network) er "det eksterne nettet", eller områdenettet der gjerne flere LAN er tilkoblet. Ofte omtaler vi WAN som "utenfor huset", mens LAN er på "innsiden".

~~WEP~~

WEP (Wired Equivalent Privacy) En kryptografisk algoritme for beskyttelse av konfidensialitet og integritet i WLAN. Definert i WLAN-standarden IEEE 802.11

~~Wi-Fi Alliance~~

Wi-Fi Alliance (som tidligere het WECA - Wireless Ethernet Compability Alliance) er en markedsorganisasjon som passer på at utstyr fra ulike leverandører snakker sammen. De godkjenner leverandører som kan merke produktene sine Wi-Fi.

Målet er også å gjøre teknologien lettere å forstå for andre enn ingeniører.

~~WPA~~

WPA (WLAN Protected Access) En utvidelse og forbedring av WEP-algoritmen, utviklet av Wi-Fi alliance.

~~Standardene 802.11b og 802.11g~~

IEEE802.11b er en anerkjent standard for trådløse nettverk, og den har en båndbredde på 11 Mbit/s. Til denne standarden finnes det en rekke produkter som rutere med innebygget aksesspunkt, løse aksesspunkt og en rekke klienter til å ha i pc'en (bl.a USB og PCMCIA)

802.11g er en annen standard, og denne gir hastigheter opp til 54 Mbit/s. Noen produsenter har videreutviklet denne standarden, og ved hjelp av komprimeringsteknikker fått hastigheter helt opp

til 125 Mbit/s. 802.11g utstyr er som oftest kompatibel med 802.11b utstyr, men da med 11 Mbit/s fart.

Begge standarder benytter 2,4 GHz-båndet

Vær oppmerksom på at hastighetene det her refereres til er mellom klient (altså PC) og ruter. Hastigheten på internettforbindelsen avhenger av den båndbredden som "går ut av huset".

IEE gruppene har ikke stoppet med A,B og G gruppene. Her får du en oversikt over hva som ligger i de forskjellige standardene:

E - skal forbedre muligheten for prioritering av trafikk i det trådløse nettet (QoS - Quality of Service). Dette er spesielt viktig ved transport av tale (IP-telefoni) og video.

F - gjør det mulig å gå mellom flere aksesspunkter uten å miste forbindelsen (roaming)

C - supplement for brigding av [MAC](#)-protokoller

boomen".

Standarder for trådløse nettverk. (802.11-familien)				
Standard	802.11	802.11a	802.11b	802.11g
Etablert	Juli 1997	16 Sept. 1999	16 Sept. 1999	Januar 2002
Kompatibilitet.	Ingen	Ingen	802.11g	802.11b
Frekvens benyttet	2,4 - 2,4835 GHz	5,725 - 5,850 GHz	2,4 GHz	2,4 GHz
Båndbredde	1 og 2 Mbps	6 - 54 Mbps.	1, 2, 5.5 og 11 Mbps	Opp til 54 Mbps