Denne guide er oprindeligt udgivet på Eksperten.dk

COMPUTERWORLD

# Introduktion til trådløst netværk og access points

**Artiklen introducerer grundbegreberne bag trådløse netværk. Standarder, sikkerhed og rækkevidde gennemgås. Artiklen kan også bruges til at danne et overblik over begreber, inden et eventuelt køb af access point.**

Skrevet den **02. Feb 2009** af **old-faithful** I kategorien **Netværk / Generelt** | ★★★☆☆

## INDHOLDSFORTEGNELSE



## 1. INTRODUKTION

Der findes flere måder at koble computere sammen i et netværk. Den "gammeldags" metode indebærer at kabler trækkes fra computer til computer, eventuelt igennem en switch/hub, som sørger for at sende data rundt i netværket.

Trådløse netværksteknologi - eller "WiFi" som det populært kaldes - er efterhånden blevet mere udbredt. Hjemmebrugere og firmaer kan opsætte deres egne trådløse netværk, der er næsten uafhængige af kabelforbindelser. Nogle forretninger, restauranter, hoteller o.lign. har desuden oprettet såkaldte "*hotspots*" der gør det muligt for fremmede at låne den trådløse Internetforbindelse på lovlig vis.

Der er flere måder at kommunikere trådløst med WiFi-teknologi. Den første mulighed er, at to computere opretter en trådløs forbindelse til hinanden. Sådanne direkte forbindelse kaldes for P2P (eller "Peer to peer" forbindelser).

Den anden mulighed gør brug af et såkaldt "*access point*". Et access point er et apparat, der sørger for fordele data mellem de trådløse enheder (f.eks. bærbare computere), som er tilsluttede. Samtidig fungerer dette "access point" som bindeleddet mellem det trådløse netværk og det ikke-trådløse netværk. Et access point kan desuden have en indbygget router (se ordforklaring i afsnit 8).

Denne artikel er dels ment som en introduktion til trådløse netværk, dels som en hjælp til folk som ønsker at købe eller opsætte et trådløst access point.

## 2. TRÅDLØSE NETVÆRKSSPECIFIKATIONER

Der findes forskellige standarder for trådløse netværk. Når du køber et trådløst apparat, skal du sørge for at det er kompatibelt med dit eksisterende udstyr (netværk og computere). De mest udbredte standarder er 802.11a, 802.11b og 802.11g. I dette afsnit vil jeg se nærmere på disse standarder.

### 2.1. 802.11a
- Årstal: 1999
- Frekvensområde: 5 GHz
- Båndbredde/hastighed: 54 Mbps (teoretisk) eller 25 Mbps (typisk)
- Maks. brugere: 64
- Sikkerhed: WEP (152 bit)
- Rækkevidde: Ca. 30 meter (indendørs)
- Kompatibilitet: Ikke kompatibelt med 802.11b-standarden (pga. forskelligt frekvensområde), men enkelte hybrider understøtter dog begge standarder
- Fordele: Højere teoretisk hastighed end f.eks. 802.11b
- Ulemper: Lav rækkevidde pga. høj frekvens. Ikke velegnet til at gennembryde mure og forhindringer.

### 2.2. 802.11b
- Årstal: 1999
- Frekvensområde: 2.4 GHz
- Båndbredde/hastighed: 11 Mbps (teoretisk) eller 6.5 Mbps (typisk)
- Maks. brugere: 32
- Sikkerhed: WEP-kryptering
- Rækkevidde: Ca. 50 meter (indendørs)
- Kompatibilitet: Ikke kompatibel med 802.11a-standarden (pga. forskelligt frekvensområde). Er dog kompatibel med 802.11g standarden!
- Fordele: Bedre til at gennembryde mure og forhindringer, end 802.11a, samt ofte billigere at producere end 802.11a-apparater. Bedre rækkevidde end 802.11a-standarden.
- Ulemper: Udsat for elektrisk støj. Lavere hastighed end 802.11a-standarden.

### 2.3. 802.11g
- Årstal: 2003
- Frekvensområde: 2.4 GHz
- Båndbredde/hastighed: 54 Mbps (teoretisk) eller 25 Mbps (typisk)
- Maks. brugere: 32
- Sikkerhed: WEP-kryptering (op til 128 bit kryptering)
- Rækkevidde: Ca. 30 meter (indendørs)
- Kompatibilitet: Kompatibel med 802.11g samt 802.11b-apparater/hardware.
- Fordele: God rækkevidde, samt mulighed for høj hastighed
- Noter: 802.11g er en nyere standard (fra ca. 2003), der er designet til at kombinere fordelene ved 802.11a og 802.11b-standarderne.

### 2.4. 802.11n
For en god ordens skyld, må også her nævnes 802.11n-standarden, som efter planen kommer i 2007.

- Årstal: 2007
- Frekvensområde: 2.4 GHz eller 5 GHz
- Båndbredde/hastighed: 540 Mbps (teoretisk), eller 200 Mbps (typisk)

- Rækkevidde: Ca. 50 meter (indendørs)
- Noter: 802.11n bygger videre på tidligere 802.11-standarder, ved bl.a. at indføre MIMO (multiple-input multiple-output). D-Link har lavet en trådløs router, der understøtter 802.11n (draft-udgaven), "D-Link RangeBooster N 650 Router DIR-635"

### 2.5. Sammenfatning

802.11a og 802.11b standarderne er lige gamle. Den primære forskel ligger i frekvensområdet der benyttes. Fordelen ved 2,4 GHz-området, er en god rækkevidde. Omvendt har 5 GHz mulighed bedre båndbredde, men har dårligere rækkevidde og har sværere ved at trænge igennem vægge og andre fysiske hindringer. Mens 2,4 GHz frekvensen trængere lettere igennem hindringer, er den dog samtidig mere udsat for elektrisk støj og interferens.

De på produkter angivne hastigheder/båndbredde er ofte meget optimistiske, så regn med at hastigheden effektivt er noget lavere (men som regel tilfredsstillende for de fleste netbrugere).

802.11a standarden (5 GHz) kan med fordel bruges, hvor der ikke er behov for så stor rækkevidde eller netværk på tværs af flere rum/vægge, men derimod behov for stor båndbredde (megen data) og mange samtidige brugere. Den korte rækkevidde kan evt. afhjælpes ved at benytte flere access points.

802.11b-g standarderne er mere egnede til hjemmebrug, hvor der er relativt få brugere og behov for god rækkevidde (f.eks. mange mure og værelser), og da disse er billigere end 802.11a-access points.

Man kan også overveje at investere i et "dual band" access point (læs mere herunder).

## 3. BEGREBER OG TEKNOLOGIER

### 3.1. Kryptering

En af de vigtigste dele af det trådløse netværk, er krypteringen. Normalt er det muligt at oprette et ikke-krypteret netværk, men det kan bestemt ikke anbefales. Krypterer du ikke din trådløse forbindelse, kan du risikere at andre opsnapper data som bliver sendt frem og tilbage - det kan f.eks. være emails, koder o.lign.

*WEP-kryptering*
WEP-kryptering ("Wired Equivalent Privacy") understøttes af alle moderne access points. De giver en grundlæggende, men ikke overvældende sikkerhed. Krypteringen anvender såkaldte nøgler, hvis længde afgøres af antallet af "bit". Nogle access points gør det muligt selv at angive, hvor mange bits der skal krypteres med. I praksis har det dog ringe betydning for sikkerheden, om du f.eks. vælger 40 bit kryptering eller 152-bit kryptering, da begge kan afkodes på omtrent samme tid.

*WPA-kryptering*
WPA står for "Wi-Fi Protected Access", blev indført i 2003 og understøttes af mange nyere access points. Generelt er WPA mere sikkert end WEP. WPA bruger - ligesom WEP - RC4 kryptering.

### 3.2. Dual band

Et "dual band" access point kan kommunikere på to frekvensområder - 5 GHz og 2,4 GHz. Således understøtter Dual Band access points både 802.11a og 802.11b/g. Dog vil hastigheden aldrig være højere end den hastighed som det  mest langsomme netværkskort understøtter. Er der således en 802.11b klient tilsluttet netværket, vil denne klient sænke hastigheden for andre, hurtigere (f.eks. 802.11a) klienter på

netværket.

### 3.3. Antal af antenner
Access points har som regel synlige antenner, som kan justeres for at få det bedst mulige signal. Et access point med flere antenner, giver dig normalt en mere pålidelige og stabil forbindelse, højere effektive hastigheder, samt bedre rækkevidde. Om du har brug for et access point med adskillige antenner, kommer an på hvordan dit påtænkte trådløse netværk skal se ud; skal du blot bruge Internet på ét og samme værelse, vil det ikke være nødvendigt at have flere antenner.

### 3.4. DHCP-understøttelse
DHCP står for "Dynamic Host Configuration Protocol", og er en funktion der står for at uddele IP-adresser dynamisk. Tilsluttede enheder har således ikke faste IP'er men får dem tildelt via DHCP-funktionen. DHCP understøttelse gør det lettere at forbinde nye enheder til netværket.

### 3.5. Netværks/LAN-porte
Hvis du vil koble dit access point på dit lokale netværk (LAN) eller koble f.eks. en stationær computer til et access point, skal dit access point have LAN port(e). De fleste access points har LAN porte/stik (i forbrugermodeller er der ofte op til 4 LAN porte).

Dette punkt er specielt vigtigt at være opmærksom på, hvis du
vil have mulighed for også at tilslutte enheder/computere via et konventionelt (kabel) LAN-netværk.

### 3.6. Understøttelse af Bluetooth
Understøttes Bluetooth, kan der forbindes til andre enheder med Bluetooth understøttelse, som regel mobiltelefoner, PDA'er, PC'er og andet elektronisk udstyr. Bluetooth har en relativt kort rækkevidde, en overførselshastighed på 2Mbps, og opererer i 2,45 Ghz frekvensen.

## 4. TRÅDLØS SIKKERHED

Sikkerheden er en central og aldeles vigtig del af ethvert trådløst netværk! Benytter man sig ikke af mulighederne for øget sikkerhed, er man mere udsat for hackerangreb, wardriving og opsnapning af personlige oplysninger. I bedste fald kan fremmede gøre brug af din Internetforbindelse, og i værste fald kan de få adgang til din computer.

Der findes flere metoder, der kan bidrage til at skabe et krypteret og relativt sikkert netværk.

### 4.1. Generelle råd
På et helt generelt plan, bør du altid have en firewall, samt et  antivirus-program installeret. Når du angiver kodeord (f.eks. i forbindelse med kryptering) bør du vælge stærke kodeord, hvilket f.eks. indebærer at kodeordet bør:
- Være langt (mindst 6 tegn, gerne over 20 tegn når vi taler WPA-nøgler)
- Indeholde både store og små bogstaver
- Indeholde et eller flere tal
- Gerne indeholde tilfældige kombinationer af tal og bogstaver (f.eks. n8b31LA0je25NI25pn2096Dn79aef24)

Hvad angår firewalls og antivirus, findes der gode betalingsløsninger men også udmærkede gratis alternativer. Find nogle af de bedste gratis muligheder her:
http://www.pricelesswarehome.org/2006/PL2006SECURITY.php

### 4.2. Kryptering: WEP, WPA og WPA2

Som absolut minimum bør du altid kryptere din forbindelse. WPA (tidl. kendt som "802.1x") er som nævnt meget mere sikkert end WEP, som ofte kan brydes på relativt kort tid.

Hvis ikke dit access point umiddelbart understøtter understøtter WPA, er WEP bedre end ingenting, men ofte kan en firmware-opgradering også give understøttelse af WPA/WPA2.

Både WEP og WPA virker i princippet ved, at der i access pointets indstillinger angives et kodeord, som tilsluttende enheder også skal angive.

WPA2 (tidl. "802.11i") er efterfølgeren til WPA, benytter stærkere kryptering (AES-kryptering i stedet for RC4) og er således mere sikkert.

Der findes to slags WPA: *WPA-Personal/WPA-PSK* og *WPA-Enterprise/WPA-RADIUS*.
*WPA-Personal* benytter princippet om en "Pre-Shared Key" (PSK). Her er der tale om en adgangskode, som kodes ind i access pointet og som enheder, der ønsker at tilslutte, skal kende.
*WPA-Enterprise* kaldes også for WPA-RADIUS, og bruges som regel i større, firmanetværk. WPA-RADIUS er anderledes idet der bruges "authentication servers", hviket er en (valgfri) mulighed for at verificere forbindelsen via en ekstern AAA/RADIUS server. Desuden benytter WPA-RADIUS også IEEE 802.1X standarden.

En sikker WPA kode bør bestå en lang, tilfældig, alfanumerisk kode (se evt. afsnittet herover). Vil du undersøge sikkerheden af dit WPA-baseret, trådløse netværk, kan du benytte WPA Cracker-redskabet fra tinyPEAP (http://www.tinypeap.com) sammen med en network protocol analyzer (prøv http://www.ethereal.com).

### 4.3. SSID

Ethvert access point skal have en SSID ("Service Set Identifier"). En SSID er et navn, som du selv vælger at give dit trådløse netværk. Af betydning for sikkerheden er dels hvilket navn du vælger, dels om du sætter "Broadcast SSID" (eller lignende) til.

Er "Broadcast SSID" eller "Accept SSID association requests" sat til, vil access pointet sende et signal ud, der fortæller omverdenen navnet på dit trådløse netværk. Det gør det lettere for dig, at "finde" dit netværk, men samtidig gøres det også lettere for uvedkommende (f.eks. hackere).

Det navn du vælger at give som SSID, bør ikke kunne henføres til dig, din adresse eller din familie. Optimalt bør der være tale om en helt tilfældig tekst på op til 32 bogstaver og tal, alternativt (og lidt mindre sikkert) et navn som blot ikke umiddelbart har nogen forbindelse med dig.

Kalder du f.eks. dit netværk for "Familien Jensens Ukrypterede  Net" og slår Broadcast SSID til, kan enhver hacker/bruger  1) se hvis netværk vedkommende har fundet, 2) lettere finde frem til den bedste placering at snylte fra, 3) lettere komme (uautoriseret) ind på dit netværk.

Derfor bør du af sikkerhedsmæssige årsager slå "Broadcast SSID" fra, og vælge en tilfældig tekst som SSID.

### 4.4. MAC-adresser

Enhver computer med netkort, har en MAC-adresse, dvs. et unikt identifikationsnummer. Access points kan

indstilles til, at kun computere med bestemte MAC-adresser, skal have adgang til det trådløse netværk. Dette kaldes ofte for "MAC-adresse-filtrering", og gør det sværere for uvedkommende at bryde ind i netværket.

Du kan finde en computers MAC-adresse, ved at trykke på "Start" og vælge "Kør...". Skriv "command" i tekstboksen og tryk på OK. Der kommer nu et DOS prompt vindue frem. Her skriver du: ipconfig /all

Din MAC-adresse eller "fysiske adresse" kan herefter aflæses, og vil ofte være noget i retningen af "02-1A-9F-E5-F3-E2". Denne adresse skal så tastes ind i access point'ets indstillinger (se produktets manual).

### 4.5. Fysiske foranstaltninger

Når du placerer dit access point bør du ikke kun overveje, hvordan bedst mulig rækkevidde opnås for dem du ønsker tilsluttet. Du bør også overveje om rækkevidden er for stor, således at der f.eks. kan skabes forbindelse fra naboens hus, fra vejen eller andre steder uden for "dit" område. Test det eventuelt ved at bevæge dig rundt uden for dit hus (eller hvor netværket konkret er sat op).

Her kan du også benytte din viden om rækkevidde (se afsnittet om rækkevidde), samt justere dit access points effekt. Det er jo ikke nødvendigt at sende signaler med størst effekt, hvis du kun benytter netværket i en lille etværelses-lejlighed. Og en for stor effekt er ikke nødvendigvis fordelagtig, da den kan forårsage støj i signalet. Læs evt. følgende artikel med kommentarer: http://www.eksperten.dk/artikler/903

### 4.6. Andre sikkerhedsforanstaltninger

Husk at lave om på standard-adgangskoden til dit access point (se apparatets manual).

Du kan evt. afprøve sikkerheden ved at bruge et program som Kismet (http://www.kismetwireless.net/) eller NetStumbler (http://www.netstumbler.com). Førstnævnte er en såkaldt "passive sniffer", modsat Netstumbler.

Dette kan særligt anbefales, hvis du er i tvivl om, hvorvidt dit netværk rent faktisk er (relativt) sikkert.

Du kan læse mere om disse programmer her:
http://csshyamsundar.wordpress.com/2006/04/07/introduction-to-netstumbler-and-kismet/

Der kan også være fordele ved at bruge evt. log-funktioner, eller generelt overvåger trafikken på netværket.

### 4.7. Avancerede sikkerhedsforanstaltninger

*4.7.1. VPN (IPsec, OpenVPN osv.)*
Til større netværk med mange brugere, kan det anbefales at opsætte et VPN ("virtual private network") system.

En fordel ved VPN, er at det giver en god bred sikkerhed med stærk kryptering af al data. Ulemperne ved VPN er, at det er besværligt at sætte op, og at der skal installeres VPN-klienter på alle computere som er tilsluttet netværket.

IPsec/IPsecurity ("Internet Protocol Security") er én måde at implementere VPN. Understøttelse af IPsec afhænger bl.a. af, om dit access point støtter IPsec. IPsec er en besværlig kryptering at bryde.

*4.7.2. Systemer til at opdage uautoriseret indtrængen (WIDS)*
Et WIDS ("Wireless intrusion detection system") kan bruges til at overvåge trådløse netværk, for at forhindre at uvedkommende får adgang til netværket. Ofte virker WIDS ved at undersøge de MAC-adresser der logger på netværket, men nyere systemer bruger også "fingerprinting". Læs mere om WIDS her: http://en.wikipedia.org/wiki/Wireless_intrusion_detection_system

### 4.8. Sammenfatning
Til sidst nogle generelle råd. Du bør som minimum altid:

1. Bruge kryptering (WPA og WPA2 er bedst, men WEP bedre end ingenting)
2. Bruge MAC-adressefiltrering (så kun bestemte computere kan komme ind på netværket)
3. Angive en anonym SSID, samt slå broadcast fra
4. Skifte adgangskoder og SSID med jævne mellemrum
5. Holde adgangskoder og andre detaljer hemmelige (lad ikke sikkerhedsdetaljerne ligge ukrypterede hen på f.eks. en bærbar eller i papirform)

## 5. FAKTORER AF BETYDNING FOR RÆKKEVIDDE OG HASTIGHED

### 5.1. Valg af trådløs apparat
Som angivet i afsnit 2, har valget af trådløs standard indflydelse på rækkevidden. For at opsummere, har 802.11a kortere rækkevidde og sværere ved at sende igennem objekter/vægge, men er ikke så udsat for interferens og elektrisk støj. 802.11b/g har en længere rækkevidde, men er også mere udsat for interferens/elektrisk støj.

### 5.2. Antenner - Antal og udformning
Generelt er det en fordel, hvis dit access point har mere end én antenne. Et access point er i grunden en radio sender, så det kan også hjælpe en hel del på rækkevidden, at koble en ekstern antenne på.

*5.2.1. Retningsbestemte antenner*
En retningsbestemt antenne, sender simpelt sagt et signal i en bestemt retning. Retningsbestemte antenner fås i flere forskellige udformninger. Retningsbestemte antenner kaldes på engelsk for "*directional antennae/antennas*". En retningsbestemt antenne kan bruges i et såkaldt "point-to-point" system (to retningsbestemte antenner peger på hinanden) eller "Multi-point" systemer.

*5.2.2. "Omni-directional" antenner*
En "omni-directional" antenne er ikke retningsbestemt, og behøver således ikke at pege i en bestemt retning.

*5.2.3. Hjemmelavede antenner*
Nogle mennesker har haft held med at få hjemmelavede antenner til at forstærke signalet. Se f.eks. http://www.freeantennas.com/ om antenner man selv kan lave med pap og sølvpapir.

Bemærk at hjemmelavede antenner ifølge *erikjacobsen* ikke er lovlige i Danmark, jf. http://www.eksperten.dk/artikler/787.

*5.2.4. Generelt om antenner*
Læs mere om antenner her: http://radiolabs.com/Articles/wifi-antenna.html

Du kan finde og købe antenner via www.edbpriser.dk i kategorien Netværk -> Antenner.

### 5.3 Fysiske forhold

Interferens og elektronisk støj kan påvirke rækkevidden af dit access point. Er dit access point omringet af metal - omkranset af en slags Faraday-bur - kan signalet godt have meget svært ved at komme igennem.

Således kan strømførende kabler, mikrobølgeovne, samt andet trådløst og elektrisk udstyr påvirke signalet. Ligeledes kan metal, f.eks. i form af kabler, metalmøber, armerede vægge o.lign. svække signalet.

Generelt vil alle objekter, sat i signalets vej, svække det. Mens dette særligt gælder metalgenstande, vil også vægge og mindre genstande påvirke signalet.

Det er altså vigtigt at vælge en god placering til dit access point, hvor signalet har de bedste forudsætninger for at komme igennem.

### 5.4. Repeatere / Relay stations / Wireless range extender

Du kan også købe en såkaldt "repeater" eller "range expander". En repeater behøver ikke at være koblet til netværket, men kræver dog strøm. En repeater fanger de trådløse signaler, forstærker og videresender dem. Fordelen ved at bruge en repeater, er at rækkevidden udvides, uden at der er behov for endnu et access point.

Forbindelsen vil som regel ikke være lige så hurtig, hvis den først skal igennem en repeater.

Det er vigtigt at være opmærksom på, at repeatere ofte kun understøtter bestemte andre enheder, så du kan ikke bare købe en tilfældig repeater og regne med at den vil virke med din opsætning.

En repeater skal naturligvis placeres inden for rækkevidde af dit access point, og de førnævnte principper angående fysisk placering finder tilsvarende anvendelse. Repeateren kan f.eks. placeres i hjørnet af en L-formet gang, for på den måde at sende signalet "rundt om hjørnet". Eller du kan placere repeateren inden for dit access points brugbare rækkevidde, for blot at fungere som en signalforstærker.

En repeater koster typisk ca. 500 kr. og kan bl.a. købes via www.edbpriser.dk

### 5.5. Valg af kanal

Man kan som regel vælge hvilken kanal ("channel"), som det trådløse netværk skal benytte. Valg af kanaler kan have betydning for rækkevidde, eftersom man ved at ændre på kanalen, kan undgå interferens med andre trådløse netværk og evt. andet elektronisk støj.

Ofte vil man kunne vælge f.eks. mellem kanal 1 - 11. Kanal 1 ligger i et lavere frekvensområde end de efterfølgende kanaler. Jo højere kanalnummer, desto højere frekvensområde. Der er et lille overlap mellem kanalerne, men jo større forskellen mellem to kanalnumre er, desto mindre overlap er der.

Antallet af kanaler afhænger af det konkrete lands lovgivning. I USA kan der være op til 11 kanaler, i Europa er der ofte op til 13 kanaler, i Japan 14, mens lande som Spanien kun tillader 2 kanaler.

Ofte vil standardkanalen være kanal 6. Har dit access point f.eks. mulighed for at vælge imellem 11 kanaler, vil der næsten intet overlap være mellem kanal 1, 6 og 11. Derfor kan det ofte anbefales at bruge en af disse kanaler tre kanaler.

Hvis din rækkevidde påvirkes af f.eks. en nabos trådløse netværk - eller du i den forbindelse har andre problemer med den trådløse forbindelse - kan du med fordel skifte til en kanal, som ligger langt væk fra

naboens kanal.

Du kan bl.a. bruge det gratis program NetStumbler, til at finde ud af hvilken kanal et andet netværk benytter: http://www.netstumbler.com/

Hovedreglen: Intet overlap betyder mindre interferens! Prøv dig dog frem med forskellige kanaler, for at se hvilken giver bedst forbindelse i dit tilfælde. Der kan jo også være andet elektronisk støj, som påvirker signalet.

Læs mere om kanaler her:
- http://en.wikipedia.org/wiki/Wi-Fi#Channels
- http://compnetworking.about.com/od/wifihomenetworking/qt/wifichannel.htm
- http://www.easypeasy.com/guides/article.php?article=146

### 5.6. Din computer

Udover de ovennævnte faktorer, har også din computer betydning for hastigheden på netværket. CPU hastighed, RAM og harddisk hastighed kan således påvirke din Internethastighed. Naturligvis kan din computer heller ikke kommunikere hurtigere end den WiFi-standard (f.eks. 802.11b) der understøttes.

## 6. MINI-KØBEGUIDE

Før du køber et trådløst access point, kan du gøre dig nogle overvejelser om f.eks.:
1) Har jeg reelt brug for et trådløst netværk? (Er der konkret nogle fordele for dig, ved at købe et trådløst netværk?)
2) Hvor mange computere vil jeg have tilkoblet via "gammeldags" kabelnetværk? (Her er antallet af LAN porte/indbygget switch relevant)
3) Hvor stort et område skal det trådløse netværk dække? (Er rækkevidden vigtig for dig?)
4) Hvilket slags område skal det trådløse netværk dække? (En lille lejlighed, eller f.eks. en stor villa med tykke, armerede mure?)
5) Hvilke teknologier understøtter mine computere? Hvilke teknologier understøtter access point'et?

Og nogle helt generelle råd...
- Hvis du vil købe dit access point over Internettet, kan du med fordel kigge på EDB-Priser.dk for at finde apparatet til en god pris (http://www.edbpriser.dk/). Det kan også anbefales at købe
- Prøv at finde og læse anmeldelser af access point'et inden du køber. Skriv f.eks. produktets navn i Google efterfulgt af "review" eller "anmeldelse"
- Det kan være en god idé at holde sig til en af de store producenter, f.eks.: Cisco/Linksys, D-Link eller Netgear.

## 7. EKSEMPEL PÅ OPSÆTNING & NOTER

### 7.1. Eksempel på opsætning

I et mindre hjemmenetværk, kunne det trådløse netværk f.eks. være opsat således:

```
Telefonstik -----> Modem -----> Trådløs router/Access point <-----> (trådløs
forbindelse)
                                                        |
                                                (kabelforbindelse, via LAN)
                                                        |
                                                Computer 1
```

**7.2. Opgradér dit firmware**
Det kan være en god idé at opgradere firmware på sit access point inden man går i gang med den helt store opsætning. Firmware opgraderinger kan som regel hentes gratis via producentens hjemmeside. Læs nærmere om firmware-opgradering i produktets dokumentation.

**7.3. Hvordan ændrer jeg indstillingerne på mit access point?**
Som regel opsættes et access point ved at først at forbinde det til en computer, dernæst indtaste apparatets IP-adresse i Internet Explorer (el.lign.). Dernæst logges ind med apparatets standard-adgangskode. Både IP-adresse og adgangskode fremgår af apparatets manual og er i nogle tilfælde endda trykt direkte på apparatet.

**7.4. At forbinde et trådløst netværk til et kabelnetværk (LAN)**
Hvis du vil "lave et trådløst signal om til kabelsignal", kan du gøre det ved at anskaffe dig en "wireless ethernet bridge" (trådløs bro), der gør det muligt at gå fra et trådløst netværk til et "kabelnetværk".

*Situationen er flg.:*
Du ønsker at forbinde en computer (uden trådløst netkort) eller et netværk til et trådløst netværk. Du køber derfor en trådløs bro, som kan omforme det trådløse signal til et "kabelsignal".

```
Access point/trådløst netværk ) ) ) ) Trådløs bro <------> Computer/LAN-
netværk
```

Du kan finde trådløse broer på edbpriser.dk:
http://www.edbpriser.dk/Products/Listproducts.asp?ID=71&Sort=Wanted&Soegeord=ethernet%2Bbridge

**7.5. Sådan finder du din basestations IP-adresse**
Basestationens IP-adresse skal du bl.a bruge når du skal ændre på basetationens/access pointets opsætning og indstillinger. Normalt indtastes IP-adressen f.eks. i Internet Explorers adressebar, hvorefter der trykkes på ENTER.

Dit access point har når du køber det en standard IP - altså en standardadresse som du selv kan ændre på, hvis det er nødvendigt. Oftest vil det dog i almindelige hjemmenetværk ikke være nødvendigt at ændre på IP-adressen (medmindre der er konflikter med andre IP-adresser).

IP-adressen vil ofte være påtrykt dit access point og/eller fremgå af manualen. Har du ændret IP-adressen, kan du ikke huske den eller finde den i manualen el. på apparatet, kan du som regel bruge Windows "ipconfig" program til at finde IP-adressen. For at bruge "ipconfig", skal du trykke på "Start" -> "Kør..." -> Skrive "cmd" (eller "command") og trykke på "OK". Herefter kommer der et DOS-vindue op, som du så skriver *ipconfig* i. Du vil nu få vist nogle detaljer om din IP. Din (standard)gateway er access pointets IP-adresse, som du kan indtaste i Internet Explorer, som beskrevet herover.

### 7.6. Sådan opretter du en direkte forbindelse (ad-hoc) uden access point

Du kan oprette en direkte forbindelse - eller »ad hoc-forbindelse« - mellem to computere, uden at benytte et access point. Det kræver blot at de to computere understøtter samme trådløse standard. De følgende instrukser gælder for Windows XP.

For at oprette en direkte computer-til-computer forbindelse skal du:
1) Klikke på "Start" -> "Kontrolpanel" (evt. under Indstilinger) -> "Netværksforbindelser"
2) Højreklik på "Trådløs Netværksforbindelse" og vælg "Vis trådløse netværk der er tilgængelige"
3) Tryk på "Skift avancerede indstillinger", derefter fanebladet "Trådløse netværk"
4) Tryk på knappen "Tilføj..."
5) Giv din netværksforbindelse et navn der ikke allerede er i brug (indtast det i Netværksnavn/SSID), f.eks. "Adhoc"
6) Sæt flueben i "Dette er et netværk, hvor computere har direkte forbindelse til hinanden. Der bliver ikke brugt tådløse adgangspunkter"
7) Er der aftalt en krypteret forbindelse, skal du gøre dette: Fjern fluebenet i "Denne nøgle angives automatisk for mig". Skriv et kodeord i både "Netværksnøgle" og gentag samme ord i "Bekræft netværksnøgle". Du kan også indstille "Netværksgodkendelse", "Datakryptering" og "Nøgleindeks". Sørg for at den computer du vil forbinde til, bruger de samme indstillinger
8) Tryk på OK for at lukke boksen "Egenskaber for trådløst netværk"

### 7.7. At bruge en trådløs router som access point og switch

Har du allerede en almindelig kabelrouter, er det ikke sikkert at du ønsker eller kan skifte denne ud med en trådløs router. Du vil måske hellere koble den trådløse router til den eksisterende router, og så kun bruge den trådløse funktion?

Har du en trådløs router, som du kun ønsker at benytte som access point og switch (og altså ikke benytte routerfunktionen), kan man gøre dette ved at slå DHCP fra (i routerens indstillinger) og kun bruge LAN-porte. Du skal desuden sørge for, at den trådløse router benytter samme IP-segment som det øvrige udstyr. Herefter følger et eksempel.

*EKSEMPEL: DLink DIR-635 BRUGES SOM ACCESS POINT*
Det følgende er et eksempel på hvordan én trådløs Dlink router er blevet sat sammen med en almindelig router. Det er ikke givet at samme fremgangsmåde ville kunne benyttes på alle trådløse routere, men principperne er hovedsageligt de samme:

1. Forbind den trådløse router til en computer via netværkskabel (tilslut kablet den trådløse routers LAN-port)

2. Gå ind i routerens opsætning (som regel ved at indtaste den trådløse routers IP-adresse i Internet Explorers adressebar)

3. Slå DHCP fra (eftersom routeren - og ikke den trådløse router - skal stå for at uddele IP'er på netværket)

4. Indstil den trådløse routers IP, så den ligger inden for samme segment som routeren. Har routeren f.eks. IP 192.168.1.1 skal den trådløse router have en IP-adresse, hvor kun det sidste tal (dvs. tallet efter det sidste punktum) er anderledes, f.eks. 192.168.1.2. De to enheder bør nemlig ikke have samme IP adresse men skal være i samme segment, før de kan kommunikere med hinanden.

5. Gem indstillingerne. Husk at notere den nye IP-adresse, da det er den du fremover skal bruge, når du vil ændre i den trådløse routers indstillinger.

6. Indsæt kablet fra routeren i en ledig LAN indgang. Man skal således slet ikke benytte en eventuel WAN eller Internet indgang i den trådløse router, når man kun vil bruge routeren som access point.

7. Det kan vaere nødvendigt at vaelge "Start" -> "Kør...", skrive "cmd" og trykke på "OK". Derefter skrive:
"ipconfig /release" (og trykke på ENTER)
"ipconfig /renew" (og trykke på ENTER)

8. Test forbindelsen. Færdig!

Hovedpunkterne er altså:
1) Slå DHCP fra i den trådløse router
2) Sæt den trådløse routers IP-adresse til samme segment som den almindelige router
3) Forbind de to routers via "LAN"-indgange og benyt ikke et eventuelt "WAN"/"Internet" stik i den trådløse router.

## 7a. FEJLFINDING PÅ TRÅDLØSE NETVÆRK

Dette afsnit (7.a.) er baseret på PC-World's artikel, som du kan læse her: http://www.pcworld.dk/art/7200?page=1. Således opsummeres nævnte artikels hovedpunkter i det følgende, og jeg har tilføjet egne kommentarer, hvor jeg har skønnet det relevant.

### 7a.1. Generelle råd
Start med det helt grundlæggende:
- Er strømkablet sat i?
- Er der tændt for strømmen?
- Er dit access point tændt?
- Er eventuelle antenner monteret (og monteret ordentligt)?

### 7a.2. Hvor er problemet?
Som noget af det første, bør du undersøger hvor fejlen er - i netværkskortet/computeren eller i din basestation (access point).
- Har du installeret netværkskortet?
- Er der et lille trådløst netværksikon i taskbaren (nederst til højre på skærmen)?
- Kan netværkskortet finde nogle netværker når du trykker på nævnte ikon? Hvis ikke kan det tyde på at basestationen ikke sender noget signal eller at signalet er for svagt.

NB: Det kan være en god idé at placere din computer tæt på dit access point (men gerne mindst 1-2 meter fra hinanden), så du kan finde mere grundlæggende fejl, før du begynder at undersøge rækkeviddeproblemer.

### 7a.3. Hvis der ikke er kontakt til basestationen
- Prøv at oprette en direkte kabelforbindelse til basestationen. Dette gør du som regel ved at trække et netværkskabel fra din PC til et netværksstik på basestationen. Du skal sætte dette kabel i det rigtige stik. Et "WAN" eller "Internet" stik vil være det forkerte, mens et stik mærket "LAN" el. lign. formentlig vil kunne bruges.
- Prøv at logge på basestationen med standardkodeord og IP. Disse detaljer vil som regel fremgå af enten basestationens manual eller kan være påtrykt selve basestationen. Hvis ikke du kan finde disse detaljer, kan du evt. prøve at finde detaljerne via en søgning på Google eller lignende.
- Som regel skal du taste IP adressen (f.eks. 192.168.1.1) ind i din Internet Browsers (f.eks. Internet Explorer) adressebar og trykke på ENTER. Så burde du blive bedt om et kodeord (brug standardkodeordet som fabrikanten har oplyst, medmindre du selv har ændret det)

NB: Har du ændret kodeordet og kan du ikke huske det, kan du prøve at se om dit access point kan nulstilles/"resettes". Se om der er en knap på access pointet til dette.

- Hvis du ikke kan komme frem til nogen konfigurationsside og ikke bliver bedt om et kodeord, kan det tyde på at basestationen er gået i stykker. Prøv dog først forbindelsen med to eller flere netværkskabler, før du drøner ned til butikken.
- Kan du godt få forbindelse til basestationen, med et netværkskabel, er det formentlig et problem med signalet

NB: Husk at du som forbruger efter købeloven kan bytte en defekt genstand i op til 2 år efter købet (jf. købelovens reklamationsregler).

**7a.4. Hvis din computer kan se netværket, men ikke logge på**
- Det er vigtigt at de indstillinger din computer bruger til at tilslutte sig det trådløse netværk svarer til de indstillinger, som basestationen bruger.
- Bl.a. skal SSID, krypteringsnøglen (WEP, WPA osv.) og kodeord stemme overens
- Prøv evt. at fjerne krypteringen midlertidigt, og se om det gør en forskel
- Basestationen skal være sat op til at fungere som "access point" og IKKE repeater
- Dit netværkskort (din computer) skal være sat til at køre "Infrastructure" og ikke "Ad hoc" (se ordforklaring i afsnit 8)

**7a.5. Hvis der er problemer med signalet eller forbindelsen falder ud**
Se mit særskilte afsnit om rækkevidde.

NB: Én måde at teste forbindelsen til et trådløst access point er at "pinge". Ligesom en u-båd kan sende et signal ud for at finde et skib, kan din computer sende et signal ud, for at se hvor god forbindelsen er. Ved at pinge får du vist svartider (i millisekunder), samt hvor meget data tabes undervejs mellem access point og computer. For at bruge Windows ping funktion skal du trykke på "Start" -> "Kør..." -> Skrive "command" eller "cmd" -> "OK". Derefter skriver du "ping" efterfulgt af dit access points IP-adresse, f.eks. *ping 192.168.1.1*, og trykker på ENTER. Du kan få vist flere muligheder ved at skrive *ping /?*.

**7a.6. Hvis der kan oprettes forbindelse til access point, men ikke til netværk**
- Sørg for at Windows har tilsluttet sig netværket (kig på ikonet i taskbaren, nederst til højre). Tilkobling sker ikke nødvendigvis automatisk.

NB: I nogle tilfælde kan problemer også opstå hvis der er adresse-konflikter på netværket, dvs. hvis to apparater (f.eks. en router og en trådløs router) kæmper om samme IP-adresse. I sådanne tilfælde kan problemet ofte afhjælpes ved at ændre på access pointets IP. Hvis dit access point har indbygget router, kan du også overveje om du overhovedet har brug for en anden (konventionel) router.

**7a.7. Problemer med computerens trådløse netværk**
- Mange bærbare har en knap (eller evt. et software program) til at tænde og slukke for det trådløse netværk. Sørg for at der er tændt

NB: Sørg også for at det trådløse netværk ikke er deaktiveret. I Windows kan du trykke på "Start" -> "Indstillinger" og så dobbeltklike på "Netværksforbindelser". Er der et ikon som hedder "Trådløs netværksforbindelse" eller lignende, skal det ikke være gråt. Hvis det er gråt, skal du højreklikke på det og vælge "Aktiver"

**7a.8. Firewall-konflikter**

- Du skal naturligvis benytte firewall, også når du har trådløst netværk
- Din firewall skal være sat til at tillade "ICMP echo requests" (pings) at slippe igennem. Hvis du bruger Windows XPs indbyggede firewall, kan du ændre på indstillingen via "Start" -> "Indstillinger"-> "Tillad indgående ekkoanmodning"

Husk at problemer med at koble på et trådløst netværk i nogle tilfælde kan skyldes en restriktiv firewall. Prøv at slå din firewall midlertidigt fra, hvis du tror at dette kan være årsagen til dine problemer.

### 7a.9. Problemer med skift fra kabel til trådløs (og vice versa)

- I enkelte tilfælde kan det give problemer, når man skifter fra et kabelnetværk til et trådløst netværk. Prøv evt. at først deaktivere det netværk du vil koble computeren fra, og derefter aktiverer det (LAN) netværk man vil koble sig på.- Dette kan i Windows gøres via
"Start" -> "Indstillinger" og så dobbeltklike på "Netværksforbindelser".

## 8. SIMPLIFICERET NETVÆRKS-ORDBOG

*Access point*: Apparat, der distribuerer data imellem trådløse netkort, samt kobler et trådløst netværk sammen med et (almindeligt, ikke-trådløst) netværk.

*Ad hoc netværk*: Bruges ofte om et trådløst netværk imellem to computere, uden et access point som bindeled

*Bridge*: Apparat, der sørger for at sende signaler mellem to LAN'er eller to LAN-segmenter. Kort sagt bruges en bridge til at forbinde to eller flere (kompatible) netværker.

*DHCP*: Funktion der sørger for at fordele/uddele IP-adresser til de enheder, som er koblet på et netværk.

*Ethernet*: En meget udbredt LAN-standard for hardware, kabler og kommunikation. Generelt har ethernet en hastighed på 10 Mbps (Ethernet) eller 100 Mbps (Fast Ethernet). Oprindeligt udviklet af Xerox, DEC og Intel.

*Hub*: Et apparat der gør det muligt for flere apparater (f.eks. computere) at blive koblet til hinanden, i et netværk. En "hub" har generelt samme funktion som en switch, men er langsommere (da den ikke kun sender data til modtager-porten, men derimod alle på netværket).

*Infrastructure*: Når det trådløse netværk ikke går direkte fra computer til computer, men gennem et access point. Det modsatte af et "ad hoc netværk". computer, men gennem et access point. Det modsatte af et "ad hoc netværk".

*LAN*: Local-area network. Er kort sagt udtryk for en måde at forbinde computere (og andet hardware) i et lokalt netværk.

*Mbps*: Megabits per second

*Modem*: Forkortelse af *mo*dulator/*de*modulator. Udstyr der konverterer data til et signal der kan sendes via telefonnettet.

*Router*: Apparat der formidler data mellem et LAN og telefonlinjen. Kort sagt bruges en router til at forbinde to (eller flere) netværker (f.eks. forbinde Internettet med et lokalt netværk) og til at sørge for at dataoverførslen sker så effektivt som muligt.

*Switch*: Kort sagt, et apparat der sørger for at sende og fordele data rundt i et netværk. En switch er en mere avanceret slags "hub", der gør netværket mere effektivt, ved kun at sende data til den rigtige "modtager" på netværket. En switch bruges ofte i hjemmenetværk, til at forbinde mere end to computere med hinanden.

*WAN*: Wide area network. Et WAN forbinder en række LAN'er. Et mindre WAN kan f.eks. bestå af 2 lokale netværk, men også Internettet som helhed kan betragtes som et WAN.

*Wardriving, WiLDing og Warwalking*: At bevæge sig rundt i et område på jagt efter ubeskyttet trådløse netværk

*WiFi*: Forkortelse for "wireless fidelity". En betegnelse for visse trådløse netværk (WLAN), der hører til IEEE 802.11-standarden for trådløse netværk. Wi-Fi bruges ofte af bærbare computere.

*Wireless router*: En trådløs router. En trådløs router indeholder også et access point.

*WLAN*: Wireless Local Area Network, dvs. trådløs netværk. IEEE 802.11 angiver WLAN standarder.

## 9. ANDRE RESSOURCER

Læs mere om trådløs teknologi m.v. her:
- Wikipedia: http://en.wikipedia.org/wiki/802.11
- Gratis hotspots i Danmark: http://www.openwifi.dk/
- Om kryptering: http://www.quepublishing.com/articles/article.asp?p=421706&rl=1

***** SVAR PÅ KOMMENTARER M.M. *****

Jeg hilser kommentarer og forslag velkommen. Vær venligst konkret i dine angivelse, så jeg ved hvad du (ikke) synes om.

---
*smashlotus:*
Det er hermed gjort. Se afsnit 5.5. Tak for kommentaren.

*pgh71:*
Vil du ikke venligst forklare hvad du ikke syntes om? Så har jeg en chance for at forbedre artiklen. Tak.

---

**ÆNDRINGER**
- 25. maj 2007: Tilføjet eksempel vedr. at bruge router som access point.
- 6. februar 2007: Smårettelser.
- 25. december 2006: Tilføjet afsnit 7.6 om direkte forbindelser. Andre mindre tilføjelser.
- 20. december 2006: Mindre tilføjelser
- 19. december 2006: Afsnit 5.6 tilføjet
- 10. december 2006: Tilføjet delafsnit om trådløse broer med inspiration fra http://www.eksperten.dk/spm/749962
- 9. december 2006: Tilføjet afsnit 7.a., samt nogle ord i ordbogen. Mindre tilføjelser.

**Kommentar af henrik22 d. 11. Jun 2008 | 1**

Meget god artikel

**Kommentar af pgh71 d. 22. Dec 2006 | 2**

**Kommentar af serene d. 12. Dec 2006 | 3**

jeg blev  meget "klogere"
mvh Bo

**Kommentar af schlumberger (nedlagt brugerprofil) d. 10. Dec 2006 | 4**

**Kommentar af brian_a d. 07. Dec 2006 | 5**

**Kommentar af per-olof d. 11. Dec 2006 | 6**

**Kommentar af htmlkongen d. 13. Feb 2007 | 7**

God detaljeret beskrivning af detaljer :) /Htmlkongen

**Kommentar af dustie d. 20. Dec 2008 | 8**

Flot og velformuleret artikel. Rigtig meget information som de fleste skulle kunne lære noget af. Skal man sætte trådløst netværk op og ved man ikke alt hvad der er værd at vide i forvejen er artiklen en super guide.

**Kommentar af smashlotus d. 11. Dec 2006 | 9**

Update: Så blev artiklen vist fuldendt. Meget flot.
########################################## Hej,
Overordnet en rigtig god artikkel - dog synes jeg du mangler at informere om de forskellige kanaler man kan indstille sit trådløse netværk til at bruge, her er det nemlig meget væsentlig at man ikke bruger samme kanal som sine naboers trådløse net idet det let kan skabe problemer med forbindelsen og hastigheden. Det er jo let at tjekke hvilken kanal nabo-netværkerne kører med og derefter evt. justere sit eget ap til en anden kanal.

**Kommentar af terrak d. 12. Dec 2006 | 10**

Jeg lærte ikke meget nyt, men stadig god og dækkende artikel.

**Kommentar af swiatecki d. 09. Dec 2006 | 11**

**Kommentar af anders_h d. 08. Dec 2006 | 12**

**Kommentar af huset d. 14. Feb 2007 | 13**

Old > post mig lge en mail på freehelp(dot)freehelp(at)gmail(dot)com

**Kommentar af sepruda d. 26. Dec 2006 | 14**

Meget grundig artikel! Jeg kunne dog godt tænke mig lidt info om IP tildeling og konflikter (især fordi det er det jeg har et problem med lige nu :) http://www.eksperten.dk/spm/752480)

**Kommentar af califfo d. 11. Dec 2006 | 15**

Supergod artikel.

**Kommentar af ingeper d. 31. Jul 2007 | 16**

**Kommentar af phpzer0 d. 12. Dec 2006 | 17**

Super artikel!

**Kommentar af vendelbo d. 07. Dec 2006 | 18**

**Kommentar af flatron d. 23. Jun 2007 | 19**

Meget flot artikel, let læselig og informativ.

**Kommentar af sjoervad d. 12. Mar 2008 | 20**

**Kommentar af signalhorn d. 04. Oct 2008 | 21**

**Kommentar af Emfuttrup d. 31. Oct 2011 | 22**

SKØN artikel, skrevet i et sprog og med en grundighed som gør, at man kan arbejde frem efter den. Tak for det!

**Kommentar af supportsiden d. 08. Mar 2013 | 23**

Ok artikel, MEN det er forkert at anbefale at slå SSID broacast fra.
http://www.brighthub.com/computing/smb-security/articles/1211.aspx
http://technet.microsoft.com/en-us/library/bb726942.aspx#EDAA

**Kommentar af Jules-JP d. 01. Apr 2016 | 24**

Fed guide i et let sprog, tak!