

Trådløse Standarder

Den trådløse jungle

Der findes i dag et hav af forskellige standarder for trådløs kommunikation: Wi-Fi, Bluetooth, DECT, Wimax, IR for bare at nævne nogle få. Nogle er dog mere udbredt end andre og de mest populære til trådløs datakommunikation hører under Wi-Fi paraplynavnet. Her er især tale om standarderne 802.11a, 802.11b og 802.11g som dette afsnit hovedsageligt skal handle om.

Udover de nævnte standarder, er der en række specielle modifikationer, som kan booste den trådløse hastighed; de såkaldte "+" modifikationer.

Sidst men ikke mindst vil vi berøre de trådløse sikkerhedsfunktioner, som er meget vigtige at benytte, når man etablerer et trådløst netværk. Det er efterhånden blevet meget nemt at gøre sit trådløse netværk sikkert, men der er stadig mange, som ikke gør det.

802.11b - 11 mbps trådløst netværk

Denne, efterhånden aldrende, standard er stadig den mest udbredte og brugte. Den udmærker sig ved at være meget stabil og have rigtig god rækkevidde. Kommunikationen foregår på et licensfrit bånd (2.4 GHz) og er dermed følsom overfor andre trådløse kilder, som f.eks. trådløse telefoner, babyalarmer, mikrobølgeovne m.m. Endvidere er standarden også følsom overfor forhindringer som vægge, mure og træer, hvis der er tale om udendørs kommunikation - ganske som alle andre trådløse kommunikationsformer.

802.11b er en del af Wi-Fi standarderne, og hvis man køber produkter, som bærer dette mærke, er man sikker på, at produkter fra forskellige fabrikanter kan fungere sammen. Det er vigtigt idet mange bærbare computere idag leveres med indbygget trådløst netkort, og man er derfor ofte tvunget til at kombinere udstyr fra producenter.

802.11b er kompatibelt med den hurtigere 802.11g standard (læs nedenfor), dog med den sideeffekt, at den samlede båndbredde på netværket vil blive trukket ned på maksimalt 11 mbps.

802.11g - 54 mbps trådløst netværk

Denne standard blev for alvor udbredt i løbet af 2004. Det er den direkte afløser for 802.11b. Fordelen ved 802.11g er at den bruger en anden trådløs modulation (samme som 802.11a) og dermed kan kommunikere helt op til 54 mbps. Standarden er bagudkompatibel med 802.11b produkter, dog vil den maksimale båndbredde på det trådløse net blive trukket ned på 11 mbps, hvis de to standarder kombineres.

Som 802.11b bruger 802.11g også 2,4 GHz båndet til at kommunikere på. Derfor vil man opleve de samme udfordringer mht. forhindringer som f.eks. andre trådløse kilder og nedsat signalstyrke i huse med tykke vægge. Rækkevidden på 54 mbps standarden er umiddelbart den samme som 11 mbps standarden. Dog vil mange opleve en anelse dårligere rækkevidde, idet standarden er mere følsom overfor forhindringer. Dette skal dog ses procentvis. Hvis man har 25% af signalstyrken, er dette jo stadig bedre end 11 mbps standarden.

g+ - 125 mbps trådløst netværk

g+ er ZyXELs egen modifikation af 802.11g standarden. Denne modifikation bruger en bredere del af kanalspektrummet og opnår dermed højere båndbredde. Alle produkter i g+ serien understøtter selvfølgelig også 802.11b og 802.11g - dog kun med hhv. 54 og 11 mbps hastigheder. For at opnå fuld udnyttelse af g+ standarden, skal man derfor bruge g+ kompatible produkter. I skrivende stund er der 7 produkter, som understøtter dette, men flere er på vej.

802.11a - 54 mbps trådløst netværk

Denne standard vil vi blot kort kommentere, idet stort set ingen producenter benytter sig af den mere. Modsat de 3 andre nævnte standarder kommunikerer den på 5 GHz båndet og er dermed enormt følsom overfor forhindringer. I praksis så følsom, at rækkevidden sjældent bliver mere end 10 meter, hvis man skal holde sig indenfor lovlige sendestyrker. Ydermere er den ikke kompatibel med de andre standarder og derfor heller ikke interessant i bred forstand.

Standarder	802.11b	802.11g	g+	802.11a
Hastighed mbps	11	54	125	54
Kompatibel med andre standarder	Ja	Ja	Ja	Nej
Rækkevidde inde*	100m	100m	100m	100m
Rækkevidde ude*	300m	300m	300m	300m
ZyXEL produkter	Ja	Ja	Ja	Nej

***Rækkevidden afhænger af omgivelserne.**

Trådløse sikkerhedsstandarder

Modsat et kablet netværk, kan man med et trådløst netværk ikke fysisk se, hvem der tilegner sig adgang. De trådløse bølger er i luften, og man ved derfor ikke, om der sidder en person ude på gaden og "lytter" med. Derfor er det vigtigt at sikre især 2 ting på sit trådløse netværk: Adgangssikkerhed (hvem bruger netværket) og datasikkerhed (kryptering, hvem kan læse mine data). Der findes indenfor Wi-Fi standarderne en række meget gode krypterings og adgangssikkerhedsfeatures, som enhver med trådløst netværk bør bruge. Her vil vi nævne de mest populære.

WEP64/128/256 kryptering:

WEP er en måde at kryptere sine trådløse data på. Det er den første standard som kom på markedet, og den har været meget udskældt, især for ikke at være stærk nok. WEP benytter sig af statiske krypteringsnøgler, hvilket betyder, at har en hacker først opsniffet denne nøgle, er der fri adgang til al kommunikation. Som det kan ses ovenfor er der foreløbig 3 grader af WEP: 64, 128 og 256. Tallet angiver antal bits, hvormed krypteringen foregår. Jo højere, jo bedre.

MAC Filter og 802.1x:

MAC filter og 802.1x er en måde at sikre adgangssikkerheden på. MAC filteret sorterer i de trådløse netværkskorts unikke MAC adresse. Dette kan dog spoofes (kopieres/snydes), så denne metode er heller ikke 100% sikker.

802.1x er en brugervalidering som foregår via et stykke software som installeres på klient computeren. Denne software validerer op imod en 802.1x brugernøgle som konfigureres i Access Pointet. Denne metode er meget sikker og giver en meget høj adgangssikkerhed.

WPA

Dette er den nyeste og bedste metode til at sikre sit trådløse net på. Den kombinerer det bedste fra de 2 ovenstående og tilføjer lidt ekstra. WPA benytter sig af TKIP kryptering med dynamiske nøgler. Det betyder, at krypteringsnøglen hele tiden skiftes ud, og hvis en hacker så er heldig at tilegne sig adgang til disse, vil det kun være meget små brudstykker af data han vil få. Ydermere benytter WPA 802.1x brugervalidering, som sikrer en høj adgangssikkerhed.

Sidst men ikke mindst skal det nævnes, at WPA er meget nemt at sætte op. Brugeren skal blot indtaste en hemmelig nøgle og trykke "OK". Dette skal gøres i Access Pointet og på klientmaskinen - så er man oppe at køre.

802.11i eller WPA2

Denne standard er endnu ikke kommet på markedet (jan 2005). Den bliver, som navnet antyder, afløseren for WPA. Den eneste forskel på de to standarder er selve krypteringen af data. I 802.11i opgraderes dette fra WEP til AES kryptering, som vi kender fra VPN. Som normal forbruger er det dog ikke af den største vigtighed, idet WEP må betegnes som rigeligt, så længe der bruges dynamiske nøgler. Endvidere skal man være klar over at AES kryptering stiller større krav til hardwaren i Access Pointet, hvilket kan betyde, at ydelsen vil blive nedsat, hvis man opgraderer til WPA2, medmindre man skifter til nyere hardware.