Trådløst LAN – hvordan sikrer man sig?

Trådløse acces points er blevet så billige, at enhver der har brug for en nettilsluttet computer et andet sted end ADSL modemmet står, vil vælge denne løsning.
Det er nemt, det er billigt og det *kan* være sikkert. Her er en kort gennemgang af hvad der skal til for at din forbindelse kan karakteriseres som ”sikker”.

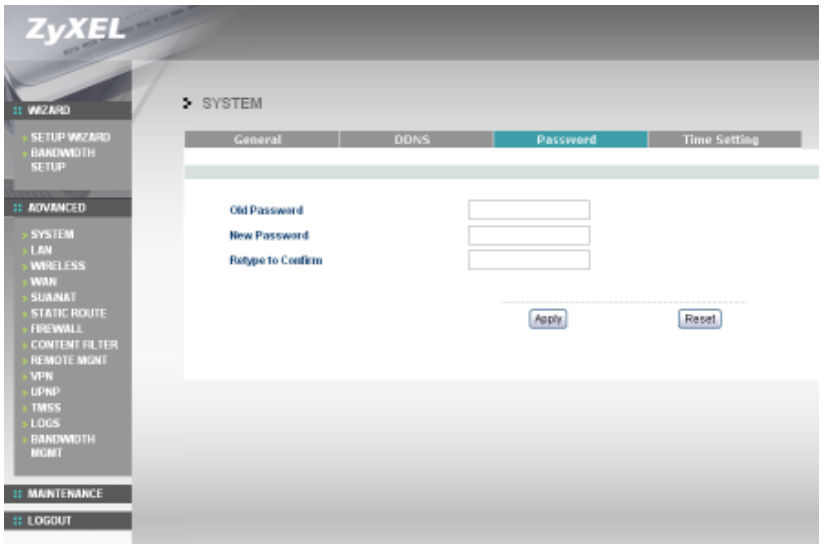
Du skal være opmærksom på, at hvis du blot pakker udstyret ud, sætter kablerne i, og tænder, vil det i de fleste tilfælde virke. Du har så samtidig åbnet en helt offentlig forbindelse for alle og enhver der kommer indenfor dækningsområdet (typisk op til 100-300 meter). De kan så bruge din ADSL forbindelse, de kan tilgå alle dine computere (slut på samtlige hemmeligheder incl. passwords), de kan downloade ulovligt materiale (på din IP-adresse – hvem tror du får skylden?) og så videre.

Derfor bør du som minimum foretage sikring som nævnt nedenfor i punkt 1 til 6, men også gerne 7.

1. Ændre altid dit password på acces pointet

Standard eller medfødte brugernavne og password er ikke sikre. Typisk er det noget i stil med brugernavn = Admin og password = 1234. Virkelig ikke noget der kræver en universitetsgrad at knække.

Åbn brugerfladen på dit acces point. Det gøres typisk ved at skrive adressen 192.168.1.1 i din browser (ellers se i din manual hvad adressen er). Tast default ID og password, og find det sted hvor password ændres. Disse eksempler er fra en ZyXEL men andre minder om denne. Her er det ”Advanced” - ”System” – ”Password”. Her indtaster du det gamle, og det ny to gange.

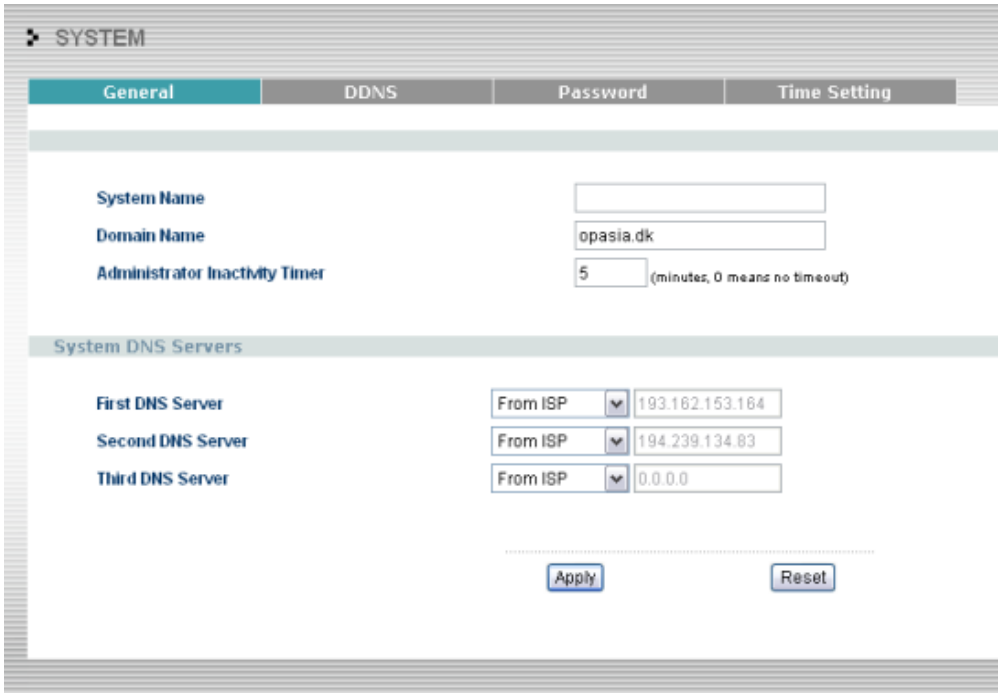


Husk at vælge et password du også kan huske om et halvt år. Dog må det ikke være til at gætte – altså ingen børnenavne, hundenavne, telefonnumre, fødselsdage eller lignende. Typisk bør det være på mindst 7 karakterer, indeholde både bogstaver og tal, og gerne både store og små bogstaver.
Tryk ”Apply” og gå ud af opsætningen for at checke at det nu også er ændret.

2. Ændre altid din SSID

SSID står for Service Set IDentifier, og er navnet på basisstationen. Typisk sætter fabrikanten deres navn ind, og det er jo nemt for en ubuden gæst at søge efter, så skift til noget der ikke lige falder i øjnene.

På ZyXEL er det ”Advanced” - ”System” hvorefter du får nedenstående billede:

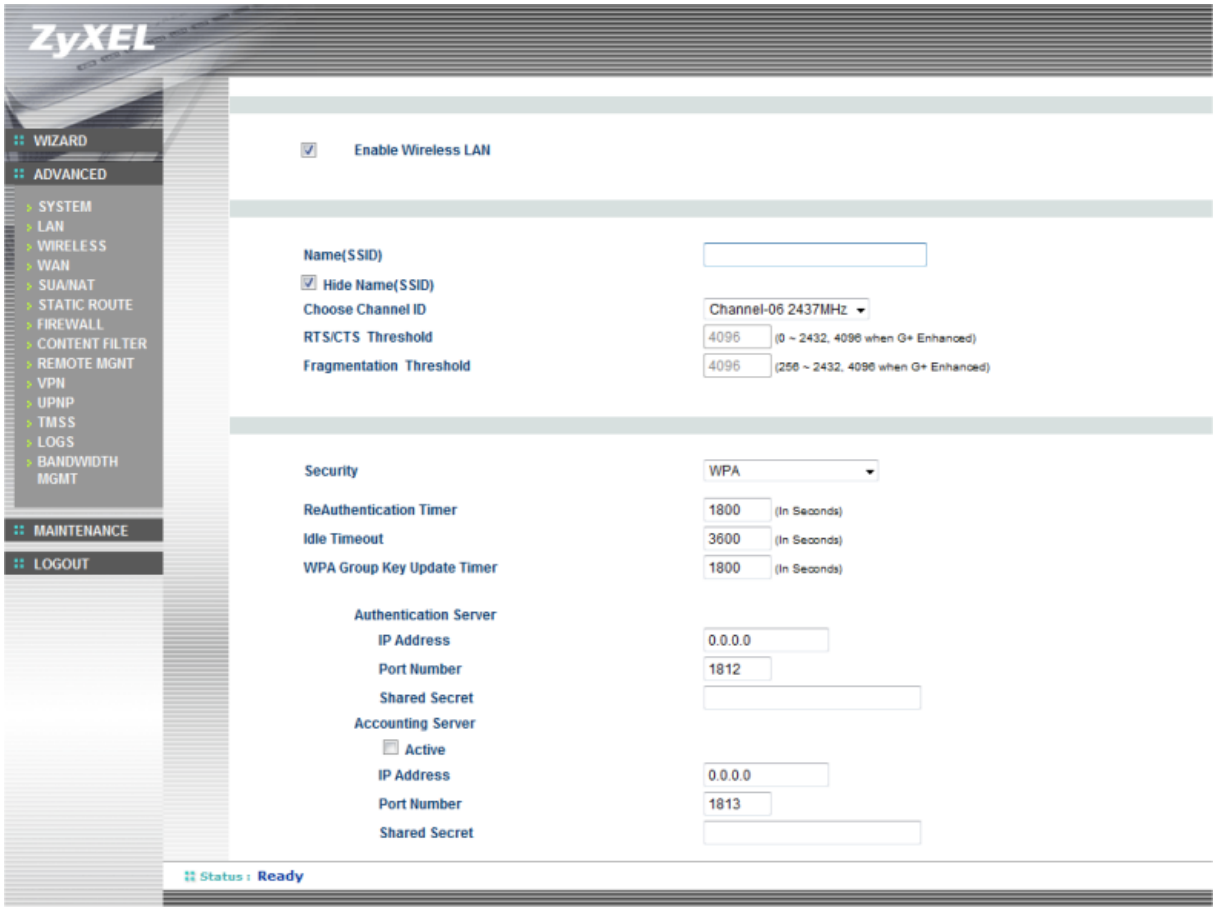


Her er det feltet System Name der skal rettes. Når du har skiftet navnet ud, trykker du ”Apply”.

3. Skjul din SSID

Ud over at ændre navnet, bør du sikre at acces pointet ikke rundspreder navnet, så alle og enhver kan opfange det.

På ZyXEL gøres det i ”Advanced” – ”Wireless”, hvorefter følgende billede kommer frem:



I dette tilfælde sættes et flueben i feltet ”Hide Name (SSID). Tryk herefter ”Apply”.

4. Benyt kryptering af den trådløse trafik

Ved at kryptere de informationer, der sendes inden for det trådløse netværk, sikres de mod at hackere, der opsnapper signalerne, umiddelbart kan læse dem. Der findes grundlæggende tre former for kryptering WPA2, WPA og WEP.

WEP står for Wired Equivalent Privacy. Det er en del af 802.11b standarden og understøttes derfor af langt de fleste leverandører.
Der er to varianter af WEP: 64 bit kryptering og 128 bit kryptering. WEP er dog ikke længere sikker, og en bare rimelig god hacker kan bryde den på mindre end et minut. Denne frarådes derfor. Er det eneste niveau dit udstyr kan, bør du investere i mere moderne udstyr.

WPA står for Wi-Fi Protected Access og understøttes primært af 802.11g udstyr. Der eksisterer også 802.11b udstyr, der kan bruge WPA. Med WPA er sikkerheden meget større end ved WEP.

WPA2 er en opdatering af WPA der forbedrer sikkerheden endnu mere. Med andre ord vælg helst WPA2, dernæst WPA, og opgrader dit udstyr hvis det kun kan WEP. Arbejd aldrig uden kryptering.

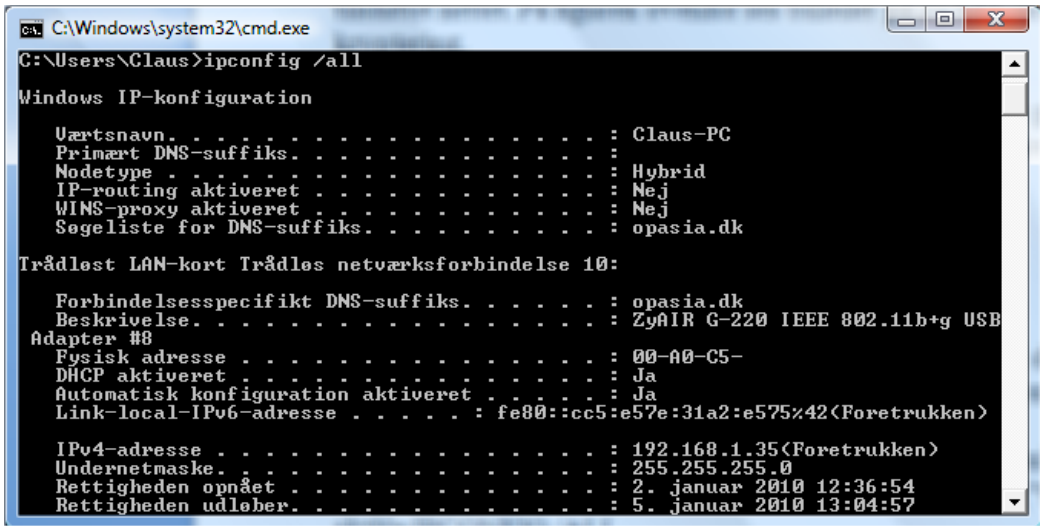
Opsætningen sker ved at der vælges en nøgle (en tekststreng) som anvendes på alle enheder tilsluttet nettet. På figuren ovenfor ses billedet på ZyXEL acces pointet. Her er valgt WPA kryptering.

Bemærk at når du sætter kryptering til, mistes forbindelsen på evt. tilsluttede enheder. De skal jo også lige have besked, ved at opsætte samme kryptering med samme nøgle her.

5. Brug MAC-filtrering

MAC filtrering er en ekstra måde at begrænse adgangen til det trådløse net. Ideen er at routeren kun vil oprette forbindelse til netkort med en ID den er oplyst om i forvejen.

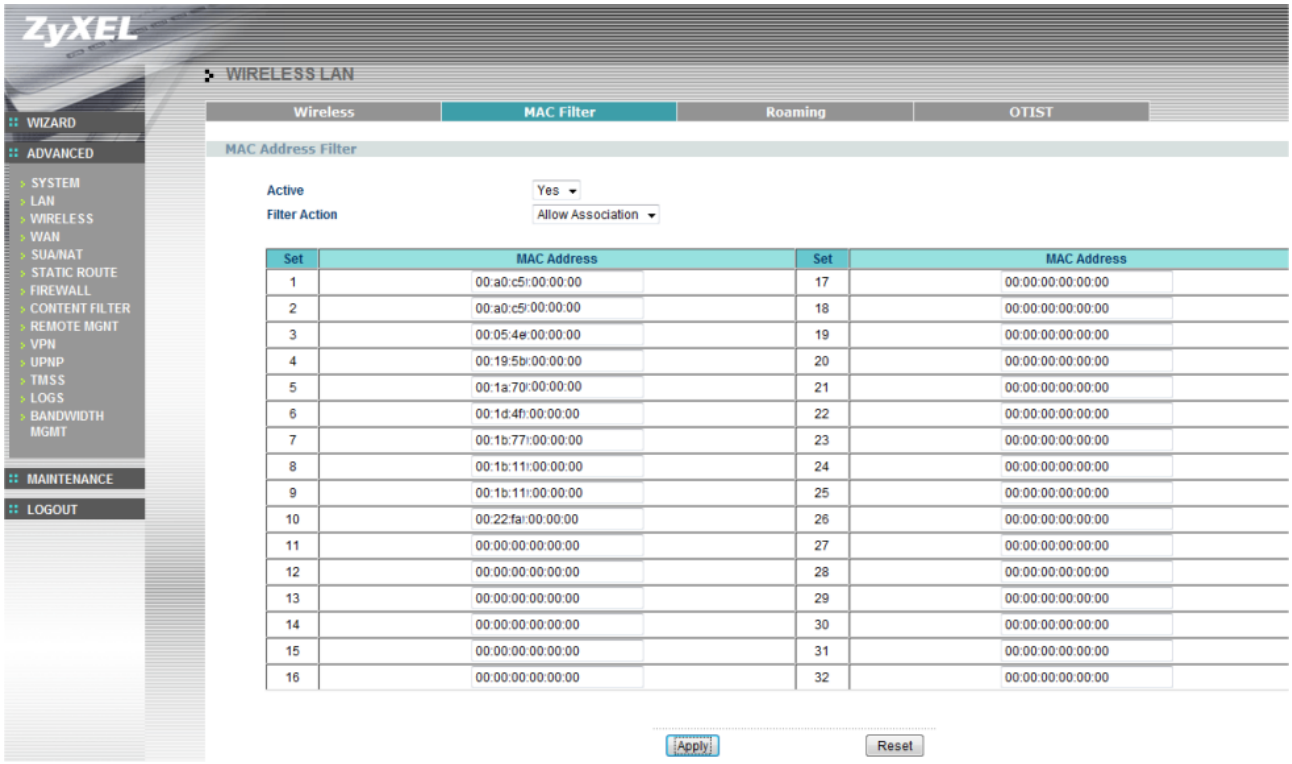
Alle netkort, såvel faste som trådløse, er udstyret med en unik kode, også kaldet MAC adresse. Du kan finde din MAC adresse ved at åbne et terminalvindue (”Start” – ”Kør” – skriv CMD), og her skrive IPCONFIG /ALL. Det ser således ud:



Her kan man se at jeg benytter en ZyAIR G-220 og den har adressen startende med 00-A0-C5…. (jeg har skjult den sidste del her). Normalt har den formen 00:11:66:77:88:99.

Denne ID indsættes så i routernes MAC tabel. Hvordan det ser ud på ZyXEL kan du se nedenfor (igen er sidste del af adresserne skjult).

Når alle adresser fra PC’er der skal have adgang til nettet er indtastet, trykkes ”Apply” og routeren tillader herefter kun forbindelse til disse maskiner.



6. Benyt firewall

Du bør altid have en firewall installeret på alle computere tilsluttet et netværk, men det er specielt vigtigt når det er et trådløst net. Du sikre på den måde at der kun foregår kommunikation du har givet tilladelse til, og får en advarsel, hvis nogen forsøger at kontakte din PC.

7. Hold øje med loggen på dit acces point / firewall

Check med jævne mellemrum loggen på dit acces point og firewall. Her kan du se, hvem, hvad, hvor og hvornår nogen har benyttet dit acces point. En log findes på de fleste udstyrstyper i dag. Det kan hjælpe dig til at se, om der sker ting, der ikke bør.

Mere info?

I så fald kan jeg anbefale at du besøger fabrikanten af dit acces point. De har typisk guider/manualer i opsætning af disse ting liggende. Mange har også uddybende forklaringer af sikkerhedsforhold på deres sites.

Ellers læs IT og Telestyrelsens: http://www.it-borger.dk/