Trådløst LAN – hvordan sikrer man sig?

Trådløse acces points er standarden i dag. Selv TDC leverer et sådant med din bredbånds-forbindelse… ☺

Har man kun én PC og står den i nærheden af routeren, bør den forbindes med kabel. Det giver fortsat den hurtigste og sikreste forbindelse. Men selv her bør man sikre sin router, som beskrevet i det følgende.

Routeren er nemlig ikke sikker når den bliver leveret fra din internetleverandør.

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 med samtlige hemmeligheder incl. passwords), de kan downloade ulovligt materiale (på din IP-adresse – hvem tror du får skylden?) og så videre.

Her er en kort gennemgang af hvad der skal til for at din forbindelse kan karakteriseres som ”sikker”.

1. Wi-Fi standarder

Måske har du lagt mærke til at firmaerne reklamerer med ”WI-FI 6 router” eller ”802.11ac kompatibel”.
Der findes forskellige måder at ”snakke sammen” igennem luften, og dette er standardiseret af IEEE (Institute of Electrical and Electronics Engineers) der er et internationalt organ, der står for standardisering af mange ting indenfor elektronik.

De første standarder for Wi-Fi blev lavet i 1997, og standarden hed IEEE 802.11.

Siden har man udvidet denne standard som vist i tabellen nedenfor.

IEEE standard	**802.11a**	**802.11b**	**802.11g**	**802.11n**	**802.11ac**	**802.11ax**
Udgivet år	1999	1999	2003	2009	2014	2019
Frekvensbånd	5 GHz	2,4 GHz	2,4 GHz	2,4 & 5 GHz	2,4 & 5 GHz	2,4 & 5 GHz
Teoretisk hastighed	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1,3 Gbps	10-12 Gbps
Wi-Fi alliance navn	Wi-Fi 2	Wi-Fi 1	Wi-Fi 3	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6

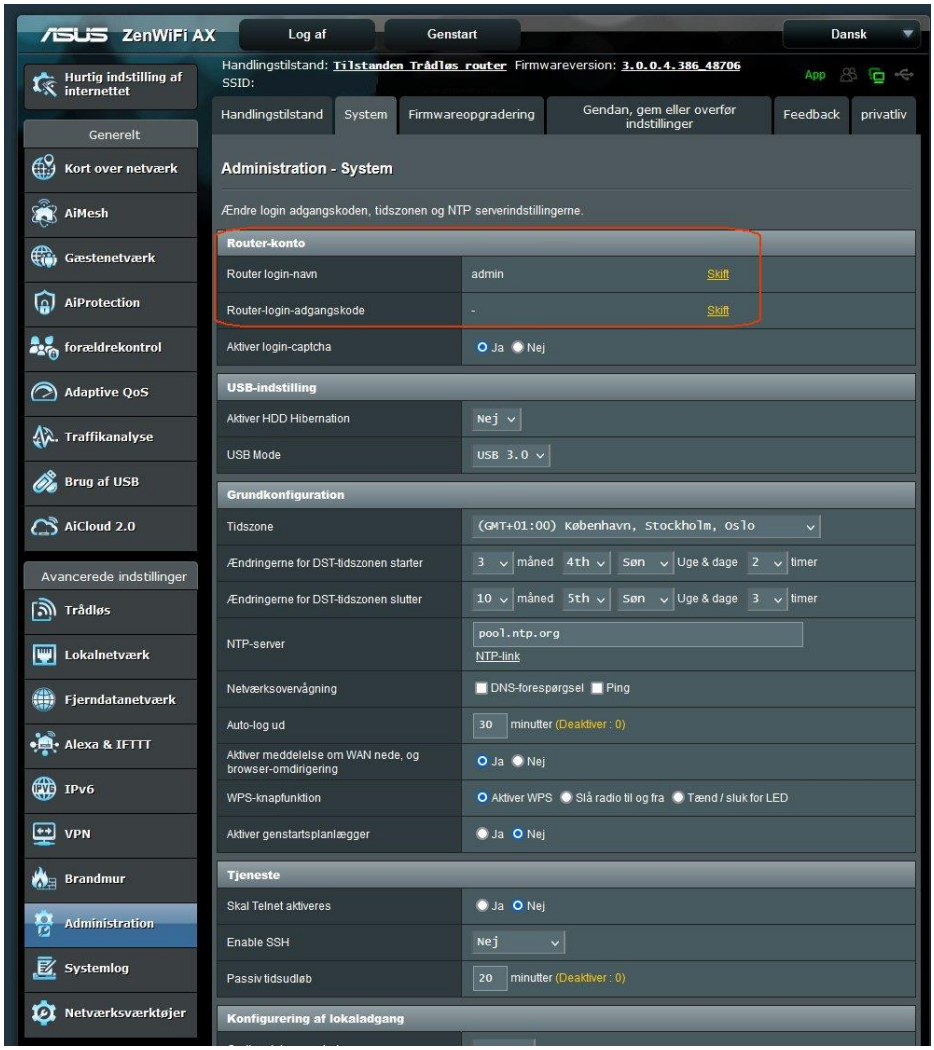
Du bør ikke benytte a – g routere, og skal du købe en ny router i dag, bør det være en ax/Wi-Fi 6 router.

2. Ændre altid dit password på routeren

Der findes to sæt id og password når man taler routere. Et sæt for at logge ind i selve routeren og ændre dens opsætning (det er det dette afsnit beskriver) og et sæt for at koble enheder på selve det trådløse netværk (se afsnit 3 til 5).

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. Nogle gange står det trykt på en label på routeren, og disse er en lille smule sikrere.

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 ASUS ZenWiFi AX router, men andre minder om denne. Her er det ”Administration”, fanebladet ”System” og ”Router konto” som jeg har markeret med den røde ring. Her kan du ændre dit password til noget sikkert (store og små bogstaver, mindst et tal og i alt mere end 8 karakterer). Skriv det ned hvis du ikke er 100% sikker på at kunne huske det.

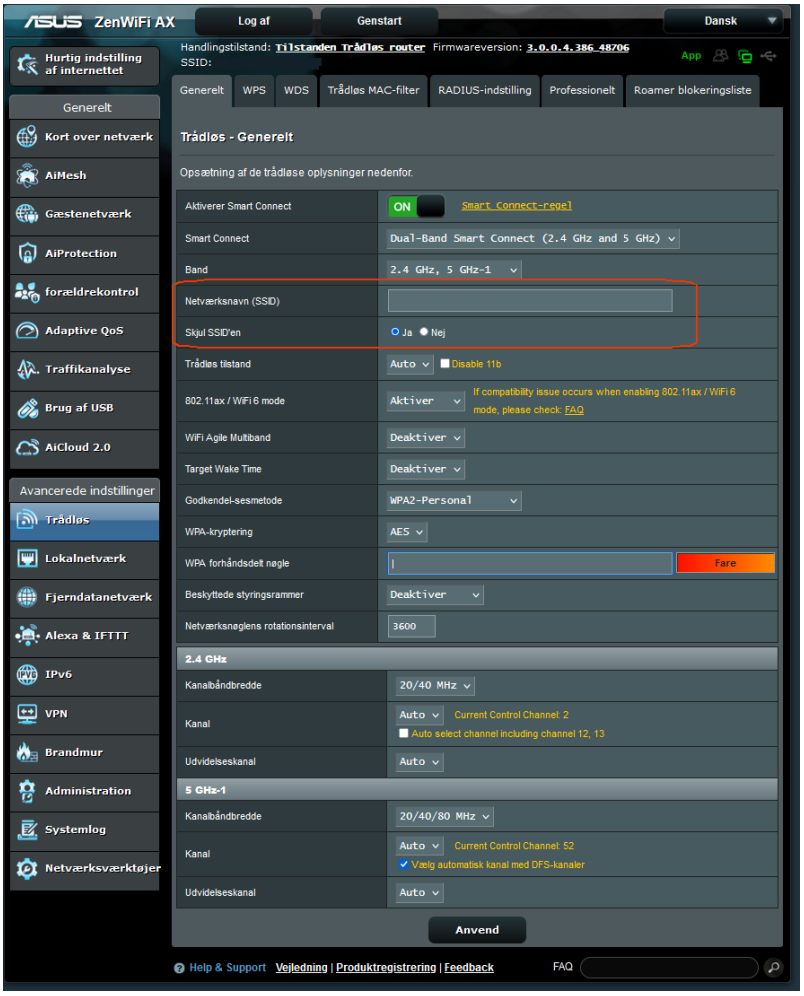


Rent principielt bør alle opsætninger af din router laves via Ethernet kabelforbindelse og ikke via Wi-Fi tilslutning.
Dette for helt at udelukke den mulighed (om end teoretisk) at nogen ”kikker med” på din trådløse forbindelse, specielt inden den er sikret.

3. 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 ASUS er det ”Trådløs” og fanebladet ”Generelt” hvorefter du får nedenstående billede:



Her er det feltet ”Netværksnavn (SSID)” (markeret med en rød ring) der skal rettes. Når du har skiftet navnet ud, trykker du ”Anvend”.

4. 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 ASUS gøres det i samme menu som punkt 3 lige neden under SSID navn (se billede i afsnit 3).

5. 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 noget større end ved WEP.

WPA2 og WPA3 er opdateringer af WPA, der forbedrer sikkerheden endnu mere. Med andre ord vælg helst WPA3, dernæst WPA2, og opgrader dit udstyr hvis det kun kan WPA/WEP. Arbejd aldrig uden kryptering.

Opsætningen sker ved at der vælges en nøgle (en tekststreng) som anvendes på alle enheder tilsluttet nettet. På figuren nedenfor ses billedet på ASUS routeren (markeret med en rød ring. Samme menu som i afsnit 3 – derfor kun et udsnit af billedet). Her er valgt WPA2 kryptering.

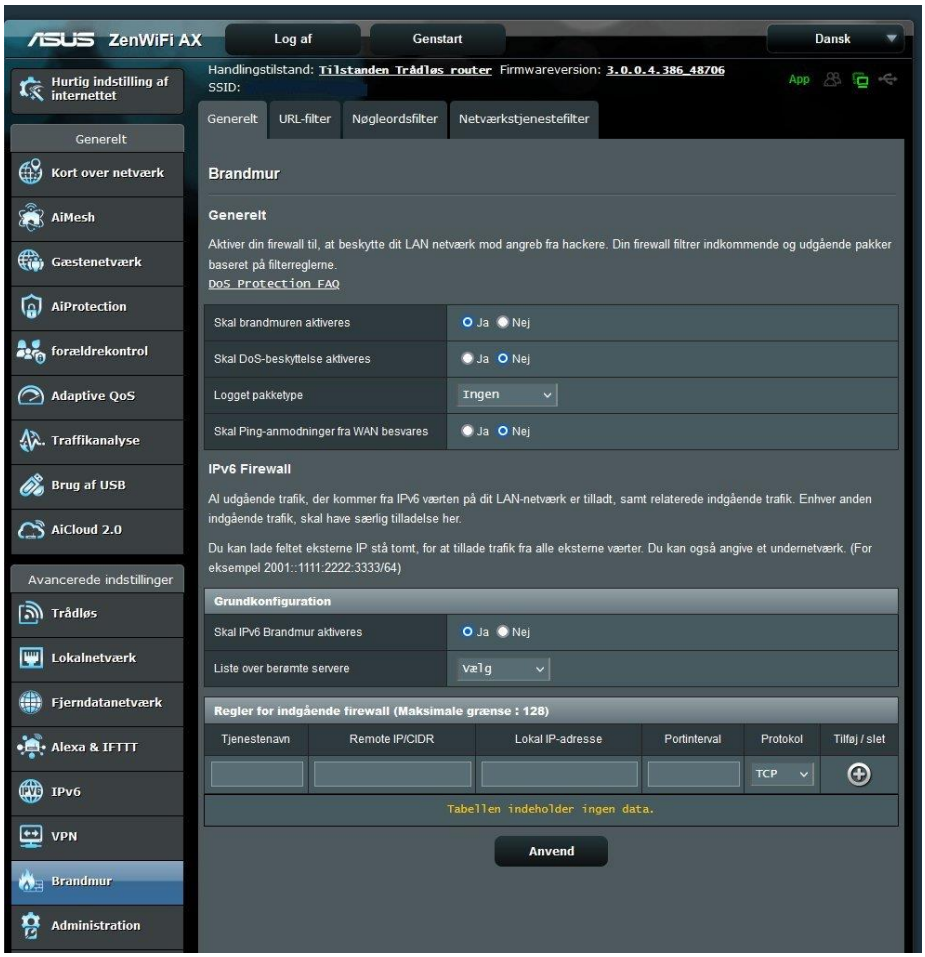
Bemærk at når du sætter kryptering til, mistes forbindelsen på evt. tilsluttede enheder. De skal jo også lige have besked, ved at opsætte samme kryptering med samme nøgle her.

Den opmærksomme vil lægge mærke til at routeren siger ”Fare” ud for nøglen. Det er fordi jeg har slettet den her, da jeg naturligvis ikke vil vise den her. Men det smarte er, at routeren fortæller dig hvor sikker den valgte nøgle er. Sørg for at den er kompliceret nok, og at du kan huske den !

6. Benyt firewall

De fleste routere har en indbygget firewall. Denne bør aktiveres. Den frasorterer det meste uvelkomne skidt der kommer fra nettet.

På ASUS gøres det under ”Brandmur” og fanebladet ”Generelt”. Aktiver den og tryk ”Anvend”.



Ud over en firewall i routeren, bør du naturligvis have en på PC’en, som en del af den sikkerhedspakke du har installeret.

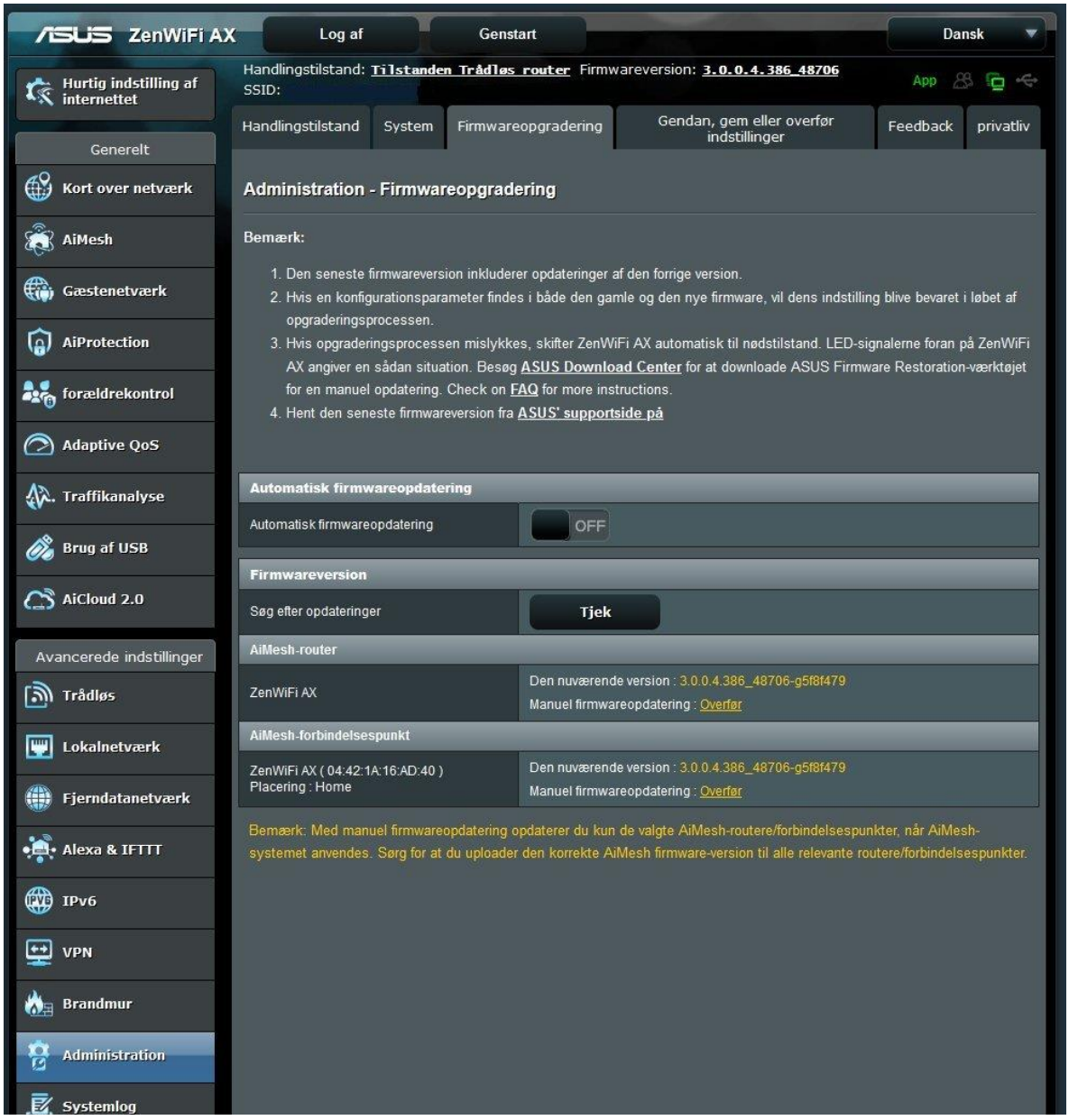
7. Hold øje med loggen på din router / firewall

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

8. Opdater firmware

Ligesom Windows styrer din PC, så har routeren også et styresystem, der skal holdes opdateret. Det kaldes opdatering af firmware.

På ASUS er det under ”Administration” og fanebladet ”Firmware opgradering”. Vælg knappen ”Tjek” midt på siden, og opdater hvis der er nye versioner. Routeren gør det selv, og det tager typisk nogle minutter, hvorefter den starter igen.



Mere info?

I så fald kan jeg anbefale at du besøger fabrikanten af din router. 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/