# Hjemme-router (del2).

Det er stor forskjell på de forskjellige hjemme-routerne. Noen er helt enkle og inneholder kun de mest grunnleggende funksjonene, mens andre kan inneholde mange flere funksjoner. Jeg skal her nevne noen av disse funksjonene, og litt av hva de gjør.

**WAN**
WAN-siden settes opp med DHCP, eller Static. Bruker du DHCP vil hjemme-routeren hente nettparametre fra ISP, ved oppstart. Bruker du Static må du skrive inn alle nettparametre selv.

**DHCP**
Denne funksjonen er grunnleggende. Den gir ut nettparametre til hosts som kobler seg til på ditt private LAN.
Denne kan settes opp med hvilken privat IP område som du velger, og hvilke private IP adresser som den skal dele ut fra. Den kan også settes opp med å gi en host, med en gitt MAC adresse, en bestemt privat IP adresse.

**NAT**
Denne funksjonen er grunnleggende. Den oversetter IP adresser på ditt private LAN til den IP adressen som du har fått fra ISP.

**Port forward**
Denne funksjonen er grunnleggende. Den gjør at en pakke, som kommer inn fra internet, med et bestemt portnummer, vil sendes til en bestemt host på ditt private LAN. Dette må du sette opp i hjemme-routeren. Du bestemmer hvilke portnummer som skal sendes videre til en bestemt privat IP adresse, med et valgt portnummer. Veldig ofte vil du velge samme portnummer inn, som det som sendes videre. Det er da viktig at den private IP adressen alltid blir gitt til den host, fra DHCP.

**Dynamic DNS**
Dette er en tjeneste du kan abonnere på, fra en aktør som tilbyr Dynamic DNS. Hvis du har et domenenavn, så må den knyttes opp mot en bestemt IP adresse. Hvis din hjemme-router får en ny IP adresse fra din ISP, må ditt domenenavn knyttes opp mot den nye IP adressen. Hjemme-routeren vil oppdage om den har fått en ny IP adresse fra ISP, og sende den nye IP adressen til den som tilbyr Dyn DNS. Den oppdaterer da din nye IP adresse til ditt domenenavn automatisk.

**WiFi**
Du aller fleste hjemme-routere tilbyr en hosts å koble seg til trådløst, via WiFi. I hjemme-routeren må du gi WiFi-nettet et navn (SSID), som er synlig for host som skal koble seg på. Du kan også velge hvilke WiFi standarder den skal dekke. Kanskje det aller viktigste du må sette opp er hvilken sikkerhet det trådløse nettet skal ha. Den beste er WPA3 (WiFi Protected Access), som kom i 2018. Det er nok ikke alle host som har den (enda). Du kan velge WPA2, som kom i 2006. WPA går også, men den er

dårligere. Den kom i 2004. WEP (Wired Equivalent Privacy)  er enda dårligere. Den kom i 1997.  Den aller dårligste er Open, - da er det ingen sikkerhet overhode.

Velg også AES (Advanced Encryption Standard)
PSK står for Pre-Shared-Key.

**VLAN**
Noen hjemme-routere kan sette opp VLAN på de forskjellige tilkoblingene (port).

**IPv6**
IPv6 begynner å komme hos hjemme-routere.

**DMZ**
**D**e**M**ilitarized **Z**one kan settes på en del av ditt private LAN. Der vil host som skal kunne aksesseres fra internet plasseres. Resten av ditt private LAN vil da være bedre «beskyttet».

**WMM**
WiFi MultiMedia er for å definere QoS (Quality of Service) i WiFi nett. Dette er for multimedia (lyd, video etc), slik at dette får bedre aksess.

**WPS**
WiFi Protected Setup er ofte implementert som en knapp på hjemme-routeren (eller en funksjon du kan aktivere i meny). Når du trykker på den vil du kunne koble til host uten å måtte skrive inn passord. Den muligheten blir borte så fort **en** host har koblet seg til. Hvis ingen host har koblet seg til i løpet av et par minutter, vil funksjonen slås av. Ulempen er jo selvsagt at andre (ukjente) kan koble seg på. Du må også ha WPS funksjonen på den host som skal koble til WiFi nettverket.  –  WPS kan også bruke PIN. Den skal eksistere, selv om det ikke er sikkert.