eStudie.no – presenterer:

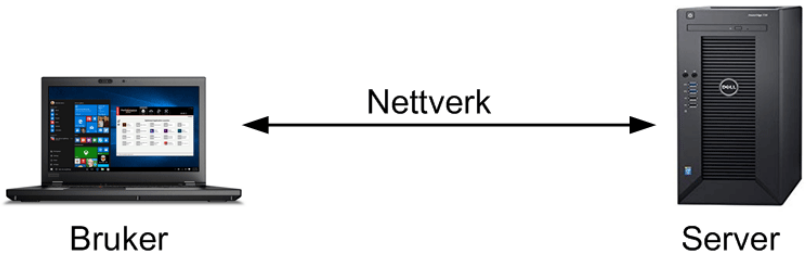
Datanettverk

... basert på TCP/IP protokollen

Skrevet av: Kjetil Sander © August 2020

Innholdsfortegnelse

1 Datanettverk

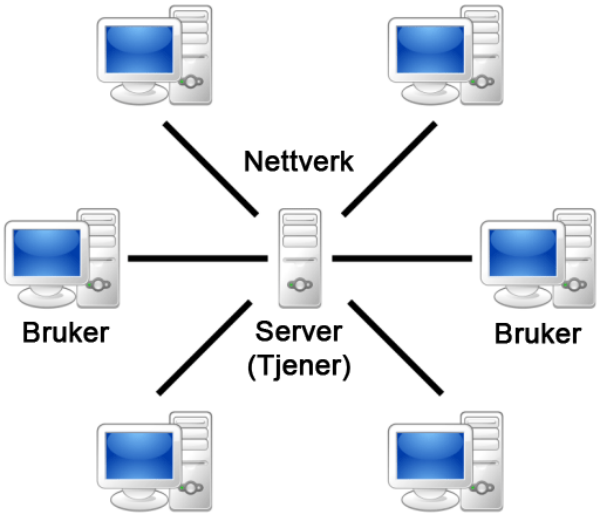


1.1 Hva er et datanettverk?

Et **datanettverk** er:

> ***"Et digitalt nettverk som kobler sammen alle brukerne i dette nettverket via en nettverktjener (nettverksserver)"***

Et typisk nettverk ser slik ut:



Som det går frem av illustrasjonen over er et nettverk et datanettverk som kobler sammen ulike datamaskiner, printere, scannere, kassaapparater o.l. utstyr til hverandre via switcher og routere og en nettverkskabel eller trådløse signaler.

1.2 Nettverkets oppgave

Nettverkets oppgave er å knytte sammen alle brukerne i nettverket til en server (tjener) slik at partene kan utveksle informasjon over nettverket.

1.3 Åpne og lukket nettverk

Et nettverk kan enten være åpent eller lukket. Forskjellen kan forklares slik:

- **Åpent nettverk** – et nettverk som alle kan koble seg på
- **Lukket nettverk** – et nettverk som kun noen utvalgte brukere og servere kan benytte for å utveksle informasjon

Internett er et eksempel på et åpent nettverk som alle kan koble seg på, mens et LAN-nettverk som knytter sammen datamaskinene til et selskap er et lukket nettverk.

1.4 TCP/IP nettverk

Det nettverket de fleste av oss vil forholde oss til er TCP/IP nettverket som idag er den vanligste protokollen (standarden) å bygge ett nettverk opp på. Her for alle enhetene som kobler seg på nettet utdelt en IP-adresse som identifiserer hvem de er og hvor kommunikasjonen mellom disse IP-adressene skjer via TCP-protokollen. Derav navnet TCP/IP nettverk.

Et TCP/IP nettverk kan enten være åpent eller lukket, eller en mellomting. Når vi snakker om TCP/IP nettverk skiller vi derfor mellom:

1. **Internett** - det åpne TCP/IP nettverket som alle med Internett forbindelse kan koble seg på.
2. **Intranett** - et lukket TCP/IP nettverk som er stengt for omverden og som kun dem som fysisk er koblet opp mot dette nettverket kan benytte
3. **Ekstranett** - en hydrid løsning, hvor brukeren må logge seg på med et unikt brukernavn og passord via Internett for å få tilgang til det lukkede nettverket på baksiden.

1.5 Kabellnettverk og trådløse (WI-FI) nettverk

Det fysiske nettverket kan enten være et kabelnettverk eller et trådløst nettverk. Forskjellen er:

1. **Kabelnettverk:** Et fysisk nettverk hvor datamaskinene i nettverket er koblet sammen via en ethernet kabel som går til en hub, switch eller router. Ethrnet kabelen som benyttes kalles kategori 5 kabel/plugg.
2. **Trådløst nettverk:** Et fysisk nettverk uten kabler, hvor all kommunikasjon skjer trådløst etter at brukeren har koblet seg på nettverket via en trådløs router.

Selv om de trådløse nettverkene har mange åpenbare fordeler ved at de ikke krever noen kablel tilknytning har trådløse nettverk også klare svakheter i forhold til kabelnettverk som fortsatt både er raskere og tryggere enn trådløse nettverk.

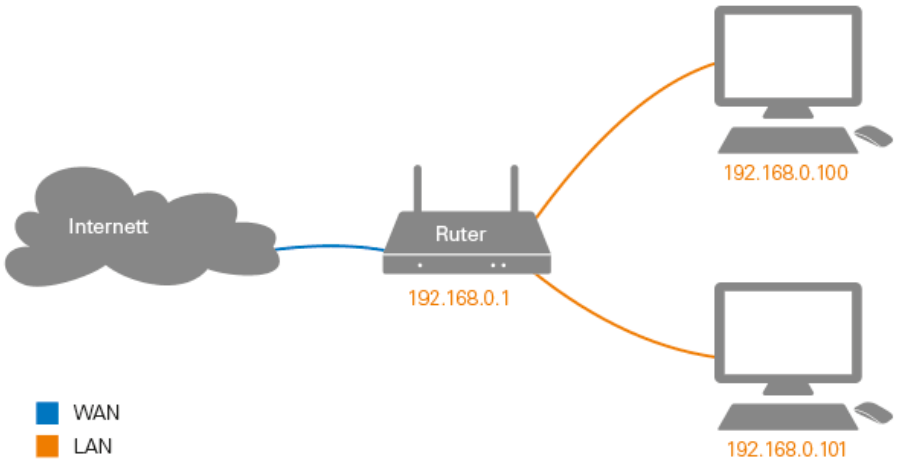
1.6 Lokalt datanett (LAN)

LAN står for *local area network* og er et **lukket lokalt datanettverk** som er geografisk begrenset, for eksempel begrenset til en bolig, et kontor eller en liten gruppe bygninger.

Et LAN nettverk er det motsatte av WAN nettverk som dekker et "stort område nettverk" eller "Wide Area Nettwork" som det heter på engelsk. Jo flere maskiner som skal kobles sammen, jo større blir også kravene til LAN-nettverket.

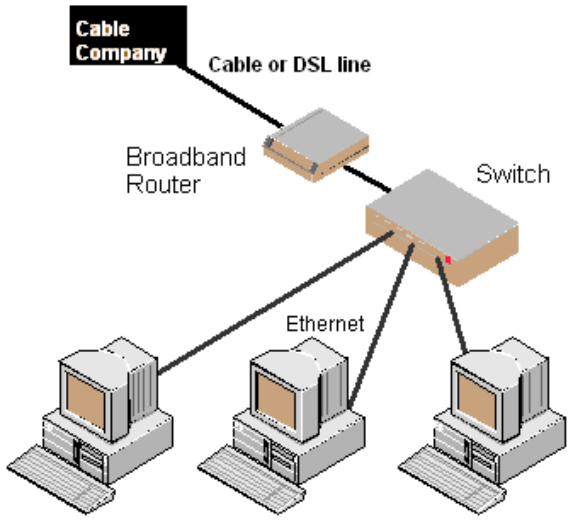
1.7 Ruter (router)

En **router** er koblingsboksen mellom LAN nettverket (nettverket på innsiden av bygningen) og Internett (WAN). Denne routeren leveres ofte fra linjeleverandøren, da den styrer tilkoblingen til Internett. Som regel inneholder også denne routeren en brannmur du kan sette opp for å hindre uønsket tilgang til ditt nettverk.



Ruteren har en funksjon som kalles **NAT (Network Address Translation)**. En funksjon som gjør det mulig å koble flere enheter til Internett enn antallet mulige IPv4-adresser tilsier. Ved hjelp av NAT oppretter ruteren et eget LAN-nettverk som den er leverandør for. Når datamaskiner senere bruker DHCP for å be om IP-adresser, tildeles de IP-adresser av ruteren (i stedet for av Internett-leverandøren).

Disse IP-adressene begynner vanligvis på 192.168.0. eller 192.168.1. Ruteren kan for eksempel gi en tilkoblet datamaskin IP-adressen 192.168.0.100 og 192.168.0.101 til en annen tilkoblet datamaskin. Rundt om i verden finnes det nesten et uendelig mange datamaskiner som har disse IP-adressene. Likevel oppstår det ingen IP-adressekonflikter. Datamaskinene har nemlig bare disse IP-adressene i sine respektive lokale nettverk. Når de går ut på Internett, er det ruterens IP-adresse som brukes.



1.8 Switch

En **switch** er en koblingsboks som kobler sammen ulike datamaskiner via en Ethernet kabel. En switch kan dermed sammenlignes med skjøteledningen vi bruker når vi trenger flere stikkontakter. Switcher finnes i ulike størrelser og hastigheter. Størrelsen angis i form av porter og angir hvor mange kategori 5 datakabler som kan kobles inn i koblingsboksen. Hastigheten angir i form av antall megabite per sekund. Å sette dem opp er enkelt. Krever ingen konfigurasjon av noe slag. Det er bare å plugge inn Ethernet kablene i switchen.

1.9 Nettverks printere

Har virksomheten et kontor e.l. hvor flere sitter på hver sine maskin, er det hensiktmessig å sette opp en nettverksprinter som alle kan dele. Dette sparer virksomheten for penger, da de ansatte ikke trenger hver sin skriver. En nettverksprinter koblet til nettverket via en ethernet kabel til en switch og fungerer på samme måte som en personlig skriver. Prisen er heller ikke nevneverdig større.

1.10 Andre nettverk ressurser

Hvilke andre nettverk ressurser som det kan være hensiktsmessig å investere i, er avhengig av virksomhetens størrelse og virksomhetsfelt. Skannere er eksempel på en annen nettverks ressurs som mange velger å sette opp som en felles nettverk ressurs. Kanskje en kombinasjonsenhet, med kopimaskin og skanner i en og samme maskin. Felles for alle slike nettverksressurser er at de kobles til nettverket via en ethernet kabel som plugges inn i nærmeste switch. Deretter tildeler DHCP serveren denne enheten med en IP-adresse som deles på nettverket og som gjør det mulig for alle brukerne av nettverket å finne og koble seg på denne nettverksressursen.

1.11 Nettverkshastighet (linjehastighet)

Hvor raskt et datanettverk er avhenger av mange forhold, men den vil uansett aldri bli større en hastigheten til det tregeste leddet i nettverket. Ønsker du f.eks. å sette opp et eget LAN-nettverk på jobben eller hjemmet hvor alt som skjer skal skje med en hastighet på 1 GB/sek må du forsikre deg om:

- **Ethernet kabelene**: Alle ethernet kablene må være feilfrie, da den minste kabelfeil kan dramatisk redusere hastigheten
- **Nettverkskortene**: Alle enhetene som kobles på nettverket må ha et nettverkskort som støtter 1 GB/sek. Støtter det kun 400 mb/sek blir den reelle hastigheten aldri større enn 400 mb/sek, selv om du skulle oppfylle alle andre vilkår.
- **Switchen**: Alle switcher på nettverket må støtte en hastighet på 1 GB/sek for å kunne formidle signalene med denne hastigheten
- **Routeren**: Routeren som tildeler IP-adressen til alle enhetene og kobler dem på Internett ved behov må også støtte en båndbreddehastighet på 1 GB/sek for at hastigheten faktisk skal bli 1 GB/sek.
- **Maskinressurser**: Maskinen som skal produsere signalene som skal distribueres med en hastighet på 1 GB/sek må ha tilstrekkelig med ressurser for å klare å produsere resultatet så fort linjen tåler å sende dem. Er harddisken, minne eller prosessoren ikke rask nok blir linjen stående ubrukt å vente på signalene fra maskinen.

Punktene over er avgjørende for den effektive nettverkshastigheten på et LAN nettverk og er forhold vi selv har god kontroll over og som vi enkelt selv kan gjøre noe med. Fult å enkelt er det ikke når vi skal koble dette LAN-nettverket opp mot noe på Internett, dvs. et åpent nettverk. Skal vi koble LAN-nettverkt vårt mot nettskytjenesten vi leier fra en av de store nettskyleverandørene er det helt andre forhold som avgjør linjehastigheten vår.

Her må vi ta hensyn til og tenke på:

- **Vår egen linjehastighet**: Ønsker vi å koble oss mot en nettsky med en linjehastighet på 100 mb/sek må vi starte med å forsikre oss om at linjeleverandøren vi har valgt tilbyr oss denne linjehastigheten. Har vi ikke denne hastigheten idag, må vi starte med å oppgradere hastigheten til ønsket hastighet.
- **Linjetype**: Dernest må vi ta hensyn til hva slags nett vi selv prøver å få tilgang til tjenesten på. Kobler du deg opp mot tjenesten via arbeidsstasjonen som er koblet til Internett får du normalt en langt høyere linjehastighet enn hvis du kobler deg opp via mobilnettverket som kjører på 3G eller 4G. De er vesentlig tregere enn bredbåndet ditt.
- **Avstand og antall sub-net**: Som om dette ikke var nok, må vi ta hensyn til hvor langt det er til nettressursen og hvor mange sub-net signalene må bevege seg igjennom for å komme frem. Jo lengre avstanden er og jo flere sub-net signalene må gå igjennom før de kommer frem jo lengre tid tar det og jo flere potensielle hastighetsdrepere kan være innblandet.

1.12 Kryptert (SSL) og ukryptert linje

Foruten hastigheten til nettverket er det viktig å tenke på nettverksikkerheten. Spesielt når vi snakker om Internett og Ekstranett løsninger. På slike nettverk bør signalene mellom tjeneren (serveren) og brukerne ikke skje på ukrypterte linjer. Dette fordi andre her kan sette opp lytteposter på nettverket som gjør at de kan snappe opp alt som sendes over nettverket i form av en kopi av innholdet.

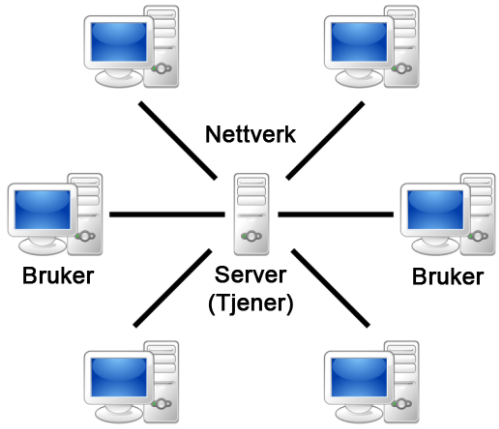
For å unngå at dette kan skje bør all kommunikasjon skje på en kryptert linje mellom brukeren og serveren. For å få satt opp en kryptert linje må vi installere et SSL-sertifikat på serveren. SSL er en forkortelse for Secure Socet Layer.

2 Arbeidsstasjon (Klient)

2.1 Hva er en arbeidsstasjon?

En **arbeidsstasjon**, også kalt **klient** i et datanettverk, er en personlig datamaskin som er laget for å være en digital arbeidsplass. Normalt er arbeidsstasjonene knyttet sammen gjennom et LAN nettverk. En nettverk som knytter alle arbeidsstasjonene på en arbeidsplass sammen til en eller flere nettverksservere som gjør det mulig for alle i nettverket å dele informasjonen seg imellom.

Arbeidsstasjonens rolle i dette nettverket kan illustreres slik:



Arbeidsstasjonene i dette nettverket er i illustrasjonen kalt brukere.

2.2 Arbeidsstasjonens grunnkomponenter

En arbeidsstasjon består normalt av:

- **Kabinett**: Den fysiske boksen som er selve datamaskinen som alt utstyret til arbeidsstasjonen er knyttet til
- **Skjerm**: En skjerm brukeren kan se på for å bruke arbeidsstasjonen (output enhet).
- **Tastatur og mus:** Normalt styres arbeidsstasjonen av brukeren gjennom å bruke et tastatur og en mus som input enheter.
- **Programvare**: For å kunne bruke datamaskinen til noe må det installeres et operativsystem på maskinen og de programmene man ønsker å bruke.

Denne arbeidsstasjonen kan så utvides med f.eks.:

- **Nettverkskort**: Et kretskort plassert i kabinettet på hovedkortet som gjør det mulig å knytte arbeidsstasjonen til et nettverk gjennom en ethernet kabel eller trådløs forbindelse.
- **Printer**: En personlig eller nettverkskriver som kobles til arbeidsstasjonen eller nettverket arbeidsstasjonen er en del av.
- **Skanner**: En skanner kan også kobles direkte til arbeidsstasjonen eller til nettverket arbeidsstasjonen er en del av som en nettverkressurs.

2.3 Arbeidsstasjonens oppbygning

En arbeidsstasjon er normalt en stasjonær datamaskin som alle kan bygge selv hvis de vil. Å bygge en stasjonær datamaskin er faktisk så enkelt at omtrent alle som ikke er redd for å lese en bruksanvisning kan gjøre. Dette er mulig fordi alle datamaskiner er bygd opp rundt den samme ISA standarden som ble etablert allerede på 80-tallet.

Alle stasjonære arbeidsstasjoner (datamaskiner) er i prinsippet bygd opp likt og består av følgende komponenter.

2.3.1 Kabinett

Skal vi bygge en datamaskin starter byggingen med at vi velger et kabinett som skal huse datamaskinen vi skal bygge. Kabinettet er laget i plastikk og finnes i mange ulike størrelser og design.

Når vi skal velge kabinett til datamaskinen må vi starte med å sørge for at kabinettet er stort nok til å huse det hovedkortet og tilleggskortene vi ønsker å benytte. Ønsker vi å sette inn 5 tilleggskort, må kabinettet også ha 5 ledige kortplasser på baksiden av kabinettet.

Alle hovedkortene er bygd opp rundt de samme standardene. Noe som gjør at hovedkortets skruefester alltid passer i kabinettet, hvis kabinettet støtter hovedkortstørrelsen du har valgt.

Strømforsyningen til datamaskinen (arbeidsstasjonen) er også standardisert slik at det er mulig å sette inn minst en strømforsyning i alle kabinett. Ønsker du å sette inn flere strømforsyninger for å få en redudant løsning eller nok strøm til å drive alle kortene må du sørge for at kabinettet støtter flere enn 1 strømforsyning.

Dernest er vi opptatt av hvor mange vifter det er mulig å sette inn i kabinettet for å sikre tilstrekkelig kjøling til datamaskinen og hvordan kabinettet ellers er utformet for å sikre en god luftgjennomstrømning. Viftene kobles til datamaskinen via egne kabler som går til hovedkortets angitt viftekoblinger.

2.3.2 Strømforsyning

For at datamaskinen skal virke trenger den strøm. Vi må derfor kjøpe en strømforsyning som vi monterer på en fast plass i kabinettet. Disse strømforsyningene har et standard design slik at de passer inn i alle kabinett. Det eneste du må ta stilling til er hvor sterk strømforsyning du trenger. Jo flere kort du ønsker å sette inn i maskinen og jo kraftigere grafikkort du ønsker å benytte jo større strømforsyning trenger du. Det samme gjelder for antall harddisker, dvd-spillere o.s.v.

Styrken på strømforsyningen angis i watt og de inneholder alle standard strømtilkobling til sett som kobles til hovedkortet for å gi strøm til alle datamaskinens komponenter.

2.3.3 Hovedkort

Hovedkortet er selve grunnmuren til en datamaskin (arbeidsstasjon). Hovedkortet er et stort trykt kretskort som skrues fast i kabinettet og som inneholder spor for alle tilleggskortene til datamaskinen, samt soketter for hovedkortets CPU og minne.

Alle datamaskiner (arbeidsstasjoner) starter derfor med at vi skrur fast hovedkortet i kabinettet og kobler det til strømforsyningen i kabinettet med bruk av en standard tilkobling.

Når dette er på plass kan vi fortsette byggingen av det som skal bli en datamaskin.

2.3.4 CPU

En CPU er en prosessor som gjør alle operasjonene til datamaskinen (arbeidsstasjonen). Prosessoren er dermed selve motoren i datamaskinen. Jo større den er, jo raskere klarer den å utføre operasjonen den er satt til å gjøre. CPUen anses derfor som en av de mest kritiske komponentene i en datamaskin og er av samme grunn også en av de dyreste enkeltkomponentene.

Ulike CPUer benytter ulike sokketter. Skal vi bygge en datamaskin må vi derfor forsikre oss om at hovedkortet vi har valgt støtter den CPU soketten vi ønsker å benytte.

Normalt gir et hovedkort kun muligheten til å sette inn en CPU, men noen hovedkort har også støtte for flere CPU-er. F.eks. gjelder dette hovedkort som er ment for å bygge servere. Ønsker du å sette inn flere fysiske CPU-er må du velge et hovedkort som støtter dette antallet og som har den rette CPU soketten.

Siden CPUen er motoren som gjør alle oppgavene datamaskinen blir bedt om utsettes den for enorme belastninger. Den blir derfor ekstremt varm når den brukes for full. For å unngå at CPUen brenner opp må vi montere en CPU-vifte på toppen av CPU-en vi setter inn på hovedkortet. Denne viften føler normalt med CPU-en når du kjøper den.

2.3.5 Minne (RAM)

For å unngå at datamaskinen (arbeidsstasjonen) konstant skal måtte lese og skrive til harddisken har alle datamaskiner et internt minne, også kalt RAM, som lagrer all informasjon datamaskinen bruker midlertidig. Dette gjør maskinen vesentlig raskere i forhold til om den konstant skulle lese fra og skrive til en harddisk.

Vi kan dermed si at jo mer minne datamaskinen har, jo raskere blir den også. Hastigheten til minne oppgis i HTZ, mens størrelsen oppgis i MB eller GB.

Minnet finnes i ulike typer, hastigheter og moduler. Hvor mye minne det er mulig å sette inn i en datamaskin avgjøres av hvor mange sokets hovedkortet har for minnene og hvilke minnetyper det støtter. Dette må derfor sjekkes før man velger hvor mye og hvilken ram man skal velge.

Minnet monteres i faste sokets på hovedkortet med å klikke minnebrikkene på plass forsiktig til de går i lås.

2.3.6 Harddisk og harddiskkontroller

For å kunne installere programmer på arbeidsstasjonen og lagre dataene vi generer trenger vi en eller flere harddisker i datamaskinen. Harddisken er lagringsplater som det er mulig å lagre enorme menger data på og som skrus fast i egne fester i kabinnettet og som kobles til datamaskinen via en harddisk kontroller som er montert på hovedkortet.

Hvor mange harddisker det er mulig å putte inn i datamaskinen avgjøres dermed av harddisk kontrolleren til hovedkortet og er noe du bør undersøke før du kjøper hovedkortet. Kontrolleren avgjør også hvilke typer harddisker du kan sette inn og hvordan du kan konfigurere harddiskene. Det er derfor viktig å bruke litt tid på også dette.

2.3.7 Grafikk kort (skjermkort)

For at det skal være mulig å se noen bilde på datamaskinen trenger arbeidsstasjonen et grafikk kort, også kalt skjermkort, som produserer disse bildene og videoene.

Grafikk kortene er et standardisert tilleggskort som settes rett i et ledig sport på hovedkortet med kortutgang mot baksiden av kabinettet.

Mange hovedkort har idag dette skjermkortet integrert som en del av hovedkortet slik at man slipper å kjøpe et eget grafikk kort.

For mange brukere, spesielt gamere, er skjermkortet noe av det viktigste de velger. Dette fordi dette avgjør hvor høy oppløsning du kan vise på skjermen, hvor mange pixler og farger du kan se på skjermen og hvor raskt spillet er.

Baksiden av grafikk kortet inneholder utganger for 1 eller flere skjermer som kobles direkte til dette grafikk kortet.

2.3.8 Lydkort

Ønsker du i tillegg å kunne spille av lyd på datamaskinen (arbeidsstasjonen) trenger du i tillegg et lydkort som generer denne lyden. Også dette er et standard tilleggskort som monteres i et ledig spor på hovedkortet. Mange hovedkort har idag et innebygd lydkort slik at man slipper å kjøpe et eget lydkort til maskinen.

Lydkortet inneholder plugger på baksiden av kabinettet for å ta ut lyd til høytallere eller plugge inn en mikrofon.

2.3.9 Nettverkskort

Det siste standardkortet som inngår i de fleste stasjonære datamaskiner (arbeidsstasjoner) er et nettverkskort som gjør det mulig å koble datamaskinen til et nettverk. F.eks. et LAN-nettverk eller Internett. Også dette er et standardkort som settes inn i et ledig spor på hovedkortet eller som følger med som en integrert del av hovedkortet.

2.3.10 Drivere

Når vi har koblet sammen alle komponentene over har vi i utgangspunktet bygd datamaskinen (arbeidsstasjonen) ferdig, men før vi kan få den til å virke må vi samtidig installere driverne til alle komponentene vi har satt inn i datamaskinen.

En driver er et lite dataprogram som utvikleren av en datakomponent har laget for å fortelle operativsystemet datamaskinen benytter hvordan denne datakomponenten virker. Først når du har installert driveren for nettverkskortet vil nettverkskortet virke. Det samme gjelder også for alle de andre komponentene du har installert.

3 Nettverksserver (Tjener)

Du skal ikke ha jobbet mye med IT før du dukker borti begrepene nettverksserver, server og tjener, men hva er egentlig forskjellen mellom disse begrepene?

3.1 Hva er en tjener, server og nettverksserver?

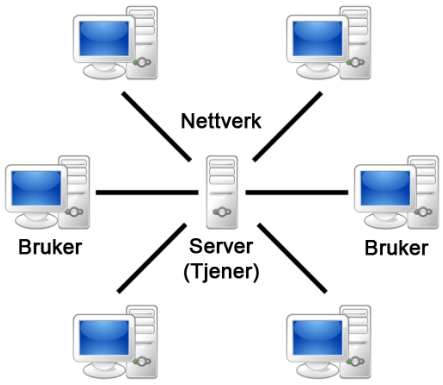
Kjært barn har mange navn, sies det. Dette gjelder i aller høyeste grad her, da en tjener, server og nettverksserver er tre begrep som betyr det samme.

En **nettverksserver** er:

> ***"kraftige datamaskiner som er satt opp til å serve en eller flere tjenester til alle brukerne av et datanettverk".***

Begrepet **server** kan også defineres som:

> ***"store felles datamaskiner som har som mål å lagre, finne, prosessere og presentere store mengder data for hundrevis hvis ikke tusenvis av brukere"***



En server er med andre ord en stor datamaskin som har som oppgave å betjene brukerne som er koblet til denne serveren med en eller flere tjenester over et nettverk. Siden serveren som fungerer som en tjener for brukerne som er koblet til serveren via et nettverk kaller vi gjerne serveren for nettverksserver.

3.2 En maskinvare- og programvareplattform

Når vi snakker om servere snakker vi om både maskinvaren og programvaren denne datamaskinen benytter seg av. Når vi snakker om servere må vi derfor skille mellom servere som:

1. **Maskinvareplattform** - Hardwaren datamaskinen vi kaller en server benytter.
2. **Programvareplattform** - Programvaren datamaskinen vi kaller en server benytter

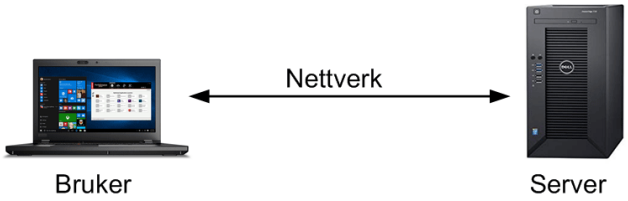
3.3 Serverplattform

Når vi snakker om servere som programvareplattform må vi først starte med å velge hvilken serverplattform vi ønsker å kjøre serveren på. I de siste 20 årene har det gått et grovskille mellom:

- **Linux servere**: Linux er den dominerende serverplattformen idag. På Internett er over 60% av alle serverne en Linux basert serverplattform. At serveren er Linux basert vil si at serveren kjører på et Linux basert operativsystem. Linux plattformens popularitet skyldes ikke bare at den er basert på åpen kildekode og er gratis, men også fordi den er mer skalerbar, fleksibel og sikker enn de øvrige plattformene. For å kunne velge en Linux plattform må man forsikre seg om at programvaren som skal kjøres på serveren er laget for Linux.
- **Windows servere**: Windows servere er serverplattformen til Microsoft og har den fordelen at den er sømløst integrert med Microsoft sine øvrige programvarer, f.eks. Office og Outlook. Denne plattformen benyttes idag av under 18% av verdens servere.
- **Andre servere**: Foruten disse to hovedplattformene finnes det en mengde andre serverplattformer, men de utgjør ennå under 20% av markedet.

3.4 Krever et nettverk

For at en nettversserver skal virke kreves det at så vel serveren som brukerne er koblet sammen i et felles nettverk som signalene mellom serveren og brukeren sendes over.



Nettverkets oppgave er å knytte sammen alle brukerne til en server slik at partene kan utveksle informasjon over nettverket. Dette nettverket kan være:

- **Åpent nettverk** - et nettverk som alle kan koble seg på
- **Lukket nettverk** - et nettverk som kun noen utvalgte brukere og servere kan benytte for å utveksle informasjon

Internett er et eksempel på et åpent nettverk som alle kan koble seg på, mens et LAN-nettverk som knytter sammen datamaskinene til et selskap er et lukket nettverk. Forskjellen mellom de ulike nettverkstypene er noe vi kommer tilbake til.

3.5 Servertyper

Det finnes mange ulike former for nettverksservere. Et grovskille er å skille mellom to ulike typer servere:

- **Applikasjons server**: Dette er en server som er satt opp til å levere en bestemt applikasjon (program) til brukeren. F.eks. et regnskapsprogram.

- **Filservere:** Dette er en datamaskin som er satt opp for å lagre og distribuere filer av ulike typer til brukerne i nettverket.

Felles for dem alle er at de er satt opp til å gi brukerne tilgang til dem, eller ulik tilgang til dem, avhengig av hvilken brukerprofil og -rettigheter de har. Å sette dette opp krever IT-kompetanse omkring så vel nettverks drift som programvaren som benyttes. For de fleste små- og mellomstore bedrifter er det nødvendig å kjøpe inn konsulenttjenester for å få satt opp dette riktig. Når det først er satt opp, kreves det lite eller ingen vedlikehold.

3.6 Applikasjons server

Når vi snakker om servere snakker vi normalt om ulike applikasjons servere. Det vil si en server som er satt opp til å kjøre en bestemt tjeneste eller program for brukerne av nettverket. Det finnes mange ulike typer applikasjons servere. Noen vanlige typer applikasjons servere alle nettverksansvarlige kommer borti er:

- **Rene applikasjons servere** - egne servere som er satt opp for å kjøre et bestemt program eller web applikasjon. F.eks. et regnskaps- eller lagerstyringprogram.
- **Database server** - en server som er satt opp for å kjøre og dele data som er lagret i et bestemt databaseformat til et stort antall brukere over nettverket.
- **Mail servere** - en server som er satt opp til å kunne sende og motta e-post via POP3, IMAP og SMTP protokollen.
- **Web server** - en server som er satt opp for å kunne produsere nettsider for brukerne som etterspør nettsider som ligger på serveren.
- **FTP-server** - en server som er satt opp til å kunne laste opp og ned filer til et webområde via ftp-protokollen.
- **Media server** - en server som er satt opp for å dele digitale videoer, bilder og lyd over et nettverk, enten i opptak eller som live media streaming.
- **Printer server** - en tjeneste som gjør det mulig å dele en enkelt skriver med alle eller utvalgte brukere av nettverket.
- **Spill server** - en server som gjør det mulig for flere spillere å spille mot hverandre samtidig eller delta i samme spill som ulike aktører i spillet gjennom et nettverk.

3.7 Hvor mange tjenester kan en server ha?

Hvor mange tjenester en server skal gi brukerne er opp til eieren av serveren. Det er ingenting i veien for å kjøre en stor menge ulike tjenester på en og samme server, men jo flere tjenester som kjøres jo større serverressurser kreves for at dette ikke skal gå utover hastigheten og ytelsen.

Hvor mange tjenester en server skal kjøre blir dermed en avveining mellom kostnader, sikkerhet og ytelsen som tjenesten krever.

3.8 Server og arbeidsstasjon

Mange lurer på hva som er forskjellen mellom en nettverksserver og en arbeidsstasjon. Forskjellen kan forklares slik:

> *En arbeidsstasjonen er den datamaskinen brukerne benytter seg av i arbeidet sitt, mens serveren er den datamaskinen arbeidsstasjonen kobler seg mot for å få tilgang til en bestemt tjeneste eller fil.*

Rent hardware messig er det i prinsippet lite forskjell på en datamaskin som er satt opp som en server i forhold til en datamaskin som er satt opp som en arbeidsstasjon. Forskjellen er normalt bare at serveren har vesentlig mer minne (RAM) og lagringskapasitet (harddisk) enn arbeidsstasjonen som ikke trenger å håndtere forespørslene fra en mengde ulike brukere samtidig. Forskjellen ligger først og fremst i valg av programvareplattform. En server er satt opp med programmer som er utviklet spesifikt for å deles over et nettverk, mens arbeidsstasjonene er satt opp med programmer som får sitt innhold over et felles nettverk.

3.9 Trenger man en egen server?

Har virksomheten få ansatte som deler virksomhetens data mellom seg, trenger man ofte ikke servere i det hele tatt. Sitter alle ansatte på egne stasjonære maskiner, kan man bare sette inn flere og større harddisker i en eller flere av dem og dele disse diskene med alle andre brukerne på nettverket på en enkel måte. Her kan man sette opp ulike rettigheter for ulike brukere, passordbeskytte mapper og filer på en enkel måte. Dette holder for svært mange småbedrifter, uten de store behovene.

3.10 Dedikerte eller virtuelle servere

Å ha egne servere er imidlertid både kostbart og kompetansekrevende. Stadig flere små- og mellomstore bedrifter finner nå ut at de ikke lenger trenger egne servere nå som det er blitt mulig å outsource alle nettverksserverne til ulike «sky-tjenester» hvor virksomheten kjøper servertjenesten fra en tredjepart leverandør som leverer dataene til nettverket og brukerne over Internett istedenfor over et LAN-nettverk. Å benytte en nettsky tjeneste er vesentlig rimeligere enn å ha egne servere. Samtidig som virksomheten ikke trenger å skaffe seg ansatte med server kompetanse.

Spørsmålet man må stille seg er om virksomheten skal satse på egne dedikerte servere eller leie seg inn på virtuelle servere. Forskjellen kan forklares slik:

1. **Dedikerte servere** - egne fysiske servere som kjører en eller flere dedikerte tjenester for alle brukerne av nettverket.
2. **Virtuell server** - en stor fysisk server som er delt opp i flere mindre servere på en og samme fysiske servere, og hvor enkelt virtuelle server installeres med et eget operativsystem, programmer og IP-adresse.

Siden de virtuelle serverne er vesentlig rimeligere å kjøpe og leie velger stadig flere å satse på virtuelle servere istedenfor dedikerte servere.

3.11 Datasenter

Et datasenter er et stort serverrom hvor det er plassert et stort antall nettverksservere på et og samme sted og som du kan leie deg inn på hvis du ønsker å plassere din server i dette datasenteret. For at et serverrom skal kunne kalles et datasenter må det ikke bare være plassert mange servere her, men rommet må også være spesielt laget for å oppfylle kravene et datanettverk og nettverksservere setter til sin infrastruktur. Datasentrene har derfor egne løsninger for redudant strøm, Internett linjer, brannmurer og sikkerhet.

4 Nettsky

4.1 Hva er en nettsky?

En **nettsky** (eng: *cloud computing* eller bare *clouding*) er en samlebetegnelse for:

> ***… leie av skalerbare eksterne IT-tjenester og -infrastruktur knyttet til datalagring, dataprosessering og programvare på servere som er koblet til Internett og som brukerne har tilgang til via Internett.***

Det finnes et stort hav av ulike nettsky tjenester, noe som ofte gjør det vanskelig å forholde seg til hva en nettsky er og sammenligne de ulike nettskyene. Det store spektret av nettsky tjenester som i dag finnes kan grovsorteres i tre hovedkategorier som ofte omtales i media:

- **Infrastructure as a Service (IaaS)**
  D.v.s. at en bruker dataressurser på en virtuell maskin som regnekapasitet, lagring og nettverk uten å kontrollere nettskyinfrastrukture.

- **Platform as a Service (PaaS)**
  D.v.s. at en bruker vertsomgivelser for egne applikasjoner uten å kontrollere operativsystemet, utstyr eller infrastrukturen som applikasjonen kjøres på.

- **Software as a Service (SaaS)**
  D.v.s. at kunden bruker en applikasjon uten å kontrollere operativsystemet, utstyr eller nettverksinfrastrukturen som applikasjonen kjører på. Alt skjer gjennom et webinterface på brukerens maskin.

Som regel refererer begrepet "*nettsky*" til en eller flere **virtuelle servere** på Internett som kjører de **tjenestene** og lagrer filene virksomheten benytter seg av, istedenfor å bruke egne servere som er lokalisert på et kontor eller serverrom. Disse serverne og tjenestene kan virksomheten og dens ansatte så koble seg på via **https, ftps, webdev, ssh og vpn** protokollen for å benytte.

Selv om det er utstrakt skepsis mot å flytte virksomhetskritiske bedrifts servere ut til en ekstern leverandør i nettskyen, forventes det at nettskyen vil påvirke både IT-bransjen og bruken av IT i stor grad i tiden fremover, da nettskyer gir virksomhetene en rekke fordeler:

- **Redusert kapitalbehov** – Infrastrukturen og utstyret leies istedenfor at det kjøpes av virksomheten.
- **Økt tilgjengelighet** – tjenesten er tilgjengelig overalt og for alle som har Internett tilkobling.
- **Skalerbarhet** – løsningen kan raskt, enkelt og uten større kostnader utvides eller nedskaleres, eventuelt legges ned hvis behovet skulle forsvinne.
- **Kompetanse** – virksomheten trenger ikke kompetanse om installasjon, sikring, drift og vedlikehold av løsningen, da dette er skyleverandørens ansvar.
- **Lavere kostnader** – ved bedre ressursutnyttelse.

Mer effektiv bruk av dataressursene, lagringskapasitet, datakraft, prosessering, programvare, drift og vedlikehold dras ofte frem som de viktigste grunnene til at såvel privatpersoner som organisasjoner og virksomheter velger å legge ut stadig større deler av sin IT-struktur ut i en nettsky.

Tap av kontroll over dataene, overføringhastigheten og sikkerhetsspørsmål brukes motsatt som de viktigste grunnene til å ikke legge IT-strukturen ut i en nettsky, noe vi kommer tilbake til i påfølgende artikler.

De største offentlige nettskyene er idag Google Drive, Microsoft, Amazon og Dropbox. Disse tilbyr ulike former for fillagring, fildeling og filsynkronisering, og de er alle amerikanske, med de svakhetene dette innebærer.

4.2 Nettskymodeller

NIST (National Institute of Standards and Technology) skiller mellom 4 forskjellige nettskymodeller (NIST 2011).

- **Privat sky:** Skyinfrastrukturen opereres for en enkelt organisasjon.
- **Offentlig/fellessky (community cloud):** Skyinfrastrukturen er delt av flere organisasjoner.
- **Kommersiell sky (Public cloud):** Skyen er eid av et privat selskap som selger tjenestene til offentligheten eller en stor industrigruppe.
- **Hybrid sky:** Kombinerer to eller flere private, kommersielle eller samarbeidsskyer som forblir selvstendige enheter, men muliggjør overføring av data og applikasjoner

I motsetning til en offentlig nettsky er en privat nettsky en nettsky som er knyttet til et domene du selv eier og kontrollerer. Du deler med andre ord ikke nettskyen med andre. Du eier den 100% selv og har selv full kontroll over alle deler av den.

4.3 Hvorfor legge virksomhetens servere og tjenester ut i en nettsky?

En spørreundersøkelse utført av Harvard Business Review blant amerikanske bedrifter fant at 85 % planla å bruke skytjenester de neste tre årene.

De begrunnet valg av skyteknologi med:

- **Kortere vei fra beslutning til realisering**
- **Øket fleksibilitet**
- **Tar i bruk ny teknologi raskere**
- **Lavere faste kostnader**
- **Lavere investeringer for å etablere et IT- system**
- **Alltid tilgang til nyeste versjon av IT-system**
- **Enklere å håndtere vekst**
- **Enklere og billigere å teste ut en ide**

I tillegg kan en ta med:

- **Reduserte implementerings- og vedlikeholdskostnader**
- **Fleksibel og skalerbar infrastruktur**
- **Kort tid fra idé til marked**
- **Skifte i IT-avdelingen fra drift til innovasjon**
- **Energibesparelser**
- **Økt tilgjengelighet til høyytelsesapplikasjoner for små og mellomstore institusjoner.**
- **Gjør det mulig å teste ut ny programvare, applikasjoner og virksomhetsideer uten å pådra seg kapitalutgifter.**
- **Gir mulighet for å prøve ut radikalt nye løsninger uten å risikere sammenbrudd i eksisterende tjenester.**
- **Applikasjoner kan tas i bruk uten å vente på komplekse installeringsprosedyrer**
- **SaaS applikasjoner tar svært liten plass på klienten og risikoen for konfigurasjonsinterferens mellom applikasjoner på klient reduseres**

En fellesnevner for punktene på listen er økt fleksibilitet. Tjenestene, enten de er nye eller utvidelse av eksisterende, blir umiddelbart tilgjengelige uten at en må gå veien om innkjøp av server, installering, opplæring av personell, nyansettelser etc. Kort tid fra planer og vedtak til anvendelse av tjenesten er viktig for alle organisasjoner, selv om det ikke blir så tydelig i offentlig virksomhet som i næringslivet, der verdien av rask implementering bl.a. kan måles ut fra de kontantstrømmene som genereres. SaaS (Software as a Service) gir fordeler både til leverandør – i form av forenklet installering og vedlikehold, og sentralisert kontroll over og styring med programversjoner – mens sluttbrukeren kan få tilgang til tjenesten hvorsomhelst, nårsomhelst og påhvasomhelst. og kan forenkle samarbeid, og får trygg datalagring (Kilde: Nettskyteknologi i UH-sektoren).

4.4 Gjør det enkelt å skalere opp og ned virksomhetens IT-systemer

Nettskyen effektiviserer hvordan programvare, forretningsprosesser, og tjenestene er tilgjengelige og brukes. En av de største fordelene med nettskyer et at de gjør det mulig å skalere driften og optimalisere sine investeringer på en langt bedre måte enn tidligere.

Vokser bedriften er det bare å øke størrelsen og kraften i nettskyen bedriften leier, uten å måtte investere store beløp i dyr maskin- og programvare. Hele oppskaleringen kan dessuten gå svært raskt. Istedenfor å vente på at en ny server skal bli produsert, installert og satt opp klar til bruk, kan bedriften med en sky tjeneste doble server kraften (CPU), minne (RAM) eller lagringskapasiteten (HDD) på minutter, med nødvendige tilleggs lisenser til programvaren som eventuelt kreves.

4.5 Minimaliserer risikoen ved IT-investeringer

Motsatt kan bedriften raskt og enkelt kvitte seg med unødvendig maskinvare, linjekapasitet og programvare hvis behovet skulle bli redusert, f.eks. gjennom nedskjæringer og oppsigelser. Det eneste man trenger å gjøre er å si opp leien av de tjenestene og kapasitetene bedriften ikke lenger trenger. Noe som igjen minimaliserer risikoen ved å lansere nye IT-tjenester, da virksomheten ikke lenger trenger å investere i nytt utstyr eller programvare.

4.6 Binder ikke kapital og krever ingen investeringer

Siden bedriften ikke trenger å investere i maskin- og programvare, bindes ingen arbeidskapital i virksomheten. Alt leies og betales gjennom månedsleien virksomheten betaler for tjenestene og de virtuelle serverne som leies. Dette gjør at alle bedrifter nå raskt og uten å måtte foreta noen som helst form for større investeringer kan etablere seg med en profesjonell IT-infrastruktur når de selv måtte ønske det, og avslutte det like raskt hvis ideen ikke skulle slå an eller behovet skulle bli redusert.

4.7 Krever ingen eller færre IT-ansatte

Nettskyer kan leies med eller uten en driftsavtale inkludert. Velger man å inkludere en driftsavtale er det leverandøren av nettskyen som står for all drift, oppdatering, vedlikehold og backup av de virtuelle serverne og dataene på dem. Dette gjør at alle IT-ansatte som jobber med dette kan sies opp og at nye virksomheter kan etablere seg raskt og rimelig med en profesjonell IT-struktur, uten en eneste IT-medarbeider.

Siden lønns- og personalkostnadene normalt er den største kostnaden i norske bedrifter, samtidig som kompetente IT-medarbeidere er svært kostbare, kan det være ekstremt mye penger å spare for små- og mellomstore bedrifter ved å legge serverne og programvaren de bruker til daglig i en nettsky.

4.8 Lavere kostnader og økt fortjeneste

Ovenstående forhold gir normalt en kraftig reduksjon i virksomhetens IT-kostnader, og dermed også en forbedret bunnlinje.

Siden nettskyen gjør det raskt og enkelt å skalere opp og ned uten å investere i ansatte, maskin- og programvare øker dette fleksibiliteten i driften og muliggjør langt mer effektive forretningsmodeller.

4.9 Ikke noe enten eller – hybride nettskyer er ofte første steg

Enkelte programmer og funksjoner kan kanskje ikke eller er ikke ønskelig å legge ut en nettsky. Løsningen er da en hybrid nettsky, hvor man legger ut enkelte av virksomhetens tjenester i nettskyen hvor alle har tilgang til dataene via sin maskin, nettbrett og smarttelefon, mens andre deler beholdes lokalt på egne servere som i dag. En fleksibilitet som gjør nettskyen aktuell for nærmest alle norske bedrifter og organisasjoner.

Er man smart når disse planene legges kan virksomheten optimalisere sine forretningsprosesser kraftig viser all erfaring så langt.

4.10 Raskere innovasjonsgrad

Har virksomheten en god ide som de ønsker å prøve ut, kan de nå leie plassen, server kraften, programvaren og ekspertisen man trenger uten noen som helst form for investering og med minimal eller ingen bindingstid. Viser det seg at tjenesten virksomheten lanserte ikke skulle slå an som ønsket, er det bare å si opp nettskyen man leier, så er prosjektet avsluttet, uten andre tap enn det man har betalt i leien for nettskyen for den ble sagt opp.

Alternativet med å investere i eget utstyr, linjer, programmer og ansatte for å teste ut ideen er langt mer kostbart og risikobetont enn å leie en sky-tjeneste til ideen man ønsker å prøve ut.

Konsekvensene av dette blir at virksomheten kan prøve ut langt flere ideer enn det de av økonomiske grunner kan gjøre i dag, noe som ikke bare øker innovasjons graden men også fremtidig lønnsomhet.

4.11 Hvordan velge rett nettsky?

Det er mange ting du bør tenke på når du skal velge nettsky leverandør, enten du er en privatperson, forening eller en småbedrift.

Datatilsynet gir på sine sider følgende råd til privatpersoner som ønsker å etablere en egen nettskytjeneste.

- **Brukervilkår**: Hva sier brukervilkårene? Bør jeg være bekymret for noen av dem? Forstår jeg vilkårene?
- **Seriøsitet**: Hvor seriøse fremstår tjenesteleverandøren? Kjenner jeg noen som kan gi med et råd om bruk av tjenesten er forsvarlig for formålet mitt?
- **Sikkerhet**: Hvordan ser det ut til at tjenesteleverandøren har ivaretatt sikkerheten? Hvor enkel ser det ut til for uvedkommende å skaffe seg tilgang? Er sikkerheten godt nok ivaretatt for det jeg ønsker å lagre?
  Søk gjerne råd hos andre som har greie på sikkerhet.
- **Passord**: Hvis tjenesteleverandør stiller krav til kvalitet på passordet er dette et godt tegn. Virker det som leverandør har ivaretatt dette på en god måte?

- **Rettigheter**: Hvilke rettigheter har jeg om all informasjonen jeg har lagret blir borte? Sies det noe om det i vilkårene? Har jeg en egen sikkerhetskopi?
- **Lovgivning**: Hvilket land er tjenesteleverandøren hjemmehørende i? Hvem kan hjelpe meg hvis noe skulle gå galt? Informasjonen på nettaserte løsninger kan i utgangspunktet være lagret hvor som helst i verden, og andre regler kan gjelde i utlandet i forhold til i Norge.

4.12 Utfordringer ved overgang til nettsky

Det er en rekke utfordringer knyttet til overgang til nettsky når det gjelder juridiske forhold, sikkerhet, avtalemessige forhold, personvern i tillegg til de teknologiske.

I et notat om "***Nettskyteknologi i UH-sektoren***" trekkes det spesielt frem følgende forhold:

- **Umodent marked. Området er fortsatt svært volatilt med store endringer både i priser, leverandører, tjenestenivå.**
- **Risikovurdering og styring med prosessene. Liten transparens hos leverandørene, mangel på sporingsmuligheter (audit trails), manglende fleksibilitet i tjenestevilkårene.**
- **Usikker kostnadseffektivitet**
- **Manglende avtaler om tjenestenivå**
- **Personvern**
- **Beskyttelse av intellektuelle rettigheter**
- **Sikring av sensitive data**

I tillegg trekker de frem følgende generelle forhold for nettskyer:

- **Avhengig av et sikkert nettverk**
- **Brukerne trenger fortsatt ferdigheter**
- **Belastningslokasjoner tildeles dynamisk og vil være skjult for brukerne**
- **Risiko knyttet til deling av ressurser med mange kunder**
- **Dataimport eksport og ytelsesbegrensninger generelt**

I samme rapport viser de til en undersøkelse fra IDC enterprise Panel (International Data Corporation) utført i 2009 som konkluderte med at utdannelsesinstitusjoner vurderte følgende som de største usikkerhetsmomentene knyttet til innføring av skyteknologi i UH-sektoren:

- **Sikkerhet**
- **Ytelse**
- **Tilgjengelighet**
- **Manglende brukertilpasning**
- **Kostnader**
- **Vansker med reetablering av drift i egen regi**
- **Offentlige reguleringer**
- **Få store leverandører**

De viser også til ENISA (European Network and Information Security Agency) har gjort en egen vurdering (Benefits, risks and recommendations for information security). De trekker frem spesielt følgende risikofaktorer:

- **Tap av styring gjennom overføring av kontroll til skyleverandøren**
- **Innelåsing til en leverandør (Prosedyrer, redskap etc. for portering av data fra en leverandør til en annen er dårlig utviklet)**
- **Svakheter knyttet til å isolere en bruker fra en annen når ressurser deles.**
- **Bibehold av sertifisering (Compliance) Overgang til sky kan være i brudd med sertifiseringsreglene. Spesielt kan dokumentasjonen bli komplisert.**
- **Økt risiko gjennom økt tilgang til økte ressurser via management interface.**
- **Databeskyttelse. (Varierende muligheter for å sjekke databehandlingspraksis og rutiner hos leverandør).**
- **Usikker eller ufullstendig sletting av data.**
- **Ondsinnet insider. (relativt sjelden forekommende, men ekstremt skadelig når det skjer.)**

4.13 Overføringshastighet til nettskyen

Mange er bekymret for hastigheten, d.v.s. tiden det tar fra du klikker på noe til resultatet kommer opp på skjermen, når de skal vurdere å legge hele eller deler av virksomhetens IT-tjenester ut i en nettsky.

For 10 år siden var den effektive linjehastigheten på Internett tilknytningen til folk flest på under 1 MB/Sek, mens hastigheten på det lokale LAN nettverket var 100 MB/sek. Noe som gjorde at de færreste engang vurderte å flytte virksomhetskritiske applikasjoner eller filområder ut i en nettsky. I dag er situasjonen heldigvis helt annerledes, selv om linjehastigheten fortsatt er en av de viktigste grunnene til at ikke alle legger alt ut i en nettsky.

På Internett blir aldri hastigheten mellom en server og en klient (deg) raskere enn det svakeste leddet.

Fra dataene går ut fra serveren som har en linje på f.eks. 1 GB/sek, til de kommer til din Internett tilkobling som er på f.eks. 100 MB/sek, vil dataene passere mange mindre sub-nett, noder, switcher, routere og brannmurer som deles med en mengde andre brukere. Dette vil ødelegge overføringshastigheten mellom serveren og din datamaskin, da dataene som overføres vil bli stående i "kø" ett eller flere steder på veien før de endelig kommer frem. Jo flere køer dataene må passere og jo lengre disse køene er, jo tregere vil overføringshastigheten bli.

En nettsky kan aldri få samme hastighet som et lokalt LAN-nettverk hvor alle brukerne sitter tilkoblet via en fysisk kabel eller et trådløst nettverk rett mot serveren av ovenstående grunner, men nettskyen gir andre unike fordeler som i de aller fleste tilfeller oppveier for de negative:

- **Tilgjengelighet**. Et lokalt LAN-nettverk er "lokalt". Det vil si bare tilgjengelig for dem som sitter knyttet til nettverket via en kabel som går til en bestemt lokal server eller serverpark. En nettsky er tilgjengelig over alt og for alle som du ønsker skal ha tilgang til nettskyen. Det eneste som kreves er at de har en Internett tilkobling.

- **Plattform uavhengi**g. Nettskyen kan du koble deg til og bruke via så vel datamaskiner (Windows, Mac eller Linux), nettbrett som mobiltelefoner (iOS og Android). Dette gjør at dataene ikke bare er tilgjengelig over alt, men også helt uavhengig av utstyret du kobler deg på med.

- **Kostnadseffektivitet og skalerbarhet.** Istedenfor å måtte investere i dyrt datautstyr og programvare leier du kapasiteten du trenger i en nettsky, samtidig som du når som helst kan øke din kapasitet når du måtte trenge det.

- **Kompetanse behov.** Egne servere og eget nettverk krever at man har ressurser og kompetanse til å installere, sikre, drifte og vedlikeholde utstyret. Leier man en egen privat nettsky er dette leverandørens ansvar og ikke ditt. Noe som sparer deg for en masse problemer og penger.

4.14 VPS (Virtual Private Server)

VPS eller virtuelle servere er noe vi hører stadig oftere om, spesielt i forbindelse med skytjenester. Er du en av dem som fortsatt ikke har satt deg inn i hva en virtuell server er, bør du lese denne artikkelen som nettopp tar for seg dette.

4.14.1 Hva er en VPS?

VPS betyr "**virtual private serve**r" (noen kaller det også en "*virtuell dedikert server*").

En VPS er en server som ikke er installert direkte på den fysiske maskinvaren den kjører på. Den kjører i stedet på toppen av et operativsystem beregnet på virtualisering av servere.

4.14.2 Flere servere deler samme maskinvare

I praksis betyr det at man på en og samme fysiske maskin kan installere flere isolerte, virtuelle servere. Hver enkelt virtuelle server får et eget skjermet område på den fysiske serveren, hvor de kan installere sine egne programmer. Dette gjør løsningen svært kostnadseffektiv, fordi du ikke trenger en maskin til hver server, noe som betyr lavere investeringskostnader, lavere strømutgifter, mindre plassbehov og bedre utnyttelse av maskiner og utstyr.

VPSen er "***virtuell***" i den forstand at den kjører uavhengig av den fysiske maskinvaren den er installerrt på. Noe som for eksempel gjør det svært enkelt å flytte en VPS mellom ulike fysiske servere (dedikerte servere).

Hele serveren, med programvare og brukerdata, kan samles sammen i en "kjempestore fil" (også kalt "snapshot") som overføres og gjenopprettes på en annen virtuell server (VPS). Så enkelt er det ikke å flytte en server du deler med andre (f.eks. en webhotell server). Dette gir deg friheten til å bytte leverandør raskt og enkelt når du selv vil, uten store kostnader.

4.14.3 Alle serverne kjører uavhengig av hverandre

En VPS er "***privat***" siden den er isolert fra de andre VPSene på samme maskinen, uten at de har muligheten til å påvirke hverandres filsystem eller prosesser.

Blir en annen virtuell server på bladet du ligger på hacket, får hackerne under ingen omstendigheter tak i dataene dine, slik de kanskje kan på en delt server (Les: webhotell server). Ondsinnet programvare som blir lastet opp til en annen VPS kan dermed aldri påvirke din virtuelle server, da de er totalt isolert fra hverandre.

4.14.4 Rask, enkel og rimelig oppgradering av maskinvaren

En annen stor fordel med VPS er at alle virtuelle servere deler de samme maskinvare ressursene. Noe som gjør det svært raskt, enkelt og rimelig å oppgradere en virtuell server med mer CPU kraft, mer minne eller større lagringskapasitet.

Trenger du mer krefter (cpu), minne (RAM) eller større lagringskapasitet (HDD) er det bare å oppgradere uten å måtte kjøpe og installere dyr hardware, i form av flere cpuer og harddisker eller mer ram. Har du en virtuell server styres alt gjennom et sentralt grensesnitt for alle virtuelle servere på blade serveren.

4.14.5 Programvare og operativsystem

Normalt leveres en virtuell server (VPS) med et ferdig installert operativsystem, fortrinnsvis Linux eller Windows2008 Server. I tillegg får du shell tilgang (SSH), hvis du velger Linux og tilgang via Terminal Client hvis du velger Windows som operativsystem. Hvilket Linux operativsystem du ønsker kan du normalt velge selv.

Hvilke andre programmer som inngår i pakken varierer fra leverandør til leverandør, men det er normalt heller ikke vanskelig å få serveren levert med ferdig mai-, web-, ftp- og database server installert. Også webbaserte kontrollpanel som Plesk og cPanel leveres også mot et tillegg i prisen av mange leverandører.

4.14.6 Server oppsett

En virtuell server blir normalt satt opp med minst tre partisjoner; En system-, en swap og en data-partisjon. Fordelene med flere partisjoner, er flere. For eksempel kan du reinstallere operativsystemet på din virtuelle server, uten at område med brukerdata blir berørt. Diskspeiling er en annen funksjon som mange tilbyr for å oppnå redudans.

4.14.7 Infrastruktur

Normalt leveres en virtuell server koblet opp mot leverandørens aksessnett for Internett. Hvilken båndbredde leverandørene tilbyr varierer i stor grad. Her går skalaen fra 10 mb/sek til 1.000 mb/sek. Hvor mye data som det er mulig å overføre i nettverket varierer også fra leverandør til leverandør, og er noe man alltid bør undersøke før valget tas.

Mange tilbyr også tilkobling mot et internt backup-nett for å overføre data til backup servere.

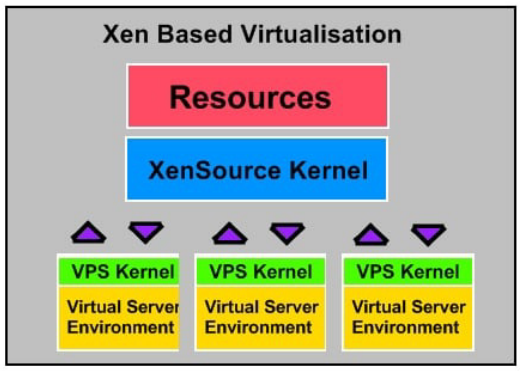
4.14.8 Drift av serveren

Normalt kan du selv bestemme om du ønsker å drifte serveren selv eller tegne en drifsavtale for serveren. Hva som inngår i disse driftsavtalene varierer fra leverandør til leverandør, og er noe som må kartlegges før det endelige valget tas.

4.14.9 Virtualisering teknikker

De 2 største og mest dominerende virtualiserings teknikkene er i dag **Xen** og **OpenVZ**.

4.14.10 Xen



Xen er generelt en litt mer pålitelig virtualiserings-programvare enn OpenVZ.

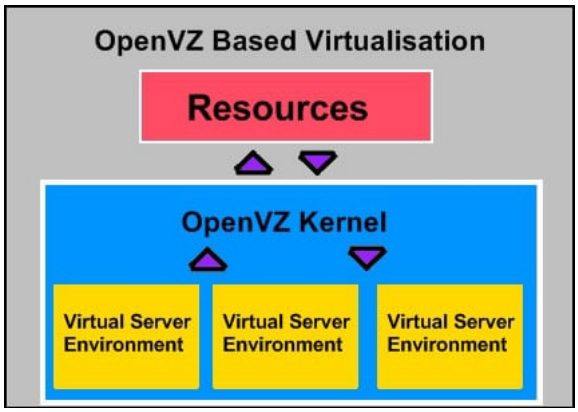
Xen er en virtualisering plattform som oppretter virtuelle servere med nesten nøyaktig de samme egenskapene som en dedikert server. En Xen VPS kjører med sin egen isolert kjerne, har et fullstendig installert operativsystem med sine egne kjernemoduler, den bruker fullt dedikert virtualisert minne, I / O og er like stabile og utvidbar som en dedikert server.

I praksis vil du aldri merke at du har en virtuell server hvis du velger Xen virtualisering, fremfor en dedikert. Den eneste forskjellen er at Xen bare koster en brøkdel av en dedikert server.

Hovedtrekk i Xen virtualisering:

- **Full root-tilgang**
- **Støtter Linux og Windows**
- **Bedre Java ytelse enn OpenVZ**
- **Ressursene (RAM , etc) er fullt dedikerte og private**
- **Para – virtualisert Linux -kjernen (dvs. , full isolasjon)**
- **Direkte tilgang til lastbare kjernemoduler**
- **Bytt plass**
- **Svært konfigurerbar**

4.14.11 OpenVZ



OpenVZ, på den annen side, er et operativsystem-nivåvirtualiserings platform som fungerer på samme måten som Xen, men OpenVZ gir bare et tynt lag av virtualisering på toppen av den underliggende OS . Alle virtuelle servere på en OpenVZ server (node) vil dele den samme Linux kjernen (Windows kan ikke kjøres), i motsetning til Xen hvor alle kjører sin egen Linux kjerne.

Til tross for disse små ulempene, er OpenVZ mer kostnadseffektiv, lettere å forstå, og utfører vanligvis oppgaver bedre enn Xen servere i for små virtuelle servere, da de deler ressurser som CPU og RAM.

Mangler en VPS som kjører på OpenVZ minne (RAM) kan den låne dette av en annen VPS på samme server (node), såfremt denne ikke bruker all det minne som er dedikert. Dette er ikke mulig på Xen, hvor RAM er bunnet til den enkelte VPS i noden som kjører i helt isolerte miljøer. I praksis betyr dette at andre ikke kan «tyvlåne» RAM eller andre dedikerte ressurser. grunn til å ha ekstra ressurser tilgjengelig som en Xen VPS ville være med å kjøre sin helt isolert miljø .

Hovedtrekk i OpenVZ virtualisering:

- **Full root-tilgang**
- **OS – nivå virtualisering**
- **Burst ‘ RAM og andre ekstra ressurser tilgjengelig når noder er underutnyttet**
- **Oppgraderinger kan brukes on-the -fly , uten omstart**
- **Flere ressurser tilgjengelig på grunn av lett virtualisering**
- **Enkel nettverk og installasjonsdisken**
- **Tilgang til de fleste iptables moduler**

4.14.12 Hva er raskest – OpenVZ eller Xen?

Sammenlignet med å kjøre på en egen dedikert server, vil all virtualisering medføre en liten redusering av ytelsen. Siden de fleste VPS leverandører kjører sine servere med high-quality hardware, vil dette ytelses tapet i praksis være svært liten.

Hva med de ulike virtualiserings teknikkene? Selv om «ekspertene» aldri blir enige om hvilken virtualiserings plattform som gir den beste ytelsen, er det vanligste svaret at OpenVZ er raskest, selv om dette er en sannhet med mange modifikasjoner.

I motsetning til Xen som er en virtualisering av hele serverens hardware, er OpenVZ's kun er vitualiserings av operativsystemet (OS). Dette gjør at OpenVZ krever litt mindre ressurser for å styre og kontrollere virtualiseringen. Mange argumenterer at dette gir en bedre ressursutnyttelse enn Xen, men dette betyr ikke nødvendigvis at OpenVZ er raskere enn Xen.

OpenVZ bygger på en teknologi hvor hver enkelt VPS får en «soft limits" for hver ressurs som skal unngå overforbruk av kritiske ressurser som CPU, RAM, nettverkskort og diskplass, men disse grensene kan (og blir) blir forbigått og misbrukt.

Av den grunn vil ytelsen til en VPS som baserer seg på OpenVZ variere i stor grad fra leverandør til leverandør og fra node til node innenfor samme leverandør.

4.14.13 Oversalg er en problem på Open VZ VPN

De fleste leverandører av Open VZ VPS overselger sine noder. Det vil si at de legger flere VPS på en node (fysisk server) med større «dedikerte» ressurser enn det serveren har, I praksis betyr dette at hvis alle kundene bruker alle ressursene de har dedikert (CPU, RAM og diskplass) så er det rett og slett ikke nok ressurser til alle. Ingen får dermed det de betaler for.

Dette er ikke bare en vanlig praksis i VPN bransjen, men har i flere 10 år vært praksis for bredebånd leverandører som overselger sine linjer både 10 og 20 ganger. Dette gjøres fordi leverandøren vet at ikke alle kundene bruker VPNen fult ut hele tiden. De fleste bruker f.eks. bare en liten del av tildelt CPU og RAM, noe som gjør at de kan selge de frie ressursene til andre. Problemet oppstår først når flere etterspør alle sine dedikerte ressurser samtidig.

Spørsmålet du må stille deg selv er derfor:

> ***– Hvor mange andre VPS deler den fysiske serveren (node) og hva bruker de sine VPS til?***

Det er stor forskjell på å kjøre noen enkle hjemmesider, og en stor database med tusenvis av spørringer til enhver tid, som samtidig skal håndtere store mailtjenester og andre ting.

Slike problemer får du ikke hvis du velger Xen VPN, hvor alle ressursene er fysisk dedikert til deg (tilnærmet isolerte ressurser), slik at ingen andre kan tyv låne dine ressurser når de selv mangler ressurser. Dette gjør også Xen mer stabil og pålitelig enn OpenVZ.

En Xen server kan ikke overselges slik en OpenVZ enkelt kan. Dette er også grunnen til at en Xen VPN er vesentlig dyrere enn en OpenVZ VPN.

4.14.14 Stabilitet og funksjonalitet.

Krasjer Linux kjernen på en OpenVZ node, vil alle virtuelle servere på denne noden (den fysiske serveren) også krasje. Dette skjer ikke på en Xen node, hvor alle kjører sin egen kjerne. Et Xen plattform er derfor mer stabil enn en OpenVZ plattform.

Siden alle VPS benytter den samme Linux kjernen, er det ikke mulig for den enkelte VPS å endre denne kjernen eller installere nye komponenter til den, uten at dette også får konsekvenser for alle andre VPS på samme server. Slike installasjoner kan derfor kun gjøres av node administrator og ikke av den enkelte VPS eier.

Av denne grunn kan ikke OpenVZ virtualisering tilby den samme funksjonaliteten som Xen virtualisering, hvor hver enkelt VPS kan gjøre hva de selv måtte ønske.

Xen scorer derfor høyere på stabilitet og funksjonalitet enn OpenVZ.

4.14.15 Sikkerhet

OpenVZ bruker en felles IP-tables for alle VPS, mens Xen VPS har hver sin egen IP-table.

En OpenVZ kan dermed ikke konfigurere brannmuren som styrer sikkerheten til systemet selv, slik kunder som kjører på Xen kan. Dette gjør Xen til en potensiell sikrere virtualiseringsform enn OpenVZ.

Siden alle OpenVZ VPS deler samme Linux kjernen blir alle VPS smittet av uønsket malware, trojanere, ormer eller virus, hvis kjernen blir infisert med slike uønskede komponenter, uten at den enkelte VPS kan gjøre noe som helst for å beskytte seg. **Dette er en annen svakhet som gjør Xen overlegen OpenVZ når det gjelder sikkerhet.**

4.14.16 Hva bør jeg velge?

Hvis du er i tvil om hvilken plattform ville være bedre for deg, vil antagelig OpenVZ være et greit sted å starte. Dette er enkelt å sette opp og koster vesentlig mindre enn Xen, med mindre du allerede vet at OpenVZ ikke støtter programmene du har planer om å kjøre (f.eks. støtter ikke OpenVZ Windows og dermed heller ingen Windows programmer/teknologier)).

Sjekk bare hvilken hastighet på cpu, ram, nettverkskort og disker du får og hvor mye de overselger serverne med. Mange tilbyr også en gratis prøveperiode slik at du kan prøve tjenesten for å finne ut graden av oversalg og om serveren gir nok ytelse og funksjonalitet til ditt bruksområde.

Etter dette er neste steg Xen som er mer stabil, sikrere og har større fleksibilitet, men koster på den andre side vesentlig mer enn OpenVZ.

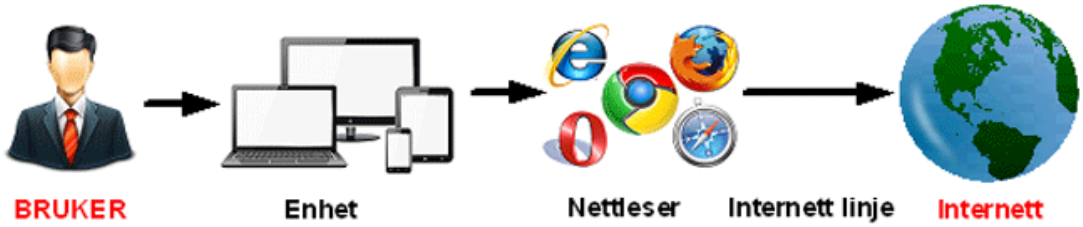
5 Internett

5.1 Hvordan fungerer Internett?

La oss kort ta for oss hvordan Internett rent teknisk fungerer før vi kommer inn på de ulike delene og komponentene i dette nettverket.

5.1.1 Brukerkrav (mottaker krav)

Hva som kreves for å benytte nettet på ønsket måte er avhengig av om vi ser problemstillingen fra en brukers ståsted eller en innholdsleverandør sitt ståsted. La oss først se på hvilke krav som stilles til alle som ønsker å bruke Internett.



5.1.1.1 Enhetsbasert kommunikasjon

For at en person skal kunne bruke Internett må de ha en enhet som det er mulig å koble til Internett for å søke etter og se informasjonen de søker etter. Enheten kan være en:

- **Datamaskin (PC/Mac)**
- **Pad/nettbrett**
- **Smarttelefon**

5.1.1.2 Nettleser

For at enheten skal kunne søke etter og vise informasjonen du ønsker må enheten ha installert en nettleser. Et lite gratis program som enten følger med enheten og som du kan laste ned fra nettet og installere på enheten.

Nettleseren gjør det mulig å søke etter og vise nettsider som bygger på HTML-standarden og TCP/IP protokollen. Den gjeldende standarden for å presentere web innhold på idag.

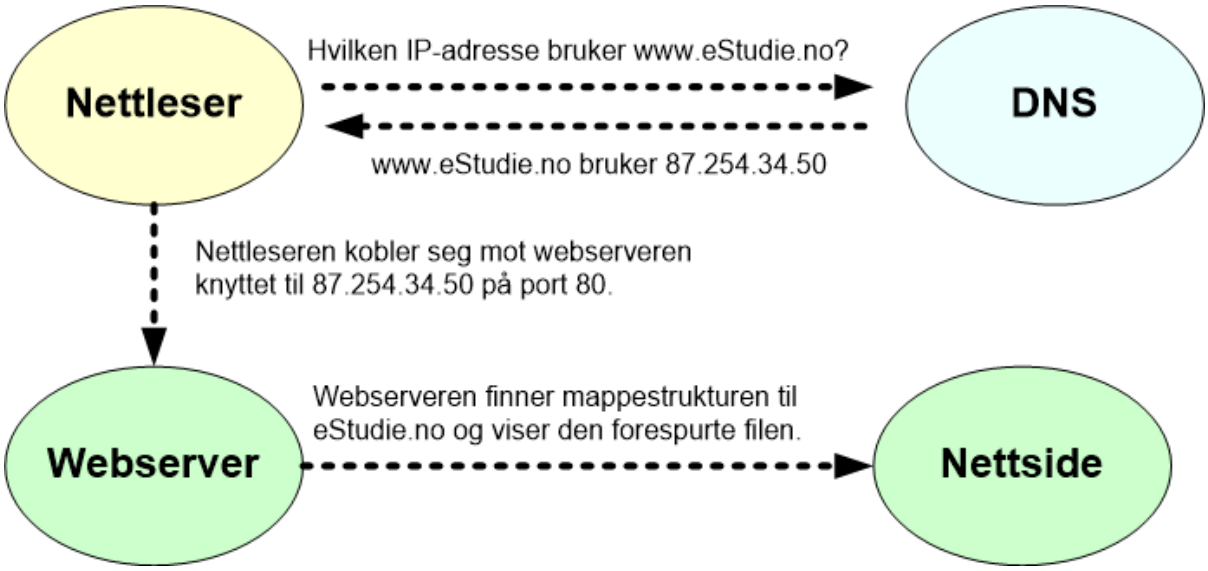
5.1.1.3 Internett linje/abonnement

Når du har en enhet med en nettleser trenger du kun en Internett linje du kan koble enheten til for å kunne benytte nettet.

For å få tilgang til en Internett linje må du tegne ett abonnement hos en ISP. En forkortelse for *Internet Service Provider*. Her betaler du normalt en fast månedlig avgift for tilgangen.

5.1.2 Senderkrav

Å være produsent og distributør av webbasert innhold krever imidlertid langt mer enn å være en vanlig bruker. Ønsker du f.eks. å vise en Internett side på nettet kreves det et nettverk bestående av følgende komponenter:



5.1.2.1 Domene

Det første du trenger er et domene til innholdet. Et domene er et navn du skriver som en del av en nettadresse (URL) for å komme til en bestemt nettside, f.eks. google.com for å komme til Google sine sider.

5.1.2.2 DNS

Når du har dette domene må domene legges inn i minst to navnetjenere som forteller alle nettlesere og andre ressurser som spør etter domene hvilke IP-adresser og servere domene bruker og ruter dem videre til denne web- eller mailserveren.

5.1.2.3 Webserver

Navnetjenernes oppgave er å fortelle brukerne hvilken IP-adresse og webserver et domene bruker. Når kallet kommer til denne serveren må webserveren svare at domene ligger her og redirekte kallet til den mappen på serveren domene bruker og som den etterspurte siden (adressen) viser til. Når kallet endelig kommer hit kjøres denne siden på webserveren.

For at denne siden skal kunne kjøres på webserveren kreves det at webserveren har installert alle de programmeringspråkene nettsiden bruker. Deretter sendes det endelige resultatet til brukerens nettleser hvor resultatet vises på brukerens skjerm.

For å kunne legge ut egne nettsider kreves det derfor at du har en webserver som du kan bruke til å legge ut nettsidene dine på.

5.1.2.4 Publiseringsløsning

Nettsidene lages ikke av seg selv. For å kunne lage sidene du ønsker å vise dine besøkende trenger du en publiseringsløsning som lager og publiserer nettsidene dine til webserveren.

5.1.2.5 Internett linje

Webserveren må så være koblet til en Internett linje med en egen dedikerte IP-adresse som gjør denne maskinen unik i forhold til alle andre webservere på Internett.

5.2 Internett sin historie

Internett (ofte kalt ***«nettet»*** er et verdensomspennende datanettverk som danner basisen for en rekke kommunikasjonstjenester. De viktigste tjenestene på nettet idag er World Wide Web, e-post, chat, filoverføring, IP-telefoni og videosamtale.

Hovedtrekkene i utviklingen har vært:

60-årene: Forskning innen pakkesvitsjede nett. Etablering av ARPANET.
70-årene: Forskning innen internetting. Utvikling av TCP/IP. Etablering av Internett.
80-årene: Den akademiske verden (universiteter og forskningsmiljøer) tar i bruk Internett.
90-årene: Resten av verden tar i bruk Internett.

Historien om internett begynner hos DARPA, direktoratet som styrer det amerikanske forsvarsdepartementets forsknings- og utviklingsprosjekter innenfor utpekte områder, på midten av 60-tallet. Målet var å utvikle et kommunikasjonssystem som kunne motstå virkningene av et atomangrep. Viktige krav som ble stilt til dette kommunikasjonssystemet var:

- **nettverket måtte være robust ved feilsituasjoner.**
- **nettverket skulle ikke være avhengig av et sentralt kontrollpunkt, men flere autonome sentra som skulle kunne kommunisere selv om noen linjer eller sentrale enheter falt ut.**

Ledende forskningsinstitusjoner og universiteter i USA (i første rekke RAND og MIT) fikk i oppgave å utvikle et datanettverk som kunne imøtegå de krav forsvars- departementet hadde utformet. Gjennombruddet kom i 1964, da forskeren Paul Baran ved RAND utviklet en banebrytende metode for å overføre data over det eksisterende telenettet. Barans nye ide fikk navnet "**packet switching**".

5.2.1 Pakkesvitsjing

I motsetning til mindre fleksible systemer, bygger pakkesvitsjing på at alle utgående meldinger dels opp i et antall mindre pakker som alle fikk samme adresse. Pakkene skulle selv finne veien gjennom nettet, gjerne forskjellige veier, før de ble samlet igjen ved målet. Et slikt system ville kunne tilpasse seg situasjoner hvor deler av nettet var ute av funksjon i korte eller lengre perioder. Ved at signalene kan ta ulike veier, uavhengig av hverandre, blir strømmen uforutsigbar og i praksis umulig å kutte, da pakkene selv starter å søke etter nye veier så snart den ene blir stengt.

5.2.2 ARPANet - Internetts forløper.

Med bakgrunn i den nye teknologien ble ARPANet etablert i 1969. Nettet hadde ingen sentral myndighet som ville være et naturlig mål for motpartens atombomber. Alle enheter av ARPANet hadde samme prioritet, og nettet skulle ikke bryte sammen selvom en enhet ble satt ut av funksjon. ARPANet var et eksperiment etablert for å gi forskere tilknyttet det amerikanske forsvaret tilgang til datakraft plassert ved noen større forskningssentra. Men nettet utviklet seg snart i retning av et elektronisk postkontor, fjernt fra dets opprinnelige hensikt. Samtidig ble stadig nye brukergrupper, f.eks. universiteter og sivile forskningsinstitusjoner, gitt adgang til datanettet. Norge ble som første land utenfor USA tilknyttet ARPANet via satellitt i 1972.

5.2.3 MILNET og NFSFNET

I løpet av 70-årene vokste ARPANet med en eksponentiell hastighet. Nye brukertjenester, som f.eks. konferanser på nettet, ble utviklet av oppfinnsomme studenter. Den militære delen av ARPANet ble stadig mindre fremtredende, og i 1983 ble den skilt ut i et eget nettverk (MILNET). Det amerikanske sivile forskningsrådet overtok administrasjonen av den sivile delen av nettet (NSFNET).

5.2.4 TCP/IP protokollen

I første halvdel av 1970-årene begynte også utviklingen av de første lokalnettene, og det ble klart at man ville få behov for en teknologi som kunne koble lokalnett sammen *(internetting)*.

For å knytte ulike nett sammen måtte det bygges *portnere* («gateways») som kunne *rute* (ta imot og videresende) informasjon til globale adresser og håndtere forskjellige pakkestørrelser. I tillegg ville man trenge en mer fleksibel og robust transportprotokoll enn den som ble benyttet i ARPANET. Dette gav støtet til utviklingen av **TCP/IP** *(Transmission Control Protocol/Internet Protocol)*, som er basis for dagens Internett.

De første TCP/IP-forsøkene fant sted i 1975, og i løpet av de neste årene ble protokollen kontinuerlig forbedret og utvidet med støttefunksjoner for et bredt spekter av tjenester. Berkeley-universitetet, som hadde kontrakt med DARPA om videreutvikling av AT&Ts UNIX-system, bygde TCP/IP inn i selve operativsystemet, som etter hvert ble stilt gratis til disposisjon for alle universiteter både i USA og Europa. Det samme skjedde med operativsystemer fra andre store leverandører.

5.2.5 Internett blir født

TCP/IP fikk etter hvert en så sentral posisjon at DARPA besluttet å innføre den som standardprotokoll i ARPANET. Dette arbeidet var ferdig i begynnelsen av 1983. Resultatet ble «et nett av nett» kalt **INTERNET**, også dette overvåket, vedlikeholdt og administrert av BBN. Alle tilkoblinger måtte fortsatt godkjennes av DARPA.

I 1986 tok National Science Foundation (NSF) i USA på seg ansvaret for å drive et høyhastighets stamnett *(backbone*) som skulle knytte sammen de fem nyetablerte supermaskinsentrene i USA. Romfartsorganisasjonen NASA tok ansvaret for et tilsvarende nett. Disse nettene ble koblet sammen med egnede rutere og hadde forgreninger til Europa.

Etter hvert ble den gjenværende delen av ARPANET overflødig: Det ble rimeligere og mer effektivt å benytte rutere og faste linjer med stor kapasitet. Mot slutten av 1980-årene ble derfor ARPANET faset ut, og dermed forsvant også INTERNET – det nettet som var blitt overvåket av BBN og kontrollert av DARPA.

I stedet kom et raskt voksende konglomerat av nett og rutere kalt *Internett*, definert som et nett av samtrafikkerende, TCP/IP-baserte datanett. Dette Internett hadde ingen overordnet struktur, og hadde mange eiere og driftsorganisasjoner.

5.2.6 Eierforhold og organisering

Internett har med andre ord ingen organisasjon som har totalansvaret for driften eller overvåkingen av nettet. Alle aktørene som opererer her er "deleiere" og har "delansvar" for det totale nettet.

En internett tilbyder eier oftest sin egen infrastruktur (eller leier den), og man kan si at tilbyderen eier sin lille del av internett, og har ansvaret for driften av sitt nett fram til dette nettets kontaktflate mot resten av internett (dette består som oftest av en eller flere routere).

5.2.7 World Wide Web (www)

Verdensveven eller bare **veven** (engelsk: *«World Wide Web»*, forkortet *WWW* eller *W3*) er et globalt informasjonsrom som gjør tekstdokumenter, bilder, multimedia og mange andre typer informasjon tilgjengelige over Internett.

Verdensveven ble utviklet i 1989 av Tim Berners-Lee ved fysikkinstituttet CERN i Sveits for bruk til intern informasjonsfremvisning. Den første vevtjeneren (*nxoc01.cern.ch*, senere omdøpt til *info.cern.ch*) kom på lufta en gang i november 1990. Den 30. april 1993 bestemte styret i CERN at World Wide Web-teknologien skulle være fri, dvs. at det ikke skal betales avgift for bruken.

Informasjonen på verdensveven betegnes som *ressurser*, som refereres til ved hjelp av en URL (internett adresse). Ved bruk av URL-er kan ulike ressurser enkelt referere til hverandre og indeksere, søke etter og kryssreferere all informasjonen på veven.

5.2.8 Nettleser

CERN og andre utviklet flere tekstbaserte nettlesere, men det var først når den **grafiske*nettleseren*** (eller *vevleseren*) *Mosaic* ble tilgjengelig i 1993 at bruken av World Wide Web spredte seg utenfor forskningsmiljøet. Etter at Mosaic ble tilgjengelig ble verdensveven raskt populær, og kan tilskrives en viktig del av æren for at Internett deretter fikk en eventyrlig rask utbredelse.

En nettleser er et lite gratis program som installeres på maskinen/telefonen din for å søke etter og vise de nettsiden som blir funnet. De største nettleserne er idag:

- **Google Chrome**
- **Internet Explorer**
- **Safari**
- **Firewall**
- **Opera**

5.2.9 Milepæler

Under finner du en kronologisk oversikt over de viktigste milepælene i Internetts utvikling. Listen er hentet fra Wikipedia.

1962: Visjonen om et «intergalactic network» – et verdensomspennende nettverk av datamaskiner hvor alle raskt kunne aksessere data og programmer fra er hvilket som helst sted – ble skapt av J.C.R. Licklider, leder av Information Processing Techniques Office ved ARPA.

1967: Plan for ARPANET ble publisert.

1968: ARPA's program plan for ARPANET, kalt "Resource Sharing Computer Networks" ble etablert. Kontrakter ble tildelt noen forskningsmiljøer som de første ARPANET sitene for å etablere ARPANET.

1969: Kommunikasjon mellom de fire første nodene i ARPANET ble etablert ved University of California Los Angeles (UCLA), Stanford Research Institute (SRI), University of California Santa Barbara og University of Utah. Remote login (Telnet) var første anvendelse.

1972: Elektronisk post ble introdusert på ARPANET. @-tegnet ble introdusert som ”at” i e-post adressene.

1972: ARPA starter programmet Internetting. Behov for å koble sammen flere nett basert på ulik teknologi (tele, radio, satellitt) skapte et behov for en overliggende nettverksarkitektur (open-architecture networking). Utviklingen av TCP/IP ble startet.

1973: Første internationale forbindelse til ARPANET: NORSAR i Norge og University College of London. Forbindelsen gikk via satellitt. NORSAR hadde allerede i 1970 overført seismiske data til USA via satellitt, og fikk i oppdrag å etablere de første

internasjonale forbindelsene til ARPANET. Flere norske forskningsmiljøer knyttet seg etter hvert til denne forbindelsen.

1973: Første versjon av TCP/IP (Transfer Control Protocol/Internet Protocoll) ble definert av Robert E. Kahn, ARPA og Vincent G. Cerf, Stanford . Dette er basisprotokollene i dagens Internett. Den ble spesifisert med 32 bits adresser som fortsatt er gjeldende – en hodepine idag med Internetts enorme utbredelse.

1977: Den første demonstrasjonen av trippel nettverk Internett basert på TCP/IP. Kommunikasjon over ARPANET, SATNET (satellitt) og mobilt Radio Packet Network ble demonstrert. Kommunikasjon fra en bil på San Francisco Bayshore Freeway gikk over Radio Packet Network til BBN, videre over ARPANET til London med satellittlink til Norge (NORSAR) og kabel til London. Deretter videre over SATNET (Atlantic Packet Satellite Network) til ARPANET i USA og gjennom ARPANET til USC Information Sciences Institute. Ikke ett bit ble borte! Implementeringen var utført av Stanford, BBN og University College London.

1979: ARPA etablerer Internet Configuration Control Board (ICCB).

1980: TCP/IP ble adoptert som standard for det amerikanske forsvaret.

1982: Norge blir tilkoblet ARPANET.

1982: ARPA sponset University of Berkeley for å legge TCP/IP inn i deres UNIX variant. Berkeley UNIX var utbredt ved en rekke universiteter i USA, og gjorde det enkelt å ta ibruk TCP/IP.

1983: ARPANET, som 113 universiteter og forskningsmiljøer da var tilkoblet, ble konvertert fra den opprinnelige protokollen NCP til TCP/IP. Dette ble nøye planlagt over flere år. ARPANET ble splittet i ARPANET og MILNET (forsvarsrelatert forskingsnett).

1984: Britiske JANET besluttet å benytte TCP/IP i sitt forskningsnett som skulle dekke alle høyere undervisningsinstitusjoner i Storbritannia. Dette var en viktig milepæl for utbredelsen i Europa.

1984: Domain Name System (DNS) introdusert. DNS er en distribuert Internett katalogtjeneste som oversetter domenenavn til IP-adresser.

1985: U.S. National Science Foundation (NSF) besluttet å benytte TCP/IP i NSFNET som skulle dekke alle høyere utdanningsinstitusjoner i USA. $200 millioner ble brukt i perioden 1986-1995 for utbygging av NSFNET. En rekke andre land knytter seg etter hvert til NSFNET som blir ryggraden i Internett. Også kommersiell virksomhet tillates tilknyttet.

1988: Første Interop utstilling ble holdt. 50 bedrifter viste at deres produkter kunne spille sammen vha. TCP/IP. Dette var en viktig milepæl for den kommersielle utbredelsen av Internett.

1990: ARPANET nedlagt. De fleste nodene er flyttet til NSFNET.

1990: Første kommersielle Internett aksess leverandør (world.std.com). Tilbyr oppringt samband til Internett.

1991: World Wide Web lanseres av engelskmannen Tim Berners-Lee, CERN (det europeiske laboratorium for partikkelfysikk). HTML (HyperText Markup Language), HTTP (HyperText Transfer Protocol) og URL (Universal Resource Locator) var definert og en nettleser utviklet. Drømmen bak Web var å skape et globalt informasjonsrom på Internett hvor hypertekstlinker gjør det enkelt å finne informasjon overalt på nettet. HTML var basert på SGML og beregnet på å definere struktur i form av kapitler, underkapitler og avsnitt. Det var opptil den enkelte nettleser å velge hvordan det skulle presenteres. Det ble raskt utviklet nettlesere i flere forskningsmiljøer. Dette er den viktigste hendelsen i internettets historie og bidro til å gjøre det tilgjengelig for hele verden.

1992: Nettleseren Mosaic ble utviklet av Marc Andresen og Eric Bina ved National Center for Supercomputing Applications ved University of Illinois at Urbana-Champaign. Denne ble den mest populære nettleseren. De fleste kommersielle nettlesere (inklusive Internett Explorer og Netscape Navigator) er basert på NCSA Mosaic. Dette er årsaken til at mange tror Web ble oppfunnet av NCSA.

1993: Mosaic tar Internet med storm; WWW-trafikken øker med 341 000 % på ett år.

1993: Internet Talk Radio begynner kringkasting.

1994: Netscape lanserer Navigator, den første kommersielle nettleseren.

1994: Første nettbutikker kommer på nettet.

1994: First Virtual, den første nettbanken, åpner.

1994: World Wide Web Consortium (W3C) blir dannet. Dette er et åpent forum hvor bedrifter og organisasjoner kommer sammen for å enes om nye standarder for Web. W3C ledes av Tim Berners-Lee, oppfinneren av World Wide Web.

1995: NSFNET går tilbake til å bli et rent forskningsnett. Kommersiell Internett trafikk er overtatt av sammenkoblede nettverksleverandører.

1995: Sun lanserer JAVA. Java er et generelt programmeringsspråk som er helt maskinuavhengig og beregnet for bruk over Internett. Java gjør det mulig å utvikle programmer som kan lastes ned fra Internett og kjøres på en hvilken som helst maskin uansett operativsystem. JAVA programmer kjøres gjerne fra en nettleser.

1995: Microsoft lanserer Internett Explorer og leverer det som en del av Windows. Dette medfører at alle PC-er med Windows (og det er de fleste), lett får tilgang til Web.

1996: Søkemotorer kommer. De mest kjente er WebCrawler, Hotbot, Excite, Infoseek og AltaVista.

2000: Web passerer én milliard web-sider. Suksessen er et faktum. Lickliders visjon har gått i oppfyllelse – i allfall på jorden.

5.3 TCP/IP

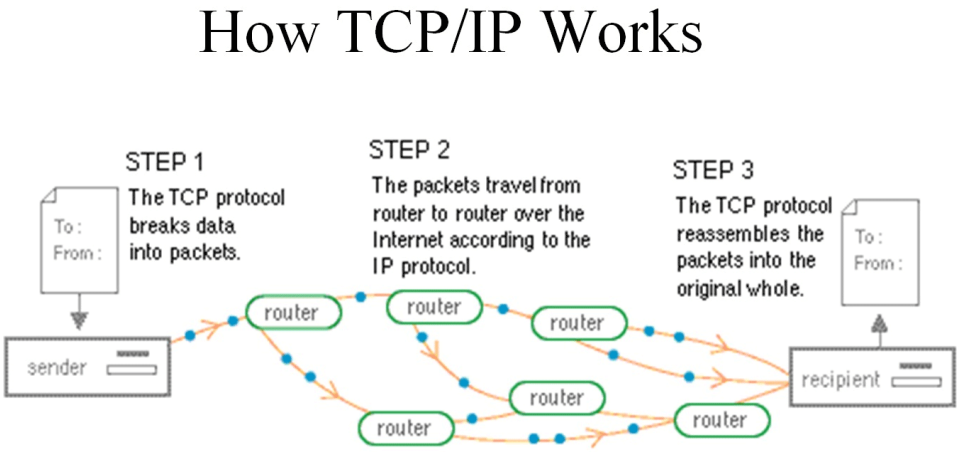


Figure 2. How data travels over the Net.

5.3.1 Hva er TCP/IP?

TCP/IP (forkortelse for *Transmission Control Protocol/Internet Protocol*) er en gruppe kommunikasjonsprotokoller som benyttes for å koble sammen datamaskiner i nettverk på Internett.

Protokollen ble utviklet av Robert E. Kahn og Vinton G. Cerf, og er idag standarden som benyttes for å koble sammen og sende data mellom enhetene på Internett. Vi kan gå så langt som å si at uten dagens TCP/IP nettverk så ville vi ikke hatt noe Internett. TCP/IP protokollen er idag grunnmuren på Internett.

TCP/IP består av to protokoller;

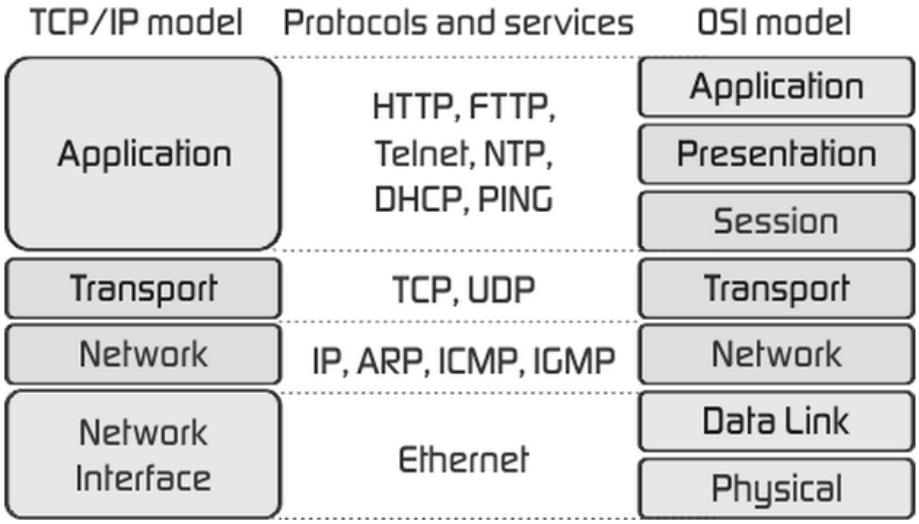
- **TCP (Transmission Control Protocol)** - er en protokoll som sikrer pålitelig transport av datasignaler mellom brukerprogrammer som kommuniserer via det logiske nettet.
- **IP (Internet Protocol)** - gjør det mulig å koble sammen forskjellige underliggende nett til et felles logisk nett. De underliggende nettene kan være basert på ulike teknologier.

5.3.2 Hva er en protokoll?

Nettverk fungerer ved at datamaskiner, skrivere og andre enheter sender data til hverandre, enten via kabler eller trådløse signaler. Denne datautvekslingen er mulig ved hjelp av et sett dataoverføringsregler som kalles ***protokoller***.

En protokoll er et slags språk, og på samme måte som språk har regler, har en protokoll regler som tillater deltakerne å kommunisere med hverandre. Reglene bestemmer hvordan tilkoblingen skjer, kommunikasjonen og dataoverføringen mellom to endepunkter (f.eks. mellom nettleseren på din datamaskin og web-serveren til din nettsider).

Det finnes i dag en lang rekke ulike protokoller som alle har sine egne unike spesifkasjoner, men de inngår alle som forskjellige lag i OSI-modellen som dokumenteres gjennom RFC-dokumenter publisert av Internet Engineering Task Force (IETF).



De viktigste lagene i OSI-modellen kan forklares slik:

- **Applikasjons-protokoller** er øverst i modellen. Nærmest brukeren og bortest fra maskinvaren: DHCP, DNS, HTTP, FTP, Telnet, SMTP og SNMP.
- **Transport-protokoller** er ansvarlig for "connection-orienterte" sessioner og "connectionless" broadcasts: TCP og UDP.
- **Internet-protokoller** er ansvarlig for ruting: IP, ARP, ICMP og IGMP.
- **Nettverks-protokoller** er nederst i modellen. Nærmest maskinvaren og bortest fra brukere. De plasserer dataframes i nettverket: Plain Old Telephone Service (PLOTS), ISDN og ATM.

5.3.3 TCP

Transmission Control Protocol (**TCP**) er en nettverksprotokoll for forbindelsesorientert, pålitelig overføring av informasjon, og opererer på transportlaget i OSI-modellen for datanett.

I protokollsettet for Internett, opererer TCP mellom Internett-protokollen (under), og en applikasjon (over). Applikasjonene trenger som oftest en pålitelig tilkobling mellom endepunktene, noe Internett-protokollen ikke tilbyr alene.

Applikasjonene sender strømmer av 8-biters tegn gjennom nettverket, og TCP-protokollen deler denne strømmen opp i pakker med en bestemt størrelse (vanligvis bestemt av nettverket som datamaskinen er koblet til). TCP sender så pakkene videre til Internett-protokollen som sørger for at de blir sendt til TCP-modulen i den andre enden av forbindelsen. TCP passer på at ingen pakker forsvinner ved å gi hvert tegn i strømmen et *sekvensnummer*, som også blir brukt for å forsikre at pakkene blir levert i riktig rekkefølge hos mottakeren.

TCP-modulen i mottaker enden sender så tilbake en kvittering for tegn som er blitt mottatt. Hvis kvitteringen ikke er mottatt innen et visst tidspunkt, vil et *tidsavbrudd* oppstå. Da vil sender anta at pakken er tapt, og pakken må sendes på nytt. TCP sjekker også at datastrømmen ikke er skadd ved å bruke en sjekksum. Sjekksummen blir beregnet av senderen, og kontrollert hos mottaker, for hver pakke.

TCP forbindelser har tre faser:

1. **opprettelsen av en forbindelse**
2. **dataoverføringen**
3. **avslutningen av forbindelsen**

Et tre-veis *håndtrykk* blir brukt for å opprette en forbindelse. Et fireveis håndtrykk blir brukt for å avslutte en forbindelse. I opprettelsesfasen av en forbindelse vil parametre som sekvensnummer bli initialisert for å oppnå riktig rekkefølge på pakkene og robusthet.

5.3.4 TCP-porter

TCP bruker portnummer for å identifisere sender- og mottakerapplikasjoner. Applikasjonen på hver side av en TCP-forbindelse får tildelt et 16-bit unsigned portnummer. Porter er kategorisert i 3 grunnleggende kategorier:

- **kjente**
- **registrerte**
- **dynamiske/private**

De **kjente portene** er tildelt av *Internet Assigned Numbers Authority* (IANA) og er typisk brukt av systemnivå eller rotprosesser. Velkjente applikasjoner som kjører som tjenere og venter passivt på tilkoblinger fra klienter bruker typisk disse portene. Noen eksempler på slike er: FTP (21), Telnet (23), SMTP (25) og HTTP (80).

Registrerte porter blir typisk brukt av brukerapplikasjoner som midlertidige kildeporter når tjenere kontaktes, men disse portene kan også identifisere kjente tjenester registrert av en tredjepart. **Dynamiske/private porter** kan også bruke av sluttbrukerapplikasjoner, men blir ikke så ofte brukt på den måten. Dynamiske/private porter har ingen mening utenfor en bestemt TCP-forbindelse. TCP-portnummeret lagres i et felt på 16-bit i TCP-hodet, og 65535 porter er dermed tilgjengelige.

5.3.5 Internet Protocol (IP)

Wikipedia forklarer begrepet Internet Protocol slik:

> *"IP er en forbindelsesløs og upåliteligpakkeleveringstjeneste som er grunnsteinen i IP-protokollsettet.*
>
> *Med upålitelig menes at det er ingen garantier for at en IP-pakke kommer frem. En årsak til at en IP-pakke ikke kommer frem kan være at en ruter går tom for bufferlager og må kaste pakker. Konfigurasjonsfeil på rutere kan også føre til pakketap, bl.a. hvis feilen forårsaker en loop.*
>
> *Med forbindelsesløs menes at hver enkelt IP-pakke behandles uavhengig, IP lager ingen tilstand til strømmene av pakker. Dette fører til at pakker kan komme ut av rekkefølge til mottakeren. Hvis det er ønskelig med pålitelighet og at pakker skal bli levert til mottakerapplikasjonen i rekkefølge, benyttes en pålitelig transportlagsprotokoll som TCP.*
>
> *Den mest brukte versjonen av IP er IPv4. Arbeidet med etterfølgeren IPv6 ble påbegynt i 1994 og er relativt moden, men har ikke blitt tatt i bruk i noen stor grad."*

5.3.6 IP-adresse

Datamaskiner forstår ikke ord. De bruker derfor tall til å kommunisere med hverandre. TCP/IP protokollen krever derfor at alle enheter i nettverket har en egen unik IP-adresse. En IP-adresse kan sammenlignes med en gateadresse eller et telefonnummer ved at den brukes til å identifisere en enhet fra andre.

IP adresser brukes til å identifisere enheter og overføre data mellom enhetene i et nettverk. En slik enhet kan være en datamaskin, skriver eller en annen enhet som har sin egen IP adresse.

IP-adresser er entydige navn i numerisk format, og tillater TCP/IP å bekrefte forespørsler om og motta data fra forskjellige enheter i nettverket.

Den tradisjonelle IP-adressen (kjent som IPv4) bruker et 32-biters tall til å representere en IP-adresse, og den definerer både nettverks- og vertsadressen. Siden en IP-adresse er basert på 32-biters nummer gir standarden oss muligheten til å gi omtrent generere 4 milliarder unike tall. Dette er den største begrensningen på Internett idag, da Internett ikke tillater at mer enn 4 milliarder unike enheter å være koblet på Internett samtidig.

En ny versjon av IP-protokollen (IPv6) er oppfunnet for å tilby nesten ubegrenset antall unike adresser, men å tilpasse alt datautstyr til denne standarden tar både tid og koster mye penger. Overgangen til denne standarden går derfor ennå sakte.

En IP adresse består av 32 bit, organisert i fire sett med et 8-biters tall (0-255) og er på formen **w.x.y.z**. Et eksempel på IP adresse er følgende adresse på desimalt format:

128.121.188.201

Denne IP adressen kan også skrives på binært format:

10000000.1111001.10111100.11001001

Grunnen til at vi har to ulike former for samme IP adressen er at desimale tall er mer forståelig for mennesker, mens datamaskiner forstår kun binære tall.

En IPv4-adresse er delt inn i to deler:

1. **nettverksadresse**
2. **vertsadresse**

Nettverksadressen bestemmer hvor mange av de 32 bitene som brukes til nettverksadressen og de gjenværende bitene brukes til vertsadressen. Vertsadressen kan videre deles inn i delnettverk og vertsnummer.

5.3.7 IP-klasser

IP adresser deles i 5 klasser som passer ulike behov.

- **KLASSE A**
  Brukes for meget store nettverk. Adressen starter med binære tallet 0
  1-126.x.y.z og subnett maske er 255.0.0.0
  Den første delen av adressen (w) brukes for nettverks-ID, de resterende tre delene (x.y.z) brukes for host-ID.
  Antall mulige nettverk = 2^7 - 2 = 126
  Antall mulige hosts = 2^{24} - 2 = 16 million per nettverk.

  127.0.0.1 er reservert for loopback som brukes for testing.

- **KLASSE B**
  Brukes for store og mellomstore nettverl. Adressen starter med binære tallet 10 og subnett maske er 255.255.0.0
  128-191.x.y.z
  De to første delene av adressen (w.x) brukes for nettverks-ID, de resterende to delene (y.z) brukes for host-ID.
  Antall mulige nettverk = 2^{14} - 2 = 16 tusen
  16 - 2 = 65 tusen per nettverk.

- **KLASSE C**
  Brukes for små nettverk. Adressen starter med binære tallet 110
  192-223.x.y.z og subnett maske er 255.255.255.0
  De tre første delene i adressen (w.x.y) brukes for nettverks-ID, den resterende delen (z) bruke for host-ID.
  Antall mulige nettverk = 2^{21} - 2 = 2 million
  Antall mulige hosts = 2^{8} - 2 = 254 per nettverk.

- **KLASSE D**
  Brukes for multicast. Adressen starter med binære tallet 1110
  224-239.x.y.z

- **KLASSE E**
  Reserverte adresser. Adressen starter med binære tallet 1111
  240-255.x.y.z

5.3.8 Offentlige og private IP-adresser

For å opprettholde unikhet innenfor globalt navneområde, er IP-adressene offentlig registrert med **N**etwork **I**nformation **C**enter (NIC) for å unngå adressekonflikter. I denne sammenheng må vi skille mellom:

1. **Offentlig IP-adresse**. Enheter som må kunne identifiseres offentlig, for eksempel web- eller e-postservere, må ha en globalt unik IP-adresse; og de tildeles en offentlig IP-adresse.
2. **Privat IP-adresse**. Enhetene som ikke krever offentlig tilgang kan tildeles en privat IP-adresse og gjøre den unik identifiserbar i en organisasjon. For eksempel kan en nettverksskriver tildeles en privat IP-adresse for å hindre at resten av verden skriver ut fra den.

For å tillate organisasjoner fritt tildele private IP-adresser, har NIC reservert bestemte adresseblokker for privat bruk. Et privat nettverk er et nettverk som bruker RFC 1918 IP-adresserom. Følgende IP-blokker er reservert for private IP-adresser.

Klasse	Starte IP-adresse	Avslutter IP-adresse
EN	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

I tillegg til overklassifiserte private adresser, er 169.254.0.0 til 169.254.255.255 adresser reservert for Zeroconf (eller APIPA, automatisk privat IP-adressering) for å automatisk opprette det brukbare IP-nettverket uten konfigurasjon.

5.3.9 Loopback IP-adresse

Loopback-IP-adressen er adressen som brukes til å få tilgang til seg selv. IPv4 utpekte **127.0.0.1** som loopback-adressen med 255.0.0.0 subnettmasken . Et loopback-grensesnitt er også kjent som en virtuell IP, som ikke knytter seg til maskinvaregrensesnittet. På Linux-systemer kalles loopback-grensesnittet **lo** eller **lo0**. Det tilsvarende vertsnavnet for dette grensesnittet kalles **localhost** .

Tilbakekallingsadressen brukes til å teste nettverksprogramvare uten å installere et **N**etwork **I**nterface **C**ard (NIC) fysisk, og uten å koble maskinen til et TCP / IP-nettverk fysisk. Et godt eksempel på dette er å få tilgang til webserveren som kjører på seg selv ved å bruke http://127.0.0.1 eller http: // localhost.

5.3.10 CIDR - Classless Inter Domain Routing

Classless **I**nter **D**omain **R**outing (CIDR) ble oppfunnet for å hindre Internett i å løpe ut av IP-adresser. IPv4, en 32-biters adresser har en grense på 4 294 967 296 unike IP-adresser. Det klassiske adressesystemet (klasse A, B og C) for å tildele IP-adresser i 8-bits inkrementer kan være veldig sløsing. Med klassisk adressering, er et minimum antall IP-adresser som er tildelt en organisasjon 256 (klasse C). Å gi 256 IP-adresser til en organisasjon som bare krever 15 IP-adresser, er sløsing. Også en organisasjon som krever mer enn 256 IP-adresser (la oss si 1000 IP-adresser) tildeles en klasse B, som tildeler 65.536 IP-adresser. Tilsvarende tildeles en organisasjon som krever mer enn 65.636 (65.634 brukbare IPer) et klasse A-nettverk, som tildeler 16.777.216 (16.7 millioner) IP-adresser. Denne typen adresseallokering er veldig sløsing.

Med CIDR tildeles et nettverk av IP-adresser i 1-biters trinn i motsetning til 8-bits i klassisk nettverk. Bruken av en CIDR-notert adresse kan enkelt representere klassiske adresser (klasse A = / 8, klasse B = / 16 og klasse C = / 24). Tallet ved siden av skråstreket (dvs. / 8) representerer antall biter som er tildelt nettverksadressen.

CIDR adresseringen har gjort at IP-adressene blir mer effektivt allokert og gjør at vi ennå ikke har gått tom for IP-adresser.

5.3.11 MAC-adresse

MAC, **M**DIAE **A**ccess **C**-regulering, adresse er en globalt unik identifikator tilordnet nettverksenheter, og derfor er det ofte referert til som maskinvare eller fysisk adresse. MAC-adresser er 6-byte (48-bits) i lengde, og er skrevet i MM: MM: MM: SS: SS: SS-format. De første 3-byte er ID-nummer til produsenten, som er tildelt av en Internett-standard kropp. Den andre 3-byten er serienummer tildelt av produsenten.

MAC-lag representerer lag 2 av TCP / IP (vedtatt fra OSI-referansemodell), der IP representerer lag 3. MAC-adressen kan betraktes som støtte for maskinvareimplementering mens IP-adresse støtter programvareimplementering. MAC-adresser blir permanent brent inn i maskinvare av maskinvareprodusenten, men IP-adresser tilordnes nettverksenhetene av en nettverksadministrator. DHCP er avhengig av MAC-adresse for å tilordne IP-adresser til nettverksenheter.

5.3.12 Hvordan finner jeg en MAC-adresse på nettverksenheten?

Operativsystemer støtter ulike kommandolinje- og GUI-verktøy for å tillate brukere å finne MAC-adressen til systemet. På Unix-varianter, inkludert Solaris og Linux, støttes "ifconfig -a" , "ip link list" eller "ip address show" kommandoen som viser MAC-adressen til nettverksenheten blant annen nyttig informasjon. Windows, inkludert NT, 2000, XP og 2003, støtter "ipconfig / all" -kommandoen som viser MAC-adressen. På en MacOS kan man finne MAC-adresse ved å åpne "System Preferences" og deretter velge "Network".

5.3.13 Rutere

En **rutere** brukes til å knytte sammen to eller flere nettverkssegmenter, og filtrerer (rute) datapakker til riktig port på samme måten som bro. Mens en ruter fungerer på nettverkslaget i OSI-modellen, fungerer en bro i det fysiske laget (MAC). Ruter kan knytte sammen segmenter fra ulike typer nettverk, i motsetning til hva en bro kan gjøre.

5.3.14 Rutingtabell

Rutingtabell brukes av en datamaskin eller ruter til å avgjøre hvilken rute en datapakke skal sendes videre til. Tabellen avgjør om datapakkene skal beholdes i samme lokale nettverkssegment, om de skal sendes til neste nærmeste ruter, eller om de skal sendes til default gateway i samme segmentet.

Du kan lese rutingtabellen ved å skrive følgende kommando via kommandolinjen:

route print

Følgende rutingtabell tilhører en datamaskin med ett nettverkskort som har IP-adressen 172.16.8.50:

Nettverksmål	Nettverksmaske	Gateway	Grensesnitt	M
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
172.16.8.0	255.255.255.0	172.16.8.50	172.16.8.50	1
172.16.8.50	255.255.255.255	127.0.0.1	127.0.0.1	1
172.16.255.255	255.255.255.255	172.16.8.50	172.16.8.50	1
224.0.0.0	224.0.0.0	172.16.8.50	172.16.8.50	1
255.255.255.255	255.255.255.255	172.16.8.50	172.16.8.50	1

Nettverksmål er destinasjonsadressen i nettverket.

Nettverksmaske er den delen av nettverksadressen som må matche hvis ruten skal brukes.

Gateway er adressen der datapakken må videresendes til. Dette er nettverkskort eller nærmeste ruter.

Grensesnitt er adressen til nettverkskortet som datapakkene må passere.

Metrikk (M) er antall hopp til destinasjonsnettverk.

5.3.15 Subnetting

Subnetting er deling av et nettverk opp i et visst antall subnett som knyttes sammen med rutere. Dette gjør nettverket raskere og mer fleksibelt.

Et nettverk deles opp i subnett ved å låne bits fra host-ID delen av IP-adressen. Med de lånte bitsene lages subnet-ID for hvert subnett. Jo flere bits som lånes jo flere subnett kan man lage, men da blir det også mindre antall mulige hosts for hvert subnett.'

Det er subnett masken som avgjør hvor mange bits som lånes fra host-ID. La oss si at vi har nettverks-ID 172.16.0.0 som skal deles i 6 subnett. For å få dette til bruker vi subnett masken 255.255.224.0. Da har vi 6 subnett med følgende mulige IP-adresser:

- 172.16.32.1 -> 172.16.63.254
- 172.16.64.1 -> 172.16.95.254
- 172.16.96.1 -> 172.16.127.254
- 172.16.128.1 -> 172.16.159.254
- 172.16.160.1 -> 172.16.191.254
- 172.16.192.1 -> 172.16.223.254

Det er som regel tungvinn prosess å regne ut subnett mask og mulig IP-adresser manuelt. Det finnes programmer for dette, for eksempel Daryl's Subnet Calculator.

5.3.16 Subnett maske

En IP-adresse har to komponenter, nettverksadressen og vertsadressen. En nettverksmaske (subnet maske) skiller IP-adressen til nettverket og vertsadressene (<nettverk> <vert>). Videre deles vertsdelen av en IP-adresse til en subnett og vertsadresse (<nettverk> <subnett> <host>) dersom det er behov for ytterligere delnettverk. Bruk Subnet Calculator til å hente undernettverksinformasjon fra IP-adresse og Subnet Mask. Det kalles en nettverksmaske fordi den brukes til å identifisere nettverksadressen til en IP-adresse ved å perfisere en bitvis AND-operasjon på nettmasken.

Dette er et 32-bit nummer som brukes til å dele en IP-adresse opp i nettverks-ID og host-ID. Hensikten er å fortelle rutere om en IP adresse er på lokalt subnett eller et annet subnett. Default subnettmaske er 255.0.0.0 for klasse A IP adresser, 255.255.0.0 for klasse B og 255.255.255.0 for klasse C.

Subnet Mask er laget ved å sette nettverksbiter til alle "1" s og sette vertsbiter til alle "0" s. Innenfor et gitt nettverk er to vertsadresser reservert for spesielle formål, og kan ikke tilordnes verter. "0" -adressen er tildelt en nettverksadresse og "255" er tildelt en kringkastingsadresse, og de kan ikke tilordnes verter.

Skal man regne dette ut manuelt bør man bruke binære tall istedet for desimale tall.

172.16.0.0 -> 10101100 10000000 00000000 00000000

For å dele 172.16.0.0 opp i 6 subnett må man låne 3 bits fra host-ID. Antall subnet får man med denne formelen: 2^n - 2. Det gir 2^3 = 8 - 2 = 6 subnett.

5.3.17 NetBIOS

Datamaskiner forstår kun det binære tallsystemet (nullere og enere), mens mennesker bruker navn (**NetBIOS-navn**) for å identifisere hver enkelt datamaskin i et nettverk. Derfor må navnet konvertere til IP-adresse og omvendt. Slike konverteringer (navn resolusjon) skjer automatisk, og brukeren trenger som regel ikke å tenke på det.

5.3.18 WINS

"Windows Internet Name Service" (WINS) er en dynamisk tjeneste som registrerer NetBIOS navn på datamaskiner (hosts) i et nettverk. WINS har altså en liste over NetBIOS navn i nettverket.

WINS servere oversetter NetBIOS navn til IP adresser, slik at datamaskiner i nettverket kan kommunisere med hverandre.

5.4 DHCP

DHCP er automatisk tildeling av IP adresser til klienter (datamaskiner).

DHCP er en forkortelse for "***Dynamic Host Configuration Protocol***", eller "*Den dynamiske vertskonfigurasjonsprotokollen*" på norsk.

DHCP er en nettverksprotokoll som fungerer på applikasjonslaget i OSI-modellen. En server som bruker DHCP, vil kunne tilordne IP-adresser og andre nettverkskonfigurasjonsparametere dynamisk til enheter på nettverket, og dermed tillater kommunikasjon til andre nettverk og enheter. Protokollen kan implementeres i nettverk av alle størrelser, alt fra små hjemmenettverk (HAN) til store campusnettverk (CAN) og til og med nettene som brukes av Internettleverandører (ISPer).

5.4.1 Hvordan virker DHCP?

DHCP kjører i en klient / server modus, hvor serveren oppretter et basseng av tilgjengelige IP-adresser for et nettverk. En DHCP-server gir også brukeren en nettverksgateway, subnetmasker, navneservere og en tid en gitt IP-adresse vil være gyldig. En DHCP-klient henter disse parametrene og bruker dem til å bli med i det eksisterende nettverket. I hjem og små kontorer fungerer en ruter også som en DHCP-server. I et større nettverk kan en dedikert server fungere som en DHCP-server sammen med å utføre andre serveraktiviteter.

Prosessen med å skaffe en IP-adresse fra DHCP-serveren er som følger.

- En datamaskin (klient) som er konfigurert til å bruke DHCP, sender en DHCP DISCOVER-forespørsel til nettverket.
- En DHCP-server mottar en DHCP DISCOVER-forespørsel. Serveren slår opp tilgjengelige IP-adresser i sin IP-adressepool og gir klienten en ledig IP-adresse. Har den samme klieenten tidligere hatt en midlertidig IP-adresse tildeler DHCP-serveren den samme IP-adressen til klienten. DHCP-serveren sender DHCP OFFER-respons til klienten.
- Klienten mottar svaret på DHCP-tilbudet og svarer på DHCP-serveren ved å sende DHCP REQUEST-pakken for å godta tilbudet.
- DHCP-serveren sender ACK (acknowledge) -pakke for å bekrefte IP-adressetildeling. Hvis IP-adressen ikke lenger er tilgjengelig, sendes NACK (No acknowledge) -pakke og prosessen gjentas til klienten mottar en gyldig IP-adresse fra serveren.

5.4.2 Hva er fordelene med å bruke DHCP?

En datamaskin, nettbrett eller smarttelefon som trenger å bli med på et eksisterende nettverk (hjemme eller kontor) må konfigureres på riktig måte for å kommunisere med andre enheter i nettverket. Manuell konfigurering av statiske IPv4- eller IPv6- adresser sammen med nettverksspesifikke opplysninger resulterer i menneskelige feil, da det er betydelig antall sifre som skal skrives inn. Manuell konfigurasjon kan også ende opp med å tilordne en samme IP-adresse til flere enheter som forårsaker en IP-konflikt. DHCP automatiserer den besværlige manuelle prosessen og tildeler IP-adressen dynamisk.

DHCP tillater nettverksadministratorer sentralt å administrere og automatisere tildelingen av IP-adressene uten å måtte bekymre seg om å tilordne en duplikat IP-adresse til flere datamaskiner og skrive inn nettverksgateway, nettverksmaske og annen nettverksrelatert informasjon til hver datamaskin og dermed lage nettverk administrasjon mye enklere å administrere.

5.4.3 Hvordan vet du om du bruker DHCP

Hvis du vil vite om du bruker en dynamisk eller statisk IP-adresse, kan du bruke kommandoen **ipconfig** på Windows. På MAC- eller Linux-maskiner kan du bruke **ifconfig-** kommandoen.

På Windows-maskinen ligner kommandoen **ipconfig-** kommandoen slik.

```
C:\>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : iplocation
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) PRO/Wireless LAN 2100 3B Mi
ni PCI Adapter
        Physical Address. . . . . . . . . : 00-0C-F1-65-5B-70
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 192.168.1.1
        Lease Obtained. . . . . . . . . . : Thursday, February 08, 2007 2:27:17 PM
        Lease Expires . . . . . . . . . . : Thursday, February 15, 2007 2:27:17 PM
```

På Mac- og Linux-maskiner vil utdataene **ifconfig** se slik ut.

```
bash %>ifconfig
eth0      Link encap:Ethernet  HWaddr F2:3C:91:DB:8A:88
          inet addr:192.168.1.96  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:27522604 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27666143 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2704290926 (2.5 GiB)  TX bytes:52580665594 (48.9 GiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:17632 errors:0 dropped:0 overruns:0 frame:0
          TX packets:17632 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:2249069 (2.1 MiB)  TX bytes:2249069 (2.1 MiB)
```

5.4.4 Struktur og funksjonalitet

En DHCP-server utfører sin funksjonalitet ved å aktivere enheter på nettverket ved å automatisk tildele hver enhet en unik IP-adresse. Denne prosessen gjør at nettverket kan fungere uten at en nettverksadministrator trenger å manuelt tilordne IP-adresser til hver enhet på nettverket. Protokollen benytter en klient-server-modell, hvor DHCP-klientprogramvaren automatisk sender en forespørsel til alle enhetene på nettverket når enheten blir koblet på nettverket for å be om informasjon fra de andre enhetene.

Spørringen blir gjenkjent av alle DHCP-server på nettverket som vil administrere en IP-adresse for et IP-basseng og andre viktige standardkonfigurasjonsinnstillinger, som standard gateway, domenenavn, tidsservere og navneserverne. Serveren som gjenkjenner forespørselen, kan svare med relevant forhåndsdefinert informasjon til klienten.

Disse spørringene sendes vanligvis umiddelbart etter en klient oppstart og med jevne mellomrom etterpå før informasjonen utløper. Det skal også bemerkes at når klienten ber om ny informasjon for et oppdrag, krever det vanligvis de samme verdiene, men dette kan endres av nettverksadministratoren avhengig av oppdragspolicyene som er konfigurert på serveren. I tilfelle at denne informasjonen ikke er forhåndskonfigurert av en nettverksadministrator, vil den i stedet svare med en bestemt adresse og annen informasjon som passer for hele nettverket og i løpet av gyldig tidsperiode.

Fordelingen av IP-adresser kan gjøres på en av tre måter, avhengig av DHCP-serverens implementering. Dynamisk allokering oppnås av nettverksadministratoren som angir en rekke IP-adresser som serveren skal bruke til å utstede til klienter i en allokert tidsperiode. Denne forespørsels- og tildelingsprosessen fungerer som en leieavtale hvor serveren kan gjenvinne adresser som ikke er fornyet av klienten for omfordeling til andre kunder.

Automatisk tildeling ligner dynamisk tildeling da nettverksadministratoren angir rekkevidden av IP-adresser for serveren som skal brukes; Disse adressene er imidlertid permanent knyttet til klienter som kobler seg til serveren. Dette betyr at serveren også vil føre en oversikt over hvilke adresser som er knyttet til hvilke klienter, slik at når en klient kobler seg til den serveren, kan de motta samme IP-adresse som den siste tiden da de var tilkoblet.

Til slutt blir manuell (eller statisk) tildeling oppnådd av nettverksadministratoren å sette opp et kartleggingsskjema for serveren som skal brukes. Når konfigurasjonen er konfigurert, utsteder serveren hver klient en privat IP-adresse basert på MAC-adressen (Media Access Control). I tilfelle at en kamp for klientens MAC-adresse ikke kan kartlegges, kan serveren i stedet bruke en av de andre allokeringsmetodene.

Protokollen brukes til både IPv4 og IPv6 og utfører de samme oppgavene i begge versjoner, men detaljene for hver av dem er forskjellige nok til at de kan betraktes som to separate protokoller. Uavhengig av dette bruker protokollen brukerdatagramprotokollen (UDP) til å bruke en forbindelsesløs modell. Den bruker to UDP portnumre for operasjonen portnummer 67 brukes til en server mens 68 er for klienten. Disse operasjonene kan da deles inn i fire faser: serveroppdagelse, IP lease tilbud, IP lease

forespørsel, og IP lease bekreftelse. Et vanlig akronym som brukes til å beskrive disse faser er DORA som står for oppdagelse, tilbud, forespørsel og bekreftelse.

I funn fasen sender klienten en DHCPDISCOVER melding til alle enheter på nettverket ved å bruke adressen 255.255.255.255 eller den spesifikke nettverksutsendingsadressen. Det skal også bemerkes at en klient også kan be om sin siste kjente IP-adresse, men resultatene kan variere. Hvis klienten er på samme nettverk som når den først er tilkoblet, vil forespørselen bli kvittert uten problem. Hvis dette ikke er tilfelle, vil det imidlertid avhenge av om serveren er autoritativ eller ikke. En autorisert DHCP-server vil nekte forespørselen og tvinge klienten til å be om en ny adresse, mens en ikke-autoritativ DHCP-server vil ignorere forespørselen som kan føre til at det utelates for klienten, avhengig av om den ble implementert og har de ber om en ny IP-adresse.

Under tilbudsfasen mottar en DHCP-server en DHCPDISCOVER-melding fra en klient på nettverket og reagerer ved å reservere en IP-adresse for klienten og svarer med en DHCPOFFER-melding til klienten. Dette responstilbudet vil inneholde IP-adressen, nettverksmasken, varighetstiden for leieavtalen, MAC-adressen til klienten og IP-adressen til serveren.

Som svar på tilbudet fra en DHCP-server svarer klienten med en DHCPREQUEST-melding for å legge inn forespørselsfasen. Denne meldingen angir at klienten godtar serverens tilbud, men det bør bemerkes at mens en klient kan motta mange tilbud fra en rekke servere, kan den bare utstede en forespørsel om å godta et av tilbudene. Avhengig av serveridentifikasjonsalternativet i forespørselen og kringkastingsmeldingen, er det mulig for alle DHCP-servere å bli informert om hvilket tilbud en klient har akseptert. Dette gjør det mulig for servere som kan ha ventende tilbud å trekke dem tilbake og returnere den reserverte IP-adressen tilbake til deres basseng av tilgjengelige adresser.

Til slutt, når serveren mottar DHCPREQUEST-meldingen som en aksept av tilbudet fra en klient, går prosessen inn i kvitteringsfasen ved at serveren sender en DHCPACK-melding tilbake til klienten. Denne meldingen vil inneholde leieavtalen og eventuelle andre konfigurasjonsparametre som klienten kan ha bedt om og bringer prosessen til slutt.

Det skal også bemerkes at det er mulig å sette opp et DHCP-relé eller DHCP-hjelpemiddel hvis klienten og serveren er på forskjellige undernettverk i et nettverk. I disse scenariene vil DHCPDISCOVER-meldingen bli sendt til det delnett som serveren er på. Dette oppnås ved å ha to relé agenter oppsett på begge delnett, slik at de kan overføre meldingene til de tiltenkte mottakere.

5.4.5 Sikkerhet

DHCP har vanligvis ikke noen systemer for godkjenning og kan bli offer for tre typer angrep.

1. Uautoriserte servere kan gi feil informasjon til klienter, da det ikke er mulig for en klient å identifisere en gyldig DHCP-server på nettverket. Disse rogue DHCP-serverne kan dra nytte av dette og bli brukt i et DOS-angrep for å forhindre riktig serverfunksjon eller i et man-i-midten-angrep for å få informasjon.
2. Omvendt kan det også være uautoriserte klienter som får tilgang til ressurser, da det ikke er mulig for serveren å autentisere en DHCP-klient heller. Dette vil tillate kundene å få en IP-adresse fra serveren til tross for ikke å være en gyldig klient ved å maskere seg som en. Nok uautoriserte klienter som gjør dette, kan faktisk eksplodere serverens adressepool og også påvirke den riktige funksjonen til nettverket.
3. Den tredje klassifiseringen av angrep er repeterende og uttømmende angrep fra ondsinnede kunder.

For å bekjempe disse angrepene ble Relay Agent Information Option Protocol skapt for å tillate nettverk å knytte autorisasjonskoder til DHCP meldinger. Denne taggen blir brukt til å kontrollere klientens tilgang til serverens ressurser. Siden klientene ikke har noen forbindelse til oppstrømsnettet av reléagenten, vil mangelen på validering ikke hindre at serveren stolte på taggen. Godkjenning av DHCP-meldinger var en annen innovasjon som gjorde det mulig å validere meldinger, selv om dette er blitt utbredt på grunn av problemene vi møter når vi administrerte nøklene til et stort antall klienter. Samlet sett blir disse teknikkene referert til som DHCP Snooping.

5.5 ISP (Internet Service Provider)

For å kunne surfe på Internett og bruke tjenestene som finnes der trenger du en internettlinje som er koblet til enheten du ønsker å bruke på Internett.

Med **internettlinje** menes:

> ***En datalinje som tillater kommunikasjon over TCP/IP protokollen og som er koblet på stamnettet for Internett via en node***

Nøkkelordene er her: TCP/IP kommunikasjon og stamnettet.

TCP/IP protokollen er den gjeldende protokollen for Internett og styrer all kommunikasjon og alle tjenestene på Internett. Uten den ville vi ikke hatt noe Internett.

5.5.1 Stamnettet

Internett er ikke ett enkelt nettverk, men en samling av millioner av mindre TCP/IP nettverk som er koblet sammen via noder til et større stamnett. Stamnettet er en angivelse av den delen av telenettet hvor hovedsentralene er koblet sammen via høyhastighetskabler.

Stamnettet i Norge eies og drives av Bane og Teletilsynet og består av en rekke høyhastighetskabler som går igjennom hele landet og som er koblet videre til andre lands stamnett via ulike noder.

5.5.2 Node

Node betegner en enhet i et nettverk bestående av ulike server, switch, router og brukere. Sender du f.eks. et nettverkssignal fra en PC, gjennom en ruter/switch, til en annen pc i nettverket, vil dette signalet gå gjennom 3 noder.

5.5.3 Switch

En **switch** er en nettverkskomponent som styrer datatrafikk mellom ulike noder i et nettverk, f.eks. PCer, servere, skriver og Internett-forbindelsen.

Ordet *switch* er engelsk og betyr *omkobler* eller *bryter*. Switchen opererer på lag 2 i OSI-modellen. Datatrafikk som passerer switchen blir analysert og sendt videre ut på den porten, eller i den retning, hvor mottakeren av datapakkene befinner seg. Switchen bruker MAC-adressen, også kalt den fysiske adressen, til mottakeren for å avgjøre hvor datapakkene skal.

Switcher fåes i mange varianter og størrelser fra 4 porter og opp til flere hundre porter. Portene kan ha ulike hastigheter og ulike tilkoblingstyper avhengig av behov. Det vanligste er porter for TP-kabling i hastighetene 10, 100 og 1000 MBps og porter for ulike typer fiberoptisk kabling.

5.5.4 Hub

En enklere variant av switch er Hub (datanettverk). En switch kan brukes på samme måte som en hub, men hub'en jobber på lag 1 i OSI-modellen og kan derfor ikke lese datapakkene og finne ut hvor de skal. En hub sender alle datapakkene ut på alle utganger i håp om at den som skal ha pakkene plukker dem opp. Denne arbeidsmetoden gjør at en hub er langt mindre effektiv enn en switch, fordi switchen kan håndtere flere datastrømmer samtidig til ulike porter, mens hub'en håndterer en strøm av gangen og pøser den ut på alle porter.

5.5.5 Kort om switchens virkemåte

1. Switchen tar imot data i form av såkalte frames, som ikke må forveksles med pakker.
2. Den lagrer i en liste hvilken port dataene kom på, og hvilken MAC-adresse de er sendt fra.
3. Dersom mottaker-MAC-adressen ligger i listen (dvs. at noen har sendt fra denne MAC-adressen fra før), blir dataene kun sendt til den porten som MAC-adressen er registrert på.
4. Ellers blir dataene sendt videre til alle porter.

På denne måten reduserer switchen effektivt unødvendig nettverkstrafikk, noe som reduserer antall kollisjoner, og dermed øker farten.

5.5.6 Hastigheten måles i mb/sek

Jo raskere Internettlinjen er, jo kortere tid tar det å åpne en side eller sende en epost. Vi ønsker oss derfor alle en så rask Internettlinje som mulig. Linjens hastighet regnes i megabyte per sekund, forkortet til mb/sek.

Siden siden du ønsker å se sjelden ligger på samme nettverket du benytter, må kallet ditt passere flere ulike nett før kallet kommer til sidene du ønsker å se. Deretter må pakkene siden består av sendes tilbake til deg gjennom de samme del-nettene før du endelig mottar siden og kan se den. Linjens reelle hastighet blir dermed aldri raskere enn det svakeste leddet.

Jo flere som benytter det samme nettverket, jo tregere blir linjen siden alle brukerne må dele den samme kapasiteten og linjehastigheten. I tillegg påvirkes hastigheten av switchenes hastighet, nettverkskortenes hastighet, pakketapet, antall pakke kollisjoner o.l. forhold.

5.5.7 Dataoverføringkapasitet

Foruten linjehastigheten må vi vurdere dataoverføringkapasiteten til datalinjen når linjens kvalitet skal vurderes. Dataoverføringkapasiteten angir hvor mye data du kan overføre på Internettlinjen i løpet av en måned før linjen blir blokkert. Dette er et viktig punkt siden alle må betale for mengden data som skal overføres på nettet. Jo mer data som skal overføres, jo større og flere linjer trenger linjeleverandøren for å dekke etterspørselen etter båndbredde.

Dataoverføringkapasiteten angis i antall GB eller TB per måned.

5.5.8 Faste og mobile linjer

Det store mangfoldet av Internettlinjer kan idag grupperes i 2 hovedgrupper:

1. **Fastelinjer** - fysiske linjer som går fra stamnettet til din enhet. F.eks. en kobberlinje eller fiberoptikk
2. **Mobile linjer** - enheten kobles opp mot Internett via mobiltelefonen på et mobilt nettverk, gjerne omtalt som 3G, 4G eller 5G nettet.

5.5.9 Fastelinjer

De faste linjene kan grupperes i:

1. **Fiberlinjer** - linjer som er tilkoblet stamnettet via fiberoptiske kabler.
2. **ADSL/SHDSL linjer** - linjer som bruker tradisjonelle telefonlinjer (kobberlinjer)

Fiberlinjer er de raskeste linjene med en hastighet som ingen andre teknologier kan måle seg mot.

Internett med ADSL/SHDSL-linjer gir lavere kapasitet enn fiberlinjer, men kan likevel fungere tilfredsstillende for mindre bedrifter og priivatpersoner

ADSL/SHDSL-linjer går via kobberkabler (tradisjonelle telefonlinjer), og dette nettet fases nå gradvis ut i Norge.Innen 2017 vil telefoni på kobbernettet være koblet ut for godt. Med en fiberlinje får du både Internett og IP-telefoni på samme linje.

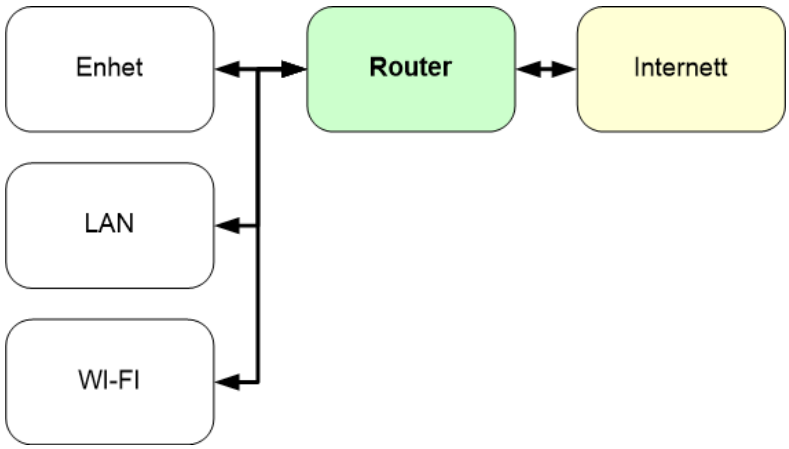
For å koble til en fastlinje trenger du ett Internett abonnement hos en linjeleverandør. Denne linjeleverandøren vil gi deg en router som er programmert med et brukernavn og passord du benytter for å koble enheten, et WI-Fi nettverk eller et LAN til Internettlinjen.

5.5.10 Mobile internettlinjer

På steder hvor man verken har tilgang til kobbernett eller fiberlinjer er mobile internettlinjer løsningen. En mobil internettlinje kan også være redningen i påvente av å få lagt inn en fiberlinje eller ADSL/SHDSL-linje og/eller fungere som en redundant løsning når høy oppetid er avgjørende. For å koblet det til en mobil internett linje trenger du et mobil abonnement med dataoverføringkapasitet.

5.5.11 ISP (Internet Service Provider)

En **internettleverandør** (forkortes iblant **ISP** fra engelsk ***Internet service provider***) er et selskap som tilbyr personer eller selskaper leie av tilgang til Internett- og andre relaterte tjenester. Som for eksempel oppbygging av nettsider og e-postkontoer på sin server.



Tjenestene leveres fra NIX og helt frem til kunden. En ISP kan enten ha egen NIX-tilknytning og eget IP-nett mellom sine servere og aksessnodene; eller leie tilknytning og IP-transport av en annen ISP. IP-nettene til ISP-ene utgjør i praksis Internett back-bone i Norge.

Som på vanlig norsk betyr at serverne til Internett leverandørene er grunnlaget for Internett. Andre firma som skal ha web sider. Kobler serverne sine til ISP sin server og har web-sidene sine på sine servere. Noen har også firma som lager og vedlikeholder Internett sidene for dem. Da ligger som regel web sidene på serverne til disse Web-side firmaene. Så Internett er egentlig bare en masse servere (datamaskiner) som er koblet sammen i et nettverk. På samme måte som et hjemme nettverk.

5.6 Proxy-server

Proxy-server er en datamaskin som sitter mellom en klientdatamaskin og Internett, og gir indirekte nettverkstjenester til en klient. Proxy-serveren kan ligge på brukerens lokale datamaskin, eller på forskjellige punkter mellom brukerens datamaskin og destinasjonsservere på Internett.

En proxy-server avskjærer alle klientforespørsler, og gir svar fra cachen eller videresender forespørselen til den virkelige serveren. En klientdatamaskin er koblet til proxy-serveren, som bekrefter klientforespørsler ved å levere den forespurte ressursen / dataene fra enten en spesifisert server eller det lokale hurtigminnet. Klientforespørsler inkluderer filer eller andre ressurser som er tilgjengelige på ulike servere.

5.6.1 Typer av proxy-servere

Proxy-servere er klassifisert i flere typer basert på formål og funksjonalitet. Noen av de vanligste typene og deres bruksområder kan beskrives som nedenfor:

Webproxy er den vanligste typen proxy-applikasjon, som svarer på brukerens forespørsler ved å få tilgang til ressurser fra bufret websider og filer som er tilgjengelige på eksterne webservere. Dette muliggjør hurtig og pålitelig tilgang til data for lokale nettverksklienter. Hvis den forespurte ressursen ikke blir funnet i hurtigbufferen, henter en webproxy filen fra den eksterne serveren, og lagrer en kopi i hurtigbufferen før den returneres til klienten.

Transparent proxy brukes for det meste til caching av nettsteder og overvinne enkle IP-forbud. Imidlertid gir slike proxyer ingen bruker anonymitet siden brukerens opprinnelige IP-adresse er eksponert. Transparente proxyer er ikke spesifikt konfigurert på klientdatamaskinene.

Anonyme proxyer skjuler ikke brukerens opprinnelige IP-adresse; De gir imidlertid tilstrekkelig anonymitet til de fleste brukere. Anonyme proxyer er lett å oppdage.

En **forvrengende proxy** , identifiserer seg selv som en proxy-server, og modifiser HTTP-overskriftene for å skjule den opprinnelige IP-adressen.

Tunnelproxyer kan klare klientforespørsler og returnere svar uten å gjøre noen endringer. Disse er også referert til som gateway proxyer.

En **proxy-proxy** svarer på klientforespørsler ved å hente data fra et bredt spekter av kilder på internett. Det er også referert til som en Internett-vendt proxy.

Åpne proxyer tilhører kategorien av videresending proxy-servere, som er tilgjengelige for alle Internett-brukere siden de kan motta og returnere forespørsler fra hvilken som helst klientdatamaskin. I mellomtiden brukes anonyme åpne proxyer for bruker anonymitet for å skjule IP-adressen.

Omvendte proxyer , også kjent som surrogater, mottar vanligvis forespørsler fra Internett og videresender dem til interne nettverksservere. En omvendt proxy-server videresender forespørsler til en eller flere proxy-servere, hvis svar returneres til klientdatamaskinen, hvis bruker ikke har noen kunnskap om opprinnelsen til svaret.

5.6.2 Hvor brukes en proxy-server?

Proxy-servere brukes til flere formål. Hvis den brukes som en caching web proxy, kan den dramatisk forbedre ytelsen til et websvar. Når en forespørsel blir gjort av en klient, returnerer en caching-proxy svaret direkte fra cachen hvis dokumentet allerede eksisterer. Ellers gjør den forespørselen til den virkelige serveren, returnerer resultatet, og lagrer den i cachen for senere bruk.

Proxy-servere brukes også som "web proxyer" for å filtrere innhold på websiden. En organisasjon eller et selskap kan bruke en proxy-server for å blokkere støtende webinnhold fra brukere. Tatt i betraktning det voksende behovet innen organisasjoner for å hindre at ansatte får tilgang til bestemte nettsteder, for eksempel facebook.com, blir proxy-servere distribuert på tvers av datamaskiner som er koblet til intranettet. Noen web proxyer kan omforme nettsider for å passe et bestemt sett av publikum, eller imøtekomme bestemte organisatoriske eller personlige internettbruksformål. Videre kan webproxyer brukes til å forhindre angrep av datavirus og malware, samt annet fiendtlig innhold overført på Internett-nettsidene.

Brukerne kan imidlertid også bruke webproxy-servere for å få tilgang til de blokkerte nettstedene indirekte. Disse webproxyene er bygd med PHP eller CGI for å implementere proxy-funksjonaliteten, og gir nettilgang til de nettstedene som er blokkert av firma og skolens proxyer. Dessuten kan Internett-leverandører (ISPer) også bruke proxyer til å blokkere datavirus og annet støtende innhold.

5.6.3 Hvorfor bruke proxy-servere?

Det er flere fordeler med proxy-servere. Vi har til hensikt å gi noen av de mest grunnleggende bruken av proxy-servere.

Ytelsesforbedring:

Proxy-servere bidrar også til forbedret webytelse, siden resultatene av brukerforespørslene lagres i hurtigminnet i en bestemt tidsperiode. Dette oppnås ved hjelp av en caching-proxy-server, som kan spare mye tid mens du spiser forespørsler fra en stor brukerbelastning. En caching-proxy-server opprettholder en lokal kopi av ofte forespurt webinnhold. Derfor kan det akselerere tjenesteforespørsler ved å hente innhold fra hurtigminnet, hvis det allerede var blitt forespurt av en annen klient på det samme nettverket. Denne funksjonen bidrar til

en betydelig reduksjon i oppstrøms båndbreddebruk og kostnader for store organisasjoner med tusenvis av ansatte.

Overvåking og filtrering Brukerforespørsler:

Som diskutert tidligere, kan webproxyer brukes til å filtrere brukerforespørsler, og blokkere visst innhold eller nettsider fra å bli tilgang til. Dette kan oppnås ved hjelp av en innholdsfiltrerende webproxy-server som skiller brukerens nivå av kontroll over innholdet, basert på brukertypen - Gjest eller Administrator.

Innholdsfiltrerende proxyer brukes vanligvis i organisasjoner og utdanningsinstitusjoner med strenge retningslinjer for internettbruk. Blokkering av bestemte nettsteder, og begrensning av tilgang til bestemte nøkkelord og censurering av uønsket innhold er noen av de grunnleggende funksjonene som tilbys av innholdsfiltrering eller nettfiltreringsproxy. Imidlertid er det visse webproxyer som brukes til å omgå geo-restriksjoner og sensurbestemmelser ved å bruke visse avanserte tjenester som hjelper tilgangen til ressurser fra svarteliste web-steder.

Anonym Browsing:

En anonym proxy server er en annen type web proxy som anonymiserer brukernes online aktiviteter. Denne typen proxy-server leder brukerens forespørsler til en destinationsserver, som i siste instans ikke har kjennskap til kilden til forespørselen. Bare proxy er oppmerksom på kilden til forespørselen, inkludert brukerens IP-adresse og -sted.

Annonser som målretter mot bestemte geografiske områder Webproxies kan også brukes til å validere og verifisere geografiske målrettede annonser. Servere av slike annonser validerer kilde-IP-adressen til brukerforespørselen, og bestemmer den geografiske plasseringen av forespørselen ved hjelp av en geo-IP-database. Brukerforespørslene besvares via proxy-servere som befinner seg innenfor den respektive geografiske plasseringen, for å sikre at annonser som vises, er rent relevante for brukerens plassering.

Oversettelse:

Med tanke på det globale publikum, har oversettelsesproxyer blitt utviklet for å lokalisere / oversette innholdet på en kildeside til et lokalt språk på klientdatamaskinen. Svar på forespørsler sendt av lokale brukere erstattes med oversatt innhold fra kildesiden, og sendes tilbake via proxy-serveren. Noen oversettelse proxyer gir også tilleggstjenester som ekskluderer kildeinnhold eller erstatter kildeinnhold med originalt lokalt innhold.

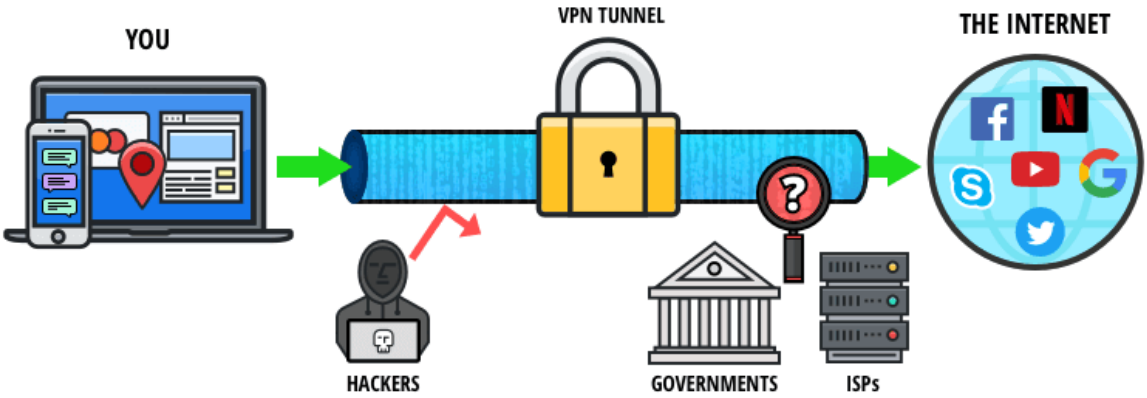
5.6.4 Konklusjon

Den mest populære proxy-serveren som brukes i dag, er et webproxy, og det brukes til å filtrere innhold og tillate anonym nettlesing. Å kunne blokkere geografisk begrenset innhold er også et bredt brukt program for bruk av offentlige web proxyer. Selv om proxyer gir anonym nettlesing og innholdsfiltrering, er de for det meste begrenset til nettlesing og mangler også sikkerhet. For sikker og kryptert kommunikasjon med personvernbeskyttelse, anbefales VPN- løsning.

5.7 VPN (virtuelt privat nettverk)

Et virtuelt privat nettverk (VPN) er en nettverksteknologi som utvider et privat nettverk (for eksempel LAN) slik at du kan koble deg på dette nettverket via et offentlig nettverk, f.eks. Internett. En VPN gjør at to datamaskiner (eller nettverk) kan sikkert kan kobles sammen som om de er fysisk koblet sammen. Bedrifter bruker VPN for å tillate eksternt arbeidere å koble seg sikkert til bedriften private nettverk (LAN). En VPN brukes også til å koble eksterne kontorer med et hovedkontor som om de er fysisk tilkoblet.

VPN teknologien kan illustreres slik:



For å beskytte brukerens identifikasjon og personvern ble den personlig VPN-tjenesten funnet opp. En personlig VPN-tjeneste er identisk med å koble til et bedriftsnettverk, bortsett fra at brukere er koblet til servere levert av VPN-provders og oppnår en ny IP-adresse fra brukerland.

5.7.1 VPN-protokoller

Et virtuelt privat nettverk opprettes ved å etablere en virtuell tunnel mellom to endepunkter via en virtuell tunneling protokoll eller ved datakryptering. Noen av de mest populære VPN-protokollene inkluderer IPsec, SSL / TLS, PPTP og L2TP.

- **PPTP** - Point-to-Point Tunneling Protocol er den eldste VPN-protokollen utviklet av et konsortium funnet av Microsoft, som støttes av det store flertallet av operativsystemer. Krypteringen basert på 128-biters nøkkel har blitt sprukket, og den anses ikke lenger å være veldig sikker.
- **L2TP / IPsec** - Lag 2 Tunnelprotokoll med IPsec-krypteringsbasert VPN gir sikrere service med flere funksjoner enn PPTP. L2TP bruker UDP port 500, slik at avansert konfigurasjon kan være nødvendig for å åpne NAT-brannmur.
- **Open VPN** - OpenVPN er åpen kildekoden teknologi utviklet på OpenSSL, som gir svært sikker tilkobling og sterk kryptering. Den har blitt standard VPN-tilkoblingstype, og støttes mye av tredjeparts programvare, inkludert iOS og Android.

5.7.2 Remote Access VPN

En VPN med ekstern tilgang, også kjent som Point-to-Point (PPP) VPN, tillater individuelle brukere å etablere en sikker tilkobling til en ekstern server. En VPN-bruker slutter seg til det private nettverket som tilbys av VPN-programvare, og får tilgang til de sikre ressursene på nettverket som om brukeren er direkte tilkoblet. VPN-fjernkontrollen krever to komponenter: en Remote Access Server og VPN-klientprogramvare som gjør at brukeren kan etablere og vedlikeholde en VPN-tilkobling. Det er nødvendig å etablere en tunnelert tilkobling til en NAS, angitt ved hjelp av en internettadresse, mens den også hjelper til med å administrere kryptering som trengs for en sikker tilkobling.

5.7.3 Nettsted-til-nettsted VPN

Et VPN-nettverk bidrar til å etablere en sikker forbindelse mellom to nettsteder eller steder, over et offentlig nettverk som Internett. Et VPN-nettverk kan utvide to nettverk i et enkelt nettverk (Intranett VPN), eller koble sammen to separate nettverk, samtidig som de opprettholder sin lokalitet (Extranet VPN).

5.7.4 VPN Tunneling

En VPN bruker tunnelingens mekanisme for å opprette et privat nettverk over Internett. unneling er en nettverksteknologi som involverer prosessen med lagring av kapsler, kjent som innkapsling. I denne prosessen opprettes en serie pakker ved å bryte ned hver datafil, og en hel pakke er plassert i en annen ytre pakke før den sendes og mottas på tvers av datamaskinene. Bevegelse av den krypterte pakken i en ytre pakke, også kjent som en virtuell tunnel, sikrer sikret overføring.

VPN-teknologien bruker en tunnelstyringsprotokollmekanisme som bidrar til å skape, vedlikeholde og avslutte tunnelen, som muliggjør sømløs dataoverføring. I mellomtiden er enheter eller datamaskiner som er til stede i begge ender av tunnelen kjent som tunnelgrensesnitt, som letter prosessen med innkapsling og gjenåpning av utgående og innkommende pakker henholdsvis.

5.7.5 Fordeler ved VPN

Det er flere fordeler med å bruke en VPN-tjeneste som spenner fra å omgå internettcensur for å få tilgang til globalt innhold uten noen restriksjoner, økt internett sikkerhet og anonym surfing. De fleste grunnleggende egenskapene til VPN som skiller dem fra andre personlige nettverk er som følger:

Sikkerhet : Den primære grunnen til å implementere VPN-teknologi er å skape en sikker forbindelse til det andre sluttpunktet. Å lage en WAN-tilkobling er svært kostbar, og kan ikke være praktisk for enkelte brukere som gjør klient til server-tilkobling. Informasjonen som utveksles mellom de to VPN-endepunktene er kryptert, og derfor kan det ikke oppstå avlyting når informasjon overføres via det offentlige nettverket. VPN-er gir høy sikkerhet, og dermed beskytter brukernes data mot hacking, spesielt på et offentlig nettverk.

Anonymitet : En VPN kan også brukes til å skjule ditt privatliv ved å skjule sann IP-adresse til brukerens datamaskin. Online spillere kan bruke VPN til å skjule IP-adressen på datamaskinene sine, og bedriftseiere kan bruke VPN til å endre IP-adresse for å beskytte sin identitet fra sine konkurrenter.

Pålitelighet : VPN er ledsaget av høy pålitelighet standarder, noe som gir tilsvarende kvalitet for tilkobling for hver bruker mens du håndterer flere og samtidige tilkoblinger.

Skalerbarhet : VPN-er kan enkelt utvides for å imøtekomme flere brukere og forskjellige steder sammenlignet med leide linjer. Dette gjør det mulig å utvide intern VPN-tjenester uten behov for å erstatte teknologien i det hele tatt.

Fleksibilitet : VPN-er gir et fleksibelt alternativ for eksterne kontorer til å bruke et felles profesjonelt intranett over en eksisterende tilkobling, som om de er direkte koblet til internett.

Foruten de bemerkelsesverdige funksjonene som er beskrevet ovenfor, tilbyr en personlig VPN følgende fordeler.

- En VPN gjør det mulig for brukere å koble til eksterne servere som ligger i ulike deler av verden, ved hjelp av utvalgte IP-adresser når som helst. Denne anonyme surfingen bidrar til å hindre hackere i å trenge inn i det personlige nettverket, samt dele filer og data over et kryptert medium.
- En VPN bidrar til å opprettholde nettverkssikkerhet og også legge til rette for anonym nettlesing fra hvor som helst i verden med en IP-adresse til et valgt sted.
- Flere land implementerer nå *internettcensur* som en del av de nasjonale sikkerhetslovene. Dette inkluderer innholdsregulering, filtrering og blokkering av politikk for å undertrykke bruken av gratis internett. Derfor velger antall personer for VPN-tjenester å benytte seg av anonym surfingfunksjon for å overvinne problemene knyttet til overvåket internettbruk.
- En VPN gir måter å omgå overvåkingsmekanismen og bli utsatt for globalt innhold på internett. En VPN-tjeneste er den sikreste måten å surfe på internett og fjerne blokkering av noen av nettstedene som kalles geografisk begrensede nettsteder, som ikke er tilgjengelige innen bestemte geografiske områder.
- Mobil VPN-er letter pålitelige forbindelser, og brukes til sømløs roaming på tvers av nettverk, og innenfor trådløse dekningsområder, uten å miste VPN-tilkobling eller applikasjonssessinger.
- Gitt det økende behovet for sikker og privat nettlesing, bruker flere routerprodusenter (som Cisco, Linksys, Asus og Netgear) VPN-tilkobling på rutere av produksjonsrutere med innebygde VPN-klienter.
- Dette tilrettelegger ikke bare ekstra sikkerhet og kryptering av dataoverføring ved hjelp av ulike kryptografiske teknikker, men tillater også enhver tilkoblet enhet (smarte TVer og spillkonsoller blant andre) å bruke VPN-nettverket mens det er aktivert.
- For å sikre høye standarder for personvern og anonyme nettleseralternativer, kan VPN-er sikre brukerne mot hackere og datatyver. Derfor utvikles nye og bedre teknologier over tid til bruk i nettverk, for å forbedre funksjonene til eksisterende VPN-er.

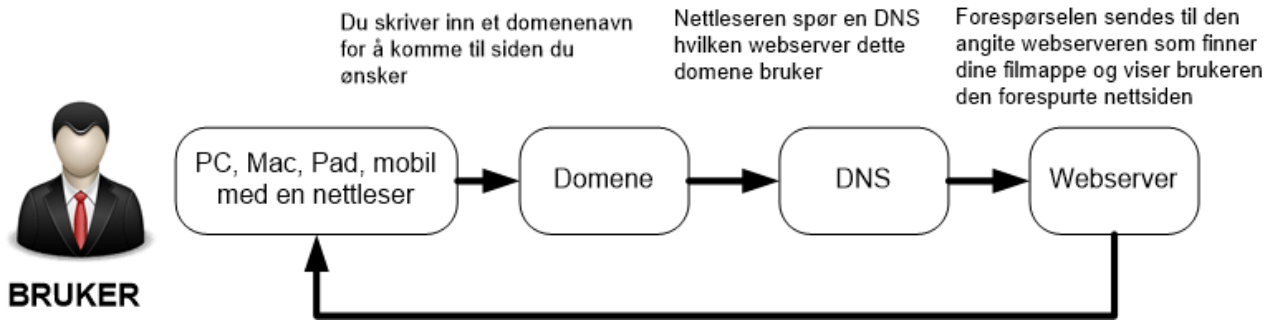
5.7.6 Ulemper ved VPN

1. Siden all virtuell privat nettverkstrafikk er kryptert, vil det bli 10-15% økning i nyttelast overført over VPN. Denne ekstra overhead forårsaker (1) databehandlingsenheter til å bruke mer prosessorkraft for å kryptere dataene, (2) sende mer data over nettverket, og til slutt (3) tar lengre tid for å overføre data da det vil være 10-15% flere data. Med videreutvikling i databehandling og nettverksteknologi har den ekstra prosessorkraften som kreves for å kryptere / dekryptere og ytterligere dataoverføring, ubetydelig innvirkning på den totale bruken av nettverket.
2. Ikke alle VPN-apparater samvirker godt, så det kan hende at en VPN-enhet fra en leverandør ikke fungerer bra fra en enhet fra en annen leverandør. En nettverksingeniør som implementerer VPN-teknologien, må verifisere kompatibilitet mellom de to endepunktene. På samme måte kan en klient til serverforbindelse føre til langsommelighet (eller nedbrytes i QoS) hvis VPN ikke er riktig oppsett.

5.7.7 Godkjenning

En VPN-tilkobling, enten det er en klient til server eller nettverk for nettverk, tunnel-endepunkter, må godkjennes før du etablerer en sikker tilkobling. En bruker som har startet VPN-tilkobling, bruker enten passord eller tofaktorautentisering, mens nettverk til nettverk-tunneler ofte bruker digitale sertifikater (privat / offentlig tastekombinasjon).

5.8 Hva kreves for å lage et eget nettsted?



For å kunne lage et eget nettsted som er tilgjengelig for andre på Internett eller et Intranett kreves det:

- **Domene** - et navn som alle nettstedene er knyttet til og som folk kan skrive i nettleseren sin for å komme til ditt nettsted. Navnet kan være hva som helst, f.eks. dittnavn.no, men som regel brukes bedriftens navn eller en forkortelse av den som nettstedets domene, f.eks. estudie.no. Domene er ikke noe du kjøper. Det er noe du leier gjennom en godkjent Registrar for det topp-domene du har valgt. Prisen varierer fra topp-domene til topp-domene, men den ligger normalt fra kr. 99/år og oppover.

- **DNS** - domene må være knyttet til minst to navnetjenere som forteller alle som spør om domene hvilken web-, mail- og ftp-server domene bruker, eller sagt på en annen måte: På hvilken webserver nettsidene ligger på og hvor epost til domene skal leveres. Navnetjenerne følger gratis med domene du registrerer.

- **Webserver** - en server hvor du kan legge ut nettsidene til domene og som har installert alle programmene som kreves for å kjøre disse nettsidene. Du trenger ikke å kjøpe en egen fysisk server (datamaskin). De aller fleste velger å kjøpe et webhotell. Det vil si plass på en webserver som de deler med andre nettsteder. Ved å dele regningen på flere blir dette en vesentlig rimeligere løsning enn å ha en egen server. At du heller ikke trenger kompetanse om drift og vedlikehold av denne serveren er en annen grunn for at 9 av 10 velger denne løsningen. Webhotell kan du bestille via en hosting-leverandør, f.eks. OnNet, og koster fra 200 kroner i året, inkludert domene.

- **Publisering løsning** - et dataprogram du kan bruke for å lage og vedlikeholde nettsidene dine. De mest populære publisering løsningene i dag er WordPress, Joomla! og Drupal. Alle programmene kan lastes ned og installeres på hvilke som helst webservere, og inngår ofte som en del av webhotell pakken. F.eks. er dette tilfelle hos OnNet.

5.9 Domene

For å kunne publisere et eget nettsted trenger du et domene som du kan knytte nettstedet til. Det samme domene kan du så knytte et ubegrenset antall e-postkontoer til. Domenets funksjon kan beskrives slik:

På internett finner datamaskinene hverandre ved hjelp av Internet Protocol adresser (IP adresser). Dette er en tallkode består av fire hele tall under 256 adskilt med punktum, f.eks. er 82.117.44.66.

Siden slike IP adresser oppfattes som intetsigende og er vanskelige å huske ble derfor «***Domain Name System (DNS)***» lansert slutten av 80-tallet som erstattet disse IP-adressene, med beskrivende ord. Dette ordet kaller vi et **domene** eller ***domain name*** på engelsk. Eksempler på domener er estudio.no, facebook.com, vg.no og google.com.

Funksjonen til et domene er dermed å gjøre om en IP-adresse til et forståelige ord som er lett å huske.

Et domene kan teknisk beskrives slik:

Et domene er et navn som inngår i en **URL**, og består alltid av to deler; – et **domene** og et **topp-domene**, også kalt **TLD**.

For at domene skal virke, må URL-en også inneholde en angivelse av hvilken **protokoll** som skal brukes. Dette kan illustreres slik:

5.9.1 URL

En «***Uniform Resource Locator***», eller bare **URL**, er en subtype av URI hvor vi identifiserer og navngir en ressurs ved hjelp av lokaliseringinformasjon eller ressursens adresse (Wikipedia). Blant folk flest kalles en URL bare for en nettadresse vi skriver for å komme en bestemt nettside på Internett. En URL må minimum bestå av:

Protokoll + Sub-domene (valgfritt) + domene + topp-domene = URL

5.9.2 Protokoll

En **protokoll** er et regelsett som avgjør hvordan tilkobling, kommunikasjon og dataoverføring mellom to endepunkter (f.eks. mellom nettleseren på din datamaskin og web-serveren til din hjemmesider) skal skje.

Det finnes en lang rekke ulike protokoller som alle har sine egne unike spesifikasjoner og som inngår som forskjellige lag i OSI-modellen som dokumenteres gjennom RFC-dokumenter publisert av Internet Engineering Task Force (IETF). De tre vanligste protokollene som benyttes i en URL er:

1. **HTTP** (Hypertext Transfer Protocol) protokollen som benyttes til å vise nettsider
2. **HTTPS** (Hypertext Transfer Protocol Secure) protokoll for sikker overføring av data mellom server og klient via et SSL-sertfikat
3. **FTP** (File Transfer Protocol) protokollen som benyttes til filoverføringer

Hvilken protokoll du benytter ser du ut av begynnelsen av en URL. Starter URL-en med http:// så benytter du HTTP-protokollen, mens FTP-protokollen alltid starter med ftp://.

5.9.3 Path

En URL kan utvides til å omfatte et mappe og filnavn for å angi hvilken side, bilde, fil e.l. i et nettsted som skal vises. Dette kalles en «path» og angir stien til destinasjonen som skal vises.

Et eksempel på en path er: https://estudie.no**/medlemskap/kontakt.php**. Her er pathen markert med rødt. Denne pathen forteller at du ønsker å gå til siden "kontakt.php" som ligger i mappen "medlemskap".

5.9.4 Hva er et topp-domene, også kalt TLD?

Den engelske betegnelsen på **topp-domene** er ***Top Level Domain***, eller bare ***TLD***.

Et domene består av et domenenavn og et topp-domene som er adskilt med et punktum mellom seg (se illustrasjonen over).

Topp-domene utgjør siste del av domene (til høyre for punktum) og angir hvilket land eller navnkategori domene tilhører. I eksemplet over er topp-domene «*no*» eller «.*no*» som man ofte feilaktig sier.

Alle verdens land har et eget geografisk toppnivå domene. F.eks. er **`.no`** (Norge), **`.se`** (Sverige) og **`.uk`** (Storbritannia).

I tillegg til landkodene finnes noen toppnivå domener som ikke er landspesifikke. Mest kjent er `.com`. Andre eksempler er `.info`, `.org` og `.net`. Disse kalles *generiske toppnivå domener*, som forkortes *gTLD* (fra engelsk *Generic TLD*).

Vi må dermed skille mellom to typer topp-domener:

- **Nasjonale toppnivå domener** – forkortet til:**ccTLD** – nasjonale domener, f.eks. .no, bestående av landskoder på minimum 2 bokstaver. Reglene for hvem som kan gjøre rett på domener under de enkelte nasjonale toppnivå domenene blir vedlikeholdt av et styringsorgan, som er ansvarlig for driften av domenet. Organisasjonen Norid er ansvarlig for det norske toppnivå domenet `NO`.
- **Genetiske toppnivå domener** – forkortet til **gTLD** – domener som ikke er landsspesifikke, f.eks. .com.

De vanligste topp-domenene norske virksomheter benytter er:

Toppdomener:	Et domene som brukes av:
.no	Bedrifter og organisasjoner i Norge
.dk	Bedrifter og organisasjoner i Danmark
.se	Bedrifter og organisasjoner i Sverige
.com	Kommersielle nettsteder, uten geografisk tilhørighet.
.net	Nettverk, uten geografisk tilhørighet.
.org	Organisasjoner, uten geografisk tilhørighet.
.int	Internasjonale organisasjoner
.edu	Universiteter, skoler
.biz	Næringsliv generelt
.info	Ingen restriksjoner

5.9.5 Hva er et sub-domene?

Et **sub-domene** er et familie- eller slekts-navn tilhørende et domene eller topp-domene. Det mest vanlige sub-domene er www. som er en forkortelse for «*World Wide Web*«, og er medlem av domene-familien. Sub-domenet må opprettes av eieren av domenet selv. Vi eier f.eks. domene onnet.no og for at sub-domenet www.onnet.no skal virke, må vi selv manuelt legge inn sub-domene www. i vår sonefil for domenet. Sonefilen er en del av navnetjeneren (DNS) som oversetter domene og sub-domener til IP-adresser som utgjør all form for kommunikasjon på Internett.

Eier du et domene, f.eks. OnNet.no, kan du selv legge til hva du vil foran .onnet.no, og det er bare du som kan gjøre det. Sub-domener kalles derfor ofte også for tjeneste domener, da de ofte brukes til å skille ulike tjenester fra hverandre. Vi bruker f.eks. mail.onnet.no til å angi mailserveren, mens ftp.onnet.no angir stien for filoverføring.

En del land og enkelte organisasjoner velger å ta med flere ledd i domenenavnet ved å innføre **sub-domener**. Et eksempel her er Storbritannia som har delt opp `.uk` i forskjellige underdomener og dermed får adresser som «`http://www.google.co.uk`».

5.9.6 Hvilke tegn og hvor mange tegn kan et domene ha?

Et domene er et navn, bestående av bokstaver, tall og bindestrek. Spesialtegn og mellomrom kan ikke benyttes.

For at domene skal være gyldig må det bestå av minimum 2 tegn, og kan maksimum bestå av 64 tegn.

5.9.7 Hvilke kostnader er knyttet til et domene?

For å kunne eie/leie et domene må domene søknaden bli godkjent av topp-registraren som etter godkjenning må legge domene ut i sine root-servere (navnetjenere) for at domene skal bli tilgjengelig på Internett. Ved eventuelle konflikter mellom to selskaper om det samme domene er det opp til topp-registraren å avgjøre hvem som har rett, med mindre saken ikke bringes inn for retten.

For denne jobben må alle som eier/leier et domene betale topp-registraren en årsavgift for å beholde domene de har registrert. Siden topp-registraren kun kommuniserer med sine registrarer og ikke direkte med innehaverne av de ulike domenene, sender topp-registraren fakturaen for årsavgiften for de enkelte domene til registraren som har registrert domene.

Årskostnadene knyttet til å eie et domen er avhengig av hvilken registrar du har valgt. En registrar er en godkjent "forhandler" av topp-domene eieren.

5.9.8 Hvem kan registrere et domene?

Hvem som kan registrere et domene avgjøres av hvilket topp-domene vi snakker om, men hovedregelen er at alle selskaper og privatpersoner over 18 år kan registrere et domene. Dette gjelder f.eks. for .dk, .se, .com, .net, .org, .info, .biz, .ws, .as og de aller fleste andre topp-domenene.

For noen topp-domener gjelder bestemte restriksjoner for hvem som kan registrere domene – deriblant .no (dot-enno) domener.

5.9.8.1 .no domener

Ønsker du å registrere et .no domene må du være et registrert selskap med organisasjonsnummer i Foretaksregisteret.eller være over 18 år. Klikk på linken under for en oversikt over hvilke organisasjonsformer Norid godkjenner som innehavere av et domene:

- **Godkjente organisasjonsformer for .no**

Dernest krever Norid at du setter deg inn i regelverket deres og «signerer» en elektronisk egenerklæring som bekrefter at du aksepterer Norid sine domene regler. Denne

egenerklæringen må sendes inn til registraren før domene registreringen kan skje, da dette dokumentet må vedlegges domene søknaden fra registraren.

Er du en privaperson som ønsker å registrere et domene, må du være norsk statsborger over 18 år. Siden personnummeret ditt er hemmelig, må du først gå til Norid for å få en PID-kode fra dem som erstatter ditt personnummer med en annen tallkode som må oppgis når du søker om .no domene.

For å opprette et .eu domene må virksomheten ha forretningsadresse i et EU- eller EØS land, mens .edu krever at du er et internasjonalt godkjent universitet.

5.9.9 Hvor mange domener kan du bestille og eie?

Du kan registrere inntil 100 ulike .no-domener på ditt firma og 5 navn privat.

For de øvrige topp-nivåene gjelder det ingen restriksjoner for hvor mange domener du kan registrere.

5.10 DNS (navnetjenere)

5.10.1 System som gjør det mulig å bruke et domene for å komme til en nettside eller nå en e-postadresse

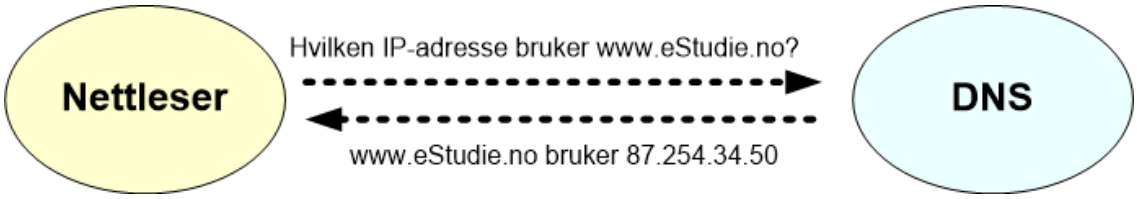
DNS er en forkortelse for **"*Domain Name System*" eller "*navnetjenere*"** på norsk. Som det går frem av ordet snakker vi om et system av navnetjenere som gjør det mulig å benytte et domene i en URL for å få frem en bestemt nettside i nettleseren eller levere e-posten til en bestemt e-postadresse. Vi skal her se på hvordan dette systemet av navnetjenere virker.

5.10.2 Et domene er en erstatning for IP-adresser

Navnetjenerne, også kalt **DNS**, er et datasystem som brukes på Internett for å gjøre om et **domene** til en **IP adresse**. En IP-adresse er en tallkode bestående av fire tall som er adskilt med et puntum. Denne IP-adressen benyttes til å finne et bestemt nettsted som ligger på en bestemt webserver eller en bestemt e-postkonto hos en bestemt mailserver. At du forstår dette prinsippet er viktig, da alle tjenester (nettsider, e-postkontoer, ftp-kontoer, servere o.s.v.) på Internett er knyttet til en unik IP-adresse.

En tallkode bestående av fire tall – adskilt med ett punktum, er imidlertid vanskelig å huske for vanlige mennesker. IP-adressen til onnet.no sine nettsider er 217.170.193.178, mens google.com har IP-adressen 172.217.15.78. Hvor mange slike tallkoder klarer du å huske og skille fra hverandre? Ikke mange.

På 1980-tallet innførte man derfor domener som erstattet disse tallkodene (IP-adressene) med beskrivende navn. Dette ble gjort fordi skrevne ord er enklere å huske og skrive enn lange tallkoder.



5.10.3 Hvordan virker navnetjenerne (DNS)?

Når du f.eks. går ut på nettet og skriver onnet.no i nettleseren din, så vet ikke datamaskinen og nettleseren din i utgangspunktet hvor nettsidene til onnet.no ligger eller hvilken IP-adresse nettstedet bruker. For å finne ut hvor nettsidene til onnet.no er vil nettleseren din spørre sin nærmeste løsende (resolverene) navnetjener om hva som er IP-adressen til onnet.no.

5.10.4 Løsende navnetjener (resolverene name server)

Nettleserens løsende navnetjenere er navnetjenere nettlesere får beskjed å spørre for å gjøre om domenenavn til IP-adresser når noen skriver en URL (nettadresse, f.eks. https://www.onnet.no). Disse navnetjenerne får du automatisk tildelt av din linjeleverandør hver gang du kobler deg på Internett med en datamaskin, nettbrett eller mobil.

Hvis disse løsning navnetjenerne ikke allerede har catched (mellomlagret) resultatet av dns spørringene vi beskriver under, for å spare tid på å finne IP-adressen til et bestemt domene, vet disse navnetjenerne i utgangspunktet heller ikke hva IP-adressen til nettsidene til OnNet.no er. For å finne dette ut vil den løsende navnetjeneren spørre Root navnetjenerne om hvor domene er.

5.10.5 Root navnetjenere

Root navnetjenerne er de navnetjenerne som hele domene systemet bygger på. Root er de navntjenerne som angis ved hjelp av et usynlig punktum etter domene du skriver. Skriver du f.eks. https://onnet.no så skriver du i virkeligheten https://onnet.no. Dette siste punktumet som aldri vises er en angivelse av å spørre root-serverne om hvor domene er.

Når den løsende navnetjeneren kommer til root navnetjenerne vil denne navnetjeneren svare at de ikke vet IP-adressen til onnet.no, men de vet hvilke navnetjenere som har ansvaret for topp-domene .no, også kalt Top Level Domain eller bare TLD.

5.10.6 TLD navnetjenere

Når den løsende navnetjeneren kommer til norid.no som er TLD registraren for .no domener, dvs. navnetjenerne for alle eksisterende .no domener vil den løsnende navnetjeneren få til svar at TLD navnetjenerne heller ikke vet IP-adressen til onnet.no, men de vet hvilke navnetjenere som er autorative navnetjenere for domene.

5.10.7 Autorative navnetjenere

De autorative navnetjenerne er de navnetjenerne som har ansvar for et bestemt domene. Hva som er autorative navnetjenere avgjøres av registraren som registrerer domene hos TLD navnetjenerne.

5.10.8 Alle domener krever minimum 2 autoritative navnetjenere

For at et domene skal virke kreves det at et domene er knyttet opp mot minimum 2 autoritative navnetjenere. Dette for å sikre at det alltid er en autorativ navnetjener som kan gi riktig svar til løsnings navnetjeneren, selv om en av dem for øyeblikket er nede eller utilgjengelig.

Når løsnings navnetjeneren spør den autoritative navnetjeneren vil de få til svar at de vet hvilken IP-adresse onnet.no benytter og gi løsnings navnetjeneren IP-adressen den spør etter.

5.10.9 Webserver

Når nettleseren din endelig får til svar hvilken IP-adresse onnet.no benytter vil den sende hele URL-en, f.eks. https://www.onnet.no, til webserveren på denne IP-adressen. Denne webserveren vil da hente opp nettsiden til onnet.no og sende den tilbake til nettleseren.

5.10.10 TTL

Når løsnings navnetjeneren har fått svaret på alle sine DNS-spørringer vil de normalt catche resultatet, dvs. lagre det for en tid, slik at de slipper å gjøre alle disse DNS spørringene hver gang noen spør etter dette domene. For facebook.com og google.com kan dette bli mange hundre tusen sparte spørringer hver dag. Hvor lenge de catcher resultatet avgjøres av hvilke TTL verdier den autorative navnetjeneren har angitt i sonefilen til recordene for dette domene. TTL er en forkortelse for "Time To Live" og er en verdi som alltid angis i sekunder. F.eks. betyr TTL = 3600 at recorden har en levetid på 1 time.

5.10.11 Hvordan velge riktige autorative navnetjenere til ditt nettsted

Når du skal velge autoritative navnetjenere til ditt domene er det mange ting du bør tenke på. De viktigste vurderingene du bør gjøre er:

- **C-klasser** - Ideelt sett bør dine autoritative navnetjenerne ligge på separert på to ulike C-klasser, slik at en hel C-klasse med IP-adresser (256 IP-adresser) kan bli utilgjengelig, uten at nettstedet ditt blir utilgjengelige på Internett. OnNet har to navnetjenere på to ulike C-klasser. Hvilke navnetjenere ditt domene benytter kan du slå opp under ved å angi ditt domene.

- **Avstand til kunden** - jo nærmere navnetjeneren er plassert dem som bruker nettstede, jo raskere for løsnings navnetjeneren svar på sitt spørsmål. Ligger den autoritative navnetjeneren i USA mens brukerne er i Norge må signalet sendes til USA før svaret kommer tilbake til Norge hvor surferen er. Dette tar vesentlig lenger tid enn hvis navnetjenerne lå i Norge, samtidig som sjansene for at noe skal gå galt øker proposjonalt med antall nettverk signalene må gå igjennom før de kommer frem. OnNet sine navnetjenere er lokalisert i Norge og knyttet direkte mot NIX punktet i Oslo for å sikre kort avstand til norske brukere.
- **Alder** - jo lengre navnetjenerne har eksistert, jo større tillit har Google til dem. Jo større tillit navnetjenerne har hos Google, jo bedre blir rangeringen (vektlegges ikke marginalt av Google). OnNet sine navnetjenere har vært online siden 1997 og er dermed godt ansett verden over.
- **Konfigurasjon** - navnetjenerne må være konfigurert riktig i forhold til alle tjenestene som brukerne vil prøve å koble seg mot. Er de ikke korrekt konfigurert i forhold til brukerne står man i fare for at tjenestene dine ikke vil virke for dem.
- **DNS Editor** - leverandøren du velger må tilby deg en DNS Editor. Et kontrollpanel for sonefilen til ditt domene som gjør det mulig for deg å legge til, endre og slette hvilke som helst record i sonefilen. Dvs. CNAME, A-, MX-, TXT, SRV og andre vanlige record typer. OnNet tilbyr kundene sine en avansert DNS Editor som du finner som en integrert del av cPanel.
- **DNSSEC** - dette er en ny sikkerhetsstandard som tilfører den usikre DNS standarden beskyttelse mot manipulerte resultat fra DNS spørringer. Du bør forsikre deg om at navnetjenerne du velger har støtte for DNSSEC og du bør aktivisere denne beskyttelsen.

5.10.12 Ikke bytt autoritativ navnetjener i tide og utide

Når du har valgt DNS for ditt domene bør du holde deg til disse navnetjenerne og ikke bytte dem i tide og utide. Dette fordi Google ser på dette som et tegn som et useriøst nettsted, da seriøse nettsteder ikke har tid eller anledning til å flytte på seg hele tiden. Bytter du navnetjenere hele tiden får du dermed dårligere rangering i Google enn hvis du holder deg til de samme navnetjenerne.

Istedefor å bytte autorative navnetjenere bare fordi du har valg en nettbutikk eller nettsider som er plassert hos en annen leverandør er det mye smartere å bare peke domene mot tjenestene du har hos denne leverandøren gjennom DNS Editoren som bør følge med navnetjenerene du velger. Dette kan du endre selv når du vil uten kostnader.

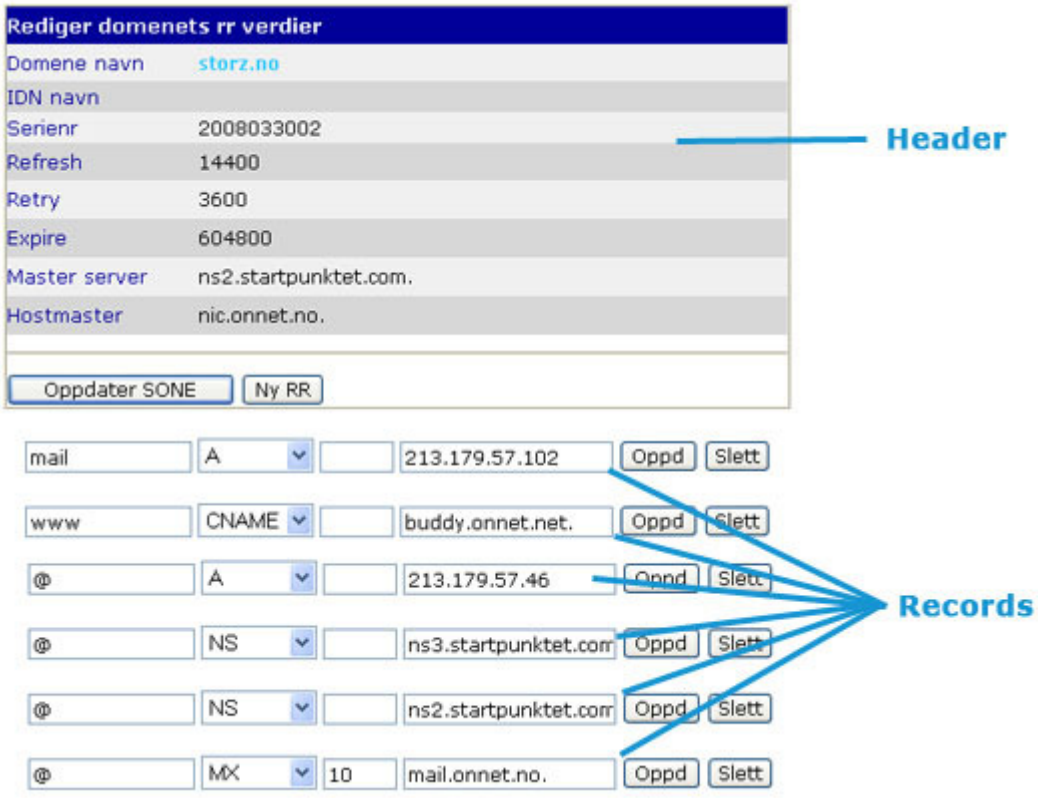
5.11 Sonefil

En **sonefilen** er en fil på navnetjeneren som forteller hvilke IP-adresser domene benytter for ulike tjenester. Sonefilen forteller med andre ord IP-adressen til hvor dine ulike Internett tjenester finnes. F.eks. forteller sonefilen hvilken web-server hjemmesidene bruker og hvilken epostserver meldinger til domene skal leveres til.

Sonefilen består av to hovedkomponenter:

1. en **header** som forteller de generelle innstillingene for domenet
2. **ulike records** som er knyttet til denne headeren, og som inneholder spesifisert informasjon om hver enkelt sub-domene og tjeneste domene benytter.

Under finner du et eksempel på hvordan en sone-fil kan se ut:



Eksempel på en sonefil fra OnNet sitt gamle webgrensesnitt

5.11.1 Headeren (SOA)

Headeren til sonefilen, også kalt SOA, forteller de generelle instillingene for domene. De viktigste parametrene i SOA er:

- **Primær navetjener** – alle domener må ha minimum 2 navnetjenere for å virke. Den primære navnetjeneren angir hvilket av disse to navnetjenerne som er masteren som den andre oppdaterer seg mot.

- **Serienummeret** – Hver gang du endrer sonefilen økes serienummeret til sonefilen med en. Dette er viktig, da de andre navnetjenerne i verden kun spør etter domenets sonefil i første omgang. Er domenets serienummer det samme som forrige gang vet de andre navnetjenerne i verden at denne sonefilen ikke har blitt oppdatert siden sist gang de sjekket sonefilen. De kan dermed bruke de gamle innstillngene for domene som de sparer på helt til serienummeret økes.

- **TTL** – TTL er en forkortelse for «*Time To Live*«. Sonefilens TTL-verdi angir sonefilens levetid. Når en navnetjener kommer for å spørre en navnetjener om et domene noterer de seg domenets serienummer og TTL-verdi. TTL-verdien er viktig, da den forteller hvor lang tid de andre navnetjenerne skal cache (mellomlagre) sonefilens innhold før de kommer tilbake å sjekker den igjen. Er denne verdien svært høy kan det dermed gå svært lang tid før eventuelle endringer i sonefilen slår i kraft. Sjekk derfor domenets TTL-verdi når du skal endre en record i sonefilen, da den forteller hvor lang tid det maksimalt kan gå før endringen slår i kraft overalt på Internett.

5.11.2 Records

Recordene til headeren forteller hvilke sub-domener domene har, hvor mailen skal leveres, hvilke navnetjenere domene benytter, hvilken webserver som har hjemmesidene, hvem som har lov til å sende e-post o.s.v.

For at et domene skal virke må sonefilen til domene ha minimum to records (linjer) som angir hvilke to DNS (navnetjenere), domene benytter. Disse to recordene kalles **NS record**.

I tillegg er det vanlig å ha minimum en **A-record** eller **CNAME** som angir hvor hjemmesidene ligger og en **MX-record** som forteller hvor e-post til domene skal leveres. Disse fire recordene er basisen for ethvert domene med hjemmesider og e-post knyttet til domene.

Type records:	Beskrivelse:
NS	En angivelse av hvilke navnetjenere domenet benytter. IKKE endre disse, da det ikke er nok å endre recordsene hvis man ønsker å bytte navnetjener. Skal navnetjenerne benyttes må også headeren endres og det må sendes inn en endringsmelding til TDL registraren. Skal du bytte navnetjener på domenet ditt må du ta kontakt med OnNet.
A	A betyr A-record. En A-record benyttes til å angi IP-adressen til en tjeneste. En gyldig A-record skal skrives på følgende måte: 217.137.23.46 (fire tall, adskilt av et punktum)
CNAME	Mens en A-record angir IP-adressen til en tjeneste, benyttes CNAME til å angi servernavnet til en tjeneste. Et CNAME skal skrives på følgende måte: buddy.onnet.net. (legg merke til at CNAME må avsluttes med et PUNKTUM!!! Gjøres ikke dette blir zone-filen korrupt).
MX	MX-recorden forteller hvor mailen til domenet skal leveres, og må alltid være et servernavn. Det er ikke tillatt å angi en IP-adresse som en MX-record.

At denne filen er korrekt skrevet er ekstremt viktig, da den minste feil vil medføre at en eller flere tjenester slutter å virke. Gjør det derfor til en regel å sjekke sonefilen 1-2 timer etter at den er endret.

5.11.3 NS-recorden

For at et domene skal virke kreves det at sonfilen består av minimum to NS-recorder**.** En **NS-record** er:

en record som forteller hvilke navnetjenere (DNS) domene benytter.

5.11.3.1 Master og slave

Sonefilens header angir hvilke av disse to navnetjenerne som er den **primære navntjeneren**, også kalt **master**. Den primære navnetjeneren (master) er med andre ord den navnetjeneren som sitter på de «*orginal dataene*«, mens den **sekundær navnetjeneren**, også kalt **slave**, er den navnetjeneren som kun inneholder en synkronisert kopi av sonefilen til den primære navnetjeneren.

5.11.4 A-record og CNAME

Hvilken webserver hjemmesidene ligger på står angitt i domenet sin sonefil i form av en **A-record** eller et **CNAME**. Forskjellen mellom en A-record og et CNAME kan forenklet forklares slik.

> ***Mens en A-record angir hvilken IP-adresse til serveren nettsidene benytter, angir et CNAME serverens servernavn.***

A record = IP adresse
CNAME = Servernavn

Et CNAME er med andre ord et alias for en A-record. Med dette menes at det ikke er mulig å avgjøre hvor en nettside eller tjeneste er hvis navnetjeneren rapporterer tilbake et CNAME istedenfor en A-record når noen spør etter en side eller tjeneste. Rapporterer navnetjenerne et CNAME når noen spør etter en side eller tjeneste, vil navnetjenerne måtte gjøre et nytt DNS-oppslag hvor de spør navnetjenerne etter IP-adressen til CNAME-et før de kan gå til siden eller tjenesten.

5.11.5 MX-record

En MX-record, eller **mail exchanger record**, er:

en record i sonefilen som forteller hvor mail til domene skal leveres.

MX-recorden angis alltid i form av et CNAME og ikke som en A-record. Det vil si at det ikke er mulig å angi MX-recorden i form av en IP-adresse. Den må angis som et servernavn (alias for en IP-adresse). Er MX-recorden til domene feil vil domene med andre ord ikke motta noe epost. Hver derfor ekstremt forsiktig når du ender denne recorden.

5.12 Webserver

En **webserver** eller **vevtjener** er et dataprogram som lagrer og utleverer data til internett.

Som vi tidligere har vært inne på så vet nettleseren din ikke hvor en bestemt nettadresse (URL) er når du skriver inn en URL i nettleseren din for å komme til en bestemt nettside. Nettleseren din vil først spørre sin nærmeste DNS om hvor domene i nettadressen (URL) du spør etter befinner seg. Navnetjeneren (DNS) vil så returnere en IP-adresse til nettleseren som forteller hvilken webserver domene bruker. Navnetjeneren vil så prøve å koble seg opp mot denne nettadressen og webserveren på port 80 eller 443 hvis det skal etableres en sikker tilkobling.

Når webserveren mottar forespørselen om en bestemt nettadresse (URL) vil webserveren først sjekke om domene er konfigurert for denne webserveren. Dvs. om domene bruker denne webserveren eller ikke. Bruker domene denne webserveren vil programmet så finne ut hvilken root mappe dette domene bruker og hvor i denne rot-strukturen den etterspurte siden befinner seg. Deretter vil webserveren redirekte kallet til denne mappen hvor siden ligger.

Når kallet endelig kommer til siden (filen) vil filen bli kjørt på webserveren hvis webserveren har installert alle de teknologiene og programmene nettsiden krever for å virke som tiltenkt. Hvilke teknologier webserveren støtter er avhengig av hostmasteren som har satt opp webserveren og hvilket operativsystem (OS) som brukes i bunn.

Etter at nettsiden er kjørt vil resultatet bli sendt tilbake til nettleseren som etterspurte siden og bli vist på skjermen til brukeren.

5.12.1 Hvilke webservere finnes?

Det finnes idag flere ulike webservere å velge mellom. Hvilken webserver det er mulig å installere på den fysiske serveren (maskinvaren) er avhengig av hvilket operativsystem serveren benytter. De to dominerende OS-plattformene på Internett er idag:

1. **Linux** (markedsandel over 66 %)
2. **Windows** (markedsandel rundt 18%)

De største webserverne er idag:

1. **Apache** (makedsandel ca. 66%)
2. **IIS** (markedsandel ca. 18%)
3. **nginx** (markedsandel ca. 8%)
4. **Google** (markedsandel ca. 5%)

Apache web server er fortsatt verdens dominerende web server med en markedsandel på rundt 2/3. Apache web servere kan kjøres på alle servere med et Linux basert operativsystem. Den raskeste webserveren er imidlertid LiteSpeed. En webserver som er en add-on til Apache webserver. Det vil si at det bare er å installere og benytte den uten at du trenger å omkonfigurere noe. Denne nye webserveren øker nettsidenes hastighet med mellom 3-75 ganger, avhengig av hvor tunge de er og trafikken mot dem.

5.12.2 Hvilken webserver bør jeg velge?

Hvilken webserver du bør velge er delvis avhengig av hvilken programmeringsteknologi du utvikler nettsidene dine i og hvilke databaseformater du gjør deg avhengig av.

Har du utviklet nettsidene dine med bruk av programmeringspråkenee ASP eller ASP.NET og/eller er avhengig av datbaseformatene MS Access eller MS SQL må du kjøre nettsidene dine på en IIS webserver. Dette fordi dette er Microsoft sine patenterte teknologier og må kjøres på en IIS webserver.

Er du ikke avhengig av disse teknologiene kan du kjøre nettsidene dine på hvilken som helst webserver, da alle de andre programmeringspråkene er åpen kildekode som kan kjøres på alle webservere.

5.12.3 Valg av hosting løsning

For å kunne publisere egne nettsider som er knyttet til ett domene kreves det at du har en tilgang til en webserver som kan kjøre de teknologiene dine nettsider krever. For å få dette til i praksis er det ikke tilstrekkelig å tilgang til bare en webserver. Normalt trenger du også tilgang til en:

- **FTP-server** som du kan bruke til å laste opp og ned filer til ditt nettsted.
- **Database server** som driver nettstedets database. Det mest brukte database formatet på Internett idag er mySQL som er en åpen kildekode som du gratis kan laste ned og installere.
- **Mailserver** som du kan benytte til å sende og motta epost til domene.

Alle disse tjenestene styrer du selv normalt gjennom et webbasert kontrollpanel på webserveren du kan logg inn på via din nettleser.

For å kunne installere webserveren og de andre server tjenestene du trenger trenger du maskinvare i form av en server koblet til Internett via raske Internett linjer. Du har er tre valg:

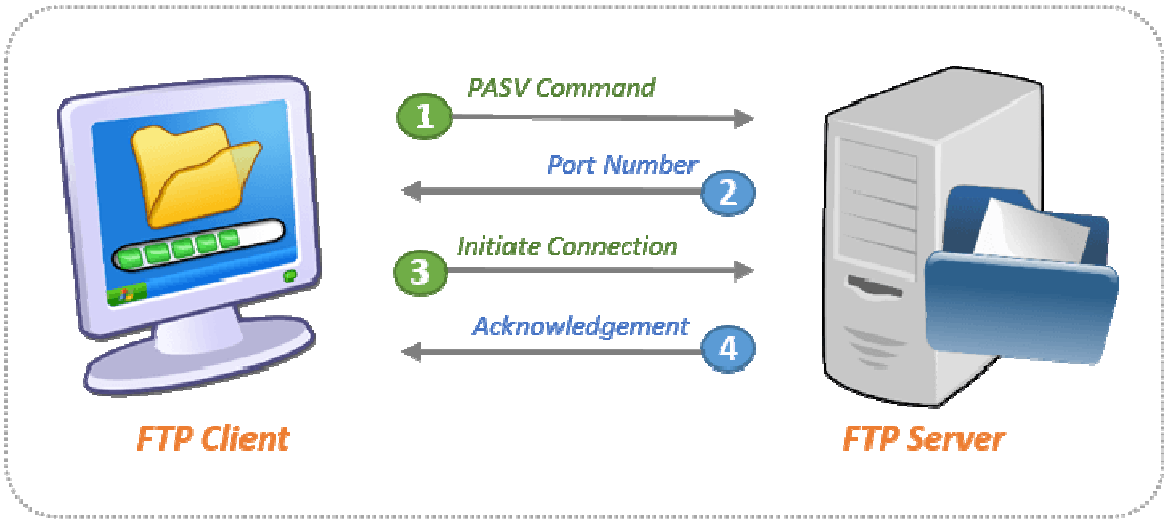
1. **Dedikert server** - en egen fysisk server som har installert alle de tjenestene du trenger og som er knyttet til en egen IP-adresse og som kun kjører ditt domene og nettsted. Dette er den dyreste og mest kompetansekrevende løsningen, da du selv må dekke alle infrastruktur kostnadene og ha kompetansen til å drifte og vedlikeholde alle tjenestene på serveren.
2. **Virtuell server** - er ikke en egen server, men en stor server som er delt opp i flere mindre servere som er satt opp spesifikt for hvert enkelt nettsted/bruker. Siden flere deler en større fysisk server en en felles linje er virtuelle servere vesentlig rimeligere enn dedikerte servere, men like kompetansekrevende siden det er du selv som er ansvarlig for drift og vedlikehold av alle tjenestene på serveren.
3. **Webhotell** - her leier du deg inn på en større webserver som du deler med mange andre domener og nettsteder. Her betaler du en månedlig leie for tjenestene du trenger og du slipper å ha ansvaret for driften og vedlikeholdet av serveren, da dette inngår som en del av leien. Siden dette er et spleiselag er dette den rimeligste og minst kompetansekrevende løsningen og derfor også den løsningen flest velger.

5.13 File Transfer Protocol (FTP)

File Transfer Protocol (**FTP**) er en *filoverføringsprotokoll* som brukes for å overføre filer mellom to enheter i et TCP/IP nettverk. F.eks. en bruker og ett nettsted.

FTP er en operativsystemuavhengig protokoll for overføring av filer, men kan kun brukes på et TCP/IP basert nettverk (f.eks. Internett).

Overføringen skjer mellom en FTP-klient og en FTP-server. Hvilken maskin som har hvilken rolle, kan i utgangspunktet velges fritt.



FTP-serveren lytter på nettverket etter forespørsler. FTP-klienten kobler til serveren og kan lese og skrive til serverens filsystem, som opp- og nedlasting av filer, sletting, navnebytte, chmoding osv.

5.13.1 Ftp-konto

For å kunne laste opp eller ned filer til en ftp-tjener (server) kreves det ikke bare at du kan koble deg på en ftp-server. Du må også ha en ftp-konto på denne ftp-serveren.

Denne kontoen setter du opp gjennom programvaren som følger med ftp-tjeneren. Har du et webhotell inngår denne funksjonen normalt som en del av kontrollpanelet som følger med webhotellet for å administrere tjenestene som følger med webhotellet.

5.13.2 Ftp-adresse

For å få kontakt med en ftp-konto på en server (tjener) må du angi en ftp-adresse til kontoen. Ftp-adressen starter alltid med ftp://. F.eks. ftp://estudie.no hvis estudie.no er ditt domene.

5.13.3 Ftp-host

En host er det samme som en tjener. Ftp-host er dermed ftp-adressen til din ftp-server, uten ftp:// foran. Har du et webhotell er ftp-hosten normalt det samme som ditt domene, da ftp-klientens oppgave er å laste opp filer til ditt webområde.

5.13.4 Protokoll

FTP virker utelukkende over TCP og bruker port 20 og 21, men andre porter kan benyttes i tillegg. Port 21 er kontrollporten (også kalt kommandoporten) som klienter sender kommandoer over og som tjeneren lytter og svarer på. Overføringen skjer på port 20 og/eller andre porter avhengig av filoverføringsmodus.

I denne sammenheng skiller vi også mellom aktiv og passiv modus. Forskjellen kan i følge Wikipedia forklares slik:

5.13.4.1 Aktiv modus

Klienten sender PORT-kommandoen til tjeneren med beskjed om et tilfeldig valgt portnummer større enn 1023 som klienten vil lytte på. Tjeneren sender først et svar samme vei tilbake, og så åpner den dataoverføringsforbindelsen mellom sin egen port 20 og klientens tilfeldig valgte port. Dette kan være noe vanskelig å få til hvis en brannmur er imellom, uten å åpne alle porter på brannmuren fra 1024 og oppover.

5.13.4.2 Passiv modus

Klienten sender PASV-kommandoen til tjeneren noe som betyr at klienten er i passiv modus. Da er det tjeneren som velger et (tilfeldig) portnummer større enn 1023 og sender det som en PORT-kommando til tilbake til klienten. Klienten åpner dataoverføringsforbindelsen mellom den spesifiserte porten hos tjeneren og en selvvalgt port hos seg selv. Port 20 er altså ikke involvert. I mange FTP-tjenere er det mulig å spesifisere et utvalg av porter som skal brukes i passiv modus.

5.13.4.3 Utvidet passiv modus

Det er som passiv modus, bare at tjeneren ikke sender sin IP-adresse som en del av svaret på klientens forespørsel. Klienten må da anta at IP-adressen er uendret. Utvidet passiv modus ble introdusert i RFC 2428 i september 1998.

5.13.5 Fordeler

- **Åpen løsning**: Det finnes mange programmer som benytter protokollen. Dersom ikke disse fyller behovene man har, står man fritt til å lage egne programmer.
- **Billig**. På grunn av tilgang til standarden er mange FTP-program enten inkludert i annen programvare, eller kan hentes gratis.
- **Funksjonell**. Så godt som all filhåndtering kan utføres uavhengig av hvilken maskin de ligger på.

5.13.6 Ulemper

- All kommunikasjon går ukryptert og kan derfor leses av alle som har tilgang til kommunikasjonen mellom de impliserte maskinene.
- Protokollen er vanskelig å håndtere for en brannmur. Port 21 er inaktiv under dataoverføringen, noe som kan medføre at forbindelsen opphører. (Dataoverføringen vil normalt bli fullført likevel, men kan gi tilsynelatende feilmeldinger.) Det kan tenkes at dataoverføring blir forsøkt på andre porter enn port 20, noe som ofte vil stoppes av brannmuren. Flere overføringer kan gå parallelt, som også krever spesiell håndtering av brannmuren.
- Det kan være mulig å be FTP-serveren å levere en fil på en tredje maskin. Selv om dette er ment å være en nyttig egenskap, har det i en del sammenhenger vært benyttet til illegal virksomhet.

5.13.7 Tjener (server)

En **FTP-tjener** er et dataprogram som gjør det mulig for andre datamaskiner med en FTP-klient å bruke protokollen FTP for å laste opp eller laste ned filer til datamaskinen som FTP-tjeneren kjører på. Administratoren av FTP-tjeneren setter opp hvilke kataloger brukeren av FTP-klienten skal ha tilgang til og hvorvidt brukeren er berettiget til å laste opp eller ned filer i de ulike katalogene.

5.13.8 Klient

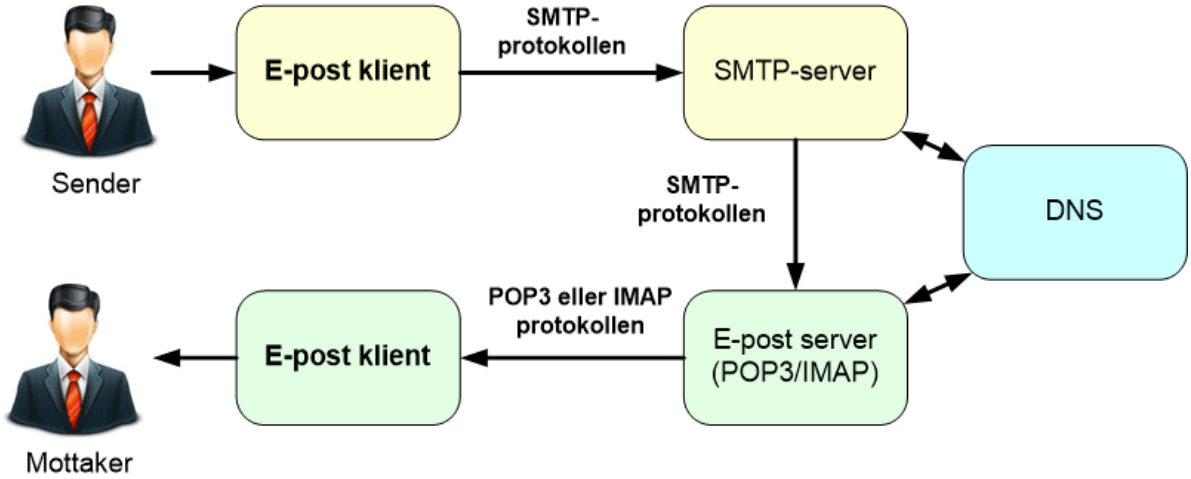
En **FTP-klient** er et dataprogram som ved hjelp av FTP-protokollen lar en bruker enten laste opp eller ned filer til en FTP-tjener fra sin datamaskin til datamaskinen som FTP-tjeneren kjører på. Mange FTP-klienter koster penger, men det finnes gratis FTP-klienter som er like gode. Den mest kjente gratisklienten er nok Filezilla, som er en Open source FTP-klient.

5.14 E-post

E-post er en forkortelse for **elektronisk post**, eller **e-mail** som det heter på engelsk.

E-post er en elektronisk posttjeneste hvor dokumenter og meldinger blir sendt fra en datamaskin, nettbrett eller mobiltelefon til en annen over et TCP/IP datanettverk.

E-postmeldinger slik vi kjenner dem ble først utviklet av Ray Tomlinson, en programmerer for BBN, i juli 1970 når han jobbet med å lage en metode for å sende meldinger over ARPANET. Senere har e-post utviklet seg til å bli en av Internett mest benyttede tjenester.



Modellen viser hvordan utvekslingen av en e-postmelding skjer fra noen sender en melding til mottakeren mottar den. Prosessen starter med at senderen skriver en e-postmelding via en e-postklient. Meldingen leveres så til en SMTP-server via SMTP-protokollen. Denne serveren vil så spørre sin nærmeste DNS om hvilken e-postserver mottakerens e-postadresse tilhører. Når DNS-serveren returnerer dette svaret til SMTP-serveren vil SMTP-serveren koble seg opp mot den angitte e-post serveren som vil motta denne

meldingen via POP3 eller IMAP protokollen og levere denne videre til mottakerens e-postkonto og e-postklient som mottakeren bruker for å lese meldingen.

5.14.1 Epostadresse og alfakrøll

En e-postadresse er en adresse du kan sende e-post til. Epostadressen angir hvilket domene som skal motta e-postmeldingen og hvilken bruker på dette domene meldingen er til. Alfakrøllen (@) brukes til å skille brukeren og mottaker domene av e-posten.

I eksemplet over er brukeren som skal motta e-postmeldingen "Kjetil", mens "estudie.no" angir hvilket domene denne brukeren tilhører og er det domene e-postmeldingen blir levert til.

Alfakrøllen @ i e-postadresser ble funnet på av Ray Tomlinson fordi han trengte noe som kunne skille navnene til sender og mottaker fra navnene på maskinene de satt på, og valget falt på dette tegnet ettersom det ikke var så ofte i bruk.

5.14.2 E-postkonto

En **epost-konto** kan sammenlignes med en meldingsboks eller en postkasse. Det er et sted der meldinger kan leveres, og der brukere kan logge inn for å hente/lese og sende meldinger.

For å kunne opprette en e-postkonto må du disponere ett domene som kontoen (brukeren) kan knyttes til. Eier du ikke ditt eget domene må du knytte kontoen til domene til en annen organisasjon, f.eks. hotmail.com (Microsoft), gmail.com (Google) eller online.no (Telenor).

5.14.3 E-post server

En e-post server er en tjener som har installert de Internett protokollene, normalt SMTP, POP3 og/eller IMAP, du trenger for å kunne sende og motta e-postmeldinger til ditt domene.

Eier du et eget domene som du har knyttet til et webhotell har du normalt denne tjenesten inkludert som en del av hosting pakken du leier. Det vil si at du deler e-post serveren med alle andre domener på serveren du bruker.

Har du knyttet domene ditt til en dedikert eller virtuell server må du selv installere denne tjenesten som en del av serveren din.

5.14.4 Metoder for å motta, lese og sende e-post

Du kan i prinsippet lese og sende e-post via din e-postkonto på to måter:

1. **Webmail**: Du kan logge deg på en nettside med et brukernavn og passord for å få tilgang til alle dine meldinger. Her kan du i tillegg skrive nye og svare på eksisterende meldinger. Dette er den enkleste måten å bruke din e-postkonto på, da den ikke krever noen som helst form for installasjon eller oppsett på enheter du ønsker å bruke for å lese og sende e-post.
2. **E-postklient**: Du kan installere e-postkontoen på en e-postklient. Ett e-postprogram på din datamaskin, nettbrett eller mobiltelefon for å lage og sende e-post. Ønsker du å motta og sende e-post via en e-postklient, f.eks. Outlook, må du sette din e-postkonto manuelt opp med å angi en e-postadresse, bruker, passord, inngående og utgående mailserver, samt hvilke porter som skal brukes for å sende og motta e-post.

5.14.5 E-postprotokoller

For å kunne sende en e-postmelding til noen kreves det at du bruker en rekke Internett protokoller før mottakeren i det hele tatt har fått meldingen. Dette er protokoller som ikke har noe med selve e-posten å gjøre, men som er nødvendige for at meldingssystemet i det hele tatt skal virke.

De mest sentrale Internett protokollene du er avhengig av for å sende/motta e-post, men som ikke er knyttet til selve e-postmeldingen er TCP/IP og DNS protokollen.

I tillegg er du avhengig av minst 2 av følgende 3 e-postprotokoller for å kunne sende og motta e-postmeldinger:

- **SMTP protokollen** - brukes til å sende epostmeldingen til en mottaker
- **POP3 protokollen** - brukes til å motta og laste ned epostmeldinger til en e-postklient
- **IMAP protokollen** - brukes til å motta og lese e-postmeldingen på epost serveren uten å laste den ned til en epostklient.

5.14.6 SMTP protokollen

Simple Mail Transfer Protocol (**SMTP**) er en standardisert protokoll som beskriver hvordan e-post skal sendes fra en datamaskin til en annen over et TCP/IP nettverk. Det er med andre ord denne protokollen du bruker hver gang du trykker på "send" knappen for å sende en e-post til en annen.

SMTP er en relativt enkel tekstbasert protokoll, hvor du først angir hvem som skal motta meldingen. Dette gjøres ved å angi en eller flere e-postadresser i ASCII-format som overføres til SMTP-serveren du ønsker å bruke til sende meldingen med. Deretter overføres avsenderens adresse og selve meldingen.

SMTP benytter normalt Følgende TCP port til å overføre meldingen med:

- **Klar tekst format: Port 25**
- **Kryptert sending (SSL): Port 465**

SMTP har vært i utstrakt brukt siden tidlig på 1980-tallet, og siden den opprinnelig kun var ASCII-basert taklet den ikke filer som vedlegg. Det var heller ingen sikkerhetsfunksjoner implementert i protokollen, som kryptering og verifisering av avsender (for å unngå spammere). Protokollen ble derfor videreutviklet slik at binære filer kunne overføres, ved å tillate MIME-standarden som definerte en metode man kunne kode binære filer på.

SMTP er en såkalt *push*-protokoll, dvs. at den har kun overføring én vei og kan ikke ta imot data fra server. For at et epostprogram skal kunne hente inn de meldingene som venter på en epost-tjener må man bruke andre protokoller som POP3 eller IMAP.

Siden SMTP protokollen ikke krever noen form for identifikasjon gjennom en form for login + passord er SMTP protokollen ubrukelig til å hente beskjeder.

5.14.7 POP3

POP står for **P**ost **O**ffice **P**rotocol (**P**ost ***K***ontor **P**rotokoll) og finnes nå i tredje versjon.

Protokollen brukes for å hente post fra en e-post server (tjener) til egen datamaskin gjennom TCP/IP-protokollen.

POP3 brukes sammen med to andre protokoller for å håndtere e-post. Disse er SMTP og IMAP. IMAP er et alternativ til POP3 protokollen for å motta og lese e-post.

POP3 benytter normalt følgende TCP port til å motta meldingen med:

- **Klar tekst format: Port 110**
- **Kryptert sending (SSL): Port 995**

5.14.8 IMAP

IMAP er en protokoll for å motta e-post via Internett. Akronymet står for **I**nternet **M**essage **A**ccess **P**rotocol, en tidligere betegnelse var **I**nteractive **M**ail **A**ccess **P**rotocol.

Den brukes for å få tilgang til en e-post-server for å motta post. Protokollen kjennetegnes ved at mottatt post blir lagret på serveren også etter at den er lastet ned, i motsetning til POP3 standarden som fjerner meldingen på serveren etter at den er lastet ned. Dette betyr at e-posten er tilgjengelig fra en hvilken som helst e-post-klient på Internett, ikke bare lokalt der hvor innholdet ble lastet ned først. En stor fordel for dem som ønsker å lese e-posten sin fra ulike enheter, f.eks. fra både sin datamaskin, nettbrett og mobiltelefon.

IMAP benytter normalt følgende TCP port til å motta meldingen med:

- **Klar tekst format: Port 143**
- **Kryptert sending (SSL): Port 993**

5.14.9 MX-record

En MX-record er en record (linje) i sonefilen til et domene og forteller hvor e-post sendt til domene skal leveres. Mangler domene denne MX-recorden vet Internett ikke hvor e-posten skal leveres.

MX-recorden oppgis alltid i form av ett CNAME. Det vil i form av et servernavn, også kalt host, istedenfor en IP-adresse (A-record).

5.14.10 E-postmeldingens oppbygning

En e-postmelding består av to hoveddeler:

1. **Header seksjon** (Strukturert i felt som sendes fra SMTP serveren din til mottakerens e-post server for å identifisere hvem meldingen er fra og til)
2. **Body seksjon** (Inneholder selve meldingen i form av ustrukturert tekst)

Header og body seksjonen er adskilt med en blank linje.

5.14.10.1 Header

Header delen av en e-postmelding er strukturert i felt. For eksempel: From, To, CC, Subject, Date, og annen informasjon om e-postmeldingen. Syntaksen som benyttes her er beskrevet i RFC 5322.

Feltnavnene og verdiene i dem kan kun bestå av 7-bit US-ASCII tegn. Non-ASCII verdier kan brukes ved bruk av MIME standarden.

Headeren må inkludere følgende felt:

- *From*: E-postadressen til avsenderen, og evt. navnet til denne personen. Det siste er valgfritt.
- *Date*: Tidspunktet og datoen når beskjeden ble strevet. De fleste e-post klienter fyller ut denne informasjonen automatisk selv når meldingen sendes.

I tillegg bør følgende felter også inngå som en del av headeren:

- *Message-ID*: Også et automatisk utfylt felt som brukes for å unngå at samme meldingen blir levert flere ganger.
- *In-Reply-To*: Message-ID av meldingen som dette er ett svar til. Brukes for å linke relaterte meldinger sammen. Brukes kun i "reply" beskjeder.

De øvrige standardfeltene for headeren er:

- *To*: E-postadressen og evt navnet til mottakeren av beskjeden.
- *Subject*: Et kort sammendrag av innholdet i meldingen.
- *Bcc*: Blindkopi sendes til denne e-postadressen. Feltet er synlige for "To" og "CC" mottakeren(e).
- *Cc*: En kopi av meldingen sendes til denne e-postadressen.
- Content-Type: Informasjon om hvordan meldingen skal vises, normalt en MIME type.
- *References*: Message-ID til meldingen dette er en reply til, og Message-id til alle foregående replys.
- *Reply-To*: E-postadressen et svar til denne meldingen skal sendes til.
- *Sender*: Adressen til den fysiske senderen (SMTP-serveren) av meldingen.

SMTP definerer også ulik sporing informasjon som også skrives i headeren i følgende to felter:

- *Received*: når en SMTP server aksepterer en beskjed setter de inn en sporing record i toppen av headeren.
- *Return-Path*: når SMTP serveren som leverer meldingen leverer den setter de inn dette feltet i toppen av headeren.

Når e-post serveren mottar en melding setter de ofte inn også andre sporing felt i toppen av headeren. F.eks.:

- *Authentication-Results*: resultatet av serverens authentication sjekk
- *Received-SPF*: resultatet av SPF sjekken e-post serveren gjorde når de mottok meldingen.
- *Auto-Submitted*: brukes for å markere at dette er en automatisk generert melding.

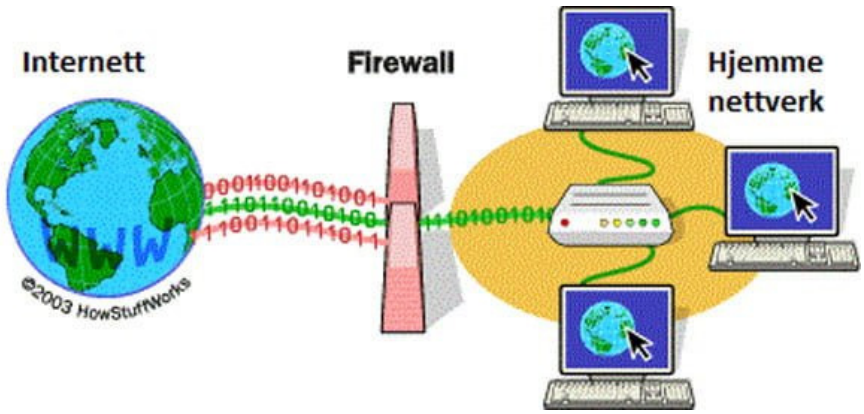
5.14.10.2 Body

Body seksjonen inneholder selve meldingen. Originalt var e-post designet for å bruke 7-bit ASCII, men MIME og andre standarder gjør at vi idag kan bruke alle tegn og grafikk i e-postmeldinger.

De fleste e-postklienter støtter idag to formater:

1. **Plain tekst** - meldingen består av uformatert tekst. Linker, farger, tabeller og bilder kan ikke brukes.
2. **HTML** - meldingen vises i et HTML-format slik at du kan formatere e-postmeldingen på samme måte som en nettside.

5.15 Brannmur



For å sørge for at ingen utenforstående får tilgang til virksomhetens nettverk, servere og datamaskiner, må man ha en fysisk nettverks brannmur som står mellom Internett forbindelsen til virksomheten og LAN-nettverket på innsiden.

I datateknikk er en **brannmur**, eller *firewall* som det heter på engelsk:

> ***"maskinvare og/eller programvare som beskytter datanett mot uønsket kommunikasjon".***

Eksempel på slik uønsket kommunikasjon kan være hackere som trenger inn i datanett koplet til internett.

5.15.1 Funksjon

Brannmuren sin oppgave er å kontrollere trafikk mellom datanettverk med ulike tillits-forhold. Typiske eksempel er Internet som er ei sone uten tillit, og et internt nettverk som er (og skal være) en sone med høy tillit. Målet er å tilby kontrollerte grensesnitt mellom soner med ulike tillitsforhold ved å påtvinge en sikkerhets-politikk og tilkoblingsmodell. En sone med et mellomliggende tillitsnivå, plassert mellom Internett og det pålitelige interne nettverket blir ofte referert til et perimeter-nettverk eller DMZ (DeMilitarized Zone).

Riktig konfigurasjon av brannmurer krever gode evner hos system-administratoren. Det krever betydelig forståelse for nettverks-protokoller og datasikkerhet. Små feilgrep kan gjøre en brannmur verdiløs som sikkerhetsverktøy. Standard sikkerhetsrutiner foreskriver et «default-deny» (avslå dersom ikke annet er spesifisert) regelsett for brannmuren.

5.15.2 Personlig brannmur

En personlig brannmur er et program som beskytter datamaskinen mot angrep fra Internett. Den kan ikke beskytte mot alle typer angrep, men er et av de grunnleggende og nødvendige sikringstiltakene. I virksomheter, som bør ha en nettverksbrannmur, bør alle bærbare maskiner ha en personlig brannmur installert. På hjemmenettverk bør alle datamaskiner ha personlig brannmur installert.

5.15.3 Trusler

Personlig brannmur gir god beskyttelse mot kartlegging av maskinen, automatiserte angrep og ormer. De fleste personlige brannmurer inneholder ofte også ekstra funksjonalitet som kan øke beskyttelsen mot spam, virus, spyware, phising og andre former for uønskede hendelser. Hvor mye og hvor godt den beskytter mot slike trusler, varierer mye mellom de ulike variantene av personlige brannmurer.

5.15.4 Typer av brannmurer

Alle de vanlige operativsystemene har i dag brannmurfunksjonalitet inkludert. Linux inneholder iptables, Mac OS X har ipfw, og Windows XP har Windows-brannmur. Alle disse kan gi god beskyttelse mot ulike former for angrep. De inneholder ikke mye ekstrafunksjonalitet for ytterligere beskyttelse, men gir en god og nødvendig basisbeskyttelse. Det finnes også mange personlige brannmurer som kan lastes ned gratis eller kjøpes. Felles for disse er at de tilbyr utvidet eller forbedret funksjonalitet enn de som følger standard med operativsystemet. For Linux og Mac OS X er det stor sett snakk om verktøy som gjør det enklere å administrere den innebygde brannmuren.

5.15.5 Virkemåte

Det finnes to hovedtyper av personlige brannmurer. **Applikasjons- og trafikkfokuserte**.

5.15.5.1 Applikasjonsfokusert

Disse styrer tilgang ut på Internett basert på hvilken applikasjon som prøver å nå nettet. Normalt lager de seg en signatur av alle applikasjoner som har fått lov til å gå på nett for å enkelt kunne se om disse endres. Inngående trafikk kan også styres til spesifikke applikasjoner og ikke bare på portnumre.

5.15.5.2 Trafikkfokusert

Disse styrer tilgang kun basert på IP-adresser og portnumre. De gir samme type beskyttelse som en nettverksbrannmur, men bare for en enkelt datamaskin. For brukere med erfaring fra nettverksbrannmurer vil det være enkelt å sette seg inn i bruken av disse.

Begge typer er effektive sikkerhetsverktøy. De applikasjonsfokuserte gir noe mer sikkerhet, da de i tillegg til å filtrere trafikken også kan oppdage at applikasjoner blir endret.

5.15.6 Installasjon

Hvis en bruker de medfølgende personlige brannmurene er det bare å ta den i bruk. Nøyaktig informasjon om hvordan dette gjøres finnes i medfølgende dokumentasjon eller i hjelpesystemet. Ofte kan en også finne utførlige veiledninger på nettet om disse brannmurene.

Hvis en i stedet velger å bruke en annen personlig brannmur enn den som følger med operativsystemet, så bør en følge installasjonsveiledningen nøye.

5.15.7 Bruk

I daglig bruk er det forskjell på hvordan brukeren må forholde seg til den personlige brannmuren avhengig av om den er applikasjons- eller trafikkfokusert.

5.15.7.1 Applikasjonsfokuserte

De fleste av denne typen er såkalt selvlærende. Det vil si at første gang en applikasjon prøver å gå på nett så vil en få spørsmål om en vil tillate dette eller ikke. Innholdet i dialogboksen som kommer opp kan være forvirrende og vanskelig å forstå. For å hjelpe brukerne med dette har de personlige brannmurene ofte ferdige regler som åpner for de vanligste nettlesere og e-postklienter. De har også ofte muligheten for å klikke på en link for å få mer informasjon om applikasjonen det gjelder.

En ting som kan forvirre er applikasjoner som kjører i en virtuell maskin eller i et større rammeverk. Da vil en ofte få spørsmål om en tillater at den virtuelle maskinen eller rammeverket skal få tilgang til nett i stedet for applikasjonen en startet. En tommelfingerregel som normalt gjelder er at hvis dialogboksen kommer opp rett etter du har prøvd å starte et program, så er det som regel det programmet det gjelder. Denne tommelfingerregelen er ikke 100 % vanntett, men vil i de fleste tilfeller fungere godt nok.

Rett etter installasjon vil du ofte få mange spørsmål om applikasjoner som skal på nett uten at du har startet dem selv. Dette er programmer som startes automatisk av operativsystemet. Etter kort tid vil dette bli redusert drastisk. Da kan du bli mer skeptisk til programmer som uten at du har bedt om det prøver å gå på nett.

Noen applikasjoner oppdaterer seg meget hyppig. Antivirusløsninger er et vanlig eksempel på dette. Slike programmer vil medføre at en må gi tillatelse til å gå på nett etter hver endring. Mange vil synes dette er plagsomt, derfor har mange applikasjonsfokuserte personlige brannmurer funksjonalitet som kan gi tillatelse til å gå på nett basert på katalog og filnavn i stedet for selve signaturen til applikasjonen. Dette gir en noe lavere beskyttelse enn bruk av signaturer, men gir mindre bryderi med dialogbokser.

5.15.7.2 Trafikkfokuserte

Disse vil utføre jobben sin i bakgrunnen. I stedet er du nødt til å på forhånd ha definert de nødvendige reglene for det du skal ha tilgang til. Denne jobben kan ta noe tid og kan også virke vanskelig i begynnelsen. Når denne jobben først er gjort så vil en slik personlig brannmur kreve lite oppfølging utenom loggen.

For å få tilsvarende beskyttelse av applikasjonene som de applikasjonsfokuserte gir, bør en vurdere ulike verktøy for å oppdage endringer av applikasjoner. Det finnes mange slike verktøy på markedet. Det finnes også flere gode gratisversjoner for dette.
Virksomheter som skal administrere mange personlige brannmurer bør vurdere en løsning med god støtte for sentralisert kontroll og administrasjon.

5.15.8 Logger

I daglig bruk vil de to ulike hovedtypene av personlige brannmurer oppføre seg noe forskjellig. Felles for begge er at logger bør følges opp jevnlig. På den måten vil en etter hvert lære seg hva som er normal trafikk og støy i loggen, slik at en i stedet kan fokusere på de alvorlige avvikene.

5.16 SSL | Secure Sockets Layer

5.16.1 Trygg overføring av data og transaksjoner!

Secure Sockets Layer, **SSL**, er en protokoll som tillater autentisering mellom en klient (maskin/mobil) og en tjener (server) for å opprette en autentisert og kryptert tilkobling. Eller som vi sier på god norsk:

> ***«En sikker tilkobling mellom to datamaskiner, hvor det er umulig for hackere og andre uvedkommende å snappe opp informasjonen som sendes mellom disse to datamaskinene».***

SSL protokollen brukes for å opprette en sikker kobling mellom en server og en klient (din datamaskin/pad/mobil).

Ved at linjen mellom A og B blir kryptert er det ikke mulig for uvedkommende å sette opp en «*lyttepost*» på linjen som tar en kopi av informasjonen som sendes mellom serveren og tjeneren (din maskin/mobil. SSL brukes derfor alltid i forbindelse med korttransaksjoner, innlogging til nettbanker og annen overføring av sensitiv informasjon.

5.16.2 Sikkerheten avgjøres av krypteringsalgoritmen

Hvor godt denne linjen blir kryptert er avhengig av krypteringsalgoritmen som brukes. Jo høyere kryptering, jo vanskeligere er det for hackere å knekke krypteringen av dataene. Den høyeste krypteringen er idag 256-bit kryptering gjennom SHA-256 algoritmen. Av den grunn bygger alle SSL-sertifikatene OnNet selger på 256/128 bits SHA-256 kryptering.

5.16.3 Hvorfor SSL?

SSL tillater sensitiv informasjon som kredittkort informasjon, personnumre og passord til å bli overført på Internett på en trygg måte.

Gjennom å installere et SSL sertifikat på ditt nettsted viser du alle kunder og brukere som besøker nettstedet ditt at dette er et seriøst og trygt nettsted, hvor ikke noe informasjon kan bli stjålet av uvedkommende. Noe som blir stadig viktigere for å få kundenes tillit.

Facebook andre sosiale medier har også begynt å kreve at nettstedet har et SSL sertifikat for å kunne utveksle informasjon med det sosiale mediet via et API-grensesnitt e.l. Det samme gjelder nettsteder som ønsker å implementere en betalingløsning.

5.16.4 Bruksområder for SSL

SSL-sertifikat brukes hovedsakelig til å kryptere følgende typer linjer og kommunikasjon mellom en server og klient:

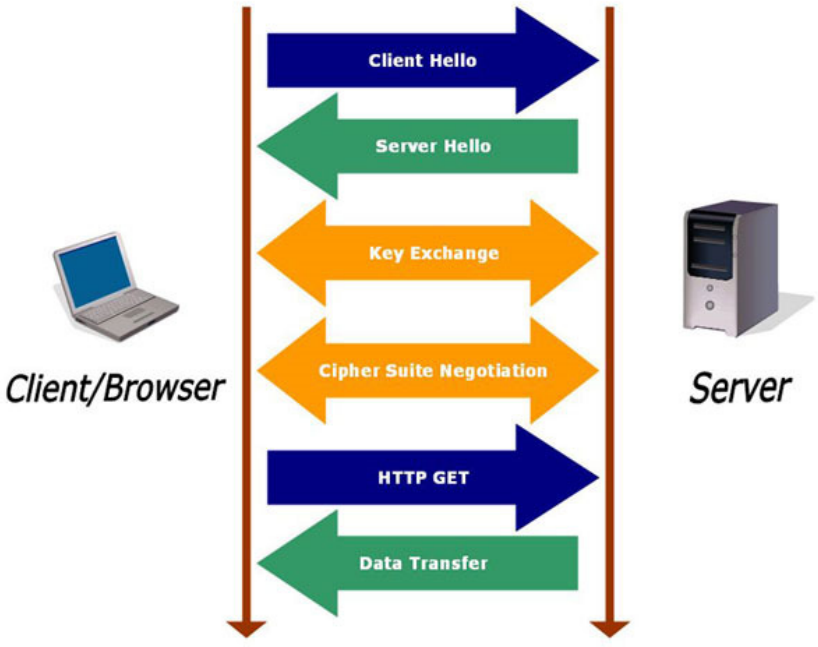
- **Nettsider** – Alle trafikk til ett nettsted kan omdirigeres til et SSL-sertifikat som krypter all kommunikasjon mellom nettstedet og de som besøker nettstedet via HTML-protokollen. Noe som er svært viktig for å sørge for at kortinformasjon, brukernavn, passord og andre sensitive opplysninger ikke kommer på avveie.
- **Epost** – Ved å kryptere kommunikasjonen over POP3, IMAP og SMTP protokollen til et SSL-sertifikat kan man sikre seg mot at andre klarer å snappe opp sensitiv informasjon som sendes på mail.
- **FTP** – Ved å kryptere kommunikasjonen over FTP-protokollen kan man sikre seg mot at ingen klarer å snappe opp filer som lastes opp eller ned mellom en server og bruker.

SSL-sertifikatet viser nettbrukeren hvilket selskap som eier domenet. Før dette kan skje må eierskapet være validert og bekreftet av en betrodd tredjepart (sertifiseringsautoritet CA), for å være gyldig.

Om et SSL-sertifikat er gyldig kan surferne på Internett enkelt se i sin nettleser. Er SSL-sertifikatet gyldig vil du se en hengelås i adressefeltet til nettleseren. I tillegg kan du se at nettsiden benytter SSL ved å se på URLen. Den begynner med med https:// i adressefeltet i stedet for http://.

5.16.5 Kryptering over TCP/IP – nivået

SSL kjører over TCP/IP-nivået, men under HTTP, LDAP, IMAP, NNTP, og andre nettverksprotokoller som kjører på et høyere nivå.



Den nyere Internet Engineering Task Force (IETF)-standarden Transport Layer Security (TLS) er også basert på SSL.

Hvordan «handshaket» er mellom klienten (deg) og serveren skjer for å etablere en trygg, kryptert linje ved hjelp av et SSL-sertifikat er vist i illustrasjonen til høyre.

Krypteringen skjer ved at tjenermaskinen (serveren/nettstedet) har en krypteringsnøkkel med to passord. Det ene kan bare brukes til å kryptere innholdet og kan derfor gis ut til alle (**offentlig nøkkel**). Den andre kan brukes til å dekryptere innholdet og må selvsagt bare være kjent for eieren (**privat nøkkel**).

Når SSL brukes f.eks for å lese e-post så sender tjenermaskinen det offentlige passordet til brukermaskinen uten at brukeren av brukermaskinen trenger å vite om dette. Dette passordet (krypteringsnøkkelen) bruker så brukermaskinen til å lage meldingen uleselig (kryptert) for tredjeparter som ikke kjenner dekrypterings passordet (nøkkelen). Deretter sendes meldingen over nettet til tjenermaskinen. Tjenermaskinen mottar meldingen og dekrypterer den ved hjelp av sitt hemmelige passord (krypteringsnøkkel), og leverer meldingen videre inn i sitt lokale system. Dermed vil ingen mellom bruker og tjener kunne avlytte kommunikasjonen.

I denne sammenheng er det viktig å merke seg at det er kommunikasjonskanalen (linjen) som er kryptert, og ikke selve budskapet (dataene). Ønsker du maksimal sikkerhet mot uautorisert adgang bør også dataene som sendes og lagres krypteres.

5.16.6 Hva er TCL (Transport Layer Security)?

TLS står for **Transport Layer Security**, og er en nyere versjon av SSL, med mindre justeringer. Brukes bl.a. til å kryptere linjer som brukes til å sende/motta epost og filer.

5.16.7 Krypterte porter

For å sikre en sikker kryptert tilkobling mellom serveren og brukeren skjer selve krypteringen ved at brukerne blir sendt til helt andre porter enn de åpne standardene bruker. Den åpne HTML standarden for nettsider bruker f.eks. port 80, mens HTMLS standarden bruker port 443. Under finner du oversikt over hvilke porter som normalt brukes.

HTML protokollen:

Åpen – Port: 80
SSL – Port: 443

FTP protokollen:

Åpen – Port: 20
SSL – Port: 21

POP3 protokollen:

Åpen – Port: 110
SSL – Port: 995

SMTP protokollen:

Åpen – Port: 25
SSL – Port: 465

IMAP protokollen:

Åpen – Port: 143
SSL – Port: 993

5.16.8 Nettlesergjenkjennelse

Dersom et SSL sertifikat ikke gjenkjennes av brukerens nettleser, vil brukeren få et varsel om at nettsiden ikke er trygg. Dette er selvsagt til stor ulempe for eieren av nettsiden som kan miste verdifulle brukere. Hvor stor andel av nettleserne som har forhåndsinstallert roten til de ulike SSL sertifikatene varierer en god del. Et godt sertifikat har minst 99 % nettlesergjenkjennelse.

5.16.9 Transaksjonsforsikring

SSL sertifikater ivaretar i hovedsak to funksjoner; sikker kryptering av informasjon og identifisering av eier av websiden. Transaksjonsforsikringen er ment å være nettbrukerens økonomiske garanti for at krypteringen ikke blir brutt under sesjonen og at informasjonen i sertifikatet er korrekt. Ved valg av forsikringsbeløp i sertifikatet må man ta stilling til hvilke økonomiske konsekvenser det vil ha dersom utvekslet informasjon kommer til feil mottaker eller blir tappet. Transaksjonsforsikring vil være med på å dekke økonomiske krav fra brukere som har blitt påført tap som et resultat av å ha blitt tappet for informasjon under en kryptert sesjon på din nettside.

5.16.10 Utstedes av et sertifiseringorgan

SSL sertifikater blir verifisert gjennom en tillitskjede. Tillitsankeret for SSL sertifikatet er rotleverandøren (Root Certificate Authority eller CA). Dersom rotleverandøren er kjent for brukeren er det større sannsynlighet for at vedkommende tar i bruk de tjenestene som websiden tilbyr, enn om det er en ukjent rotleverandør. Årsaken er at brukeren vil anse det som mindre sannsynlig at dette er et svindelforsøk fordi vedkommende stoler på rotleverandøren. Velg derfor sertifikater med mest mulig kjent og tiltrodd rotleverandør. Et godt eksempel på en velkjent rotleverandør er Verisign.

5.16.11 Hvordan ser jeg at en nettside bruker SSL?

Normalt skjer all kommunikasjon mellom en webserver og en besøkende av din nettside på den åpne HTML-standarden. Dvs. via en adresse som starter med http://.

Skjer kommunikasjonen på en sikker linje starter nettadressen med https://.

I tillegg vil du normalt få et symbol i nettleseren din som forteller at dette er et SSL-beskyttet område. De dyreste SSL-sertifikatene gir i tillegg en «grønn sidebar» med firmanavnet og ett stort grønt felt som en del av nettadressen for å vise at nettstedet benytter et SSL-sertifikat.

5.16.12 Anbefaling

Vi anbefaler at du alltid bruker SSL protokollen på nettsider som inneholder sensitiv informasjon eller informasjon som du er redd for at andre kan snappe opp via en lyttepost på linjen din. Klassiske eksempler er innloggingssider til brukerne dine.