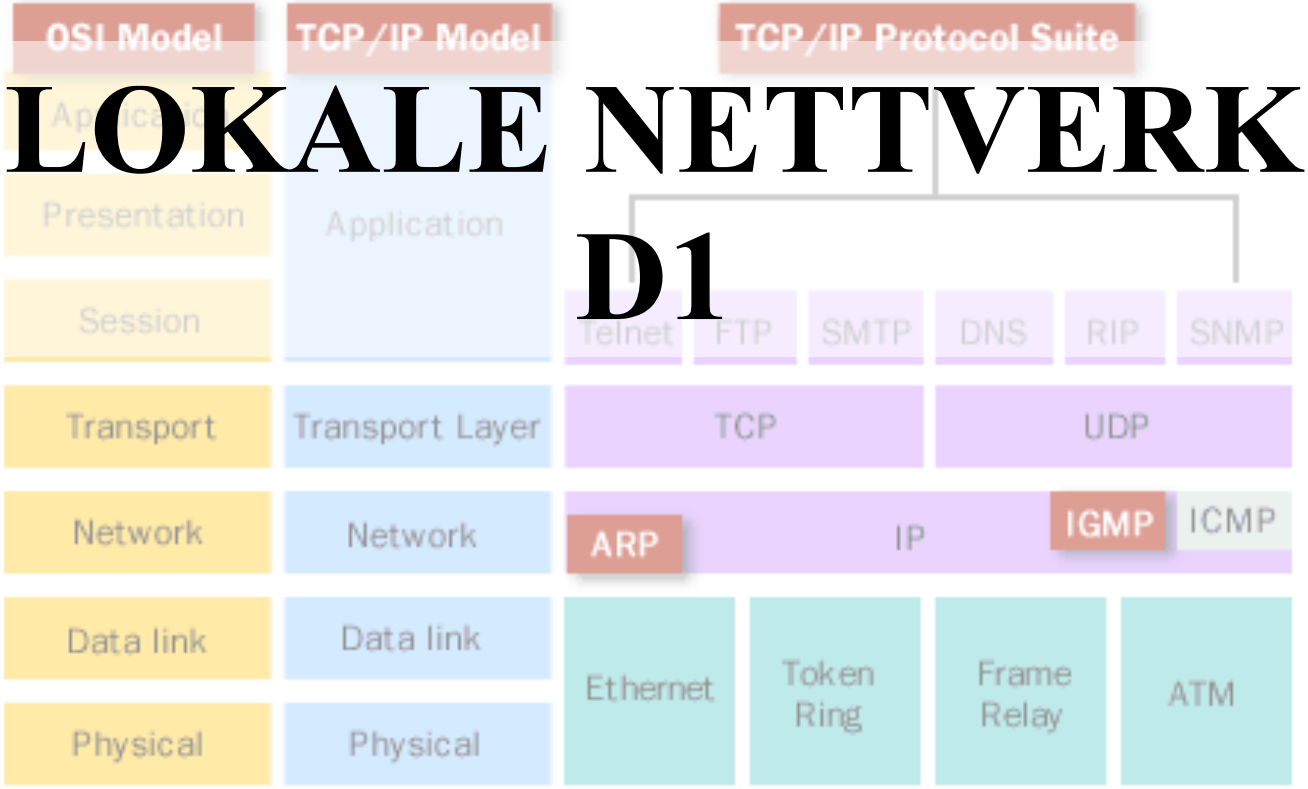
LOKALE NETTVERK D1



Innholdsfortegnelse

Lokale nettverk

Datanettverk brukes i dag i de fleste hjem og bedrifter. Alle slags størrelser og utforminger finnes og tilpasses kundenes individuelle behov og størrelse. Et godt oppsatt nettverk vil være pålitelig, fungerer og sikre brukerne mot uønskede hendelser og data tyveri.

Under denne gjennomgangen, Lokale Nettverk, skal vi innom disse områdene og tjenestene:

Delmål 1, grunnprinsipper

- ***Tall funksjonene og ASCII***

Prinsipielt trenger man ikke å kunne så mye om tallsystemene for å arbeide med IP- adresser, men for å ha en forståelse av hvordan nettverksmaskene fungerer, er det nødvendig å kunne sette den opp binært.

- ***TCP/IP***

TCP, Transmission Control Protocol og IP, Internet Protocol, er kommunikasjons- protokoller som hver for seg har ansvaret for sikker kommunikasjon, adressering og ruting av data mellom enheter i et TCP/IP-nettverk. I all hovedvekt handler dette om regler og prosedyrer.

- ***Nettverksmaskene***

En IP-adresse har to komponenter, nettverksadressen og vertsadressen. En nettverksmaske (subnett maske) skiller IP-adressen til nettverket og vertsadressene («nettverk»- «vert»). Videre deles verts delen av en IP-adresse til en subnett og vertsadresse («nettverk» - «subnett» - «host») dersom det er behov for ytterligere del-nettverk. Vi kaller det en nettverksmaske fordi den brukes til å identifisere nettverksadressen til en IP-adresse

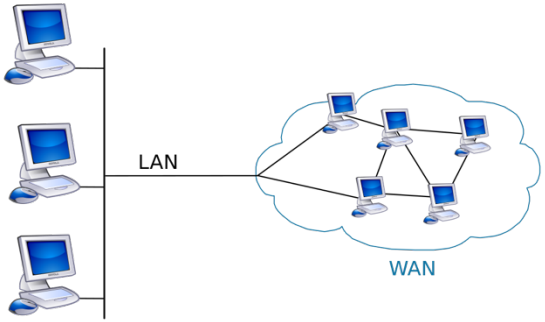
- ***DHCP***

DHCP (Dynamic Host Configuration Protocol) er en kommunikasjonsprotokoll som brukes i UDP/IP datanettverk. Ved hjelp av en **DHCP** server er det mulig å automatisk tildele IP-adresser og andre nettverks-parametere til tilkoblede klienter.

- **Oppgaver og test på delmål gjennomgås eter hvert fagområde**

Nettverksbegreper

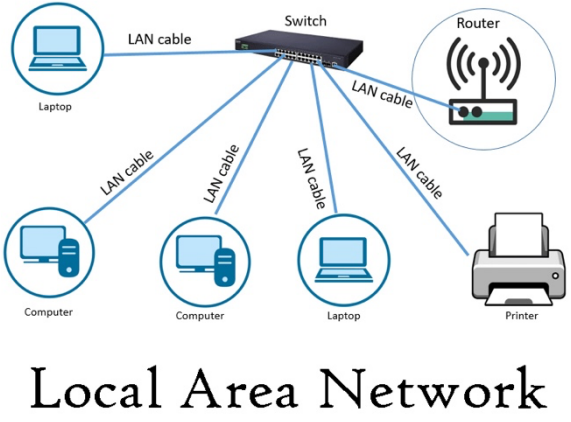
WAN



Som navnet tilsier så dekker WAN eller W*ide area of Network* et større område. Et WAN-nettverk består som regel av to eller flere lokalnett (LANs) som er koblet sammen via et offentlig nettverk som for eksempel en telefonlinje det beste eksempelet på WAN er internett.

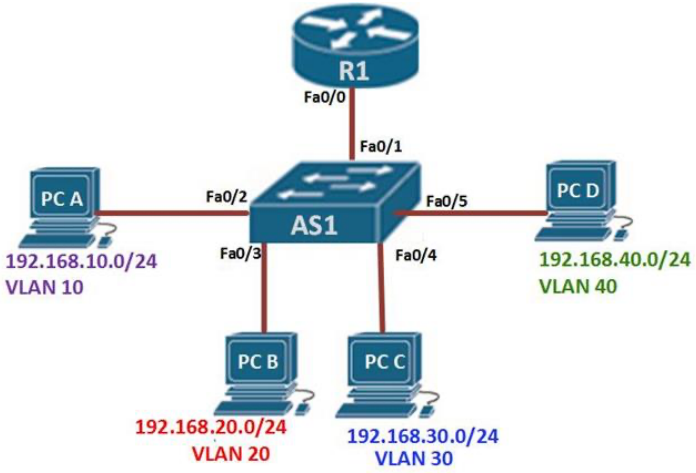
WAN brukes for at flere lokalnett og andre typer nettverk kan kobles sammen og kommunisere mellom hverandre fra et lokale til et annet. Mange WAN nettverk er bygd for privat bruk slik at en hel organisasjon kan kobles mot hverandre privat, andre typer WANs er bygd av internettleverandører som gir deg tilgang fra ditt lokalnett til internett. Det gjøres ofte ved hjelp av en kabel som trukket fra en Ruter til en telefonlinje (ISP).

LAN



LAN er en forkortelse for *Local Area Network (Lokalnett)* og er et datanettverk som kobler sammen to eller flere datamaskiner innenfor et begrenset område. Dette begrensede område kan for eksempel være ditt eget hjem eller arbeidskontor/arbeidsplass. Det som karakteriserer Lan i motsetning til WAN (Wide Area Network) er at det gir deg en høyere overføringshastighet av filer og at du ikke trenger å være koblet til Internett.
Et LAN-nettverk er som regel satt opp ved hjelp av en Ethernet-kabel som er koblet via to eller flere datamaskiner til en Hub, Switsj eller Ruter. Disse datamaskinene kan på denne måten kommunisere via hverandre ved å dele filer mellom hverandre.

VLAN



Vlan er forkortelsen for *Virtuelt LAN*.
VLAN er en teknikk som gjør det mulig å logisk kunne dele opp ett fysisk nettverk i flere logiske nettverk. VLAN er en ganske vanlig og grunnleggende funksjon i administrasjon av svitsjer for Ethernet. En fysisk svitsj kan håndtere flere adskilte nett. Med VLAN-teknikken kan trafikk fra flere ulike LAN transporteres i et og samme nettverk, dette kalles gjerne en trunk (Cisco) eller Tagged link (HP/ZyXCEL). VLAN funksjonen er en Software-funksjon som styrer koblingsvevet i svitsjene.

Merk:
Svitsjene kan også settes opp med egne IP adresser og Gateway for å sikre nettet enda bedre.

Typiske boligsystemer

Sammensatte enheter i opplæring og nettverksmodeller

Eksempel på komponentene som kan være inkludert i en trådløs ruter:

- Modem/medieomformer
- Ruter
- Brannmur
- Svitsj
- Aksesspunkt

For å forstå hvordan datanettverk fungerer trenger du kunnskap om hver enkelt komponenttype som brukes i nettverkene og hvordan disse er koblet sammen. I sammensatte enheter som trådløse rutere er mye av denne informasjon skjult, noe som gjør det vanskeligere for en nybegynner å forstå hvordan komponentene er satt sammen.

Derfor skal vi se på hver komponent for seg selv. Når du/dere senere skal sette opp nettverks-modellen skal vi benytte oss av følgene enheter:

- Kontroll svitsj
- Avdelings svitsjer
- Ruter med innebygget brannmur
- Printer
- Kamera
- Aksesspunkt for trådløst nett
- RJ45 tilkoplinger/kabler
- Egne PCer
- En serverløsning
- Windows 2019 server og Linux server med kontroll og web aplikasjon

Tallsystemene og TCP/IP

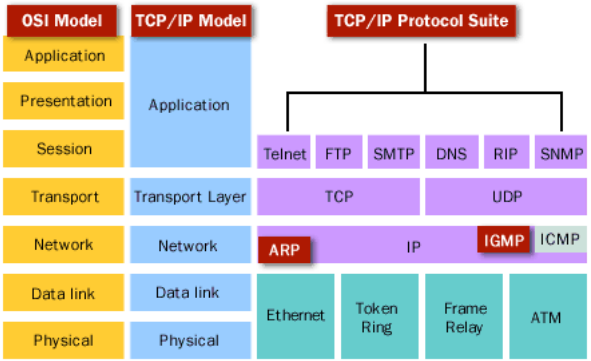
Siden vi allerede har vært inne og kikket på tallsystemene og ASCII, under fagområdet digitalteknologi, går vi rett på en kort beskrivelse av hvordan nettverksmaskene fungerer og videre inn på TCP/IP i sin helhet.

Eksempel
Nettverksmasker begrenser nettverkskommunikasjonen. Datamaskin 1 kan kommunisere med datamaskin 2.
Datamaskin 1
IP- adresse: 192.168.1.2
Nettverksmaske: 255.255.255.0
Datamaskin 2
IP- adresse: 192.168.1.3
Nettverksmaske: 255.255.255.0

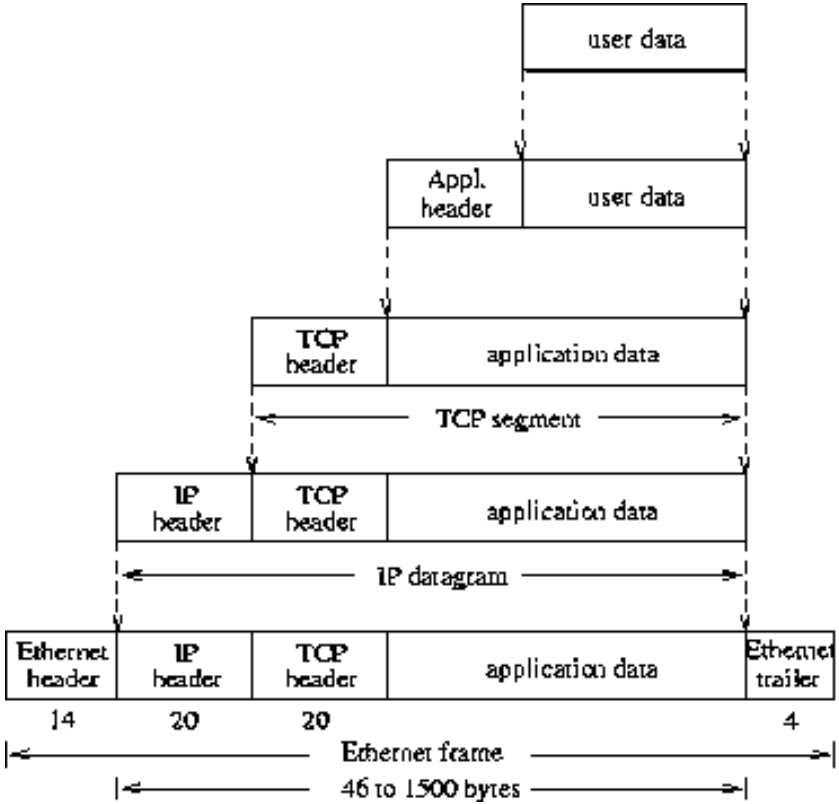
0 indikerer at det ikke er noen begrensning for kommunikasjon i denne **delen** av adressen.
I eksempelet ovenfor, kan vi kommunisere med alt som har en IP-adresse som begynner med 192.168.1.X.

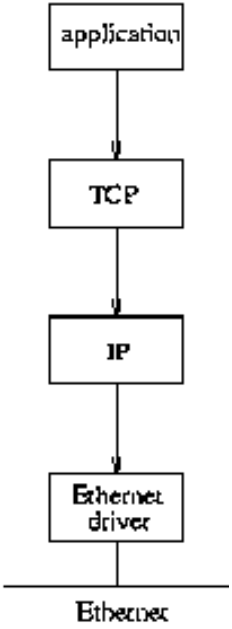
TCP/IP

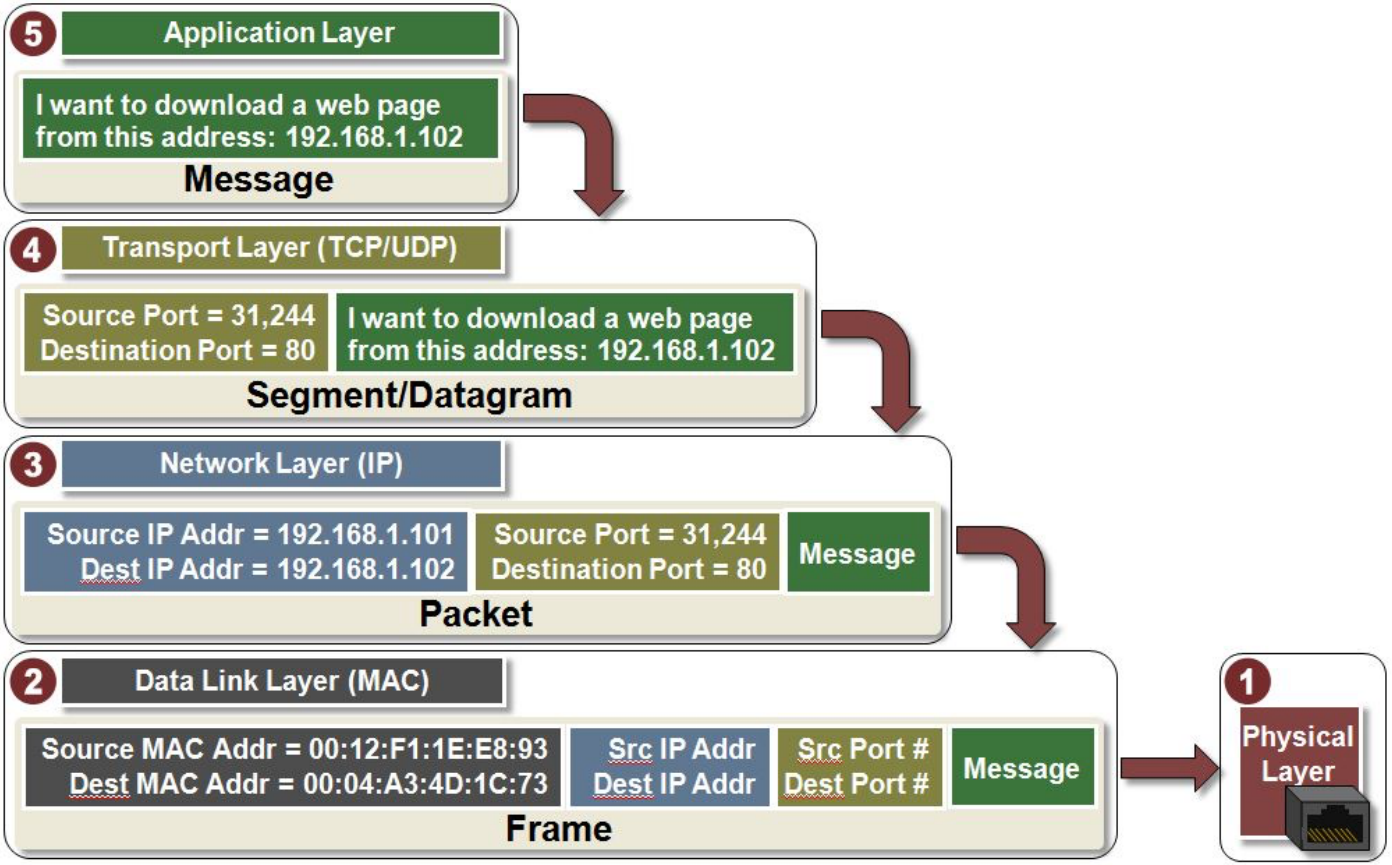
TCP/IP-modellen er bygget opp av fem nivåer (lag) og kalles ofte for femlagsmodellen mens OSI modellen er 7 lags. Hvert lag representerer en tjeneste eller protokoll som trengs for å kommunisere over et nettverk.



Hvert lag gjør en bestemt serie med oppgaver og kommuniserer bare med laget rett over og rett under. Når et program ønsker å sende data, sender denne informasjonen til tjenester og protokoller nedover i modellen. Hvert lag nedover legger til informasjon(header) til datapakken. Når pakken når det fysiske laget, sendes den over til mottakeren, og her går prosessen i revers oppover i modellen helt til programmet på den andre siden har mottatt dataene.


user data
Appl. header
user data
TCP header
application data
TCP segment
IP header
TCP header
application data
IP datagram
Ethernet header
IP header
TCP header
application data
Ethernet trailer
14
20
20
4
Ethernet frame
46 to 1500 bytes


application
TCP
IP
Ethernet driver
Ethernet


5
Application Layer
I want to download a web page from this address: 192.168.1.102
Message
4
Transport Layer (TCP/UDP)
Source Port = 31,244
Destination Port = 80
I want to download a web page from this address: 192.168.1.102
Segment/Datagram
3
Network Layer (IP)
Source IP Addr = 192.168.1.101
Dest IP Addr = 192.168.1.102
Source Port = 31,244
Destination Port = 80
Message
Packet
2
Data Link Layer (MAC)
Source MAC Addr = 00:12:F1:1E:E8:93
Dest MAC Addr = 00:04:A3:4D:1C:73
Src IP Addr
Dest IP Addr
Src Port #
Dest Port #
Message
Frame
1
Physical Layer

UDP vs TCP

TCP står for Transmission Control Protocol og UDP er en forkortelse for User Datagram Protocol. Dette er to ulike nettverksprotokoller som overfører data over internett fra din enhet til en nettserver. Du bruker enten en TCP protocol eller en UDP protocol når du skal snakke med venner på Skype, sende e-poster, se på videoer eller surfe på nettet.

Både UDP og TCP deler dataen din inn i mindre enheter som kalles for datapakker. Disse pakkene inkluderer også IP-en til både sender og mottaker, flere konfigurasjoner, dataen du sender samt dataen som indikerer slutten på pakken. Den eneste forskjellen på disse to nettverksprotokollene er måten datapakkene flyttes på.

Sammenligningstabell

Grunnlag for sammenligning	TCP	UDP
Betydning	TCP etablerer forbindelse mellom datamaskinene før overføring av data	UDP sender dataene direkte til destinasjonsdatamaskinen uten å sjekke om systemet er klar til å motta eller ikke
Utvider til	Transmisjonskontrollprotokoll	User Datagram Protocol
Tilkoblingstype	Forbindelse orientert	Tilkobling Mindre
Hastighet	Langsom	Rask
Pålitelighet	Svært pålitelig	upålitelig
Overskriftstørrelse	20 byte	8 byte
Bekreftelse	Det krever bekreftelse av data og har evnen til å bli overført, hvis brukeren ber om det.	Det krever heller ikke bekreftelse, og det overfører ikke de tapte dataene.

Dette er TCP

TCP IP er den mest bruke protokollen på nettet, og det skyldes ikke annet enn at den anses som den mest pålitelige av de to. TCP gir hver enkelt datapakke et unikt identifikasjons- og sekvensnummer. Dermed kan mottakeren identifisere hvilken pakke som ble mottatt og hvilken som er på vei.
Så snart datapakken er mottatt, og dersom den er i korrekt rekkefølge, sender mottakeren en bekreftelse til senderen. Dermed kan senderen sende ut en ny pakke. Det smarte med dette er at dersom pakken blir borte eller sendes i feil rekkefølge, vil mottakeren være stille. På den måten indikerer den at pakken må sendes på nytt.
Det at dataen sendes i rekkefølge bidrar til å forebygge overbelastning samtidig som det sørger for flytkontroll. Det bidrar også til at det blir lettere å oppdage og fikse eventuelle feil. Videre er det mer sannsynlig at data som sendes over TCP når destinasjonen sin. Imidlertid har den en ulempe. Det er mye kommunikasjon frem og tilbake mellom de to partene, så det tar lengre tid å etablere en forbindelse og utveksle data.

Dette er UDP

Nettverksprotokollen UDP fullfører den samme jobben uten behov for unike identifikatorer eller sekvensnumre. Den sender data i en jevn strøm og har bare én sjekk for å sikre at dataene ankommer uforstyrret. UDP har nesten ingen feilretting, og bryr seg heller ikke om pakker/meldinger som har gått tapt.
Denne protokollen er mer utsatt for feil, men den sender data mye raskere enn TCP.

DNS

DNS står for Domain Name System, og kan egentlig beskrives som adressebøker på internett. Alle nettsider har et domenenavn, for eksempel nrk.no eller vg.no. Det er dette du skriver inn i nettleseren din. Disse navnene blir så oversatt til IP-adressen den aktuelle siden du vil besøke har, og det er dette DNS som sørger for. En IP-adresse består av mange tall, og derfor er det lettere for folk flest å heller huske domenenavnet. DNS er dermed en veldig stor database, som befinner seg på en lang rekke servere. Typiske DNS servere er 1.1.1.1 og 8.8.8.8, sistnevnte er Google.

Hvordan finner jeg min DNS?

Du får internettet ditt levert av den internettleverandøren du har valgt, og det er også denne som sørger for din DNS. Om du lurer på hvordan finne DNS server, så er det fullt mulig å gå utenom internettleverandøren og velge en annen. Da bør du tenke over en rekke elementer før du bestemmer deg for hva du skal velge.

- Sørg for at DNS server Norge ikke logger din IP-adresse eller sporer hvor på nettet du har vært. Du må også velge et selskap som ikke selger din data videre til tredjeparter. For ekstra sikkerhet på nettet kan du bruke en sikker nettilgang. Dette gjør det fullt mulig å koble seg til en VPN i Norge.
- Hurtighet er et viktig element, så sørg for at den DNS-server du velger har den hurtigheten du trenger.
- nettkriminalitet av ulik art.

VPN står for «virtuelt privat nettverk» (på engelsk «Virtual private Network») – en tjeneste som krypterer internettrafikken og beskytter nettidentiteten din. Dette gjør den ved å sende IP adressen din gjennom en kryptert tunnel til VPN serveren, denne tunnelen skjuler hvem du egentlig er fra inntrengende tredjeparter, noe som er spesielt nyttig hvis du er tilkoblet offentlige nettverk. Med en VPN kan du få tilgang til apper, nettsteder og underholdningsplattformer fra hvor som helst i verden.

Forskjellige typer oppslag (DNS records) kan gjøres mot DNS. Forkortelsene under står for for, og hvilken type oppslag de brukes til?

A står for 'adresse', og dette er den mest grunnleggende typen DNS-post: den indikerer IP-adressen til et gitt domene. Hvis du for eksempel trekker DNS-postene for cloudflare.com, returnerer A-posten for øyeblikket IP-adressen: 104.17. 210.9. En post inneholder bare IPv4-adresser.

AAAA-poster ligner veldig på A-poster ved at de peker et domenenavn til en IP-adresse. Fangsten er at IP-adressen ikke er en vanlig IPv4-adresse som: 255.255. 255.0. I stedet peker AAAA-poster på IPv6-adresser som: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

CNAME en Canonical Name-post er en type ressurspost i Domain Name System som tilordner ett domenenavn til et annet. Dette kan være praktisk når du kjører flere tjenester fra en enkelt IP-adresse.

MX, en postvekslerrekord spesifiserer postserveren som er ansvarlig for å godta e-postmeldinger på vegne av et domenenavn. Det er en ressursregistrering i domenenavnsystemet. Det er mulig å konfigurere flere MX-poster, vanligvis peker på en rekke postservere for belastningsbalansering og redundans.

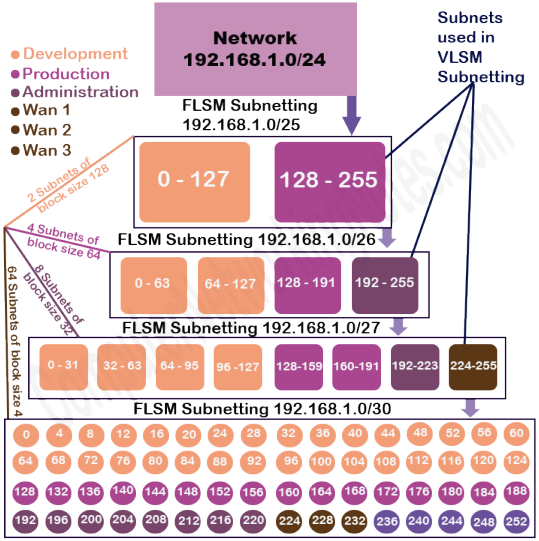
NS står for 'nameserver', og navneserverposten angir hvilken DNS-server som er autoritativ for det domenet (dvs. hvilken server som inneholder de faktiske DNS-postene). I utgangspunktet forteller NS-poster Internett hvor du skal gå for å finne ut domenets IP-adresse. Et domene har ofte flere NS-poster som kan angi primære navneservere og sikkerhetskopiservere for det domenet. Uten riktig konfigurerte NS-poster kan ikke brukere laste inn et webområde eller program.

LINK CLOUD FLARE

Subnetting

Et subnett eller subnett er en logisk underavdeling av et IP-nettverk. Praksisen med å dele et nettverk i to eller flere nettverk kalles subnetting. Datamaskiner som tilhører samme del -nett adresseres med en identisk mest betydelig bitgruppe i IP-adressene.

La oss se på et eksempel som nedenfor, man har behov for 4 subnett til eksempelvis regnskap, produksjon, administrasjon og drift.



Original networkID:
192.168.4.0/24

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

Network ID	Subnet Mask	Host ID Range	# of Usable Host	Broadcast ID
192.168.4.0	/26	192.168.4.1-192.168.4.62	62	192.168.4.63
192.168.4.64	/26	192.168.4.65-192.168.4.126	62	192.168.4.127
192.168.4.128	/26	192.168.4.129-192.168.4.190	62	192.168.4.191
192.168.4.192	/26		62	192.168.4.255

Klasseinndeling av nettverk

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 nettverk. 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

DHCP

Når PC-er, mobiltelefoner og andre enheter skal kobles til nettverk, må de ha en unik IP-adresse i nettverket. De trenger også informasjon om SUB nettmaske, Gateway og DNS-adresse for å kunne bruke internett. DHCP gir enhetene denne informasjonen automatisk.

DHCP (Dynamic Host Configuration Protocol) er en tjeneste som er satt opp i de fleste nettverk. Tjenesten gjør det mulig for enheter å koble seg til nettverket uten å være forhånds konfigurert med IP-adresse og informasjon om SUB nettmaske, Gateway og DNS-adresse. Vi kaller ofte dette å bruke dynamisk IP-adresse. Alternativet er å legge all slik informasjon inn på hver enhet manuelt. Det kalles statisk IP-adresse. I nettverk kan begge deler brukes. For eksempel har servere og nettverksutstyr ofte statisk IP-adresse.

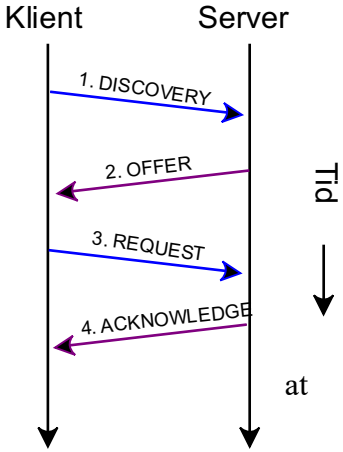
I små hjemmenettverk og mindre bedriftsnettverk er det ofte ruteren i nettverket som leverer DHCP-tjenesten. I større nettverk, spesielt nettverk med domenekontrollere, er DHCP-tjenesten tilordnet en egen server eller en egen tjeneste som kjører på en server.

1. Discovery

Maskinen som kobler seg til nettverket (klient), sender en Discovery-datapakke ut i nettverket. Pakken er adressert slik at den blir sendt til alle enheter i nettverket. Enheter som ikke er en DCHP-server, vil forkaste datapakken. DHCP-serveren vil ta imot den.

2. Offer

DHCP-serveren vil finne en ledig IP-adresse fra en intern tabell og sende denne og annen informasjon til klienten som en Offer-datapakke. For at pakken skal komme fram til riktig mottaker, bruker DHCP-serveren klientens MAC-adresse, som er en unik og permanent adresse hvert nettverkskort har.



3. Request

Klientmaskinen sender en ny datapakke ut i nettverket for å be om bekreftelse på at den skal bruke informasjonen den fikk i Offer-pakken. Denne mottar DHCP-serveren.

4. Acknowledge

DHCP-serveren bekrefter adressen ved å sende den på nytt til klienten med en Acknowledge-datapakke. Når klienten mottar informasjonen, vil den bruke den til å kunne fungere i nettverket og få internett-tilgang.

Vanlig informasjon DHCP-servere gir til klienter

- **IP-adresse** som klienten skal bruke. Denne adressen er unik i nettverket.
- **SUB nettmasken** til nettverket. Den forteller klienten hvilke IP-adresser som er innenfor det lokale nettverket, og hvilke som bare kan nås gjennom ruteren.
- **Gateway** er adressen til ruteren i nettverket. Ruteren kobler sammen nettverk, for eksempel for å få tilgang til internett.
- **DNS-adresse** forteller klienten hvor den skal spørre hvis den skal gjøre DNS-oppslag.
- **DHCP-leasetime** forteller klienten hvor lenge den kan ha IP-adressen før den må be om fornyelse. Hensikten er å frigjøre IP-adresser som ikke har vært i bruk på en stund.
- **DHCP-serverens IP-adresse**. Dette er nyttig informasjon for feilsøking.

Link til DHCP 01

Link til DHCP 02

Domenekontrollere

PC-er, skrivere og annet datautstyr i bedrifter er oftest underlagt en domenekontroller. Domenekontrolleren gjør det lettere for de IT-ansvarlige å administrere utstyret og ivareta IT-sikkerheten.

Begrepet domene er oversatt fra det engelske ordet *domain* og det franske ordet *domaine*. Opphavet er imidlertid latin, der ordet betydde herredømme og ble brukt om et område der noen hadde eierskap og kontroll. Begrepet brukes på forskjellige fagområder, men meningen er nokså lik. (NDLA)

Hvorfor bruker vi domenekontrollere?

Domenekontrollere er til stor hjelp for de IT-ansvarlige i bedrifter. La oss ta et eksempel: Det skal installeres ny programvare på jobbdatamaskinene til alle ansatte. I stedet for å installere programvaren manuelt på hver enkelt maskin, kan prosessen styres fra ett sted via domenekontrolleren. Et annet eksempel: En bedrift ansetter en ny person. I stedet for å opprette en bruker på hver enkelt datamaskin som den nyansatte kan komme til å bruke, kan man opprette brukeren i domenekontrolleren, slik at den nyansatte kan benytte den samme påloggingsinformasjonen på alle maskinene i bedriften – eller de maskinene som de IT-ansvarlige ønsker at den nyansatte skal ha tilgang til. Når en person slutter, kan vedkommendes bruker slettes fra registeret i domenekontrolleren. Det gjør at personen mister tilgangen til å logge seg på maskinene i bedriften. Samlet gir dette god mulighet for å administrere utstyr, og det øker i tillegg sikkerheten.

Fordi domenekontrollere fratar vanlige brukere mange av styringsmulighetene på egen maskin, kan det oppstå misnøye og problemer. Tenk deg for eksempel at en ansatt trenger å installere spesialprogramvare, men ikke lenger har rettighetene som trengs for å gjøre det. Det kan den ansatte oppleve som frustrerende. Det er derfor viktig å finne en balanse mellom å ha kontroll over utstyret og å gi de ansatte den friheten de trenger.

Hva er en domenekontroller?

En domenekontroll (DM) refererer til et Microsoft Windows®-basert datasystem som lagrer brukerkontodata for det tildelte domenet i en sentral database. Den bruker disse lagrede dataene for å tilby viktige domenetegnede tjenester, for eksempel:

- Brukerautentisering
- håndheving av sikkerhetspolitikk
- tilgang til ressurser

I hovedsak tillater en domenekontroller en systemadministrator å gi enhver spesifikk bruker tilgang til visse systemomfattende ressurser - applikasjoner, skrivere - via et brukernavn og passord.

Den første DM ble implementert på Windows® NT via en database kjent som Security Accounts Manager (SAM). Dette systemet er avhengig av en primær domenekontroller (PDC) kombinert med en eller flere sikkerhetskopidomenekontrollere (BDC). PDC håndterer alle domenerelaterte problemer, for eksempel brukergodkjenning, mens de skrive beskyttede PDC-ene fungerer som sikkerhetskopier for forbedret feiltoleranse. I tilfelle PDC mislykkes, må en av BDC-ene konfigureres om til en PDC.

Problemet med Windows® NT-domenekontrollermodellen er at den ikke er skalerbar, noe som betyr at den bare kan brukes til småbedrifter. For å bedre dette erstattet Microsoft SAM, PDC og BDC med Active Directory (AD). Denne teknologien gjør nettverket til en stor katalog, liksom de gule sidene, som er mye enklere å administrere og kontrollere.

Enda viktigere er at Active Directory-systemet lar flere domener fungere på et likt nivå. Hver domenekontroller har en kopi av AD-databasen. Videre forblir alle DC-er på domenet kontinuerlig synkronisert med en prosess kjent som Multi master replikasjon. I denne prosessen, når informasjon om en DC endres, sendes et signal til alle de andre DC-ene, og sikrer dermed all informasjon forblir oppdatert og korrekt. Det kan imidlertid være viktig å merke seg at en fungerer som master, ved at den er ansvarlig for å bekrefte alle datamodifiseringer og løse eventuelle konflikter som kan oppstå når det samtidig fremsettes forespørsler om dataendring. I tilfelle denne lederen mislykkes, overtar en annen DC straks rollen.

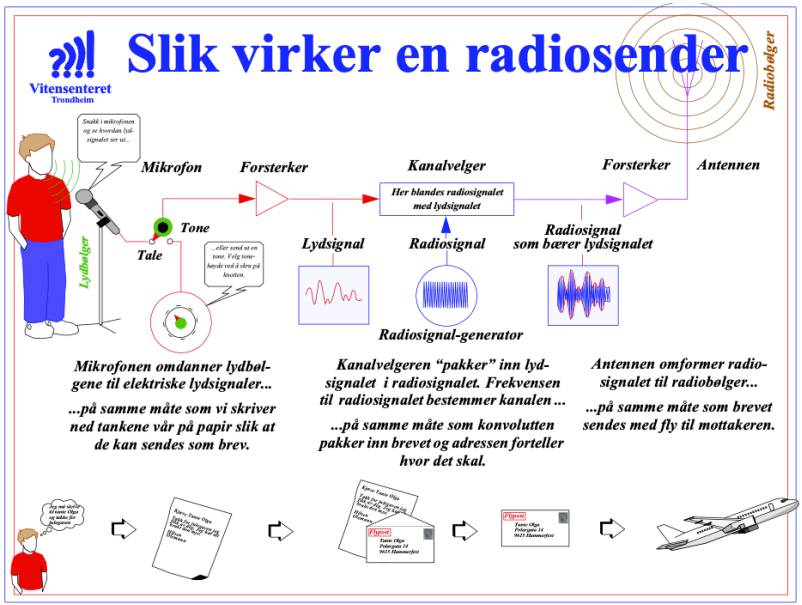
Det er imidlertid en hoved begrensning for Active Directory-systemet. Domenekontrolleren må tydelig være vert for et Windows®-basert operativsystem, noe som derfor betyr at alle andre domenemedlemmer eller arbeidsstasjoner også må bruke Windows®.

Dette ble løst ved innføringen av Samba, en åpen kildekode / gratis programvarepakke som lar arbeidsstasjoner med andre operativsystemer - for eksempel UNIX, Linux, IBM System 390 og OpenVMS - kommunisere med domenekontrolleren. Dette gir en nettverksadministrator eller ingeniør mye mer fleksibilitet. Det er spesielt nyttig i store selskaper der forskjellige avdelinger krever forskjellige operativsystemer.

Radiosignaler

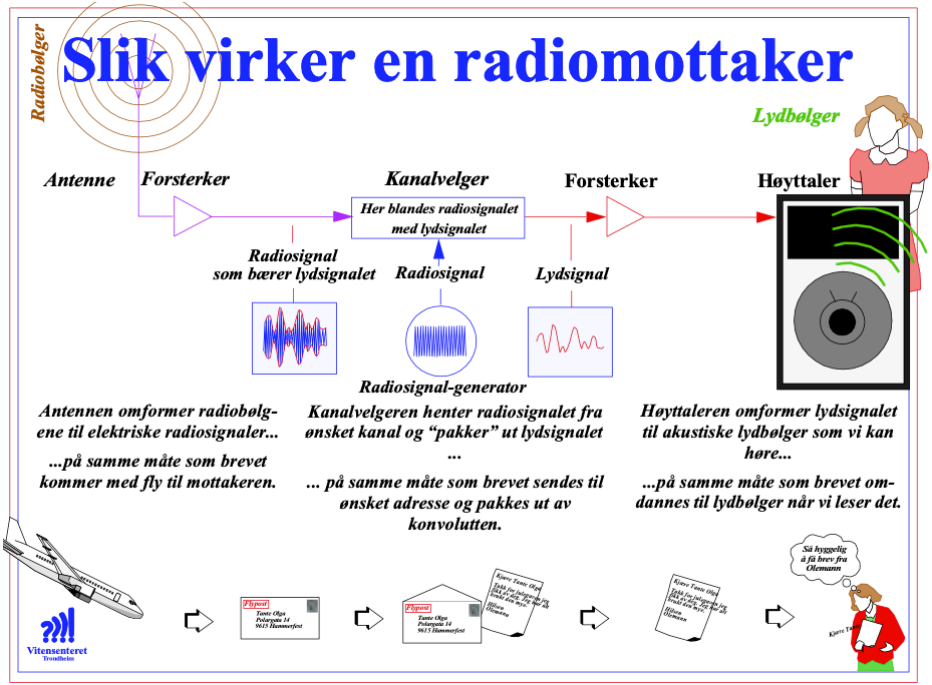
Radiosignaler er elektromagnetiske bølger som vi modulerer (forandrer), slik at de kan formidle informasjon trådløst. Denne illustrasjonen gir et kort innblikk i hva radiosignaler er og hvordan de brukes til overføring av informasjon.

Radiosender, her ser du hvordan lyden først omdannes til lydbølger når du snakker eller synger. Disse lydbølgene gjøres om til elektrisk spenninger som varierer i takt med stemmen vår ved hjelp av mikrofonen. Dernest blir det elektriske tale- signalet flyttet opp til riktig radiokanal ved hjelp av kanalvelgeren, for å sendes ut til antennen som gjør om radiosignal- et til radiobølger som kan bre seg gjennom tomt rom.



Radiomottakeren virker omtrent omvendt av radiosenderen.

Antennen "fanger" opp radiobølgene og omdanner disse til et elektrisk radiosignal. Kanalvelgeren velger ut den kanalen eller den frekvensen vi ønsker å høre på, og tilslutt omdanner høyttaleren det elektriske lydsignalet til lydbølger som øret vårt kan høre.



SNL, radioteknologi

Oppgaver

- Beskriv de ulike tallsystemene og deres oppbygging og hvor/hvordan de benyttes i datateknisk sammenheng
- Hva er ASCII, og hvordan er forholdet mellom binærsystemet og ASCII kodene, vis eksempler
- Hva står TCP/IP for og hvilke oppgaver har disse funksjonene
- Hvilket lag arbeider TCP/IP på?
- Hvilke tjenester kan man finne i TCP/IP nettverk
- Hva står UDP og DNS for, og hva er deres oppgave/oppgaver i nettverket
- Hva er forskjellen på de 5 IP adresseformatene?
- Hvis du har 29 bit til nettadressen, hvor mange bit er igjen til node adressen?
- Hvor mange maskiner er det plass til på et slikt nett?
- 10.0.0.1/21, hva blir nettmasken desimalt og hva blir antall noder?
- Hva blir nettmasken til denne binære desimaltall rekken?
    - 11111111 . 11111111 . 11111111 . 00000000
- Hva står DHCP for og hvordan virker DHCP?
- Hvordan vet du om du bruker DHCP?
- Hvilke fordeler er det ved å bruke DHCP?
- Hvilke sikkerhetsangrep er vanlige på DHCP?
- Hva er en domenekontroller DC og hva er AD
- Hva er et radiosignal
- Hvordan fungerer en radiosender og mottaker?

Link til dypdykk i TCP/IP Link til Ipv4 og nettmasker fordypning

Link til delmål 2, bli kjent med svitsjen

Kompetansemål

- beskrive, utforske og konfigurere datanettverk med egne subnett
- gjøre rede for hvordan internett fungerer, og hvordan det blir brukt til kommunikasjon og lagring

Har du forstått?

Kan du svare ja på alle spørsmålene nedenfor, har du god greie på hva digital teknologi er.

_____ Jeg kan de ulike tallsystemene og hvordan de benyttes i en datamaskin

_____ Jeg kan forklare hva ASCII koder er

_____ Jeg vet hva TCP/IP står for og hvordan disse fungerer og på hvilke lag de arbeider

_____ Jeg vet hvilke tjenester man finner på TCP/IP nettverk

_____ Jeg kan forklare UDP og DNS og forskjellen mellom TCP og UDP

_____ Jeg kjenner de 5 IP formatene

_____ Jeg kan forhold mellom nettadresse og node adresser

_____ Jeg kan regne meg frem til nett og node adresser

_____ Jeg kan forklare DHCP funksjon og virkemåte

_____ Jeg vet forskjell på DC(Domenekontroller) og AD (Activ Directory)

_____ Jeg kan forklare hva et radiosignal er og hvordan sender og mottaker fungerer