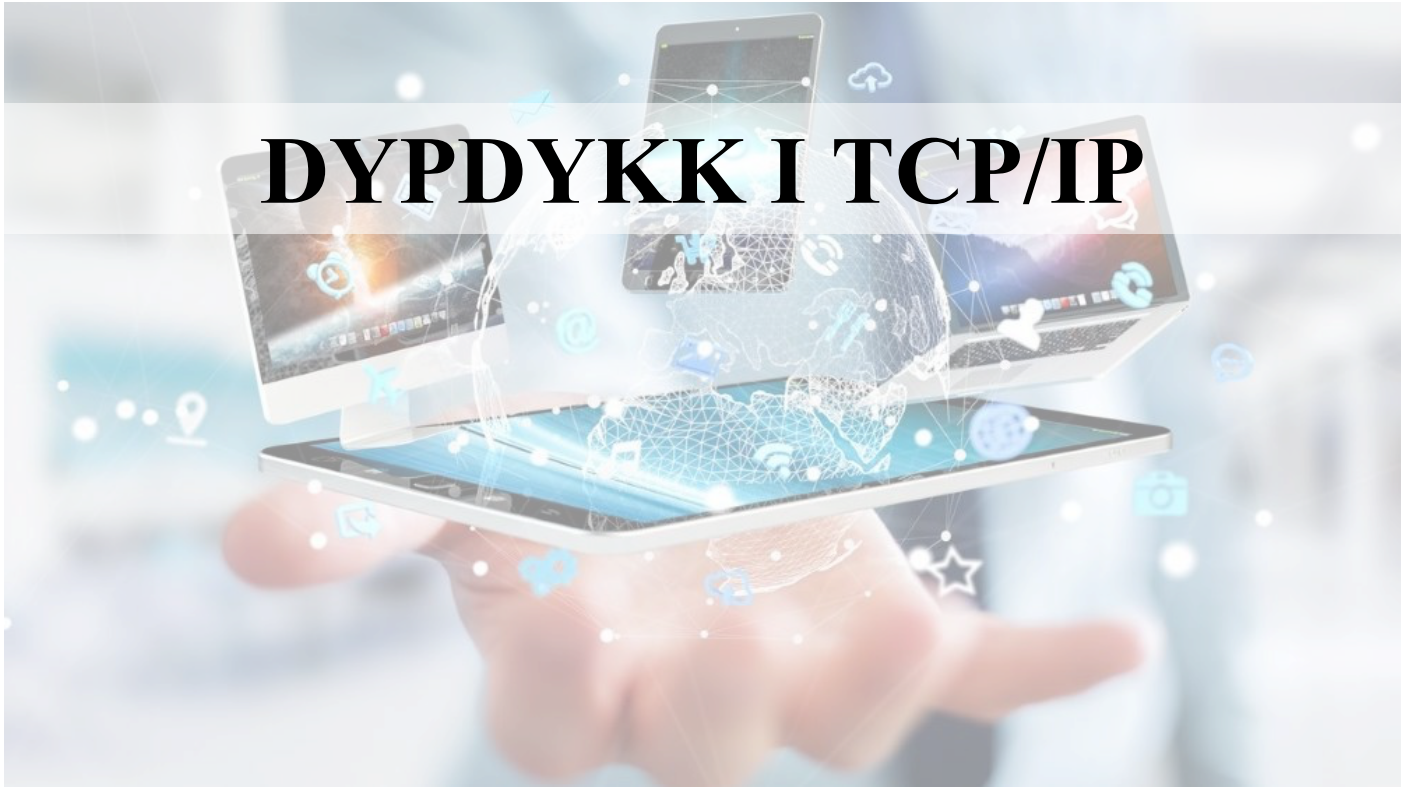
DYPDYKK I TCP/IP



Innholdsfortegnelse

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.

How TCP/IP Works

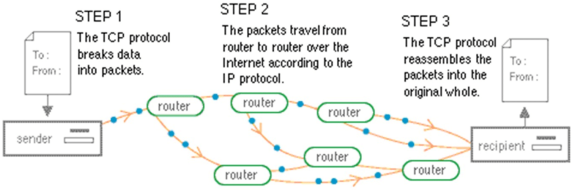


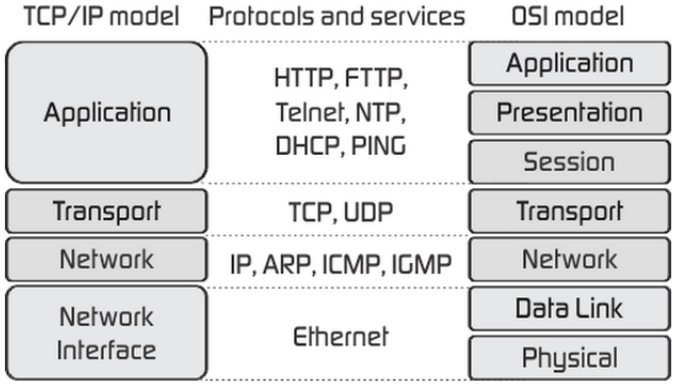
Figure 2. How data travels over the Net.

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 i dag 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.

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 dine nettsider).

Det finnes i dag en lang rekke ulike protokoller som alle har sine egne unike spesifikasjoner, 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 "connection less" broadcast: 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.

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 parameter som sekvensnummer bli initialere for å oppnå riktig rekkefølge på pakkene og robusthet.

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 kilde porter 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.

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."

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 4 milliarder unike tall. Dette er den største begrensningen på Internett i dag, 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.

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

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 epostservere, 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 over klassifiserte 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

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 SUB nettmasken. 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.

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 adresse kan enkelt representere klassiske adresser (klasse A = / 8, klasse B = / 16 og klasse C = / 24). Tallet ved siden av skråstreken (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.

MAC-adresse

MAC, **M**edia **A**ccess **Control** 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**. 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.

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" (systemvalg)og deretter velge "Network".