

# Notater: INF1060 - Datakommunikasjon

Veronika Heimsbakk  
veronahe@student.matnat.uio.no

9. januar 2013

## Innhold

<b>1</b>	<b>Internet</b>	<b>3</b>
1.1	Pakkesvitsjing . . . . .	3
1.2	Linjesvitsjing . . . . .	3
1.3	Lagdelte Kommunikasjonsmodeller . . . . .	4
<b>2</b>	<b>Transportlaget</b>	<b>4</b>
2.1	Adressering . . . . .	5
2.2	Pålitlig og upålitlig kommunikasjon . . . . .	5
2.3	Forbindelsesorientert og forbindelsesløs kommunikasjon . . . . .	5
2.4	Glidende vindu . . . . .	6
2.5	Pålitlig dataoverføring med TCP . . . . .	6
2.5.1	TCP pakkeformat . . . . .	6
<b>3</b>	<b>Nettverkslaget</b>	<b>8</b>
3.1	Ulike typer nettverk . . . . .	8
3.2	IP-adresser . . . . .	9
3.3	Nettadresser . . . . .	9
3.3.1	Nettmasker . . . . .	9
3.4	Reserverte IP-adresser . . . . .	9
3.5	IP-protokollen . . . . .	10
<b>4</b>	<b>Lenkelaget og det fysiske laget</b>	<b>11</b>
4.1	Lenkelaget . . . . .	11
4.1.1	Praktisk håndtering av arbeidsoppgavene på lenkelaget	11
4.2	Konstruksjon av nettverk . . . . .	12
4.2.1	Eksklusiv og delt tilgang . . . . .	12
4.2.2	Full dupleks-, halv dupleks-, og simpleksforbindelser .	12
4.2.3	Punkt-til-punkt og multipunkt . . . . .	12
4.3	Det fysiske laget . . . . .	13
4.3.1	Praktisk håndtering av arbeidsoppgavene på det fysiske laget . . . . .	13

4.3.2	Medier . . . . .	13
-------	------------------	----

# 1 Internet

**Internett** Er navnet på et bestemt datanettverk som egentlig er en sammenkopling av mange nettverk. Internett bruker en bestemt protokollfamilie for datakommunikasjon, TCP/IP. Poenget med Internett er å kunne kommunisere mellom program som kjøres på ulike maskiner.

**Internetts infrastruktur** Dette innebærer nettverk og utstyr. Internett består av kjernenett og kantnett, og endeutstyret er i kantnettet. I kjernenettet er det kraftige rutere som formidler trafikken. Kommunikasjonslinjer knytter utstyret sammen, og forbindelsene varierer fra vanlige kobberlinjer til fiberkabler.

**Internetts tjenester** To av de mest populære anvendelsene av Internett er e-post og web. Felles for alle anvendelsene er at det er applikasjoner som kommuniserer med hverandre over Internett.

**Internetts roller** Tilkopling til Internett skjer gjennom en Internet Service Provider (ISP), en tjenesteleverandør.

**Internetts trafikk** Datatrafikken på Internett er basert på pakkesvitsjing. Det betyr at data samles i blokker og sendes hver for seg. Pakken får en merkelapp som kalles pakkeheader. Den viktigste informasjonen i en pakkeheader er sender- og mottakeradresse.

## 1.1 Pakkesvitsjing

Dette kjennetegnes ved at mange brukere deler på overføringskapasiteten i nettverket. Det er ikke mulig å foreta reservasjoner av kapasitet, man deler på den som til enhver tid er ledig. Kommunikasjonen mellom avsender og mottaker foregår her ved hjelp av pakker. Vi skiller mellom to typer pakkesvitsjende nettverk: datagramnettverk og virtuelt-kanal-nettverk.

Internett er et eksempel på pakkesvitsjing.

## 1.2 Linjesvitsjing

Dette kjennetegnes ved at en forbindelse må koples opp før vi kan begynne å overføre data. Denne linjen koples opp mellom avsender og mottaker og er oppkoblet så lenge kommunikasjonen varer. Fordelen med en slik svitsjetechnik er at vi får en dedikert transmisjonkanal der vi disponerer hele kapasiteten, og det oppstår små eller ingen forsinkelser.

Telefonnettet er et eksempel på linjesvitsjing.

### 1.3 Lagdelte Kommunikasjonsmodeller

OSI	Forenklet OSI	TCP/IP
Applikasjon	Applikasjon	Applikasjon
Presentasjon		
Sesjon	Transport	Transport
Transport		
Nettverk	Nettverk	Nettverk
Lenke	Lenke	
Fysisk	Fysisk	

Tabell 1: OSI-modellen og TCP/IP-protokollfamilien.

**Applikasjonslaget** Er grensesnittet mellom programmene som en maskin og kommunikasjonsdetaljene i de lavere lagene. Implementerer protokoller som FTP, HTTP etc.

**Sesjonslaget** Legger til konseptet av sesjoner (sessions). Applikasjoner og endesystemer setter opp en sesjon (kobler seg til hverandre).

**Presentasjonslaget** Oversetter data som utleveres, slik at det kan brukes i forskjellige strukturer. Eks. big endian til little endian kode.

**Transportlaget** Har ansvar for ende-til-ende kommunikasjonen og sørger for at data utveksles.

**Nettverklaget** Sier ifra til systemet at de er koblet til nettverket, og føre dataene fram over nettverket til riktig mottaker.

**Lenkelaget** Fører data mellom to maskiner som er koblet direkte sammen.

**Fysisklag** Omhandler overføring av fysiske signaler. Signalene er en bitstrøm av 0 og 1.

## 2 Transportlaget

Transportslagets oppgave er å overføre data mellom applikasjoner som om de var direkte sammenkople. Transportlaget tilbyr en logisk ende-til-ende forbindelse mellom program som kjører på forskjellige maskiner. Typiske protokoller: UDP og TCP.

## 2.1 Adressering

Det første kravet man stiller til en pakke, er at den er adressert. Transportlaget er koplet til applikasjonslaget gjennom adressbare *porter*. Mottakerens og avsenderens portnummer må være oppgitt.

- Velkjente portnummer: Vanlige protokoller benytter faste porter (0 til 1023).
- Kortlivede portnummer: Opprettes etter behov (1024 til 65535).

Eksempel på velkjente portnummer:

- Webtjeneren lytter på port 80 (HTTP).
- E-posttjeneren lytter på port 25 (SMTP).
- Navnetjeneren lytter på port 53 (DNS).

Når klientapplikasjonen overlater en melding til transportlaget, skjer det gjennom en port som ble opprettet da klientprogrammet startet. Når klientapplikasjonen avsluttes, blir det kortlivede portnummeret frigjort og kan brukes på nytt av en annen applikasjon.

## 2.2 Pålitlig og upålitlig kommunikasjon

**Pålitlig kommunikasjon** Betyr data som kommer frem, er korrekte og i rett rekkefølge; man får en transparent forbindelse, hvor det som blir sent ut på den ene siden, er nøyaktig likt det som kommer inn på den andre. Dette er ikke det samme som *sikker* overføring, hvilket krever kryptering i tillegg.

For å oppnå pålitlig kommunikasjon kreves *kvittering*, tilbakemelding på at data er mottatt. Avsender må få vite noe om hvordan overføringen gikk. For å kunne få kvittering på sendte data forutsettes det at man har en *forbindelsesorientert kommunikasjon*, og at de to kommuniserende partene holder oversikt over hva som er sendt og kvittert for.

**Upålitlig kommunikasjon** Dette er et varsel til brukeren av protokollen om at det kan oppstå feil i overføringen, og at det ikke blir gjort tiltak for å rette på disse. Det er da opp til brukeren å avgjøre om dette er tilstrekkelig, eller om det må benyttes kontrolltiltak.

## 2.3 Forbindelsesorientert og forbindelsesløs kommunikasjon

- **Forbindelsesløs kommunikasjon:** Datapakken sendes uten at man vet om mottaker finnes og er klar til å ta imot data. Det gis ingen kvittering på mottatte data.

- **Forbindelsesorientert kommunikasjon:** Denne etablerer først en forbindelse mellom de to partene. Så kan data overføres. Til slutt koples forbindelsen ned.

Forbindelsesløs kommunikasjon er mer avansert enn den forbindelsesløse. For det første må partene holde rede på hvilken tilstand eller overgangsfase de er i. For det andre trengs det flere felter i pakkeheader med informasjon om overføringen, og det må settes av bufferplass. Så det å tilby en pålitlig overføringstjeneste koster i form av kompleksitet og linjekapasitet. TCP er et eksempel på en protokoll som sørger for at feilaktige eller manglende data sendes på nytt.

## 2.4 Glidende vindu

Glidende vindu er betegnelsen på en metode som regulerer hvor mye data man kan sende før man får kvitteringen tilbake.

Rundetiden (Round Trip Time(RTT)) er tiden det tar fra en pakke er sendt til den er kvittert for. Tiden det tar å sende en pakke, er pakkelengde delt på hastighet.

## 2.5 Pålitlig dataoverføring med TCP

I TCP/IP-protokollfamilien er det TCP som tilbyr pålitelig overføring. TCP er alltid ende-til-ende forbindelse mellom sender og mottaker; mellomliggende utstyr er uvitende om hva det er som sendes frem og tilbake.

### 2.5.1 TCP pakkeformat

En TCP-pakke kalles for et segment og består av et pakkehode og eventuell nyttelast.

Avsenders port (16 bit)		Mottakers port (16 bit)	
Sekvensnummer			
Kvitteringsnummer			
Lengde (4 bit)	Ubrukt (6 bit)	Flagg	Vindu (16 bit)
Sjekksum (16 bit)	Viktig peker (16 bit)		
Tilleggsinformasjon (n * 32 bit)			
– Nyttelast –			

Tabell 2: Formatet på TCP-segment.

**Avsenders port** Dette feltet identifiserer portnummeret til avsenderapplikasjonen.

**Mottakers port** Dette feltet identifiserer portnummeret til mottakerapplikasjonen.

**Sekvensnummer** Her finner vi sekvensnummeret til første databyte i nyttelasten. Når en ny TCP-forbindelse blir etablert, velger TCP en tilfeldig startverdi, Initial Sequence Number (ISN). Fra denne verdien øker sekvensnummeret med 1 for hver overført byte, opp til verdien  $2^{32} - 1$ . Deretter starter tellingen fra 0 igjen.

**Kvitteringsnummer** Her finner vi kvitteringsnummeret. Nummeret som blir brukt, er sekvensnummeret som mottakeren ønsker å motta i neste segment. Dette nummeret virker som en bekreftelse på at alle oktetter i datastrømmen frem til hit er korrekt mottatt.

**Lengde** Feltet forteller oss lengden på en TCP-pakkeheader inkludert opsjonsfeltet, uttrykt som antall 32-bit ord. Feltet er nødvendig fordi opsjonsfeltet kan variere i størrelse.

**Ubrukt** Dette feltet på 6 bit er reservert for fremtidig bruk. Ikke tatt i bruk ennå.

**Flagg** Feltet inneholder 6 bit, som representerer seks ulike flagg. Dersom en bit har verdien 1, sier vi at flagget er satt. Flaggene har følgende betydning:

1. URG (*Urgent*): Pakken inneholder informasjon i viktig peker-feltet.
2. ACK (*Acknowledgement*): Pakken inneholder informasjon i kvitteringsfeltet.
3. PSH (*Push*): TCP blir tvunget til å vidreformidle data straks.
4. RST (*Reset*): Varsler at port ikke (lenger) er i bruk.
5. SYN (*Synchronize*): Pakken inneholder informasjon i synkroniseringsfeltet.
6. FIN (*Finish*): Brukes når man avslutter og kopler ned en forbindelse.

**Vindu** Feltet brukes til flytkontroll og forteller hvor mye data avsender av pakken er i stand til å ta imot for øyeblikket, altså et uttrykk for ledig bufferkapasitet.

**Sjekksum** Sjekksummen brukes for bitfeildeteksjon. Den beregnes ved å summere pakkeheader, nyttelast og noe informasjon fra nettverkslaget (avsenders og mottakers IP, protokolltype og segmentlengde).

**Viktig peker** Feltet inneholder bare relevant informasjon dersom URG-flagget er satt. Summen av viktig peker og sekvensnummer peker på siste byte av prioriterte data.

**Tilleggsinformasjon** Tilleggsinformasjon brukes mest i forbindelse med oppkopling av forbindelse. En vanlig parameter som brukes er Maximum Segment Size (MSS).

**Nyttelast** Dette er data fra applikasjonslaget. Feltet er tomt i oppkopplings- og nedkopplingssegmenter samt i rene kvitteringssegmenter.

### 3 Nettverkslaget

Nettverkslagets oppgave er å overføre datapakker mellom maskiner hvor applikasjonene kjører. Typisk protokoll: IP.

#### 3.1 Ulike typer nettverk

**Tjenestenett** Nettverk kan kategoriseres i forhold til de tradisjonelle tjenestene som mobiltelefoni, fasttelefoni, datakommunikasjon og kringkastingsnett for TV. Det er på gang en konvergens, som betyr at flere tjenester kan tilbys på samme infrastruktur.

**Logiske nett og fysiske nett** I vår sammenheng brukes disse begrepene for å skille mellom nettverk på nettverkslaget og lenkelaget. På nettverkslaget har man IP-nett, og hver maskin har sin IP-adresse. IP-adresser er logiske adresser, og et IP-nett er et logisk nett. Lenkelaget omhandler nettverkskort og kommunikasjonslinjer som kopler utstyret sammen. Nettverkskort bruker MAC-adresser, og disse kalles for fysiske adresser.

**IP-nett** Et IP-nett er et logisk nett som hører hjemme på nettverkslaget. Sammenkoplingen av IP-nett skjer alltid ved hjelp av rutere. En ruter har alltid minst to utganger, og hver av disse utgangene har IP-adresser som hører hjemme i hvert sitt IP-nett. En ruter stopper kringkastingspakker.

**Lokalnett, LAN** Et lokalnett er en fysisk nettstruktur som hører hjemme på lenkelaget. Vi bruker lokalnett som et samlebegrep på det kommunikasjonsutstyret en virksomhet rår over. Et lokalnett kan gjerne inneholde flere logiske IP-nett. Lokalnettet kan være bygd opp av flere typer teknologier, for eksempel trådløs og kablet teknologi.



**Virtuelle nett** Denne betegnelsen brukes i to sammenhenger: virtuelle lokalnett (VLAN) og virtuelle privatnett (VPN). VLAN er en teknikk for å separere enheter på samme lokalnett slik at de tilhører forskjellige IP-nett. VPN er en teknikk for sammenkopling av bedriftsinterne IP-nett som er geografisk adskilte. VPN bruker kryptert overføring.

**Hjemmenett, bedriftsnett, Internett** Hjemmenett er vanligvis et IP-nett som deler en felles IP mot Internett. Bedriftsnett består av flere IP-nett, og hver maskin kan ha sin egen IP. Internett er navnet på det store internettverket hvor hundretusenvis av IP-nett er koplet sammen.

**Andre nettverksbegrep** *Subnet* er en betegnelse som henger igjen fra tidligere tider, da nettadressene var klassedelte. En virksomhet fikk tildelt en nettadresse som igjen kunne deles opp i subnett ved hjelp av subnettmasken. *Intranett* har blitt betegnelsen på bruk av web internt i bedriften, tjenesteportaler som ikke er åpent fra Internett. Intranett er derfor ikke et nett, men en tjeneste.

### 3.2 IP-adresser

IP-adressen er på 32 bit i IPv4. Det betyr at det finnes  $2^{32}$  mulige kombinasjoner, som gir omlag 4 milliarder IP-adresser. IPv4 har ikke tilstrekkelig med adresser, derfor er IPv6 nylig innført. IPv6 har 128 bit adressefelt.

### 3.3 Nettadresser

De hundretusenvis av IP-nettene i Internett har hver sin unike nettadresse. Rutene på Internett ser bare på nettadressen når IP-pakker skal videresendes, og overlater til siste ruter å sørge for at IP-pakken kommer til rett maskin.

IP-adressen består av to deler, en nettadresse (nett-id) og en nodeadresse (host-id). Man kan ikke se på IP-adressen hva som er hva.

#### 3.3.1 Nettmasker

Det er nettmasken som forteller hvor skillet i IP-adressen går mellom nettadresse og nodeadresse. Nettmasken viser hvor mange bit, regnet fra venstre i IP-adresse, som inngår i nettadressen. Jo flere bit som brukes i nettadressen, desto færre bit blir det igjen til nodeadresser i dette IP-nettet. Summen av nett- og node-adresse er alltid 32 bit. Hver eneste maskintilkopling på Internett må kjenne sin egen nettmask.

### 3.4 Reserverte IP-adresser

Følgende IP-adresser er reservert til privat bruk:

- 10.0.0.0–10.255.255.255
- 172.16.0.0–172.31.255.255
- 192.168.0.0–192.168.255.255

### 3.5 IP-protokollen

Beskrivelse av IPv4.

**Versjonsnummer** Feltet spesifiserer versjonen av IP-protokollen. Vi skiller mellom IPv4 og IPv6, som har ulikt format på sine IP-pakker.

**Headerlengde** Feltet forteller hvor mange 32-bits grupper som er i pakkeheader, medregnet tilleggsinformasjonsfelt (som kan variere). Innholdet i feltet brukes til å bestemme hvor nyttelastdelen av IP-pakken begynner.

**Type of Service – TOS** Feltet skiller mellom ulike typer IP-pakker. Feltet består av 3 bit precedence-felt (ubrukt), 4 bit TOS og 1 bit som må være 0. TOS-bitene er flagg for å skille mellom tjenestekvalitetene: minimere forsinkelse, maksimere gjennomstrømming, maksimere pålitelighet, minimere kostnader.

**Totallengde** Inneholder lengden til hele IP-pakken i byte. Kombinert med feltet headerlengde kan lengden og starten på nyttelastfeltet regnes ut. Feltet er på 16 bit, så store IP-pakker sendes vanligvis ikke.

**Identifikasjon, flagg og fragmentering** Alle disse tre feltene brukes i forbindelse med fragmentering av IP-pakker. Identifikasjon inneholder en entydig ID for hver IP-pakke. Flagg brukes for å fortelle at pakkene er fragmentert, og når siste IP-pakkefragment kommer. Fragmentering identifiserer hvert enkelt pakkefragment.

**Time to live – TTL** Dette feltet inneholder et maksimumstall for hvor mange ruter som IP-pakken kan passere. Hver ruter som IP-pakken passerer, dekrementerer feltet. Dersom feltet når 0 i en ruter, returnerer ruterens en ICMP-feilmelding til senderen.

**Protokoll** Inneholder en kodeverdi som forteller hvilken protokoll nyttelasten i IP-pakken bruker. Feltet benyttes bare hos mottaker og ikke hos de mellomliggende ruterne.

**Headersjekksum** Inneholder en sjekksum som er kalkulert på bakgrunn av de ulike feltene i en IP-pakkeheader. Siden IP ikke kan detektere bitfeil i datafeltet, må eventuell feilkontroll overlates til lag lenger opp. Formålet med kontrollen er først og fremst å stanse pakker med feil i IP-adressene.

**Avsenders IP-adresse** Inneholder IP-adressen til mottakeren av IP-pakken.

**Tilleggsinformasjon** Her kan det legges inn flere ulike tilleggstjenester. Feltet er lite benyttet.

**Nyttelast** Her legger vi inn de dataene vi ønsker å overføre til mottakeren. Dette feltet har for eksempel for Ethernet vanligvis en størrelse på cirka 1460 byte.

## 4 Lenkelaget og det fysiske laget

### 4.1 Lenkelaget

Ansvarer til lenkelaget er å overføre pakker mellom nettverkslagene på tilstøtende noder. Dette innebærer å klargjøre pakker, gjennom innramming og andre mekanismer, slik at innholdet kan overføres på det fysiske laget. Eksempler på protokoller er Ethernet, LAN, trådløst lokalnettverk og WLAN.

Lenkelaget rammer inn IP-pakkene med nødvendige felter for den aktuelle nettverksteknologien. Innrammingen inkludere typisk å påføre avsender- og mottakeradresser, sjekksum og et felt for beskrivelse av nyttelasten.

På lenkelaget finner vi også funksjonalitet for å administrere overføringsmediet. På lenkelaget kan det finnes funksjonalitet for feilkontroll.

Når IP-pakker og andre lag 3-pakker innrammes på lenkelaget, må avsenderen på en eller annen måte fortelle mottakeren hva nyttelasten består av. Ethernet og andre lenkelagsteknologier har derfor et typefelt i rammeheaderen som angir hva nyttelasten består av. Lenkefunksjonalitet hos mottakeren leser ut denne verdien og behandler nyttelasten i henhold til dette. Dette er en form for multipleksing og er noe som også utføres på de andre lagene.

#### 4.1.1 Praktisk håndtering av arbeidsoppgavene på lenkelaget

Hva skjer når IP-pakken blir behandlet når de skal sendes ut i et Ethernet-nettverk? Det første som skjer er at OSet tar IP-pakkene fra nettverkslaget og legger disse i Ethernet-rammer. Det innebærer å legge på Ethernet-headerfelter, som angivelse av innholdet i nyttelasten og avsender- og mottaker-MAC adresse.

Fra OSet sendes Ethernet-rammen ut til nettverkskortet. I nettverkskortet er det egen programvare som står for videre behandling av rammen. Når

programvaren i nettverkskortet er klar til å begynne overføring, sendes en bitstrøm ut til maskinvaren som har ansvaret for det som skal skje på det fysiske laget.

Når OSet mottar rammen fra nettverkskortet, må det tas en avgjørelse om hva som skal gjøres med innholdet av rammen. Dette gjøres ut fra protokolltypefeltet i Ethernet-headeren. Dersom innholdet er IP, vil OSet fortsette behandlingen av pakken ved hjelp av sin TCP/IP-protokollstakk.

## 4.2 Konstruksjon av nettverk

### 4.2.1 Eksklusiv og delt tilgang

Når vi ved hjelp av et overføringsmedium, for eksempel en kobberkabel, knytter en node til nettverk, har noden enten en eksklusiv eller delt tilgang til mediet. Dette er egenskaper som hører til på det fysiske laget.

Tar utgangspunkt i et enkelt nettverk hvor to noder knyttes sammen med et medium. Dersom mediet har to separate overføringskanaler, kan de to nodene sende signaler uavhengig av hverandre. Dette betyr at partene ikke behøver å bry seg om den andre parten sender eller ikke, siden begge har en uavhengig kanal å sende sine signaler på. Vi sier at noden har en *eksklusiv tilgang* til mediet.

Dersom to eller flere noder deler på en felles overføringskanal, har de delt tilgang til mediet. Dette kalles også å ha en *multiaksessforbindelse*, fordi flere parter trenger aksess til den samme overføringskanalen. Partene må da ha en *aksessmekanisme* for å dele mediet. Dette for å sikre at kun en part sender signaler om gangen.

### 4.2.2 Full dupleks-, halv dupleks-, og simpleksforbindelser

Forbindelsen mellom to tilstøtende noder kan være enten *full dupleks*, *halv dupleks* eller *simpleks*.

Dersom en forbindelse er full dupleks, kan det overføres signaler i begge retninger samtidig. For eksempel en telefon.

Dersom en forbindelse er halv dupleks, kan det bare overføres signaler i en retning av gangen. Vi kan da bare sende eller bare motta signaler. For eksempel en walkie-talkie og WLAN.

Simpleksoverføring betyr at vi bare kan sende signaler i en retning. For eksempel TV-signaler.

### 4.2.3 Punkt-til-punkt og multipunkt

Når to parter skal kommunisere, er det ikke nødvendig at teknologien benytter adressering, men man må ha dette når det skal være mulig å ha flere enn to parter.

Punkt-til-punkt muliggjør kommunikasjon mellom kun to noder. Multipunktteknologier muliggjør kommunikasjon mellom flere enn to noder.

### 4.3 Det fysiske laget

Ansvaret til det fysiske laget er å overføre binær informasjon fra en maskin til den neste ved hjelp av elektromagnetiske signaler. Elektronikk for å kode og dekode bitstrøm før og etter overføring på mediet hører også til det fysiske laget.

#### 4.3.1 Praktisk håndtering av arbeidsoppgavene på det fysiske laget

Ut fra lenkelaget kommer en bitstrøm som er klare for overføring på det fysiske laget. På det fysiske laget kodes bitstrømmen på en egnet måte før et signal genereres og sendes ut på mediet gjennom en kontakt eller en antenne. Her reserveres prosessen; signalet tas imot, tolkes og dekodes før en strøm av bit genereres og sendes til lenkelaget.

#### 4.3.2 Medier

**Trådparkabler** Kobberkabel, spesifikt trådparkabel, benyttes både i tele- og datanett. I telenett brukes trådparkabel både i aksessnett mellom telecentralen og kunden og internt i bygningsmassen til kunden. I datanett basert på Ethernet brukes trådparkabel til såkalt sprednett.

En trådparkabel består av et eller flere par med tynne, isolerte kobberledere lagt inn i en isolert plastkappe. Trådparkabler har i utgangspunktet ikke spesielt gode elektriske egenskaper. Det elektriske signalet forringes lett når det passer gjennom kabelen, som følge av forstyrrelser. En av de viktigste kildene til støy er de elektriske signalene i de andre lederne i kabelen. Dette fenomenet kalles *crosstalk*. For å redusere støy brukes to mekanismer: balansert transmisjon og tvinning av kabelen.

Balansert transmisjon innebærer at vi bruker to ledere, et par, for å overføre ett signal. Ved analog telefontilkopling sendes det signaler i begge retninger i trådparene. Dette muliggjøres gjennom *ekkokansellering*. Balansert transmisjon er en teknikk som gjør signalet mindre sårbart for støypåvirkning, samtidig reduserer støyen trådparet selv genererer.

Det finnes flere ulike typer trådparkabel, de mest utbredte er Unshielded Twisted Pair (UTP) og Shielded Twisted Pair (STP). I så og si alle installasjoner er det den rimelige UTP-kabelen som benyttes. STP-kabel har en skjerm rundt hvert trådpair for å redusere støyen på vei inn til og ut av trådparet, men er dyrere og mer tungvint å bruke.

**Fiber** Fiberkabler har egenskaper som gjør at de er velegnet der hvor trådparkabler ikke er det. Fiberkabler er derfor vanlige å benytte mellom

etasjer og mellom bygg. Fiberkabler er naturlig nok vanlig brukt i nettverkene til tele-/nettleverandører, hvor det er behov for lange kabelstrekk og høy overføringskapasitet.

En fiberoptisk kabel til bruk i tele- og datakommunikasjon består av en kjerne av glass (core) og en kappe av glass (cladding), som er beskyttet av et primærbelegg av plast (buffer coating). Informasjonen sendes inn i kjernen som små pulser av lys. Lyset holdes inne i kjernen fordi kappen er konstruert for å gi totalrefleksjon av lysbølgen. Lyset genereres enten ved hjelp av LED eller Laser Diode (LD). Laser er den kraftigste og mest presise kilden. Så og si all kommunikasjon over fiberkabler er full dupleks.