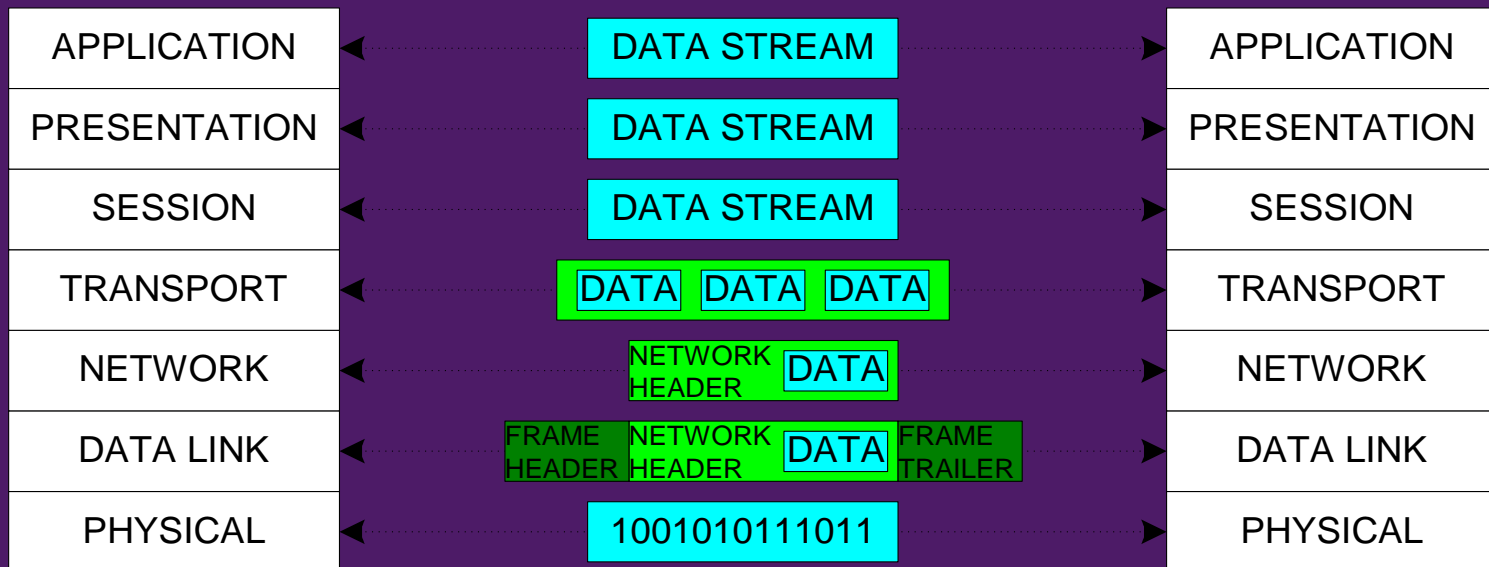


# Netværk 1 ifølge OSI modellen





# Lag 1, Fysisk



# Den fysiske sammenkobling

- **Point-to-point:**

Hver maskine kommunikerer direkte med kun én maskine på hver forbindelse.

- **Multipoint:**

Hver maskine kan kommunikere direkte med alle de andre. Her er brug for adressering.



# Det fysiske netværk

- Der er tale om **stjerne-topologi** når hver maskine er koblet direkte til en central enhed, typisk en **Switch eller en Hub**.
- Der er tale om **ring-topologi** når maskinerne sender til hinanden rundt i en ring – énvejs.
- Der er tale om **bus-topologi** når hver maskine er koblet op på det samme transmissionsmedie, som perler på en snor, f.eks. **Thin Ethernet (RG58) kabel**



# Logisk contra fysisk topologi

- En Hub arbejder internt som et forlænget Thin Ethernet kabel (kun én kan tale ad gangen) og derfor er Hub'ens logiske topologi en **Bus**.
- En Switch arbejder internt ved at opdele Ethernetsegmenter i kollisionszoner og adresserer de enkelte porte på MACadresser. Derfor er switchens logiske topologi en **Stjerne**.



# Ethernet

- Udviklet af Xerox sidst i 1970'erne, i samarbejde med Digital og Intel – kaldenavn Ethernet DIX. Videreudviklet af IEEE organisationen til Ethernet II. Der findes flere versioner af Ethernet.

TEKNOLOGI	NAVN	FART	KABEL
Ethernet	10BASE-5	10 Mbps	COAX
Ethernet	10BASE-2	10 Mbps	COAX
Ethernet	10BASE-T	10 Mbps	UTP
Fast Ethernet	100BASE-T	100 Mbps	UTP
Gigabit Ethernet	1000BASE-T	1 Gbps	UTP
Gigabit Ethernet	1000BASE-SX / LX	1 Gbps	Fiber
10 Gigabit Ethernet	10Gb Ethernet	10 Gbps	Fiber



# Forbindelses typer

- POTS - Plain Old Telephone Service (PSTN)
  - Dial up modem (9600 - 56000 bps)
  - Taksering pr. minut
- ISDN - Integrated Services Digital Network
  - ISDN terminaladapter. ( 2 x 64000 bps)
  - Taksering pr. minut pr. 64000 bps kanal.
- PPP protokollen er designet til at blive overført både via Asynkron og Synkron datatransmission på OSI lag 1
- Hvis man anvender Asynkron datatransmission:
  - Data sendes i en kontinuerlig strøm uden naturlig start og slut. For eksempel via en COM-port på en Pc og standarden her kaldes RS232C, seriel datatransmission.
  - PPP anvender her, i stedet for normal dataframe-overførsel, en teknik der kaldes *Byte Stuffing* for at afmærke start og slut på en dataramme.



# IEEE 802.11 - MAC

- Media Access Control laget ligger som tilpasning mellem netværkslaget og det fysiske medie
- Infrastructure netværk (med Access Point)
- Ad-hoc netværk (uden Access Point)
- Wireless Equivalent Privacy (WEP)
- MAC Management
- Bemærk: Et Access Point - AP - deler båndbredden mellem klienterne
  - Jo flere klienter - jo mindre båndbredde til hver klient (Bus - topologi)





# IEEE 802.11 Base standard

- 802.11
  - 2.4 GHz Frequency Hopping Spread Spectrum FHSS (1 Mbit/s)
  - 2.4 GHz Direct Sequence Spread Spectrum DSSS (2 Mbit/s)
- 802.11a Wi-Fi 5 GHz DSSS Extension (6, 12, 18 ... 54 Mbps)
- 802.11b Wi-Fi 2.4 GHz DSSS Extension (5.5 og 11 Mbps)
- 802.11g Wi-Fi 2.4 GHz DSSS Extension (6, 12, 18 ... 54 Mbps)
- 802.11gt Wi-Fi 2.4 GHz DSSS Extension (104 Mbps)
- 802.11n Wi-Fi 2.4 GHz DSSS Extension (300 Mbps)
- Wi-Fi = Wireless Fidelity = Godkendt og certificeret udstyr





# Lag 2, Data Link



# WLAN

- Et Wireless Local Area Network er et netværk som
  - modtager og sender data med radio signaler i stedet for kobber ledninger.
  - har samme funktionalitet som et netværk med kobber ledninger.



# WLAN sikkerhed



- WEP - Wired Equivalency Privacy
  - Den oprindelige WLAN sikkerhedskryptering.
  - Der findes desværre mange Crack programmer på nettet til WEP security (WEPcrack....)
- EAP - Extensible Authentication Protocol
  - Videreudvikling af WEP
  - Standarden kaldes IEEE 802.1X
  - Port baseret authentication til WLAN
  - Usikker
- LEAP - Lightweight Extensible Authentication Protocol
  - Videreudvikling af EAP
  - Bygger på IEEE 802.1X, WEP samt kontrol af MAC adresser
  - Udviklet af Cisco



# WLAN sikkerhed



- PEAP - Protected Extensible Authentication Protocol
  - En udbygning af LEAP protokollen
  - Nyt er kryptering af al brugervalidering med certifikater.
  - Udviklet af Cisco, Microsoft og RSA i samarbejde.
- WPA - Wi-Fi protected Access
  - Bygger på 802.11i sikkerheds standard
  - Erstatning for den usikre WEP sikkerhed
  - Bruger TKIP - Temporal Key Integrity Protocol.
    - Genererer nye nøgler for hver 10KB data.
- WPA – 2
  - Bygger på WPA, med mere sikker beregning af krypteringsalgoritmen.
  - Mest sikre standard p.t.



# VPN

- VPN - Virtual Private Network
- Et privat net (tunnel) gennem et offentligt net, fx Internettet
- Et VPN er et antal tilslutninger til et Backbone net som må udveksle trafik.
- Medlemmerne i et VPN må ikke udveksle trafik med andre.
- Et VPN er defineres af et sæt regler der
  - Definerer connectivitet og QoS mellem tilslutninger i VPN'et.



# Ethernet

- Transmissionsteknikken Carrier Sense, Multiple Access with Collision Detection
  - forkortet CSMA/CD

	Ethernet	Fast Ethernet	Gigabit Ethernet	10 Gigabit Eth.
Hastighed	10 Mbit/sek.	100 Mbit/sek.	1 Gbit/sek.	10 Gbit/sek.
Adgangsmetode	CSMA/CD	CSMA/CD Full duplex MAC	CSMA/CD Full duplex MAC	Full duplex MAC
Standard	IEEE 802.3	IEEE 802.3u	IEEE 802.3z	IEEE 802.3ae
Rammestørr.	64-1518 bytes	64-1518 bytes	64-1518 bytes	64-1518 bytes
Topologi	Bus eller Stjerne	Stjerne	Stjerne	Stjerne
Kabeltype	Coax,UTP,Fiber	UTP,STP,Fiber	UTP,STP,Fiber	Fiber



# ARP protokollen

- ARP - Address Resolution Protocol
  - kan opfattes som et 'bindeled' mellem adresserne på OSI lag 2 (datalink) og adresserne på OSI lag 3 (netværk), f.eks. mellem Ethernet- og IP-adresser.
  - er en fast del af TCP/IP protokol suiten
  - dækker over en række af standarder, f.eks. er RFC 826 navnet på standarden for Ethernet Address Resolution Protocol.





# STP

- Spanning Tree Protocol er en switch-teknologi der er indført for at kunne håndtere de forskellige problemer der opstår på et netværk, når man kobler nettet op med flere veje mellem de enkelte switche (redundans). Problemerne kan være:
  - Broadcast storms
  - Dublerede pakker
  - Ustabile MAC-adresse tabeller
- STP tilbyder flere fysiske veje mellem to enheder:
  - Kun en aktiv vej mellem to enheder åben
  - Alternative veje lukkede
  - Finder den mest effektive vej mellem to enheder
  - Sender og modtager opdateringer for at bygge bedste vej gennem nettet - kontinuerligt



# VLAN

- VLAN's er en logisk opdeling af enheder eller brugere og teknikken resulterer i et system der minder om IP adressering; man gør sig elegant næsten uafhængig af strukturen i selve det fysiske Ethernet netværk.
- VLAN's opdeler selve Ethernet-trafikken på switchene i et antal fuldstændig adskilte virtuelle LAN's, der er geografisk uafhængig af hinanden.
- Hver Ethernet ramme mærkes med et bestemt VLAN tilhørsforhold og dermed fungerer teknologien primært på OSI lag 2.
- Har man efterfølgende brug for det kan man få en router på OSI lag 3 til at flytte rammer imellem VLAN's, f.eks. for at skabe adgang til Internet.





# Lag 3, Netværk



# IP

- En IP-adresse fylder 4 bytes.
  - For eksempel 194.182.53.14
- En IP-adresse er sammensat af to adresser:
  - En net-adresse **194.182.53.14**
  - En maskine-adresse 194.182.53.**14**
- Sagt på en anden måde:
  - Maskinen hedder 14 og er medlem af netværket 194.182.53



# Subnet maske

- Klasse A er til meget store net
  - Første byte er net-del (Første byte 0 - 127)
  - Subnet mask = 255.0.0.0
- Klasse B er til store net
  - Første 2 bytes net-del. (Første byte 128 - 191)
  - Subnet mask = 255.255.0.0
- Klasse C er til mindre net
  - Første 3 bytes net-del. (Første byte 192-223)
  - Subnet mask = 255.255.255.0



# Ping kommandoen

- En indbygget testfunktion i TCP/IP
- Ping kommandoen findes i næsten alt TCP/IP udstyr
- Sender en testpakke til modtager som besvarer med en testpakke.



# Routetabellen

- Alle Host har en routetabel
- Routetabellen indeholder liste over alle kendte logiske net.
- Routetabellen indeholder ofte også en Default Route til alle andre net
- Routetabellen bruges til bestemme hvor den enkelte Host skal sende IP-pakker hen.



# Opbygning af Routetabellen

- Routetabellen kan modtage informationer både statisk og dynamisk:
  - Statisk opbygning
    - Informationer til tabellen indtastes manuelt.
  - Dynamisk
    - Informationer til tabellen modtages automatisk via routningsprotokollerne:
      - RIP, OSPF, IGRP, BGP...
    - Der er 2 typer dynamiske routningsprotokoller:
      - Distance Vector
      - Link State





# Routed contra Routing protokoller

- **En routed protokol** er enhver netværks protokol som har information om netværks adresser, så data kan sendes fra node til node og fra netværk til netværk. Eksempler på routede protokoller er:
  - IP (Internet Protokol).
  - IPX (Internetwork Packet eXchange).
- Men protokollen NetBEUI (Net BIOS Extended User Interface) er ikke fordi den mangler netværks adresser.
- **En routing protokol** tillader routere at kommunikere med andre routere for at opdatere og vedligeholde deres router tabeller. På den måde deles router informationen mellem routerne. Eksempler på routing protokoller er:
  - RIP (Routing Information Protocol)
  - IGRP (Interior Gateway Routing Protocol)
  - OSPF (Open Shortest Path First)
  - IS-IS (Intermediate System to Intermediate System)



# routningsprotokol?

- Vi tager udgangspunkt i protokollen RIP
  - en ældre protokol - Routing Information Protocol
  - RIP er en Distance Vector protocol
  - Routere som bruger RIP sender som standard hele sin Routetabel til alle sine naborroutere hvert 30. Sekund.
  - RIP findes i to versioner
    - RIP Version 1. Kan ikke finde ud af subnetting
    - RIP Version 2. Kan finde ud af subnetting.



# RIP - teknisk set

- Maksimum HOP-Count = 15
  - Dvs. pakkerne kan maksimalt passere 15 routere på deres vej gennem nettet.
- HOP-Count = 16 betyder uendeligt langt væk
  - I praksis betyder det, at det interface på routeren der normalt har forbindelse med IP nettet (det logiske net) hvor HOP-Count er på 16, ikke har kontakt til nettet. Det logiske netværk kan ikke nås og fjernes derfor fra routetabellen.
- Split-Horizon.
  - En router sender ikke oplysninger tilbage til naboroutere som den har modtaget fra dem.



# RIP - teknisk set

- Fordele
  - Simpel opdatering.
  - Simpel implementering.
  - God til mindre net. Op til Ca. 20 routere
  - Hvis nettet kun består af Cisco-routere se IGRP
- Ulemper
  - Periodiske opdateringer fylder båndbredde
  - Langsom til at "konvergere". (Opdatere)
  - Uegnet til større net.
  - Tager ikke hensyn til båndbredde eller andre parametre.



# IGRP

- IGRP - Interior Gateway Routing Protocol
  - Den er Cisco proprietær.
  - Det er en forbedret RIP protokol.
- Fordele:
  - Kan finde ud af store net
    - Maksimum HOP-Count = 255
  - Kan "måle" afstand mellem net på kombinationer opsat af:
    - Hop-count, Båndbredde, forsinkelse, belastning, pålidelighed og pakkestørrelse.



# SPF

- Link State routings-protokoller er en helt anden type protokol:
  - De sender ikke hele Route-tabeller, men kun Link State Advertisements -LSA'er
  - Hver LSA indeholder liste over tilsluttede netværk til den enkelte Router.
  - Alle Routers sender LSA til alle andre routers
  - Alle Routers lærer alle andre Routers at kende.
  - Bedste Route udregnes på denne baggrund.
    - SPF – Shortest Path First
- Routers på meget store netværk kommunikerer næsten altid ved hjælp af Link State protokoller:
  - Eksempler: OSPF eller IS-IS



# NAT

- NAT: Network Address Translation
  - én til én IP adresse omsætning
- Oversætter IP adresser fra Indre net til IP adresse på Ydre net (WAN)
- Private IP adresser benyttes oftest
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- NAT skjuler det Indre netværk effektivt for hackeren på Internettet



# Firewalls



- Firewalls fungerer efter 2 forskellige teknikker: Proxyanalyse og "stateful inspection".
  - En proxyfirewall analyserer hver enkelt pakke og er de mest sikre.
  - Stateful inspection analyserer sessioner hvilket giver ringere sikkerhed men højere hastighed. Nyere firewalls er hybrider hvor der benyttes proxyanalyse hvor det er en fordel og stateful inspection hvor det er en fordel.
- En firewall bruges til at håndhæve de regler for netværkstrafik man har bestemt sig for er acceptable.







# Lag 4, Transport



# TCP og UDP oversigt

- TCP (Transmission Control Protocol) opbygger virtuelle forbindelser mellem slut bruger applikationer. Karakteristisk for TCP er:

- Forbindelsesorienteret (virtuel forbindelse).
- Sikker transport.
- Opdeler data som skal sendes i segmenter.
- Samler data segmenterne igen hos modtageren.
- Der kvitteres for alle data og hvis data ikke er modtaget sendes de igen.

- UDP (User Datagram Protocol) transporterer data mellem hosts, men der garanteres ikke for om data afleveres. Karakteristisk for UDP er:

- Forbindelsesløs.
- Usikker - ingen garanti for at data afleveres.
- Samler ikke data segmenterne igen hos modtageren.
- Ingen flow kontrol.
- Ingen fejl kontrol og korrigering af fejl.



# NetBIOS protokollen

- NetBIOS er en ældre protokol, hvor vi kan navngive hosts i en arbejdsgruppe.
- En host udnævnes til Browsermaster, ud fra det nyeste operativsystem og serienummer, og har listen over medlemmer.
- Listen opdateres kun hvert 12. minut, så husk tålmodighed ved ændringer.





# Lag 5, Session



# Domain Name Service DNS

- Oversætter domænenavne til IP-adresser
  - F.eks: [www.jp.dk](http://www.jp.dk) oversættes til 80.80.12.116
  - Bruges dagligt i Internet Browsers
- Oversætter IP-adresser til domænenavne
  - F.eks: 80.80.12.116 til [www.jp.dk](http://www.jp.dk)
  - Bruges ofte til at finde afsender af data



# Domain Name Service

## DNS

- Domænenavne er delt op med punktum.
  - Et punktum betyder en uddelegering
- Domænenavne læses fra højre mod venstre
  - `www.teknik.intranet.eucmidt.dk`.
    - Punktum er root-server (Højeste autoritet)
    - `.dk` er barn af forfaderen punktum
    - `.eucmidt` er barn af `.dk` og har flere forfædre
    - ....



# DNS . = root-serverne

- Der findes pt. 13 root server installationer spredt rundt om i verden (se [www.root-servers.org](http://www.root-servers.org) )
- Der kan være flere kopier af hver server.
- Root-serverne administrer zonerne
  - .com, .org, .mil, .dk, .biz, .info .....
- Root-serverne har store databaser
- ISP (Internet Service Provider) har DNS-servere for at aflaste root-serverne



# DHCP

## Dynamic Host Configuration Protocol

HOUSE OF  
TECHNOLOGY



- en del af mercontec\*

- En DHCP servers funktion er at styre og konfigurere TCP/IP opsætningen på computere/klienter som selv anmoder om det.
- DHCP serveren er ofte placeret direkte på lokalnettet, men den kan også godt placeres på den anden side af et antal router. Mange ISP'ers DHCP servere sidder centralt i deres IP net.
- DHCP klienterne kan være alle IP hosts: Pc'er, printere, routere etc.
- En DHCP server kan konfigurere DHCP klienter med mange forskellige parametre som fx:
  - En IP adresse ,Subnet maske, Gateway adresse, En eller flere DNS servere, WINS servere, Proxy server

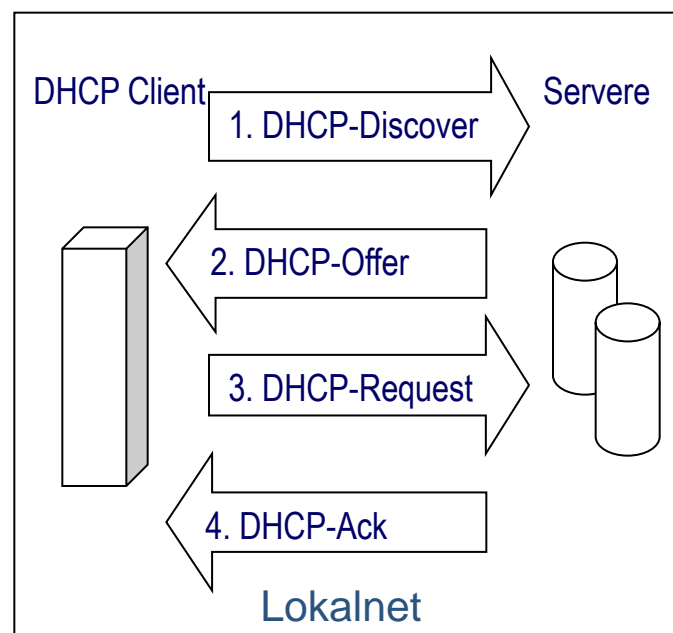




# DHCP

## Dynamic Host Configuration Protocol

- DHCP server-klient kommunikationen foregår via specielle datapakker transmitteret over netværket i følgende rækkefølge:





# Lag 6, Præsentation



# TCP og UDP port numre

- Et datagram finder modtageren og modtagernettet vha. IP adressen.
- Adressering af applikationer i den enkelte host udføres vha. port numre i TCP og UDP protokollerne.
- En IP adresse med tilhørende port numre kaldes en socket.
- Et port nummer kan have en værdi fra 0–65535, hvor porte fra 0–1023 kaldes kendte porte hvilket vil sige at deres brug er fastlagt (fx 21 ftp port).
- Porte kan være destinations og source porte:
  - En destinations port beskriver hvor i modtager maskinen datagrammet skal hen, dvs. hvilket program eller service det skal adresseres til.
  - Source porte anvendes til at beskrive afsenderens sessions nummer og betyder at man fx kan se på flere hjemmesider (sessioner) på en gang. Source porten vælges af afsenderen og kan være alle ubrugte / ukendte porte, minus destinations porten.
- Den officielle liste over portnumre administreres af IANA.



# TCP og UDP port numre

Navn	Port nr.	Protokol	Beskrivelse af service
Ftp	21	tcp	File Transfer Protokol
Telnet	23	tcp	Telnet remote login
Smtpt	25	tcp	Simple Mail Transfer Protokol
Domain	53	udp	Domain Name Server
Bootsps	67	udp	Bootstrap Protocol Server / DHCP server
Bootpc	68	udp	Bootstrap Protocol Client / DHCP client
Tftp	69	udp	Trivial File Transfer Protocol
Www-http	80	tcp	World Wide Web http
Pop3	110	tcp	Post Office Protocol – Version 3
Nntp	119	tcp	Network News Transfer Protocol
Netbios-ns	137	tcp	NETBIOS Name Service
Netbios-ns	137	udp	NETBIOS Name Service
Netbios-dgm	138	tcp	NETBIOS Datagram Service
Netbios-dgm	138	udp	NETBIOS Datagram Service
Netbios-ssn	139	tcp	NETBIOS Session Service
Netbios-ssn	139	udp	NETBIOS Session Service
	1023		
Frie porte	1024-65535		Kan bruges af alle

# TCP og UDP port numre

- Et datagram finder modtageren og modtagernetet vha. IP adressen.
- Adressering af applikationer i den enkelte host udføres vha. port numre i TCP og UDP protokollerne.
- En IP adresse med tilhørende port numre kaldes en socket.
- Et port nummer kan have en værdi fra 0–65535, hvor porte fra 0–1023 kaldes kendte porte hvilket vil sige at deres brug er fastlagt (fx 21 ftp port).
- Porte kan være destinations og source porte:
  - En destinations port beskriver hvor i modtager maskinen datagrammet skal hen, dvs. hvilket program eller service det skal adresseres til.
  - Source porte anvendes til at beskrive afsenderens sessions nummer og betyder at man fx kan se på flere hjemmesider (sessioner) på en gang. Source porten vælges af afsenderen og kan være alle ubrugte / ukendte porte, minus destinations porten.
- Den officielle liste over portnumre administreres af IANA.





# Lag 7, Applikation



- **HTTP (HyperText Transfer Protocol)** anvendes til World Wide Web. HTTP er et sæt regler for overførsel af filer som kan være grafik, tekst, lyd, video ol. på fx Internettet. Hypertekst er en tekst der fx kan henvide til en anden tekst. Anvender port 80.
  - `HTTP://host.domæne.navn/sti_til_ressourcen,` fx  
`HTTP://www.fts.dk/dokumenter/a3.doc`
- **FTP (File Transfer Protocol)** bruges til at overføre filer mellem to maskiner på et netværk, fx. Internettet. Anvender port 20 og 21.
  - `FTP:// host.domæne.navn/sti_til_ressourcen,` fx  
`FTP://www.fts.dk/nyefiler/programmer`
- **POP3 (Post Office Protocol ver.3 )** bruges til at hente e-mail fra en mailserver. Anvender port 110.
- **SMTP (Simple Mail Transfer Protocol)** bruges til at sende e-mail fra en klient maskine og mellem mailservere. Anvender port 25.
- **Telnet** bruges til at få terminal adgang til en computer/host til fx konfigurering. Telnet kan også bruges at teste fx POP3 og SMTP servere. Anvender port 23



- Slutbruger enhed på LAN som normalt er IP telefoner eller PC'er.
- Understøtter real-time 2-vejs kommunikation med en anden H.323 enhed.
- En terminal skal indeholde følgende:
  - Voice - audio codec
  - Signalering og setup (Q.931, H.245, RAS)
  - Et netværks interface
  - Medie transmission
- En terminal kan indeholde følgende:
  - Video mulighed
  - Data mulighed

