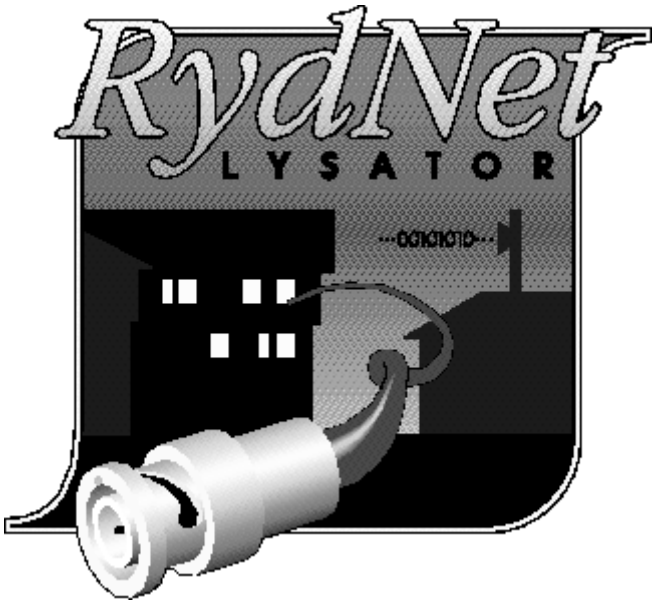


En kort introduktion till datornät

Av: Kjell Enblom (kjell-e@lysator.liu.se)

En kort teoriintroduktion till datornätverk.

2:a upplagan 3:e utgåvan, Mars 1996.

Detta dokument återfinns även i postscriptformat på:
http://www.lysator.liu.se/~kjell-e/rydnet/intro1.ps

Av: Kjell Enblom, 1994, 1995, 1996

Denna text får distribueras fritt endast i sin helhet och den får användas fritt.
Betalning får ej tas ut för någonting mer än papperskostnaden och eventuell fraktkostnad.
Texten får ej användas för kommersiellt bruk.
Denna text måste finnas med vid vidare distribuering.

© Kjell Enblom, kjell-e@lysator.liu.se

Innehåll:

NÄTTOPOLOGIER: 4

LITE KORT OM NÄTSKIKT: 4

NÄTVERKSUTRUSTNING: 6

ACCESSMETODER: 9

KODNINGSPRINCIPER: 10

OSI-SKIKT 1 OCH 2: 11

LÄNKSKIKTET, ISO 8802-2: 11
ISO 8802-3, FYSISKA SKIKTET: 14
OLIKA ETHERNET-STANDARDER: 18

HUR MAN BERÄKNAR OLIKA PARAMETRAR FÖR ETT LITE STÖRRE NÄT 20

TCP/IP: 21

ARP, ELLER HUR EN UPPKOPPLING GÖRS. 23
MULTICAST 23

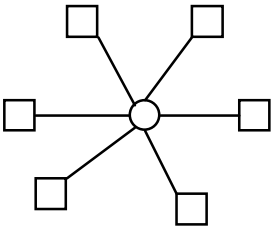
LITTERATURHÄNVISNINGAR: 24

ÖVRIG LITTERATUR: 24

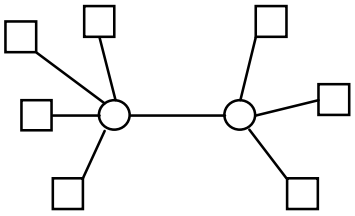
Nättopologier:

Det finns tre grundläggande topologier, ringnät, stjärnnät och bussnät.

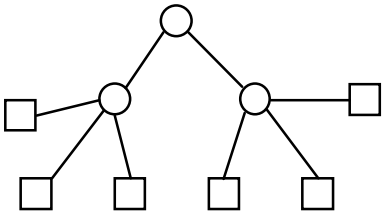
I ett stjärnnät finns det en central station som kan fungera som en ren kopplingsenhet och i fall med en mer avancerad central kan den dessutom ha hand om all access till nätet.



Äkta stjärnnät



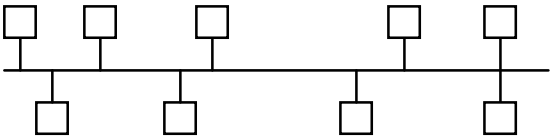
Distribuerad stjärna



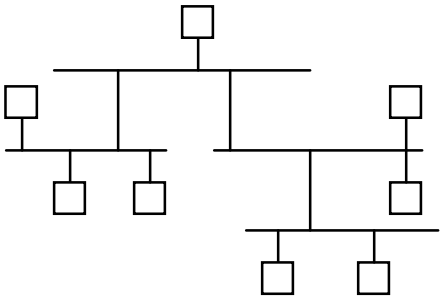
Snöflinga

I ett ringnät är alla maskiner kopplade efter varandra i en ring. Alla paket passerar hela ringen och alla stationer i den. Till skillnad mot bussnät kommer ett paket inte fram till alla maskiner samtidigt utan passerar dem en i taget.

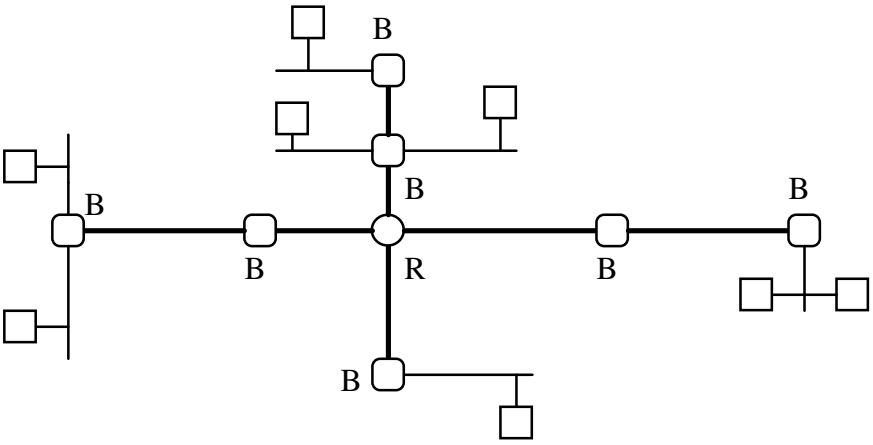
Ett bussnät är uppbyggt så att alla maskiner är kopplade till en och samma ledning.
I ett basbandsnät är det en ledning och i ett bredbandsnät är de kopplade till en gemensam kanal.
Är det ett litet nät kan alla maskiner kopplas till en ledning, men med många maskiner i ett större nät är det lämpligare att strukturera upp nätet i form av ett träd.



Bussnät



Trädformat bussnät



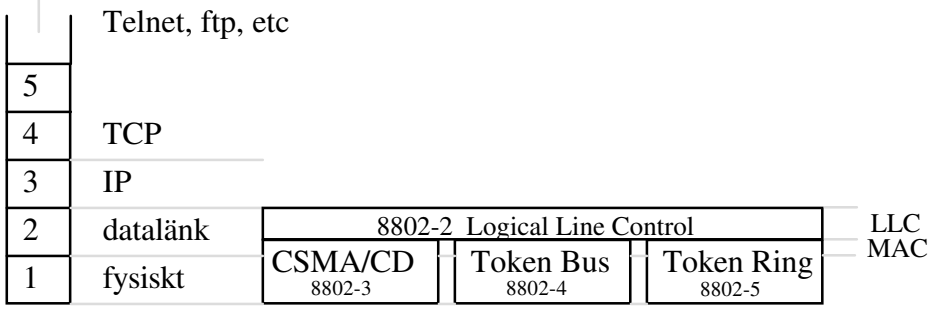
Ett trädformat nät med ett stamnät, och en router i mitten

B=Brygga (eller eventuellt repeater). R=Router

Den vanligaste accessmetoden är CSMA/CD

Lite kort om nätskikt:

OSI-skikt



MAC=Medium Access Control

Nivå 1 och lite av nivå 2 i OSI-modellen sköter om så att de elektriska signalerna, radiosignalerna, IR-signalerna eller laserssignalerna kommer ut i det aktuella mediet. Mediet i RydNets fall består mestadels av koaxialkabel och till viss del av Partvinnad kabel.

Resten av nivå 2 sköter om hårdvaruadressering. Varje nätverksport i all utrustning har en egen unik hårdvaruadress. Datalänk-nivån tittar också på den inkommande trafiken och ser efter ifall den ska till just den här datorn. Om den är till denna dator skickas paketet upp till nästa nivå annars så ignoreras det.

Nivå 3 håller reda på nätverksadressen, IP-adressen, och vilket ovanliggande protokoll som används, TCP, UDP etc. Om en loop skulle uppträda i nätet så sköter nivå 3 om så att paketet dör till slut. All utrustning har alltså en nätadress vilken bland annat underlättar mycket för en del nätverksutrustning. Nätadressen fungerar ungefär på samma sätt som telefonnummer. De första siffergrupperna talar om på vilket nät datorn finns vilket motsvarar riktnummer. De sista siffrorna är datorns nummer, vilket motsvarar telefonabonnentens nummer inom riktnummerområdet. Skillnaden är att när de sista siffrorna i en IP-adress är 0 så talar det om vilket nät det handlar om. En dator kan alltså inte ha 0 som sista siffror i sin IP-adress. I ett telefonnät kan en abonnent ha nollor som sista siffror.

Högre nivåer sköter om saker som felkontroll och ser till så att rätt paket kommer till rätt program i mottagaränden.

När en dator skickar en stor mängd data delar den upp datamängden i små paket som skickas enskilt på nätet till mottagaren. Vid en filöverföring talar programmet om för tcp att skicka iväg den här filen till den andra datorn. TCP delar upp filen i smådelar och ger dem till IP som i sin tur lägger till sin IP-adress och mottagardatorns IP-adress till paketet och ger det vidare till nästa lägre nivå som ser till att skicka iväg det till rätt dator.

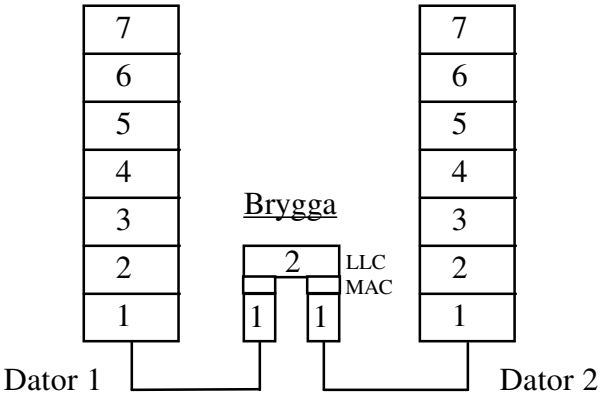
Paketen ser ut så här när de kommer ut på nätet:

Ethernetheader
IP-header
TCP-header
Data

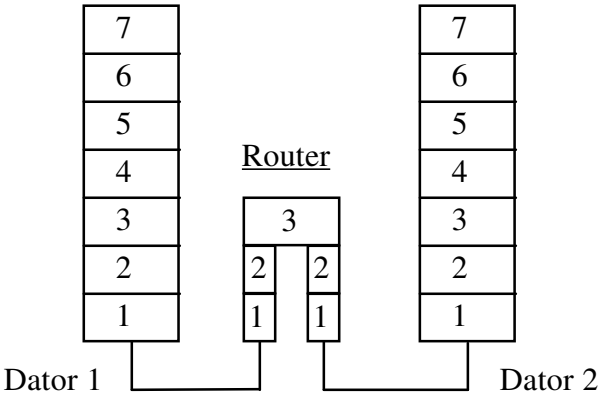
Skikt 4, 5, 6 och 7 i OSI-modellen tas ej upp i denna skrift.

Nätverksutrustning:

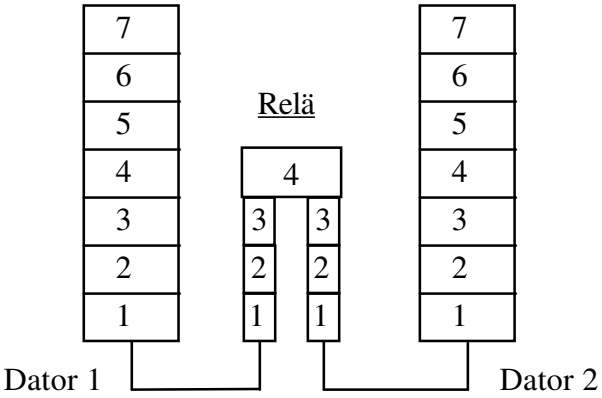
REPEATRAR, HUBBAR arbetar på elektrisk nivå och förstärker signalen så att det går att förlänga ett nätsegment. SLOT TIME som är ett pakets minimilängd måste vara något längre än ett segment. Detta innebär att det inte går att förlänga ett segment med hur många repeatrar som helst. För att kunna förlänga nätet mer behövs mer intelligent utrustning som tittar på paketen. Ett nät får inte bestå av fler än fem segment med fyra repeaters mellan. Dessutom så får bara tre av dessa segment innehålla anslutna noder och de två resterande får bara användas för transport mellan två repeatrar. Repeatrar finns som har fler än 2 portar, så kallade multiportsrepeatrar. En multiportrepeater brukar ha en port för inkoppling på stamnätet och sedan ett antal portar för inkoppling av flera noder. En variant på multiportrepeater är en HUB som har ett antal RJ-45 kontakter för TP-anslutningar, Twisted Pair.
BRYGGOR, switchande HUBBAR arbetar på en lite högre nivå än REPEATRAR, närmare bestämt länkskiktet, skikt 2. En brygga kan brygga trafik mellan olika nät med olika media och olika accessmetoder. Datapaket upp till och med skikt 2 översätts, men paketen i skikten ovanför skickas vidare så som de är. En brygga filtrerar på nivå 2 så att trafik som är lokal inom ett segment inte skickas vidare till nästa segment. I ett ethernet innebär detta att filtreringen sker på ethernetpaket nivå. Det finns även bryggor som inte filtrerar.



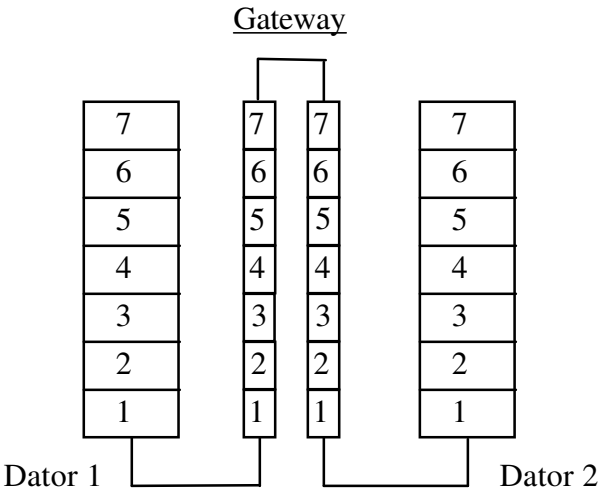
ROUTRAR En router (gateway i engelskspråkig litteratur) arbetar på skikt 3. Den översätter paket upp till och med skikt 3 och skickar dem vidare till det segment de ska till. Nätet kan delas upp i flera smånät, som t ex nät-1, nät-2, nät-3 och nät-4. Routern har då 4 st portar (ethernetinterface) och sätts upp så att den känner till på vilken port vilket nät finns. Om en dator på nät-1 vill kontakta en på nät-3 tittar routern på IP-adressen och ser att paketet ska till nät-3. En router måste alltid adresseras då trafik ska passera den. Ett paket som ska passera måste innehålla adressen till routern (MAC). Då flera routrar ligger på vägen byts routerns adress (MAC) i paketet ut mot adressen till nästa router (MAC). Den sista routern på vägen byter ut "nästa"-adressen mot slutadressen. MAC-adressen får datorn på det lokala nätet reda på genom ett ARP-anrop (se avsnittet om ARP). Ibland används sourcerouting vilket innebär att avsändaren bestämmer vilken väg som paketen ska gå. En router kan ta reda på vilka maskiner som är inkopplade var genom att skicka ut broadcast på de olika segmenten. Moderna routrar innehåller programvara för övervakning av nätet och dessutom kan de prata direkt med andra routrar i nätet. Övervakningsprogramvaran brukar då baseras på SNMP, Simple Network Management Protocol.



RELÄ En variant på router som arbetar på skikt 4 kallas för relä. Den kan routa trafik där näten skiljer sig åt upp till och med nätskikt, t.ex. ett TCP/IP-nät och ett XNS-nät.



GATEWAY En gateway kopplar samman två helt olika nät där alla skikten skiljer sig åt. Gatewayen översätter protokoll för protokoll för varje nivå.



TRANSCEIVER En transceiver är en form av mediaberoende interface (Medium Attachment Unit, MAU) och kopplas till t.ex. ett ethernetkort i en dator eller till någon av ovanstående typer av nätverksutrustning. Transceivern ansluts till AUI-porten på den aktuella utrustningen med en droppkabel. Den här typen av transceiver finns i OSI-skikt 1 i ISO 8802-3. Till tunn ethernet ansluts en transceiver med en BNC-kontakt, till tjock ethernet används en vampyrtappning som är ett stift som sticks in i kabeln, till Twisted Pair används en RJ-45 kontakt som påminner om en telefonkontakt.

Accessmetoder:

Hårdvaran kan inte bara skicka ut paketen rakt ut på kabeln för då skulle alla ”prata i mun på varandra” och ingen trafik skulle komma fram. Därför har man uppfunnit olika accessmetoder som bestämmer när någon dator får skicka ut någonting på kabeln eller ut i luften för radionät eller IR-nät. Nedan finns korta beskrivningar av några av de vanligaste. I RydNet används CSMA/CD.

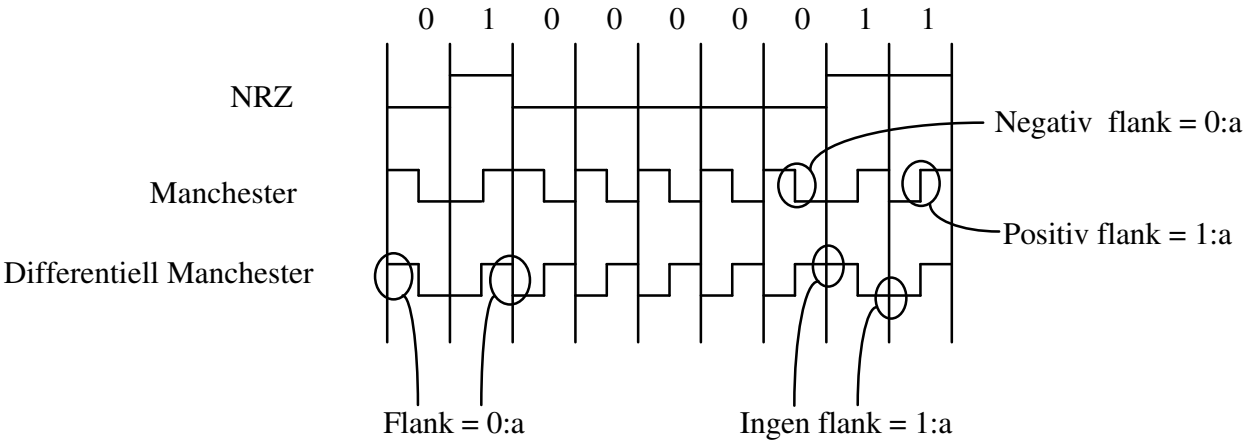
CSMA/CD (Carrier Sense Multiple Access/Collision Detect) är en vanlig typ av accessmetod för nätverk. Det är den accessmetod man använder i ethernet. Med collision detect testar man först och ser så att ingen annan sänder för att sedan skicka det egna datapaketet. Om kollision uppstår väntar man en slumpmässig stund för att testa och sända igen enligt ovan. Ett datapakets minimilängd kallas för SLOT TIME och den är något större än fördröjningen mellan noderna i ytterändarna. Detta är för att alla noder ska kunna uppfatta en kollision.
CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) är vanligt i radionät och IR-nät. Denna accessmetod fungerar så att man först testar och ser så att kanalen är ledig för att därefter sända ut en reserveringssignal. Om ingen kollision inträffade sänds en definitiv reserveringssignal ut följt av datapaketet som avslutas med en klarsignal när ett accepterande (acc) från mottagaren har kommit.
TOKEN BUS används i en del trädformade nät. En nod som har någonting att sända väntar tills dess att den har fått en fri token sänd till sig då den sänder så mycket som får plats i den TIME SLOT den har fått sig tilldelad. När alla data är överförda skickas TOKEN vidare till nästa nod enligt en lista som sätts upp i samband med nätinstallationen.
TOKEN RING används i ringformade nät. En TOKEN cirkulerar runt i nätet och om en nod vill sända data tar den in den lediga TOKEN, skickar iväg datapaketen på nätet följt av TOKEN som nu är markerad upptagen. Sändningen av datapaket får bara ske under ett visst tidsintervall, därefter måste TOKEN skickas ut igen. Mottagaren kopierar datapaketet och flaggar paketet som mottaget för att skicka det vidare tillbaka till avsändaren som pockar bort det från ringen. En övervakningsnod behövs för att plocka bort trasiga paket och paket som har vandrat runt utan att ha tagits bort, och för att ta bort en TOKEN då det ibland kan förekomma två eller fler i en ring.
EMPTY SLOT används även det i ringformade nät. Här finns ett antal paket som antingen är tomma eller upptagna. När en nod behöver sända någonting väntar den på ett tomt paket som den fyller med data och markerar som upptagen. Mottagaren tar emot paketet och markerar det som mottaget varvid sändaren slutligen markerar det som ledigt.
FIXED SLOT är en variant på EMPTY SLOT där varje nod har ett eget speciellt paket.

BREDBAND utnyttjar kabeln så att dess kapacitet delas upp i olika frekvensband, där olika maskiner skickar sina data på olika frekvensband. Bredband är låst till 75 Ohms koaxialkabel.
BASBAND är sådant att ett paket utnyttjar hela kabelns kapacitet. Förr användes 50 ohm koax men partvinnad kabel och optofiber är vanligare i dag.

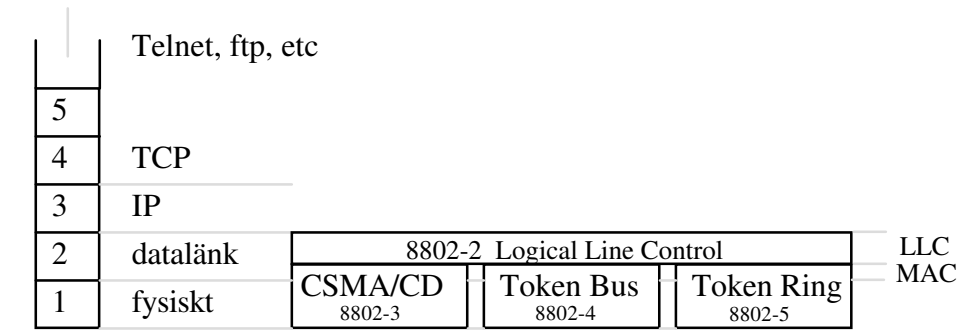
Kodningsprinciper:

De elektriska signalerna på kabeln måste se ut på något lämpligt standardiserat sätt för att det ska fungera. En etta och en nolla måste representeras av elektriska spänningsnivåer/flanker etc. Digitalteknikens representationsform fungerar inte speciellt bra på den här typen av transmissionsmedium. Dels blandas noll volt lätt ihop med att ingen sänder alls på kabeln, och med spänningsnivåer får man synkroniseringsproblem. Ett par kodningsprinciper beskrivs kort nedan.

NRZ, Non Return to Zero, representerar en etta med en positiv spänning och en nolla med en negativ spänning.
Manchester Encoding används för att slippa synkroniseringsproblem. Spänningen byter polaritet mitt i varje tecken där en övergång från negativ spänning till positiv (positiv flank) betyder en etta och en övergång från positiv spänning till negativ (negativ flank) betyder en nolla. Polariteten måste i vissa fall även skiftas mellan tecknen.
Differentiell Manchester Encoding. Spänningen byter alltid polaritet mitt i varje tecken och om det finns en övergång i början på tecknet betyder det en nolla och avsaknad av en övergång innebär en etta. Det finns dessutom ett teckenläge utan någon mittövergång som inte är vare sig noll eller ett. Beroende på om det finns en övergång i tecknets början eller inte så finns det två sådana som utnyttjas som speciella ickedata-tecken.



OSI-skikt 1 och 2:

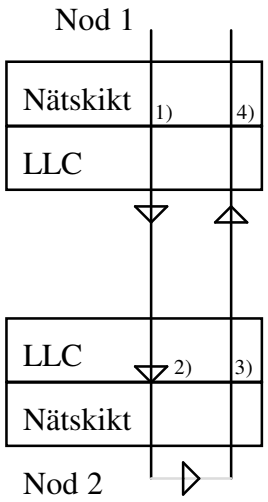


MAC=Medium Access Control

Länkskiktet, ISO 8802-2:

Gränsen mellan OSI-skikten 1 och 2 följs inte riktigt av ISO-standarden. De olika accessmetoderna återfinns i skikt 1 och delvis i 2 (se figur ovan). I övre delen av skikt 2 hittar vi LLC, Logical Line Control, som har till uppgift att upprätta och hålla igång en eller flera logiska länkar med andra noder. Det den gör är att den genererar och tolkar nödvändiga styr och kontrollsignaler, översätter datapaket, organiserar dataflödet och sköter en del felkontroll och felkorrigering. Uppåt pratar LLC med nätskiktet, nedåt med MAC och den kommunicerar med LLC i andra noder. Det finns 2 typer av tjänster som LLC uträttar åt nätskiktet. *Typ 1* skickar ut paketen rätt ut på nätet utan någon bekräftelse eller kontroll. Paketen kan skickas till en eller flera mottagare. En typ-1 förbindelse är förbindelsefri. *Typ 2* är förbindelseinriktad och paketen kan endast skickas till en nod, en så kallad peer to peer förbindelse. I en typ-2 förbindelse kvitterar mottagaren alla mottagna meddelanden. Här sker även felkontroll och en kontroll att paketen kommer i rätt ordning. 4 typer av anrop finns i typ2, etablering av en förbindelse och ett upphörande av förbindelsen, flödeskontroll och felhantering (kontrollera fel, begära återsändning och kontroll av sekvens), och en återställning av förbindelsen till utgångsläget. Noder av klass 1 klarar endast av att hantera typ-1 förbindelser och noder av klass 2 kan hantera både typ-1 och typ-2 förbindelser. Klass 2 är ett tillägg och är inte obligatorisk så som klass 1 är enligt standarden. I gränssnittet mellan de olika nivåerna finns det ett antal anrop som i sin tur använder sig av ett antal serviceprimitiver. Mellan LLC och skikt 3 finns Data Request och Data Indication som används vid en typ-1 förbindelse. Request begär en dataöverföring av paket som finns i skikt 3 och indication talar om att LLC har mottagit paket. Vid en typ-2 förbindelse finns det lite fler anrop mellan LLC och skikt 3. Vid upprättandet av en förbindelse används Connect Request/ Indication/ Confirm, vid brytandet av en förbindelse används Disconnect Request/ Indication/ Confirm, vid dataöverföring används Data connect Request/ Indication/ Confirm, vid återställande av en förbindelse används Reset Request/ Indication/ Confirm och för flödeskontroll används Connect Flowcontrol Request/ Indication.

Ett exempel på en förbindelse



1) Request
2) Indication
3) Request
4) Confirm

Mellan LLC och MAC finns också ett antal anrop och primitiver. Från LLC ner mot MAC finns Data Request som även måste ha destinationsadress, önskad serviceklass och dataenhet (PDU). Uppåt mot LLC har MAC primitiverna, Data Indication med tillhörande parametrar destinationsadress, avsändaradress, dataenhet, mottagningsstatus och önskad serviceklass, och primitiven Data Confirm med parametrarna överföringsstatus och effektuerad serviceklass. En dataenhet, PDU (Protocol Data Units), består av 4 fält

DSAP	SSAP	Kontroll	Data

DSAP (Destination Service Access Point) =mottagaradressfält och är en byte långt, SSAP (Source Service Access Point) =avsändaradressfält och är en byte långt, kontrollfältet är 1-2 bytes långt och datafältet 1-n bytes långt. SAP, Service Access Point, är varje punkt på någon nivå som kan upprätta en förbindelse. Datautbytet mellan två noder i ett nät sker alltså som ett utbyte av datapaket mellan de två SAP. Tre olika huvudtyper av PDU:er finns, U-format, S-format och I-format.

U-format är onumrerade, det finns alltså inget ordningsnummer eller någon form av identifikation i kontrollfältet. Kontrollfältet är alltid en oktett långt och inleds med två ettor. 8 olika typer av U-format finns:

Kontrollfält	U-format (PDU) typ
1100P000	Unnumbered Information command, UI
1100P110	Unnumbered Acknowledgement response, UA
1100P010	Disconnect command, DISC
1111P000	Disconnected Mode response, DM
1111P110	Set Asynchronous Balanced Mode Extended command, SABME
1111P101	Exchange Identification command, XID
1111P001	Frame Reject response, FRMR
1111P111	TEST

P är en Poll/Final-bit som bland annat används för att begära bekräftelse. De PDU:er som används vid en typ-1 förbindelse är UI, XID, och TEST. UI skickar en dataenhet till en annan nod. Med XID går det att testa om en nod är tillgänglig och det går att ta reda på vilka tjänster som den stöder. TEST är till för att testa överföringsförbindelsen mellan två noder. SABME är en PDU som används för att initiera en förbindelse mellan två noder. Svaret på en SABME kan bli antingen ett accepterande med ett UA eller ett nekande med ett DM. FRMR används av den mottagande noden då den har indikerat ett överföringsfel som den vill uppmärksamma den sändande noden på.

S-format har ett två oktetter långt kontrollfält där den första oktetten inleds med bitmönstret 10.

Kontrollfält	S-format (PDU) typ
1000xxxx Prrrrrrr	Receive Ready command, RR
1010xxxx Prrrrrrr	Receive Not Ready command, RNR
1001xxxx Prrrrrrr	Reject Command, REJ

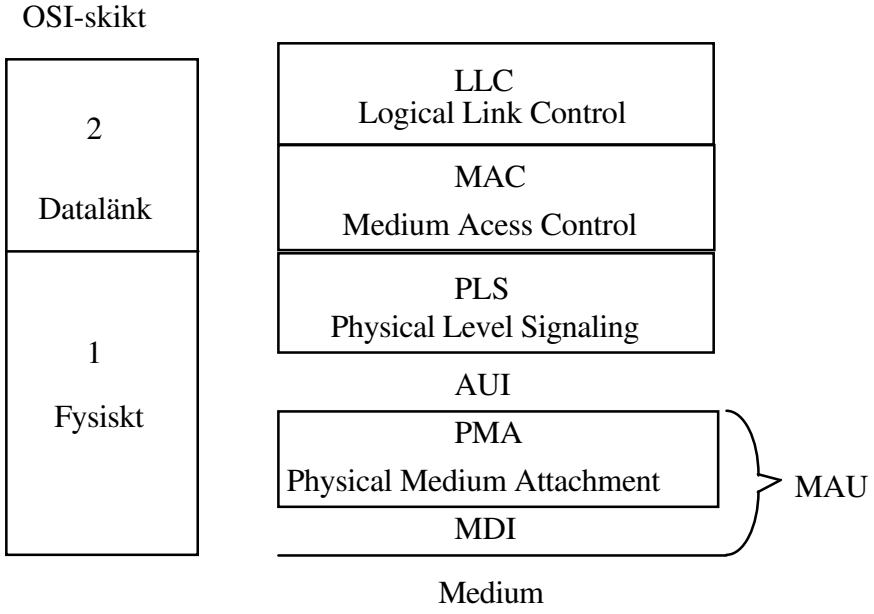
P är här samma Poll/Final-bit som i U-format, r är ett räknarfält för antalet mottagna paket och x är reserverat fält.

I-format är två oktetter långt där den första inleds med en nolla. Det finns bara en typ och den är uppbygd enligt följande: 0sssssss Prrrrrrr. s är en räknare för antalet avsända paket och r är en räknare för antalet mottagna paket. P är även här en Poll/Final-bit.

I samband med upprättandet av en förbindelse kan en fönsterstorlek bestämmas (window) efter vilken bekräftelse sedan sker. Fönsterstorleken kan vara på maximalt 127 paket eftersom räknarna som är på sju bitar och inte kan hålla reda på fler paket. Ett annat sätt att hantera detta är genom att ettställa P-biten som då talar om att bekräftelse måste ske omedelbart efter varje mottaget paket. En bekräftelse kan tex göras med Unnumbered Acknowledge (UA), Receive Ready (RR), Receive Not Ready (RNR). I-format kan användas till en jakande bekräftelse. Reject (REJ) och Frame Reject (FRMR) används till nekande bekräftelse och som också samtidigt begär en omsändning av paket. Räknarfältet kan ange från och med vilket paket som omsändning ska ske.

ISO 8802-3, fysiska skiktet:

Det finns olika standarder på den fysiska utrustningen som betecknas enligt följande:
<Överföringshastighet><BASE/BROAD><segmentlängd>
Överföringshastigheten anges i Mbit/s, nästa fält anger om det är bredband eller basband, segmentlängden anges i hundratal meter. Mer om de olika standarderna se nedan. De två lägsta skikten 1 och 2 ser ut så här:



AUI: Attachment Unit Interface
MAU: Medium Attachment Unit
MDI: Medium Dependent Interface

PLS är alltså den hårdvara som manchesterkodar signalen.
MAU är tranceivern som är anslutningen till det fysiska mediet. Det kan vara tunn koax, fiber, Twisted Pair etc.

Dataenheterna på MAC-nivå kallas ram och består av åtta fält.

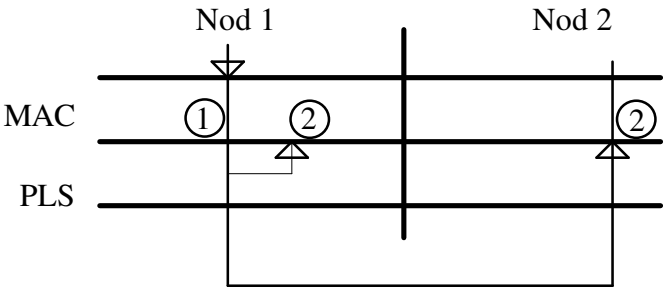
	Pre amble	SFD	Dest adress	Avs adress	Längd	LLC data	PAD	FCS
Längd	7	1	2 eller 6	2 eller 6	2	n		4

Preamble består av 7 oktetter, 56 bitar, med omväxlande ettor och nollor vilket vid 10 Mbit/s och Manchester Encoding ger en 5 MHz fyrkantvåg vilken används för att få igång och synkronisera logiken i PLS. Start Frame Delimiter, SFD, är en oktett med bitmönstret 10101011. Själva ramen börjar efter SFD. De två adressfälten är antingen 2 eller 6 oktetter långa (16 eller 48 bitar). Standarden stöder bägge men endast en kan förekomma samtidigt i ett nät. Den första biten i mottagaradressen talar om ifall det rör sig om en gruppadress eller en individuell adress. Ett anrop till alla noder, broadcast, görs genom att sätta alla bitar till 1. För 6-oktettsformatet används 2 bitar för skilja mellan lokala och globala adresser. Avsändaradressen används inte av något skikt i standarden utan skickas bara vidare. Längdfältet är på två oktetter och den anger hur långt datafältet är eller snarare hur många av tecknen i datafältet som är data. Datafältet fylls ut med lite krafs om det inte uppfyller minimilängden. LLC data är LLC:s PDU som skickar rätt igenom MAC utan några förändringar. PAD-fältet är det fält som används för utfyllnad ifall datafältet är så litet att det inte uppfyller minimilängden. FCS-fältet består av en 32-bitars kontrollsumma som beräknas

enligt en polynomalgoritm för bitfälten från och med första adressfältet till och med PAD-fältet. Denna kontrollsumma, CRC (Cyclic Redundancy Check), skickas med och jämförs på mottagarsidan med en likadan framräknad kontrollsumma. Är de olika är ramen felaktig och accepteras ej. LLC-data och avsändaradress skickas rakt igenom MAC och kan användas godtyckligt av högre skikt. I DECnet utnyttjas längdfältet för att tala om för högre skikt vilket protkoll som används istället för att ange datafältets längd enligt standarden. Detta är möjligt genom att de koder man använder för detta indikerar datafält som ger större ram än tillåtet, och därför ignoreras av MAC-skiktet. En ethernet-ram är snarlik en MAC-ram där det enda som skiljer dem åt är att istället för ett längdfält på 2 oktetter finns där ett typfält på 2 oktetter som talar om vilken typ av protokoll som används på nivån över ethernet, t ex TCP/IP, DECnet, Xerox NS. En ethernet-ram ser ut på följande vis:

	Pre amble	SFD	Dest adress	Avs adress	Typ	LLC data	PAD	FCS
Längd	7	1	6	6	2	n		4

Det MAC gör är att dels sköta om datahanteringen (datainkapsling, adressering och felkontroll) och dels hantera accessen till nätet. De serviceprimitiver som MAC använder mot LLC är Request och Indication. Request är en begäran från LLC om dataöverföring från den egna LLC:n till en annan LLC i en annan nod. Till request skickas parametrarna, destinationsadress, dataenhet och serviceklass. Indication är en indikering upp till LLC att MAC har tagit emot ett inkommande paket. Parametrarna till Indication är destinationsadress, avsändaradress, dataenhet och mottagningsstatus. Serviceprimitiver ner mot PLS är Request och Indication. När MAC gör en Request för att skicka data till en annan MAC i en annan nod får den själv också en Indication från PLS.



1) Request
2) Indication

PLS har även primitiverna CARRIER.indication och SIGNAL.indication som bägge används för att MAC ska kunna sköta accesshanteringen. Carrier indikerar med sina två lägen, on och off, för MAC om en bärvåg finns eller ej. Carrier slås på och av när PMA detekterar att en bitström inleds eller avslutas på kabeln. Signal indikerar kvaliteten på signalen och används bland annat till för att indikera kollissioner. Kollisionshanteringen görs på följande vis: En process kallad Deference kontrollerar om nätet är ledigt eller ej (Carrier Sense). Om nätet var upptaget startar ett Deferring-tillstånd. När så nätet blir ledigt initieras en fördröjning på en "inter frame spacing" varefter det väntande paketet skickas iväg. Om kollision uppstod sänds en störsignal och sändningen avbryts. En backoffprocess startar som beräknar en väntetid innan det är dags för att försöka sända igen. Väntetiden beräknas enligt $0 <= r < 2^k$, där k=min(n, backoffLimit), n= antalet misslyckade omsändningsförsök, och backoffLimit vanligtvis är satt till 10. Väntetiden blir då en multipel av slotTime som är tidsbehovet för den kortaste möjliga ramen. Första omsändningen sker alltså efter 0 eller 1 SlotTime, andra efter 0-3, tredje efter 0-7 osv upp till 0-1024. Denna algoritm kallas "Truncated binary exponential backoff".

För 10 Mbit/s anger standarden följande parametervärden:

Benämning	Betydelse	Värde
slotTime	Vänteenhet efter kollision	512 bit times
interFrameGap	Avståndet mellan ramar	9.6 µs
attemptLimit	Max antal omsändningsförsök	16
backoffLimit	En beräkningsparameter	10
jamSize	Störsignallängd	32 bits
maxFrameSize	Max ramlängd	1518 oktetter
minFrameSize	Min ramlängd	64 oktetter
adressSize	adresslängd	48 bits

MAU, Medium Attachement Unit, består av PMA, Physical Medium Attachment, och MDI, Medium Dependent Interface. MAU kallas också i vardagstal för transceiver. AUI är droppkabeln mellan ethernetkortet och transceivern och PLS sitter på nätverkskortet.

MAC:s uppgifter kan sammanfattas enligt följande:
Sänder ramar:
1) tar emot data från LLC
2) Kontrollerar om det behövs någon utfyllnad occh skapar i sådana fall ett PAD-fält.
3) Kontrollerar att det är ett helt antal oktetter i ramen och bräknar CRC (kontrollsumma).
4) Lägga till inledningen i form av Preamble och Start Frame Delimiter och adressfältet i början.
5) Sända ut hela ramen bit för bit (seriellt) till PLS.

Tar emot ramar (och tar isär):
1) Acepterar en ram från PLS (seriell överföring).
2) Kontrollerar att det är rätt destinationsadress (individuell adress, gruppadress eller broadcast).
3) Kontrollerar längden på ramen så att den är tillräckligt lång och att CRC stämmer med den som MAC räknar ut.
4) Skalar bort preamble, Start Frame Delimiter (SFD) och adressfält. Skalar också bort en eventuell PAD efter att ha undersökt längdfältet.
5) Skickar data till LLC

Undviker kollisioner:
1) Låter bli att sända när nätet är upptaget.
2) Väntar en viss fastställt tidsperiod när nätet väl är ledigt.

Hanterar kollisioner:
1) När kollision uppstår sänder MAC ut en störsignal bestående av ett slumpmässigt bitmönster med längden jamSize så att andra noder skall hinna upptäcka att en kollision har inträffat.
2) Efter kollision räknas ett slumptal fram varvid MAC väntar den slumptiden innan ett nytt sändningsförsök görs.
3) Om nätet nu är ledigt sänds data ut.
4) Om en ny kollision inträffar görs upprepade försök enligt ovan med maximalt attemptLimit antal gånger varefter ett felmeddelande genereras.

Olika Ethernet-standarder:

10BASE2 tunn ethernet, 50 ohm koax, maxlängd för ett segment 185m. Byggs i bussnätform.

10BASE5 tjock ethernet, 50 ohm tjock koax, maxlägd för ett segment 500m. Byggs i bussnätform med ring-markeringar på kabeln var utrustning kan kopplas in.

10BASE-T tvåtråd ethernet, 100 ohm partvinnad kabel, maxlängd 100m.
Tre typer av TP-kabel finns:
oskärmad kabel, UTP (unshielded)
med plasthölje, FTP (foiled)
skärmad, STP (shielded)
TP-kabel finns i olika kategorier, kategori 1 som klarar av mindre än 1Mbit/s, kategori 2 som klarar av max 4Mbit/s, kategori 3 som klarar av max 10Mbit/s, kategori 4 som klarar av max 16Mbit/s, och kategori 5 som kan klara upp till 100Mbit/s. TP-nät byggs i stjärnnätform med någon form av hub i mitten som i sin tur brukar vara ansluten till ett större nät exempelvis 10BASE2, 10BASE5, fiber etc.

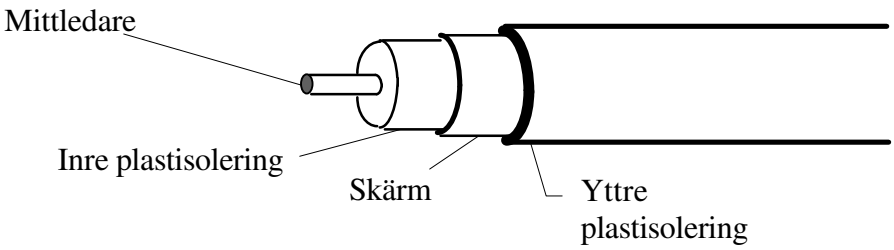
10BASE-F innehåller tre olika typer av fibertillämpningar, FOIRL, 10BASE-FA och 10BASE-FP
FOIRL (Fiber Optic Inter Repeat Link), optofiber-ethernet. Är antagen som tillägg till IEEE 802.3 och till ISO 8802-3. FOIRL kan kopplas ihop med ett nät bestående av 10BASE2 och/eller 10BASE5 genom en fibertransceiver, FOMAU, Fiber Optic Media Access Unit. Ett nät får inte bestå av mer än ett FOIRL segment med en längd av 1 km eller två på 500 m vardera.

10BASE-FA innebär en fiberoptisk aktiv kopplingsenhet även kallad AFOHU, Active Fiber Optic Hub Unit, alltså ett aktivt fiberoptiskt nav.
10BASE-FP Passiv fiberoptisk kopplingsenhet kallad PFOHU, Passive Fiber Optic Hub Unit. En vidarekoppling sker med hjälp av prismor. Maxradien är på 500 meter.
10BASE-FL ersätter FOIRL.
10BASE-FB är till för att koppla ihop repeatrar och är inte direkt tänkt för att koppla in några noder.
Fibernät byggs punkt till punkt. Dessa punkter går att logiskt bygga som ihop till en ring. Så görs t ex med FDDI. Varje punkt består sedan av någon utrustning som har olika typer av anslutningsportar så som 10BASE2, AUI, 10BASE-T

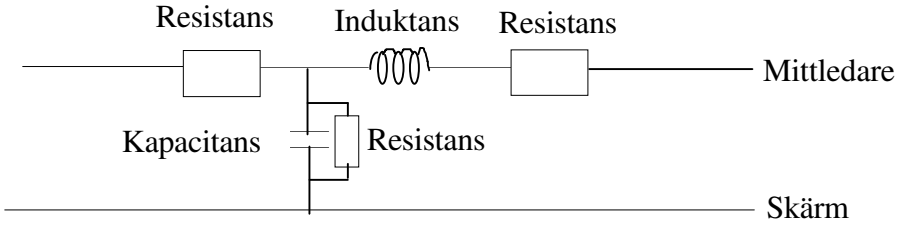
Multimode fiber kan användas i segment om upp till 2 kilometer.
För längre sträckor används singlemode fiber.

Med 50 ohm och 100 ohm ovan menas impedans.

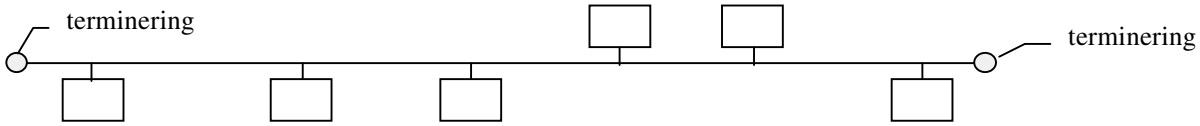
I ett 10Base2-nät byggs nätet upp med hjälp av tunna koaxialkablar.



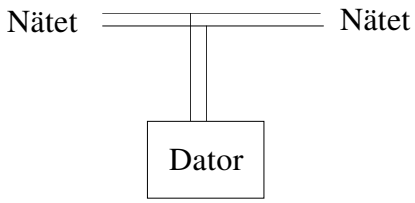
En koaxialkabel ser elektriskt ut så som bilden nedan visar. Tack vare den resistans och kapacitans som finns i kabeln dämpas alla elektriska signaler. Vanligt är 9dB på 100 meter. Den resistans och kapacitans som finns i kabeln ger kabeln dess impedans.



Då datasignalerna är högfrekventa beter de sig som radiovågor eller som vågor i ett hav. Ett avbrott eller en kortslutning på kabeln ger reflektioner som studsar tillbaka i kabeln. För att undvika detta termineras kabeln med ett motstånd (en resistor) mellan skärm och mittledare. Detta motstånd ger en oändlig utsträckning av kabeln för de högfrekventa signalerna. I ett nät med tunn ethernet ska detta motstånd vara på 50 ohm. Av denna anledning termineras alltid en tunn koax i bägge ändar. En sådan slinga kan i RydNets fall vara långt ifrån rak fysiskt men elektriskt är den en lång rak kabel. En slinga är alltså en kabel med två termineringar och ett antal datorer inkopplade på kabeln .



Avståndet mellan två anslutna datorer (eller annan utrustning) får inte understiga 0.5 meter. En dator ansluts med hjälp av ett T-kors.



”Benet” i T-korset får under inga omständigheter förlängas. Som man kan se av skissen så gör det ingenting om ”benet” inte är anslutet till någon dator. Resten av nätet kommer fortfarande att fungera. När det gäller skillnaden mellan en skarv och ett T-kors så är det ingen större skillnad elektriskt sett.

Hur man beräknar olika parametrar för ett lite större nät

Tillsvidare se http://wwwhost.ots.utexas.edu/ethernet/10quickref/ch7
En omarbetad svensk version kommer i nästa utgåva av detta dokument.

TCP/IP:

IP nät finns i form av klass-A , klass-B och klass-C nät. För att organisera upp Internet används dessa typer av delnät. Ett A-nät är ett nät där första oktetten är bestämd där nätadministratören bestämmer över de sista 3 oktetterna till datorerna i ”hans” nät. Ett B-nät är ett nät där de första två oktetterna är bestämda och nätadministratören förfogar över de två sista. Ett C-nät är således ett nät där de tre första oktetterna är bestämda och administratören förfogar över den sista. I ett C-nät går det bara att ha 254 inkopplade datorer eftersom 0 är nätets nummer och 255 är broadcast. Till detta kommer även multicast, D-nät, för att skicka trafik till mer än en dator kontinuerligt. Detta används för video, ljud whiteboard etc.

Dessutom är IP-adresserna för de olika näten uppdelade enligt följande:

Första bitten 0 för A-nät
första två bittarna 10 för B-nät
första tre bittarna 110 för C-nät
första fyra bittarna 1110 för multicast

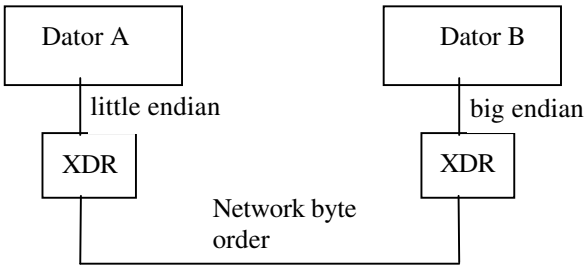
I ett nät med TCP/IP behöver man ställa in dels den egna datorns IP-adress, den närmsta routerns adress, nameserverns adress och netmask. Netmask är till för att tala om vilken trafik som är lokal för det egna nätet. Om t.ex. ett C-nät delas upp i 4 delar maskas de 3 första oktetterna bort plus de två mest signifikanta bitarna i den 4:e som talar om vilket delnät (subnät) som adresseras.
Om C-nätet har adressen 192.165.122, ska netmask vara 255.255.255.192 eller ff.ff.ff.c0 .
Ett C-nät som inte delas upp i subnät ska ha netmask 255.255.255.0 .
När man pratar om tcp/ip så menas oftast ip och någonting ovanför som vanligtvis är tcp, men inte alltid. Bilden nedan visar de olika protokollen som förekommer.

OSI SKIKT	RFS TCP/IP:	RFS XNS:	NFS
7	Streams		RPC
6	Telnet, FTP	Courier	XDR
5			
4	TCP	SPP	UDP
3	IP	IDP	IP
1 & 2	Fysiskt nät		

RFS, Remote File System, är ett filhanteringssystem som är integrerat i unix och som följer vanlig kommandosyntax. Ett filsystem tillhörande en maskin kan monteras över nätet in i filträdsystemet på en annan maskin. Ett RFS-nät delas upp i domäner med en övervakande station för varje domän som håller reda på användarnas rättigheter till de olika resurser som finns. Vid start av nätet talar varje maskin om vilka resurser som den har tillgänglig för andra. Alla maskiner kan fungera både som server och klient.

NFS som är SUNS Network File System, är väldigt lik RFS men med den skillnaden att gränssnittet upp mot applikationerna i RFS bygger på streams medans det i NFS finns ett eget Remote Procedure Call (RPC). NFS utnyttjar också virtuella filsystem vilket gör att man kan montera ett filsystem med en annan struktur än det egna. NFS använder oftast UDP förutom i solaris 2.5 och

BSD 4.4 där NFS ligger ovanpå TCP. En stor nackdel med NFS är den dåliga säkerheten, alla maskiner litar på varandra. Telnet och FTP utnyttjar TCP och IP. Under NFS och RPC finns XDR (eXternal Data Representation). XDR behövs då olika datorer använder sig utav olika representationsformer för data. En del maskiner kör till exempel med minst signifikanta byten först, little endian, andra med den mest signifikanta byten först, big endian. XDR omvandlar data till ett standardiserat format som används på nätet, network byte order. XDR i mottagaränden omvandlar data, om det behövs, till det dataformat som den mottagande datorn använder sig av.



IP, Internet Protocol är det protokoll som finns i OSI-skikt 3. Och om man ska vara petig så sträcker sig faktiskt IP upp en bit i OSI-skikt 4. IP används både till RFS och NFS förutom till XNS.

ARP, eller hur en uppkoppling görs.

Först ska nämnas att ett ethernet-broadcast är ett paket där mottagande ethernetadressen består av enbart ettor. Alla ethernetkort i alla datorer på den lokala slingan lyssnar på sådana broadcast. I vanliga fall så lyssnar ethernetkorten annars bara på sin egna ethernetadress. Ethernetbroadcast går igenom repeatrar och bryggor.

I grova drag kan man säga att det går till på följande sätt i ett IP-nät:
Dator A vill ha kontakt med dator B. Dator A skickar ut ett ethernet-broadcast och frågar efter dator B:s ethernetadress. I detta broadcastpaket finns B:s IP-nummer med så att B vet att han ska svara, plus lite annat som vi inte går in på här. Alla inkopplade datorer tar emot denna förfrågan men då de ser att det inte är till dem gör de ingenting förutom dator B. B känner nu till A:s ethernetadress och kan skicka ett svar direkt till A som därmed får reda på B:s ethernetadress. Dessa två maskiner kan nu skicka paket direkt till varandra via ethernetadressen. Alla andra datorer ignorerar dessa paket som går mellan A och B. Detta förfarande kallas ARP, Address Resolution Protocol.

Då kan man fråga sig vad är det för skillnad på och varför behövs både IP-nummer och en ethernetadress? Då man bygger upp ett nät behöver varje dator i det nätet ha en lämplig identitet. Genom identiteten ska man lättare kunna hitta i vilket nät en viss dator finns. Denna identitet är IP-adressen. Om vi har två nät, nät-1 och nät-2 som är två stycken C-nät kan utrustningen mellan de två näten, oftast en router, väldigt lätt känna igen om en dator finns på det ena eller det andra nätet genom att titta på datorns IP-adress. Ethernetadressen bestäms av tillverkaren av ethernetkortet. Detta medför att datorerna i nät-1 kan ha väldigt olika ethernetadresser. För att utrustningen mellan de olika näten ska veta var en dator finns måste den då ha en tabell över alla datorer i de olika näten. Med IP-adresser räcker det att veta var de olika näten finns. Dessutom ligger ethernet-adresser och IP-adresser i olika skikt i OSI-modellen.

Om dator A inte känner till dator B:s IP-adress måste dator A först fråga en nameserver efter B:s IP-adress.

Multicast

Istället för att kommunicera dator till dator eller skicka paketen till alla datorer kan man skapa grupper för kommunikation. Detta är speciellt lämpligt för videokonferenser, whiteboardtavlor, etc. Multicast fungerar så att man har en reserverad ethernetadress 01:00:5E:xx:xx:xx där de sista siffergrupperna fylls i beroende på vilken multicastgrupp paketet ska till. Dessutom har man reserverat IP-adresserna 224.0.0.0 - 239.255.255.255 för multicast. När en dator vill skicka ut någonting till en grupp, t ex gruppen med IP-nummer 224.0.0.1 gör den det till ethernetadressen 01:00:5e:00:00:01. De sista 3 grupperna i ethernetadressen fylls i med de sista tre grupperna i IP-adressen. Alla datorer på nätet som lyssnar på multicast får då detta paket. Ethernetkortet får av nätverkskoden i kärnan (skikt 3 i OSI-modellen) reda på att den ska lyssna på vissa multicast-ethernetadresser. I multicastpaketen finns även IP-adressen till gruppen med.

Litteraturhänvisningar:

IP, RFC 791
TCP, RFC 793
UDP, RFC 768
SLIP, RFC 1055
PPP, RFC 1331, RFC 1332, RFC 1661, RFC 1662, RFC 1663
ICMP, RFC 792
FTP, RFC 959
Telnet, RFC 854/5
Mail, RFC 821/2
POP2, RFC 937
POP3, RFC 1734
SMTP, RFC 1651, RFC 1652, RFC 1653
Subnets, RFC 950
Gateways, RFC 875

SNMP, RFC 1089, RFC 1140, RFC 1147, RFC 1155, RFC 1156, RFC 1157, RFC 1158, RFC 1161, RFC 1212, RFC 1213, RFC 1215, RFC 1298, RFC 1418, RFC 1441, RFC 1442, RFC 1443, RFC 1444, RFC 1445, RFC 1446, RFC 1447, RFC 1448, RFC 1449, RFC 1450, RFC 1451, RFC 1452, RFC 1503
How to setup a nameserver, RFC 1033
Introduction to Administration of an Internet-based Local Network
Introduction to the Internet Protocols
Firewalls FAQ
Cisco-networkning FAQ
SNMP FAQ

RFC:erna finns att hämta på gopher://ftp.sunet.se:70/11/pub/Internet-documents/rfc

Ethernet Quick Guide http://wwwhost.ots.utexas.edu/ethernet

Övrig litteratur:

Prentice Hall
Computer Networks, A Tanenbaum. En grundläggande bok om datornätverk.
Internetworking with TCP/IP volume 1, Douglas E. Comer En bok om hur TCP/IP fungerar
Internetworking with TCP/IP volume 2, Douglas E. Comer En bok om hur man implementerar TCP/IP
Internetworking with TCP/IP volume 3 AT&T TLI, Douglas E. Comer En bok om hur man programmerar ovanpå TCP/IP med hjälp av TLI.
Internetworking with TCP/IP volume 3 BSD Sockets, Douglas E. Comer en bok om hur man programmerar ovanpå TCP/IP med hjälp av sockets.
The Whole Internet User's Guide an Catalog, Ed Krol (introduktion till de vanligaste applikationerna, mail, www, ftp etc)

O'Reilly & Associates inc.

Sendmail, Bryan Costales, Eric Allman & Neil Rickert (den stora tjocka boken om hur sendmail verkligen fungerar)
DNS and BIND, Paul Albitz & Cricket Liu
TCP/IP Network Administration, Craig Hunt
Building Internet Firewalls, D. Brent Chapman & Elizabeth D. Zwicky

Övrigt

Zen and the Art of the Internet (ännu en introduktion till de vanligaste applikationerna)