Benthemstraat 15
3032 AA Rotterdam

CISCO NETWORKING

ACADEMY PROGRAM

CNAP

VOORWOORD

Waarom is het bestuderen van communicatienetwerken van belang?
Het ontwerpen, installeren en beheren van hardware en software voor communicatienetwerken is een van de snelst groeiende technieken. De groei loopt parallel aan de ontwikkeling van computers en communicatie-technologie. Computers en werkstations nemen een steeds belangrijkere plaats in het bedrijfsleven in. Steeds vaker worden gegevensbanken (data bases) met elkaar gekoppeld via een netwerk. Het bedrijfsleven kan niet meer functioneren zonder goed werkende computersystemen en netwerken. Om dit te waarborgen heeft men goed opgeleide werknemers nodig met kennis en vaardigheden op dit gebied.
Wat zou je moeten leren over communicatienetwerken?
Een algemeen begrip van de manier waarop netwerksystemen functioneren en de telecommunicatie-principes die hierbij toegepast worden, helpt iedereen die werkt met communicatienetwerken. Het curriculum biedt deze kennis aan en traint de gebruiker in het installeren en beheren van Cisco-apparatuur. De overstap naar apparatuur van een andere fabrikant is eenvoudig omdat de principes niet veranderen alleen de manier waarop.

Het Cisco Networking Academy Program is een educatief programma voor studenten van het middelbaar en hoger onderwijs op het gebied van netwerking, in veel opleidingen ook wel datacommunicatie genoemd.
Dit dictaat is een Nederlandstalig ondersteunend en aanvullend onderdeel in het CNAP-programma dat gebruikt kan worden naast het lesmateriaal van Cisco.
Het materiaal is ontwikkeld en wordt jaarlijks onderhouden door een groep gekwalificeerde instructors die werken met het programma en verbonden zijn aan diverse ROC's in Nederland.

Rotterdam juni 2002,

Nederlandse Cisco Ontwikkelgroep

INHOUDSOPGAVE

Blz.

INLEIDING

Cisco Systems Inc. is een multinational op het gebied van apparatuur voor computernetwerken. Het hoofdkantoor is gevestigd in **San Jose, California, USA.** Cisco heeft in zeer veel landen een nevenvestiging. Cisco Nederland bevindt zich in Amsterdam.
Cisco heeft, zoals bijna alle leveranciers van hardware en software een scholingsprogramma.
Dit programma is verdeeld in drie niveaus

- **Expert Level (specialisten),**
- **Professional Level,**
- **Associate Level (gebruikers/beheerders).**

Het programma is voor het associate en professional level verdeeld in twee trajecten:

- **Network (Installatie en beheer),**
- **Design (Ontwerp).**

De opleidingen zijn als volgt gecodeerd:
- **CCNA**, Cisco Certified Network Associate,
- **CCNP**, Cisco Certified Network Professional,
- **CCDA**, Cisco Certified Design Associate,
- **CCDP**, Cisco Certified Design Professional,
- **CCIE**, Cisco Certified Internetworking Expert.

Daarnaast bestaat er nog een groot aantal productspecifieke opleidingen.
Bovenstaande opleidingen zijn bedoeld voor werknemers in de ICT-branche die te maken hebben met netwerken.

In 1996 heeft Cisco gemeend een internationaal scholingsprogramma te moeten opzetten om aan de groeiende vraag naar werknemers met kennis op het gebied van computernetwerken te kunnen voldoen. Tevens kon dit bijdragen aan de bekendheid van het bedrijf en de kennis van hun apparatuur. Hierdoor hoopt Cisco zijn positie in dit marktsegment te kunnen verstevigen (een goede marketingzet dus).
Het scholingsproject kreeg de naam: **Cisco Networking Academy Program** (afgekort tot CNAP)**.**
Het scholingprogramma is bedoeld voor ICT-opleidingen op middelbaar, hoger en universitair niveau.
Het programma is in twee niveaus verdeeld: het associate level en het professional level. Elk level is verdeeld in 4 semesters (dus het totale programma omvat 8 semesters).
Het associate level is bedoeld voor middelbare beroepsopleidingen en het professional level is bedoeld voor het hoger en universitair niveau.
De scholingsinstellingen die aan het programma mee doen, mogen zich **CCNA** (**Cisco Certified Networking Academy**) noemen. De docenten hebben de **CCAI** (**Cisco Certitied Academy Instructor**) bevoegdheid.
ROC Zakine is een **CRNA** (**Cisco Regional Networking Academy**), waar opleidingen op het associate level (semester 1 t/m 4) worden gegeven aan studenten en waar instructors van locale academies worden opgeleid.

De leerstofinhoud van semester 1 t/m 4 is gebaseerd op de onderwerpen uit het CCNA, CCDA-programma en het A+ programma maar heeft een meer algemene opbouw.

Voor het overbrengen van theoretische kennis heeft men gekozen voor het **e-learning** principe. Het lesmateriaal wordt dus op een computer aangeboden en kan via de browser worden bekeken.

De inhoud bestaat uit tekst met grafische voorstellingen, animaties, simulaties en gesproken tekst. Daarnaast is er een groot aantal **weblinks** aanwezig die je doorverwijzen naar sites waar aanvullende informatie te vinden is.

De studenten kunnen het materiaal bestuderen in het CISCO-lokaal. Op een server is het lesmateriaal opgeslagen zodat voldoende snelheid gewaarborgd is.
Cisco heeft het materiaal ook op zijn **community server** staan. Om hiervan gebruik te kunnen maken moet je in het bezit zijn van een Internetverbinding met voldoende bandbreedte en een **username** met **password** om in te kunnen loggen.

De username en het password worden door de docent verstrekt. De site voor studenten heeft de volgende URL: http://students.netacad.net/

Het lesmateriaal van een bepaald semester is verdeeld in hoofdstukken. Elk hoofdstuk begint met een review, dit zijn een aantal open vragen bedoeld om je kennis van het vorige hoofdstuk te testen. Daarna moet het lesmateriaal doorgenomen worden. Afsluitend is er een quiz met 10 meerkeuze vragen over de leerstof van het hoofdstuk.
Na bijna elk hoofdstuk moet er een meerkeuze toets gemaakt worden (soms een toets over meerdere hoofdstukken). Deze toetsen bevinden zich op de **assessment server** van Cisco. Dit zijn **evaluatietoetsen** die de kennis van geleerde onderzoeken. Om een toets te kunnen maken moet je kontact maken met de assessment server via de volgende URL: http://cisco-aas.netacad.net/. Hier wordt weer gevraagd om een username en bijbehorend password.
Aan het eind van een semester moet de **final** toets gemaakt worden. Dit is een toets die onderdeel uitmaakt van je eindcijfer. Cisco verstrekt per semester een certificaat als de score van de final toets **70% of hoger** is. Voor het behalen van het semester binnen de opleiding is een score van **60% of meer** nodig (scores onder de 70% leveren echter geen Cisco certificaat op).

Naast het theoretische deel bevinden zich in het programma ook een aantal practicumopdrachten (**LAB's**). Hiervoor is een practicumopstelling met 10 computers en een netwerk met routers, een switch en hub's aanwezig. Gezien het beperkte aantal practicumplaatsen en het grote aantal studenten is hiervoor een strakke planning nodig. Daarom is elke student verplicht, om op de ingeroosterde uren, in het Cisco-lokaal aanwezig te zijn. Het verzuimen van de lessen betekent dan al heel snel dat de labs niet uitgevoerd kunnen worden en het gehele semester in een volgend halfjaar opnieuw gedaan moet worden.
Labs worden individueel of in groepen uitgevoerd. Naast de labs waar de practicum opstelling voor nodig is, zijn er ook labs die thuis gemaakt moeten worden.
Elk semester wordt afgesloten met een individuele **final lab**. Op de helft van een semester wordt een toets afgenomen over het eerste deel.

Het slagen voor een semester wordt bepaald door:

- De score van de halfsemester toets en de final toets (=> 60%),
- De score van de final lab (voldoende),
- De uitvoering van de labs (alle opgegeven labs),
- De aanwezigheid in de lessen (=> 80%)
  (een te lage opkomst betekent uitsluiting van de finals).

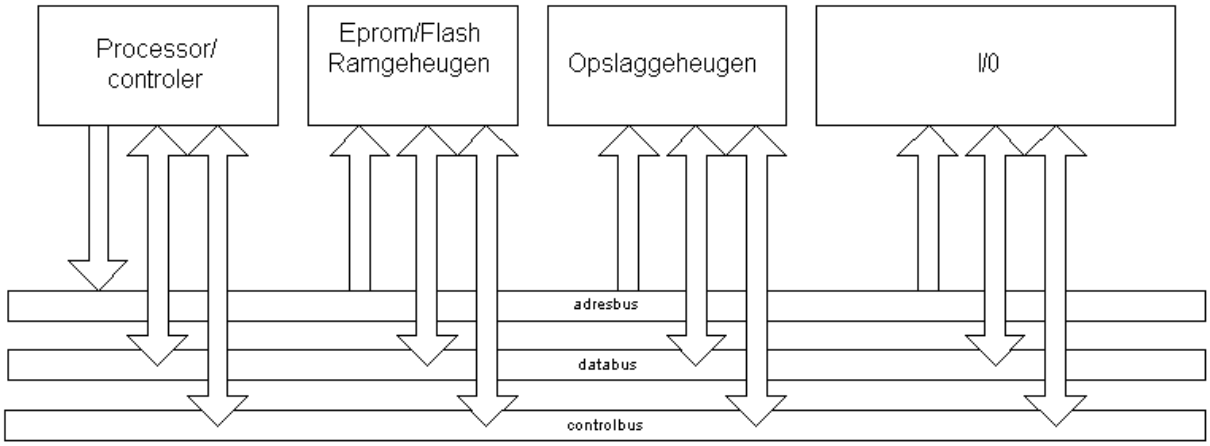
Dit zijn ook de criteria die bij de externe legitimering worden gehanteerd!!

1 SEMESTER 1

1.1 Computer basics

Computer hardware/software
Alle onderdelen van een computernetwerk die met elkaar communiceren, kunnen we zien als computersystemen.
Om netwerken te installeren en te beheren is een goede kennis van computersystemen noodzakelijk.
Al eerder zijn de hardware en software-onderdelen besproken, zodat wij ons nu beperken tot de behandeling van de onderdelen die voor netwerken van belang zijn.
Een computersysteem bestaat uit:

- Een voeding. Een computersysteem is een elektronische apparaat;
- Processor/controler. Dit is het hart van een systeem dat de software-instructies uitvoert;
- Intern geheugen, Eprom/flash voor de BIOS, Ram voor programma-opslag, werkruimte voor programma, data en cache;
- Opslag geheugen (HD, FD, CDROM, ZIP, Tape), voor opslag van programma's en data files;
- I/O-elektronica voor aansturing van I/O-onderdelen, zoals: keyboard, muis, printer, opslaggeheugen, monitor, audio, IR, netwerken;
- Bussysteem. De elektrische verbindingen tussen de onderdelen. De computer heeft op het moederbord een **parallel** systeem bestaande uit een **adresbus** om aan te geven naar/van welk I/O register of geheugenplaats de processor data wil transporteren. Een **databus** waarover de data getransporteerd wordt en een **controlebus** om te zorgen dat dit proces goed verloopt. Het transport naar externe I/O onderdelen gebeurt in bijna alle gevallen via een **seriële bus,** zoals: het keyboard, de muis, USB/Firewire-onderdelen, modem en netwerkverbindingen. Er is maar één **parallelle** verbinding waarop meestal een printer wordt aangesloten.
- Software. Het operating system, drivers voor I/O en applicaties.



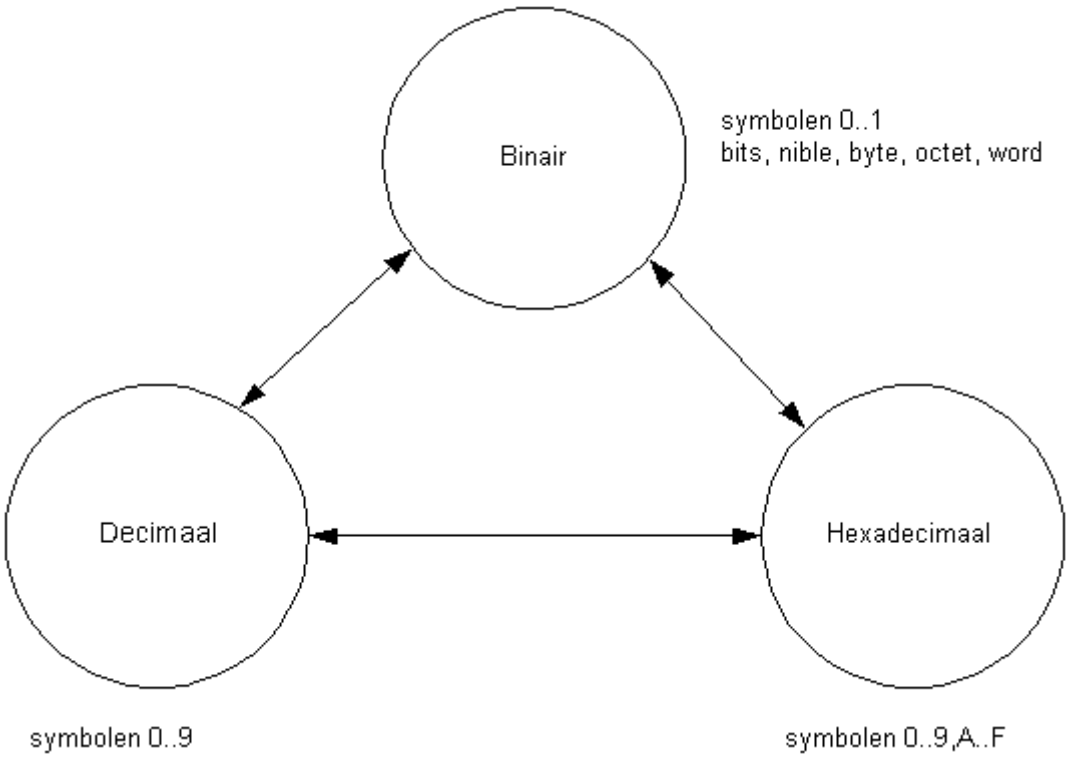
Om een computersysteem in een netwerk te kunnen gebruiken, moeten we kennis hebben van het installeren en beheren van de hardware-onderdelen zoals modem (RS232C, COMx) en NIC (network interface card), de OS- instellingen en de aanvullende software voor het modem, de netwerkkaart, IIS, Webbrowser, FTP en e-mail.

De hardware voor de modemverbinding is standaard aanwezig en wanneer de NIC niet geïntegreerd is op het moederbord dan wordt deze in een vrij ISA/PCI-slot (in een desktop-model) geplaatst of in een PCMCIA-slot (in een laptop).
Na de hardware-installatie moeten er diverse instellingen aangebracht worden. Dit gebeurt in MS-Windows systemen door, via het control panel, het dial-up-, network- of pcmcia-icoon te activeren. Voor de dial-up betekent dit het invullen van de instellingen en voor de netwerkkaarten het laden van

een driver, het aangeven van de gebruikte protocollen met hun instellingen en het activeren van de nodige netwerkservices.
Wanneer gebruik gemaakt wordt van netwerkapplicaties zoals: webbrowser, FTP, e-mail en/of IIS dan moet deze software geïnstalleerd worden en de juiste instellingen geplaatst. Dit vraagt een goede kennis van deze applicaties.

Met de Windows management tools en commando's als 'winipcfg', 'ipconfig', 'ping' en 'trace' kan de status bekeken en getest worden.

Binaire getallen
Een computer is een elektronisch apparaat dat werkt met elektrische signalen die twee toestanden kunnen aannemen. Deze toestanden kunnen weergegeven worden met een 0 of 1. Een reeks nullen en enen stelt een bepaald gegeven voor zoals getallen, tekst, vectoren, geluid enz. De processor verwerkt deze gegevens als getallen en de I/O-onderdelen interpreteren dit als tekst, vectoren voor tekeningen, frequenties voor audio enz.
De relatie tussen de getallen en de betekenis is vastgelegd in gedefinieerde data formaten zoals: ASCII, Unicode, Postscript, au, avi enz.
Omdat de processor de gegevens ziet als getallen die bestaan uit cijfers met twee waarden (0, 1) kunnen we deze getallen zien als binaire waarden. Een cijfer noemen we een **bit** en omdat de processor werkt met reeksen van bits zijn hiervoor ook benamingen gemaakt: een groep van 4 bits heet een **nibble**, een groep van 8 bits heet een **byte** of een **octet** en een groep van 16 bits een **word**.
Een gebruiker wil kunnen communiceren met een computer via decimale getallen en tekst. De applicatie vertaalt de ingevoerde symbolen naar binaire getallen en omgekeerd voor de presentatie van de symbolen.
Een andere manier om een reeks nullen en enen aan te geven is door groepjes van 4 bits weer te geven met één symbool. Een reeks van 4 bits kan uit 16 verschillende nul-één-combinaties bestaan. Dit komt overeen met het 16-tallig of hexadecimale stelsel met de symbolen 0..9,A..F.
We dienen dus kennis te hebben van:
- binaire getallen om een computer te kunnen begrijpen,
- decimale getallen en de omzetting naar binaire getallen,
- hexadecimale getallen omdat hiermee reeksen nullen en enen verkort worden weergegeven.

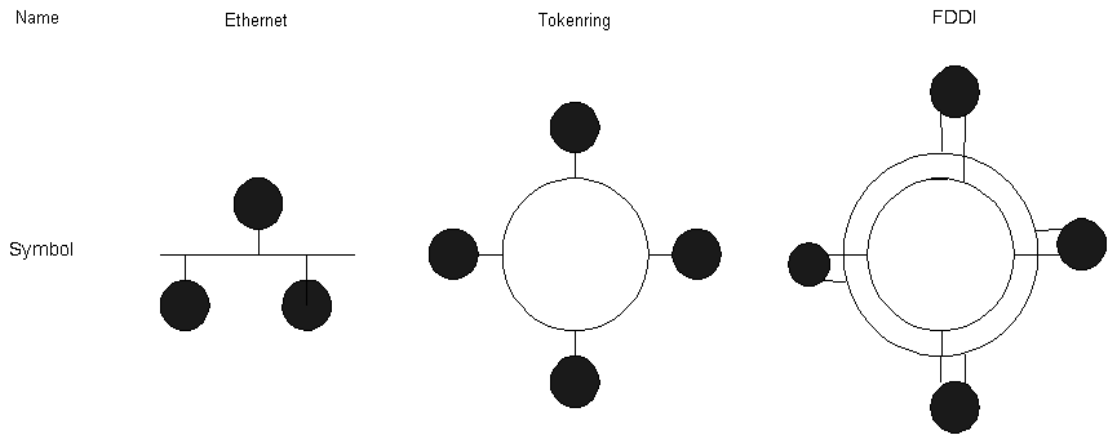


In een netwerkomgeving wordt gewerkt met adressen om een computer te identificeren. De computer gebruikt hiervoor een reeks nullen en enen.
Het hardware- of MAC-adres bestaat bij ethernet uit een 48 bits binair getal dat hexadecimaal wordt weergegeven.
$00001010.10110101.01110110.01100110.10111001.10000110_{bin}$ = $0A.B5.76.66.B9.86_{hex}$.
Het logische adres bij het IP protocol bestaat uit 4 bytes (32 bits) en wordt met 4 decimale getallen gescheiden door punten weergegeven. $10110000.10100000.00110100.0010000_{bin}$ = $176.160.52.32_{ddf}$ (DDF is dotted decimal format).
In het cursusmateriaal wordt uitgebreid ingegaan op deze talstelsels en de conversies.

Netwerken
Netwerken is een veel gebruikt begrip zoals: een netwerk van wegen, een netwerk van waterwegen, een groep kennissen, het telefonienetwerk enz. De wegen en rivieren worden gebruikt om personen en/of goederen met een vervoersmiddel van plaats A naar B te brengen.
Onder een computernetwerk verstaan we een aantal computers en randapparatuur die via een netwerkmedium en netwerkapparatuur met elkaar communiceren of data uitwisselen. We spreken hier over een **data netwerk**.

In de loop van de tijd zijn er verschillende netwerktypen ontwikkeld. De keuze van het type is afhankelijk van de **hoeveelheid data** die tussen de computers wordt getransporteerd en de **betrouwbaarheid** van de verbindingen. Als er veel data verkeer is, vraag dat om een snel netwerk. Bedrijven die afhankelijk zijn van het goed werken van het netwerk vragen om een netwerk dat, bij het uitvallen van een netwerkapparaat of een verbinding, niet volledig onbruikbaar is maar de mogelijkheid biedt voor een alternatieve route.

Een intensief data verkeer vindt vooral plaats tussen de PC's en servers binnen bedrijven. Hiervoor worden snelle netwerken gebruikt die voldoende snelheid kunnen leveren over relatief korte afstanden, van 100m tot enkele kilometers. We noemen dit **LAN**'s (**Local Area Network**). We onderscheiden drie typen: Ethernet, Tokenring en FDDI.



Deze netwerken hebben een snelheid van 4Mbps t/m 1Gbps.

Het data verkeer tussen LAN netwerken is veel minder intensief en de onderlinge afstanden bedragen meestal vele kilometers. De netwerken die de LAN's verbinden noemen we **WAN**'s (**Wide Area Network**)

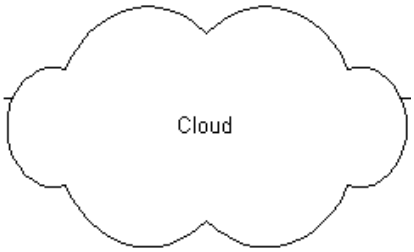
Name WAN link

Symbol 

De verbinding met een WAN wordt gemaakt met een Wan link. We kennen een aantal verschillende links:

- een analoog modem via een telefoonverbinding,
- een ISDN-verbinding, (Integrated Services Digital Network)
- een Frame relay-verbinding,
- een ADSL-verbinding, (Asymmetric Digital Subscriber Line)
- een cable-modem via een kabelnet.

De verbindingen en de netwerkapparatuur van een WAN zijn meestal geen eigendom van de gebruiker, maar van kabelmaatschappijen zoals KPN en UPC.
We huren een verbinding en het gebruik van een WAN van de eigenaar van het netwerk. Wanneer de verbinding voor één gebruiker bestemd is, noemen we dit een **huurlijn**. Wanneer binnen de WAN de verbindingen gedeeld worden door verschillende gebruikers, huren we **bandbreedte**.
Wanneer we de samenstelling van een netwerk niet kennen of niet willen weergeven dan gebruiken we een wolk (**Cloud**) als symbool in een schema.



Een ander netwerk waarmee tegenwoordig bijna alle LAN's verbonden zijn, is het wereldwijde **Internet**. Dit is een WAN tussen alle aangesloten netwerken. De hogere lagen van dit Internet bestaan uit **ATM** (Asynchronous Transfer Mode) netwerken.

Naast de LAN en WAN is er nog een aantal netwerktypen zoals:

- WLAN(wireless local area network). Het gebruik hiervan neemt sterk toe,
- MAN (metropolitan area network). Een verbinding van LAN's binnen zeer grote bedrijven zoals Shell Pernis,
- PAN (personal area network). Een netwerk binnen woningen waarin alle elektronische apparatuur is opgenomen.

Bandbreedte
Het begrip bandbreedte geeft aan hoeveel data er per tijdseenheid door een netwerkverbinding getransporteerd kan worden. De hiervoor gebruikte eenheid is **bps** (**bits per second**). Een ethernetverbinding kent verbindingen met een bandbreedte van **10Mbps, 100Mbps** of **1Gbps**, een analoge modem verbinding werkt meestal met **56Kbps** en een ISDN verbinding haalt een snelheid van **128Kbps**. Als we een bestand willen downloaden van **10MB** (mega byte) dan duurt dit, over een 10Mbps verbinding, in theorie 8 seconden (1 byte is 8 bits).

In de analoge telecommunicatie druk men de bandbreedte uit in **Hz** (perioden per seconde). Een databit wordt in bepaalde ethernetverbindingen gecodeerd binnen twee perioden. Een ethernetverbinding met een data bandbreedte van 10Mbps heeft dus een kabel nodig die een analoge bandbreedte heeft van 20MHz.

Throughput
Het begrip throughput geeft de **effectieve bandbreedte** van een verbinding op een bepaald moment voor een gebruiker. Enkele factoren die de waarde ervan beïnvloeden,

- De hoeveelheid data die gebruikers transporteren,
- Snelheid van de PC's, servers en netwerkapparatuur,
- Netwerktopologie,
- Hoeveelheid netwerkmanagement activiteit,
- Moment. Internet is 's ochtends sneller omdat het in Amerika nacht is, waardoor er minder gebruikers op het net actief zijn,
- Aantal gebruikers. De beschikbare bandbreedte moet gedeeld worden door het aantal gebruikers.

Een van de belangrijkste facetten bij het ontwerpen van een netwerk is het bepalen van de benodigde effectieve bandbreedte en daarbij rekeninghoudende met de toekomstige ontwikkelingen van een bedrijf. Dit is van groot belang voor het bepalen van het netwerktype, de topologie, de keuze van netwerkapparatuur en de bandbreedte van de te gebruiken media.

Vragen en opdrachten

1. Geef een algemene omschrijving van een computer.

2. Welke hardware onderdelen kunnen gebruikt worden om een PC te koppelen aan een netwerk?

3. Op welke manier kunnen we binnen een Windows O.S. de software voor deze netwerk-verbindingen instellen?

4. Met welke commando's we de netwerkinstellingen van de NIC zichtbaar maken?

5. Welke commando's kunnen we gebruiken om een netwerkverbinding te testen?

6. Geef de symbolen en hun naam die in netwerkschema's gebruikt worden.

7. Op welke manieren kunnen we verbinding maken met een WAN?

8. Geef een omschrijving van de begrippen bandbreedte en throughput.

9. Geef omschrijving van de volgende begrippen:
   - Motherboard, FD, HD, CDROM, USB, NIC,
   - Bussysteem, parallelle bus, seriële bus,
   - IIS, Webbrowser, FTP, e-mail,
   - LAN, WAN, MAN WLAN, WAN-link,
   - Ethernet, Tokenring, FDDI,
   - ISDN, Cable modem,
   - Binaire talstelsel, decimale talstelsel, hexadecimale talstelsel,
   - Bit, nibble, byte, octet, word,
   - Bandbreedte, throughput.

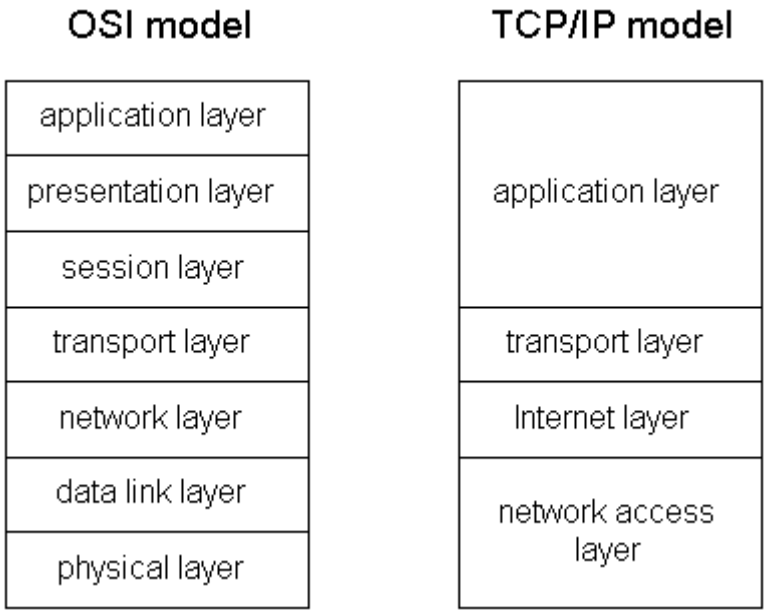
Aantekeningen.

1.2 OSI- en TCP/IP reference model

In de beginjaren van de computernetwerken maakte elk bedrijf zijn eigen hardware en software in zijn computers om datacommunicatie te realiseren. Dit betekende dat in een IBM-netwerk alleen IBM-apparatuur en software te gebruiken was en er geen communicatie met computers en netwerken van andere fabrikanten mogelijk was zonder speciale apparatuur en software toe te passen. Er was dus geen uniformiteit in datacommunicaties.

Het ministerie van defensie (D.o.D. Department of Defence) van de VS heeft als eerste opdracht gegeven om regels op te stellen. Dit heeft geleid tot het **TCP/IP reference model**. Dit is een beschrijving van alle onderdelen die nodig zijn om computerapplicaties via een netwerk met elkaar te laten communiceren. Het beschrijft de hardware zoals de netwerkinterface, connectoren, bekabeling, elektrische eisen ed.en de software-functies. Een nadeel was dat het gekoppeld is aan de TCP/IP **protocol set** (**groep regels**). Bedrijven als IBM, Digital, Novell en Apple gebruiken andere protocollen.

In 1984 heeft het Internationale normaliseringinstituut ISO (**International Organization for Standardization**) het **Open Systems Interconnection (OSI) reference model** beschreven. Deze norm is op dit moment de algemene standaard. De Amerikaanse regering heeft bij wet vastgelegd dat alleen nog maar apparatuur gebruikt mag worden die deze norm ondersteunt.

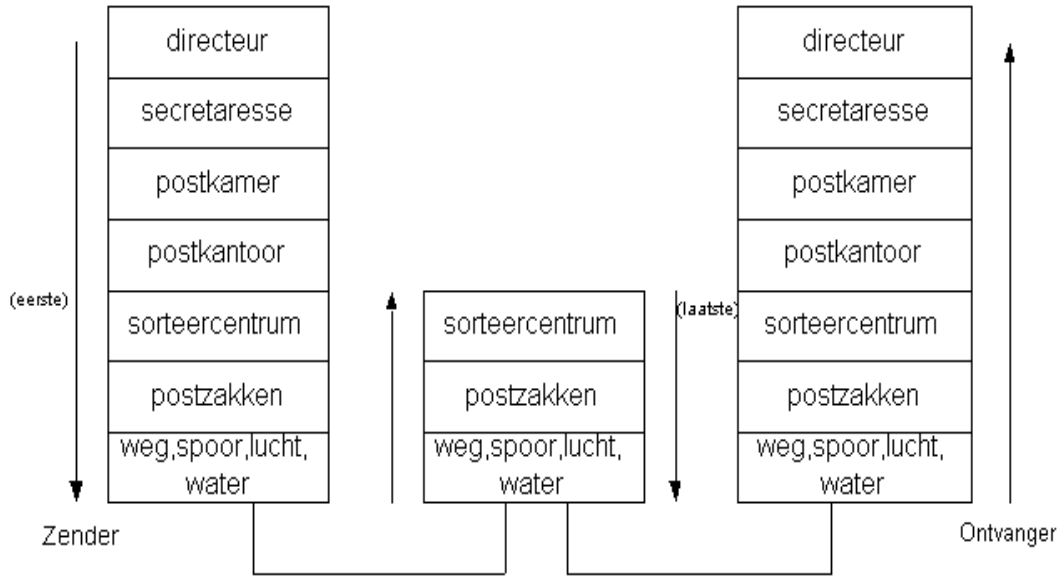


Het model is in lagen (layers) of schijven verdeeld. Dit is gedaan omdat:
- het bestuderen van een duidelijk omschreven deel eenvoudiger is dan het geheel,
- de maker van een netwerkkaart alleen maar de onderste drie layers nodig heeft.
- fabrikanten een product kunnen maken die de functies van een of meer layers invullen en kunnen samen werken met producten van andere fabrikanten voor de aangrenzende layers. Dus het model kan opgebouwd worden met producten van diverse producenten.

In het model worden de functies van de afzonderlijke lagen beschreven en de manier waarop de lagen informatie uitwisselen. De koppeling tussen de lagen noemen we een interface.

Om enig begrip van de werking van een model te krijgen gebruiken we als voorbeeld de organisatie-structuur die binnen bedrijven gebruikt wordt.
Als de directeur van een Nederlands bedrijf een bericht wil versturen naar een firma in Frankrijk dan schrijft hij zijn bericht en geef dat aan zijn secretaresse. De secretaresse weet dat het bedrijf in

Frankrijk het bericht in het Frans verwacht en vertaalt het bericht. Het bericht wordt doorgegeven aan de postkamer die het bericht inpakt en de verpakking voorziet van een bestemming (destination adres) en een afzender (source adres). Een grote zending wordt verdeeld over meerdere pakketten. Door een codering aan te brengen kan de ontvanger zien uit welke pakketten de totale zending bestaat en wat de volgorde is. Men kan dan ook zien of een deel van het bericht niet is aangekomen en vragen om dit nogmaals op te sturen.
De pakketten worden afgeleverd bij het postkantoor. Dit is verantwoordelijk voor de bezorging van het bericht.
De pakketten gaan naar het sorteercentrum die aan de hand van de adressering kunnen bepalen via welke weg de pakketten naar de plaats van bestemming vervoerd moeten worden. De pakketten worden afhankelijk van de manier van vervoeren (weg, lucht, spoor) opnieuw verpakt in postzakken. De postzakken worden via een van de vervoersmanieren verplaatst.
Bij het vervoer over grote afstanden worden de pakketten meerdere keren door een sorteercentrum verwerkt en via dezelfde of een andere vervoersmanier verder getransporteerd.



Uiteindelijk komt het bericht bij het laatste sorteercentrum. Hier is de fysieke plaats van het bedrijf bekend en wordt het bericht daar afgeleverd. In de postkamer wordt gekeken voor welke persoon of afdeling het bericht bestemd is en eventueel via een secretaresse bereikt het bericht zijn bestemming.

In bovenstaand communicatie model kunnen fouten gemaakt worden die de communicatie verstoren. Dit komt vooral omdat het mensenwerk is. Om het aantal fouten zo klein mogelijk te houden en om gemaakte fouten te kunnen herstellen worden er voor elke laag, regels vastgelegd (protocol) waaraan iedereen zich dient te houden.

Bij de communicatie tussen computersystemen is de invloed “mens” op het proces gereduceerd tot het communiceren met een applicatie (programma). De programma’s maken via API (application programming interface) contact met software modules die de functies van een laag uitvoeren via een vastgestelde set regels. De lagen geven de gegevens aan elkaar door voorafgegaan door informatie (header) die de volgende laag nodig heeft om de communicatie te kunnen voortzetten. De informatie in de headers wordt begrepen door de overeenkomstige laag in het destination systeem. Het doorgeven van de gegevens+header gebeurt in een computer via **buffers** en **pointers**.

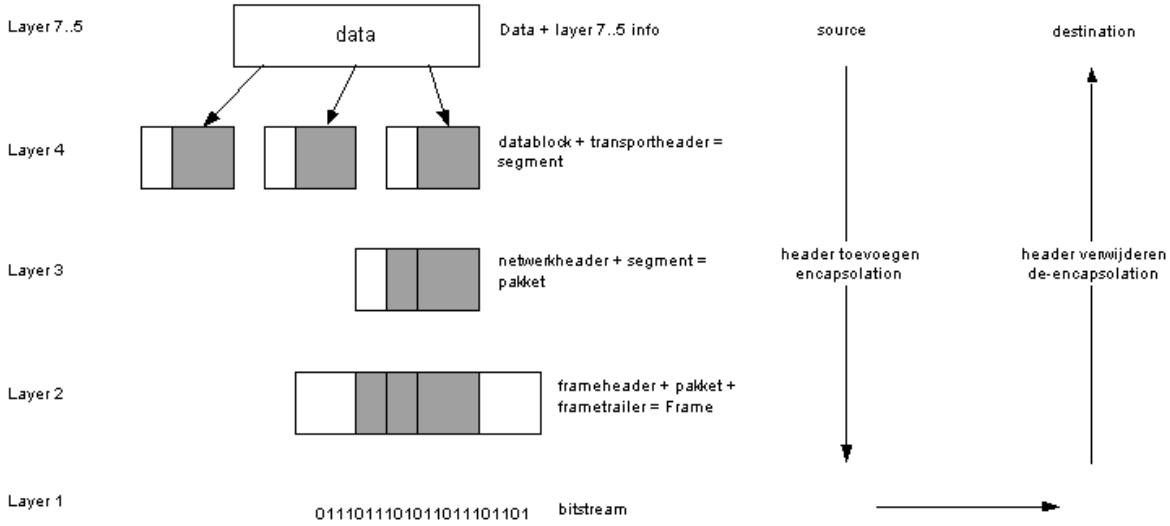
Om de modelstructuur beter te kunnen bestuderen zullen we voor het OSI *reference model* de gebruikte terminologieën en een korte beschrijving met een voorbeeld geven.

OSI reference model

Layer naam	***Functionele beschrijving***	***Voorbeelden***
Application, Layer 7	**De application layer verwijst naar communicatie services waar applicaties gebruik van maken.** Voorbeeld: **Een applicatiebouwer (bv tekstverwerker) hoeft zich niet bezig te houden met de OSI layer functies, maar bij een file transfer actie koppelt hij ze via een API aan zijn programma.**	FTP, WWW browsers, Telnet, NFS, SMTP, SNMP, X400 mail, FTAM
Presentation, Layer 6	De data formaten beschreven zoals ASCII tekst, EBCDIC tekst, binary, BCD en JPEG. Encryption wordt ook hier gedefinieerd. Voorbeeld: **Bij FTP kan je kiezen voor binary of ASCII transfer. Als de binaire vorm is gekozen dan wordt de data een op een overgedragen. Als de ASCII vorm gebruikt wordt dan vertaal de zender de tekst van zijn karakterset in een standaard ASCII en verzend de data. De ontvanger vertaalt de standaard ASCII naar de door hem gebruikte karakterset**.	TIFF, GIF, JPEG, PICT, ASCII, EBCDIC, Encryption, MPEG, MIDI, HTML
Session, Layer 5	Hier wordt het starten, controleren en beëindigen van een conversatie (sessie) gedefinieerd. Dit omvat het controleren en beheren van meerdere bidirectionele berichten zodat de applicatie kan beoordelen of een deel of alle berichten zijn uitgevoerd. Voorbeeld: **Een geldautomaat transactie mag niet een deel van de acties uitvoeren (verminderen van je saldo) als niet alle acties zijn uitgevoerd.**	RPC, SQL, NFS, Netbios names
Transport, Layer 4	In deze layer wordt een keuze gemaakt over het te gebruiken protocol en over het wel of niet uitvoeren van error recovery (herstel) Het opdelen van een bericht in meerdere segmenten voor verzending en het ordenen van de data pakketten die niet in de juiste volgorde zijn binnen gekomen. Voorbeeld: **TCP geeft een 4200 bytes segment door aan IP om te verzenden. IP zal dit verdelen in kleinere eenheden als de maximale pakketgrootte van het transport medium daarom vraagt (bv. 3x1400 bytes). De ontvangende TCP kan deze in andere**	TCP, UDP, SPX

	volgorde ontvangen en moet deze herschikken tot het originele segment.	
Network, Layer 3	In deze laag wordt de end-to-end bezorging van de pakketten beschreven. Om dit te kunnen realiseren wordt hier de logische adressering gedefinieerd. Ook wordt hier aangegeven op welke manier de routers de route bepalen. Verder wordt hier beschreven hoe pakketten in kleinere maximum transmission units (MTU) worden verdeeld.	IP, IPX, AppleTalk DDP
Data link, Layer 2	Deze laag is verantwoordelijk voor het transport van de data over een bepaalde link of medium. Voor elke link type is een ander protocol nodig. OSI refereert hiervoor aan beschrijvingen van andere instituten zoals IEEE. Elke link heeft een eigen adressering (MAC adressen). We maken hier onderscheidt tussen LAN en WAN-links.	Frame relay, HDLC, PPP, IEEE 802.3/802.2, FDDI, ATM, IEEE 802.5/ 802.2
Physical, Layer 1	Hier refereert OSI aan de beschrijvingen van andere organisaties die de fysieke eigenschappen van bepaalde media, connectoren, functie van de pinnen, elektrische en optische specificaties hebben gedefinieerd.	EIA/TIA-232, EIA/TIA-499, V35, V24, RJ45, Ethernet, 802.3, 802.5, FDDI, NRZI, NRZ.

Data flow door de OSI-lagen.
De gegevens die van een source systeem naar een destination systeem worden verzonden, worden door de software uit de 7 lagen structuur op een speciale manier verwerkt. Elke laag in het source systeem voegt informatie toe die door de overeenkomstige laag in het destination systeem begrepen, gebruikt en verwijderd wordt.



De gegevensblokken die in de diverse lagen voorkomen noemen we **PDU**'s (protocol data unit). Op elke laag en daarbinnen de gebruikte protocollen hebben allemaal hun eigen **format**. We noemen de PDU's in laag 7 t/m 5 **data**, in laag 4 **segment**, in laag 3 **pakket** en in laag 2 **frame**. In laag 1 worden de frame's als seriële **bitstromen** verzonden/ontvangen.

Het toevoegen van protocol informatie in de lagen van het OSI model noemen we **encapsulation**. Dit vindt plaats in het source systeem als een applicatie data naar een destination systeem verzendt. In het destination systeem gebeurt het omgekeerde, **de-encapsulation**.

Vragen en opdrachten

1. Noem de twee modellen waarin de communicatie tussen computersystemen beschreven wordt.

2. Geef een omschrijving van het begrip protocol.

3. Geef een omschrijving van het functie van de lagen in het OSI model.

4. Hoe noemen we de koppeling tussen twee aangrenzende lagen?

5. Wat zijn de redenen om een gelaagd model te gebruiken?

6. Hoe worden de gegevensblokken in de verschillende lagen genoemd en wat is de algemene naam?

7. Welke begrippen worden gebruikt voor het toevoegen en verwijderen van layer-info?

8. Geef een omschrijving van de volgende begrippen:
   - OSI, ISO,
   - TCP/IP,
   - reference model,
   - API,
   - Error recovery,
   - PDU, Data, Segment, Pakket, Frame, Bit stream,
   - Encapsulation, de-encapsulation.

Aantekeningen

1.3 LAN

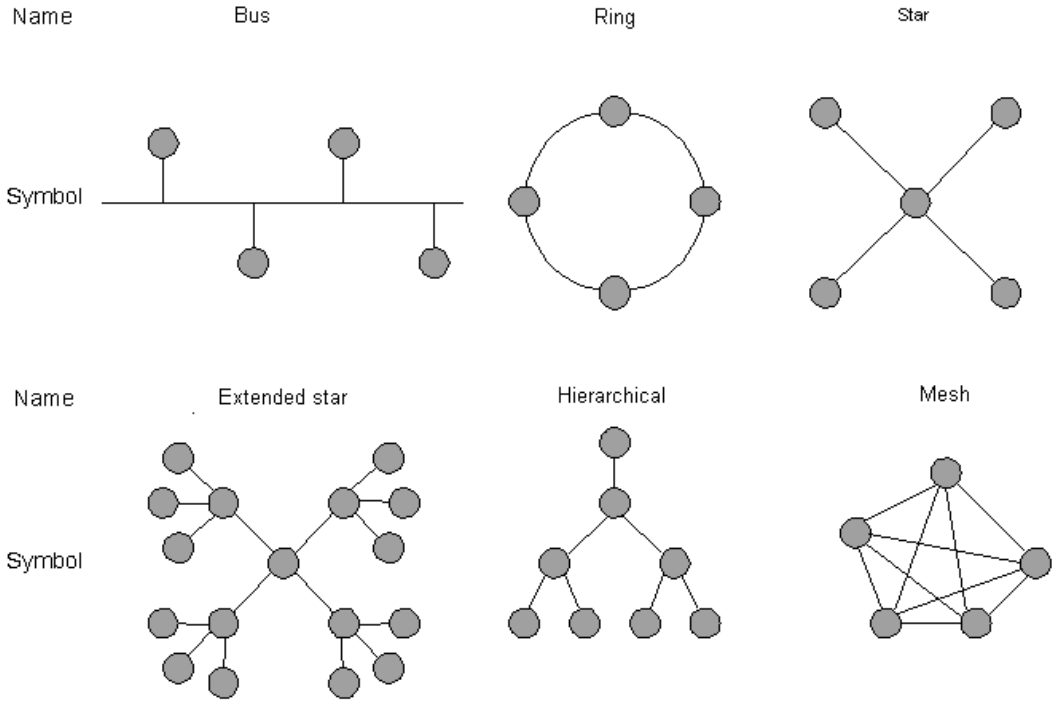
Een Local Area Network of LAN is een netwerk met computers, randapparatuur en netwerkapparatuur binnen een gebouw. Hierbij is de snelheid en omvang van data transport over korte afstanden de belangrijkste eis.

Om een LAN te ontwerpen moeten we een aantal zaken onderzoeken:
- de afmetingen van het gebouw, plattegronden,
- de plaats van de PC's, serverruimte en patch kasten, plattegronden,
- toekomstige uitbreidingen, meer PC's e.d.,
- de snelheid en de hoeveelheid data verkeer tussen de computers, gebruikte applicaties en de applicaties die men in de toekomst wil gaan gebruiken,
- de bedrijfszekerheideisen, (moeten zaken dubbel worden uitgevoerd?)
- de koppeling met externe netwerken, bv Internet,
- de financiële mogelijkheden.

Het ontwerpen van netwerken wordt in hoofdstuk 8 behandeld.

Bij het ontwerp van een LAN krijgen we te maken met:
- de **topologie**, dit is de manier waarop de bekabeling, de plaats van de netwerkapparatuur en de computersystemen wordt aangebracht,
- de **media**, dit zijn de te gebruiken netwerkverbindingen zoals: coax, utp/stp, glasvezel of de lucht (wireless),
- het **netwerktype**, hiervan kennen we ethernet, tokenring, fddi en wireless,
- de **netwerkapparatuur**, zoals nic's, repeaters, hub's, bridges, switches en routers.

Topologie
Voor de fysieke opbouw en installatie van netwerken kennen we een aantal vormen:



De toepassing van het type topologie is afhankelijk van de grootte van een LAN. Bij kleine LAN netwerken maakt men gebruik van een bus of star. Bij grotere netwerken wordt de extended star en hierachical topologie toegepast en in grote intranetten worden de routers in het bovenste deel van het netwerk in mesh topologie uitgevoerd zodat er meerdere links tussen routers ontstaan. Een andere toepassing in dit deel is een zeer snelle ring topologie.
De **nodes** op de uiteinden zijn de computersystemen en de **knooppunten** worden gevormd door netwerk- apparatuur

Media
De transportmedia zijn het materiaal waardoor de bits getransporteerd worden.
De vormen die we kennen zijn:

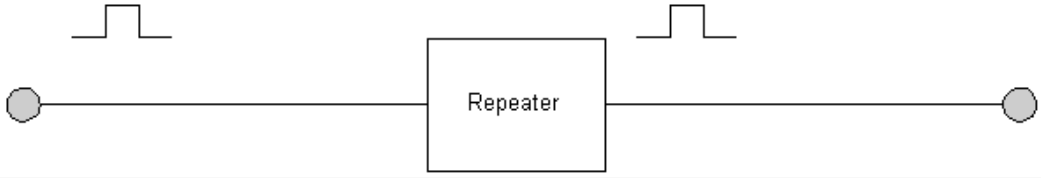
- Thick en Thin coax, een medium dat gebruikt wordt in bus topologieën maar steeds minder vaak wordt toegepast. We duiden deze aan met bv 10Base2 en 10Base5.
- UTP en STP (unshielded en shielded twisted pair) Dit zijn kabels met 2 of 4 in elkaar getwiste koperen aderparen. Deze bekabeling is onderverdeeld in categorieën om het verschil in eigenschappen aan te geven. Cat 3 wordt toegepast in de telefonie en Cat 5, 6 en 7 in computernetwerken. Deze bekabeling komen we tegen in alle topologieën behalve als bus. We duiden deze aan met bv 10BaseT, 100BaseTx.
- Fiber, dit zijn zeer dunne glasvezeldraden waardoor de bits via optische signalen worden vervoerd. Deze bedrading is ook verdeeld in categorieën die aangeduid worden met hun naam en de diameter van de kern en de mantel. Bv SM (single mode) en MM (multimode) 62.2/125 micron. Deze bedrading wordt toegepast als verbinding tussen netwerkapparatuur in de verschillende topologieën behalve als bus.
- De atmosfeer, dit wordt toegepast in WLAN's waarbij een groep computers communiceren met een wireless netwerkapparaat via elektromagnetische golven met een frequentie van 902 MHz.

De verschillende media worden gekoppeld met de computers en netwerkapparatuur via connectoren zoals: BNC, AUI, RJ45, ST.
Er zijn een aantal normaliseringinstituten die de media en hun connectoren beschrijven zoals: IEEE, EIA/TIA, AWG e.d. In hoofdstuk 5 meer hierover.

Netwerkapparatuur.
Buiten PC's, servers en printers is er nog een aantal netwerkapparaten zoals repeaters, hub's switches, bridges en routers in een netwerk opgenomen. Al deze onderdelen worden aan het netwerk gekoppeld via een NIC.

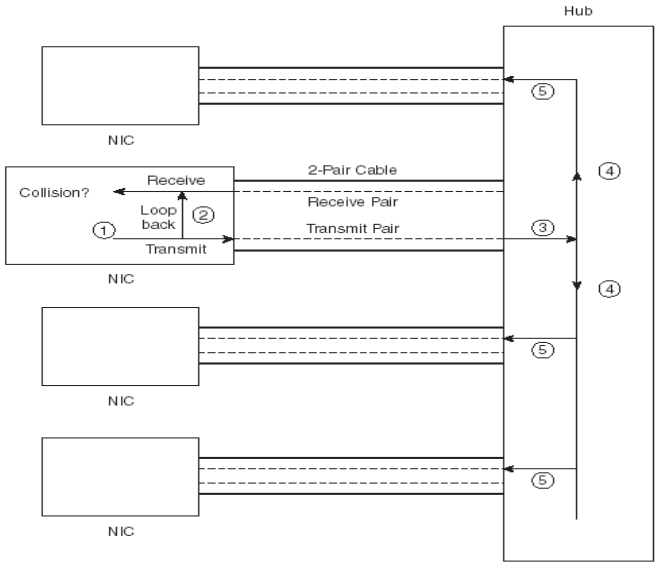
NIC
De network interface card is het hardware deel dat in een computersysteem geplaatst moet worden of op het motherboard geïntegreerd is waarmee de koppeling met een netwerk gemaakt wordt. Wanneer we een NIC moeten gebruiken, moeten we letten op het netwerktype, de snelheid, het gebruikte medium en het computerbustype (ISA, PCI; bij laptops is dit PCMCIA).

Repeater
Een signaal dat door een medium loopt, wordt vervormd door de kabeleigenschappen en invloeden van buiten (ruis). Hoe langer de kabel hoe groter de vervorming. Op een bepaald moment is het signaal niet meer herkenbaar voor de ontvanger(s). De maximale lengte van een medium is zo gekozen dat het signaal nog net herkenbaar is. Wanneer we grotere afstanden moeten overbruggen dan lukt dit alleen met een apparaat dat het signaal weer in zijn oorspronkelijke staat brengt en doorstuurt naar het volgende deel van de verbinding. Zo'n apparaat nomen we een repeater.



Met een repeater kunnen we de verbinding verdubbelen en wanneer we meerdere repeaters gebruiken, kunnen we de afstand nog verder vergroten.

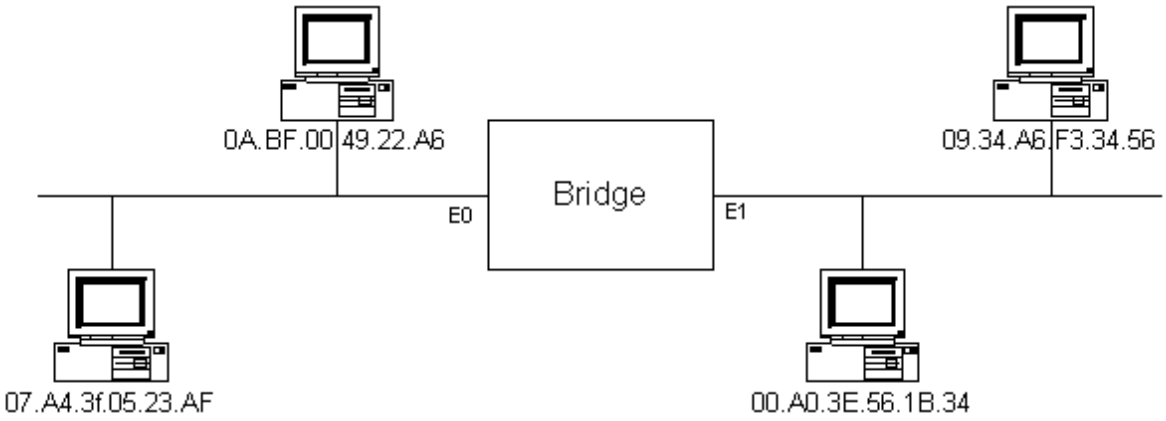
Hub
Een hub is een apparaat dat als knoppunt dient in een star topologie. Hieraan worden een groep PC's, printer en server, via een individuele verbinding gekoppeld. Deze topologische star heeft voor ethernet een **logische bus** functie. Dit betekent dat de bus in de hub door alle aangesloten systemen gemeenschappelijk wordt gebruikt.
De toegangsmethode is **CSMA/CD**, dit wil zeggen dat alle systemen luisteren of er geen verkeer is, als dit het geval is, kan er een signaal op de lijn gezet worden. Het kan nu voorkomen dat meerdere systemen gelijktijdig een signaal aanbieden waardoor er een botsing (**collision**) van deze signalen optreedt. Als dit het geval is, stoppen de systemen met zenden en wachten tot het weer stil is en doen dan een nieuwe poging. Via een hub kan er dus maar één systeem gelijktijdig zenden. Alle andere systemen ontvangen dit bericht en kijken of het voor hun bestemd is. We noemen dit **half-duplex**. Er is dus geen een systeem dat gelijktijdig kan zenden en ontvangen.
De poorten van een hub werken tevens als repeater, dus de signalen worden weer in hun oude staat gebracht waardoor de afstanden tussen de computersystemen tweemaal de lengte van een link bedraagt.



Bridge
Wanneer systemen via een hub communiceren dan is er maar één communicatie mogelijk. Bij grotere netwerken en veel communicatie is dit een nadeel. Een oplossing is om het netwerk in meerdere **segmenten** te verdelen waardoor op alle segmenten gelijktijdig gecommuniceerd kan worden. Pas wanneer er communicatie tussen segmenten plaatsvindt is er maar één verbinding mogelijk. Het apparaat dat we hiervoor gebruiken is een **bridge**.
Om te onderzoeken of een bericht naar een ander segment moet, maakt de bridge gebruik van de hardware of **MAC adressen** van de systemen die op de segmenten zijn aangesloten. Hiervoor maakt de bridge een tabel met MAC adressen die gekoppeld zijn aan de bridge poort naar hun segment.

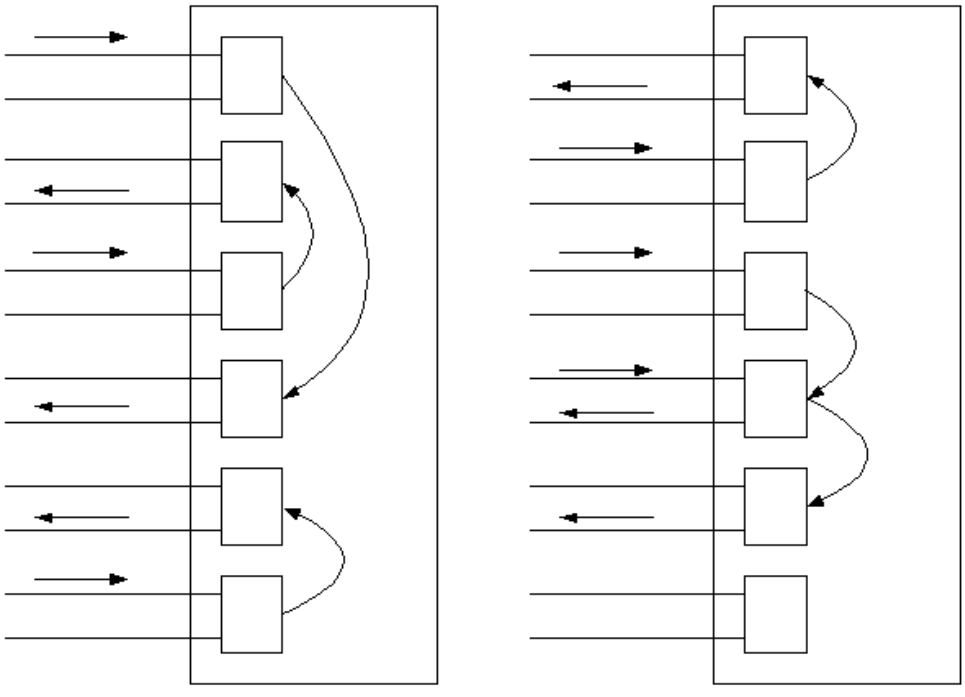
Switching table

MAC address	Port
07 A4 3F 05 23 AF	E0
00 A0 3E 56 1B 34	E1
0A BF 00 49 22 A6	E0
09 34 A6 F3 34 56	E1



Er kan nu gelijktijdig gecommuniceerd worden tussen de systemen op beide segmenten of tussen twee systemen op verschillende segmenten. Ook de bridge poorten hebben een repeater functie.

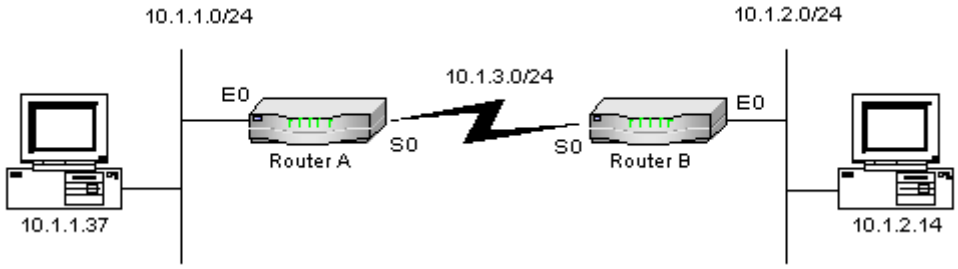
Switch
Een switch is een netwerkapparaat dat een bridge functie vervult tussen meerdere segmenten. Hierdoor kan er gelijktijdig communicatie plaatsvinden op de afzonderlijke segmenten of tussen segmenten onderling. Als de switch 12 poorten heeft dan kunnen er kunnen er gelijktijdig 6maal 2 segmenten onderling communiceren. Dit geeft een veel hoger rendement dan wanneer we een hub zouden gebruiken. Bij het gebruik van switches plaats men op elk segment meestal maar één computersysteem. Hierdoor is het mogelijk dat bv een server gelijktijdig data kan zenden naar systeem A en ontvangen van systeem B. We noemen dit **full-duplex**.



Switch Switch

De switch maakt voor het bepalen van de koppeling van segmenten ook gebruik van een tabel waarin de relatie tussen de poorten en de MAC adressen van de aangesloten systemen. Ook de switch poorten hebben een repeater functie.

Router
Bij grotere netwerken wordt, om het rendement van het netwerk, het beheer en de beveiliging te kunnen regelen, het netwerk verdeeld in meerdere subnetten of wordt het totale netwerk opgebouwd uit meerdere netwerken.
Deze subnetten of afzonderlijke netten worden gekoppeld met routers.
De routers regelen het verkeer tussen de afzonderlijke netwerken. De router werkt met de **logische adressen** van de computersystemen. Deze adressen bestaan uit een netnummer en een hostnummer.
De router kijkt naar het netnummer om te bepalen naar welke poort hij de data moet sturen. Hij maakt hierbij gebruik van een routerings tabel waarin de relatie tussen de poorten en de netnummers is opgenomen.



Router A (routing table)

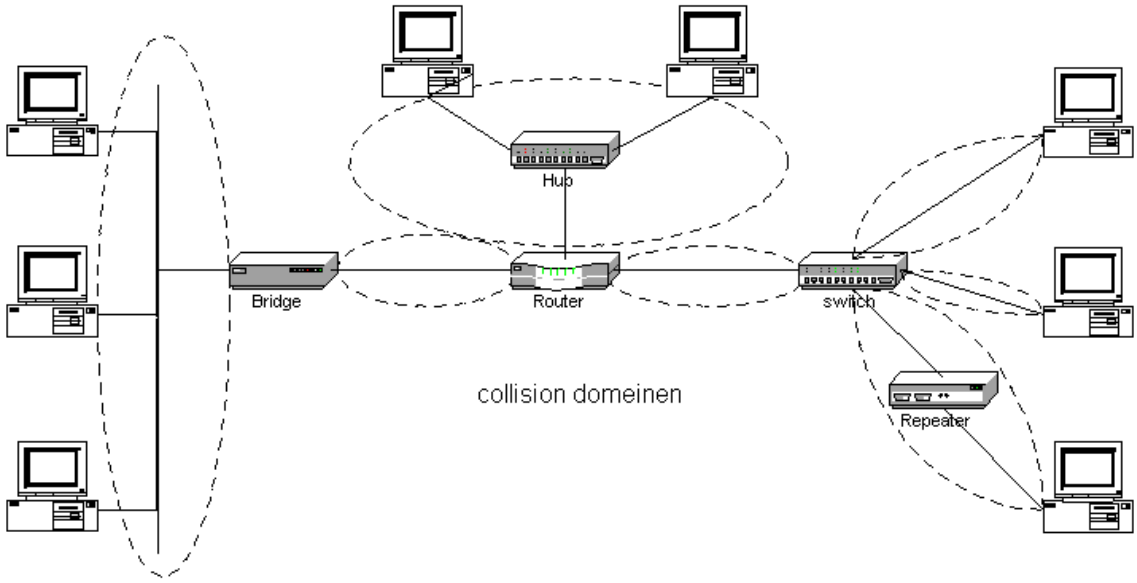
Netnummer	**Port**
10.1.1.0	Direct op E0
10.1.3.0	Direct op S0
10.1.2.0	Via S0

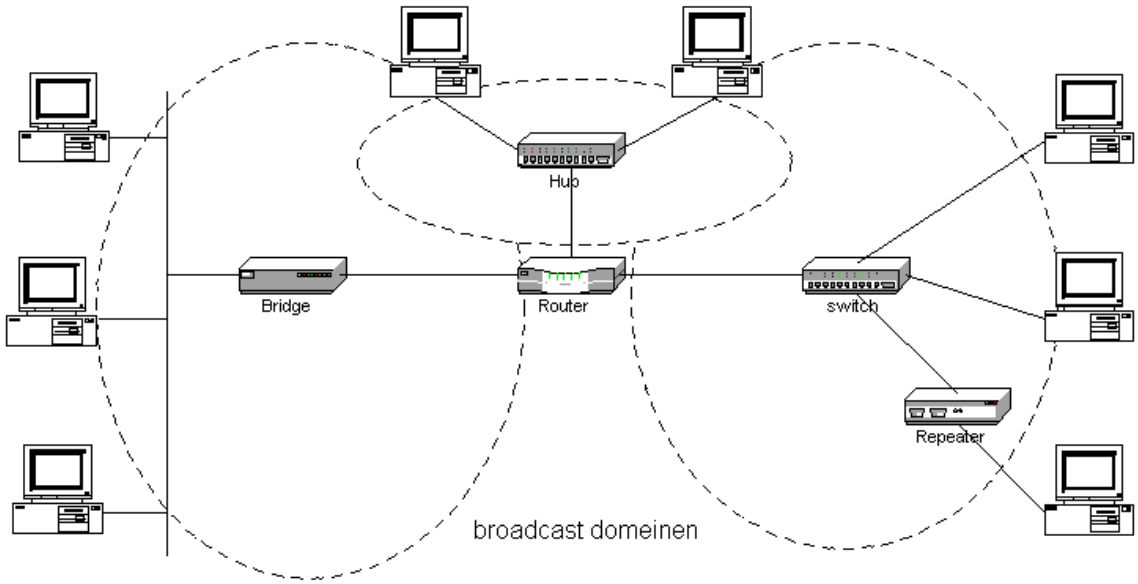
Router B

Netnummer	**Port**
10.1.1.0	Via S0
10.1.3.0	Direct op S0
10.1.2.0	Direct op E0

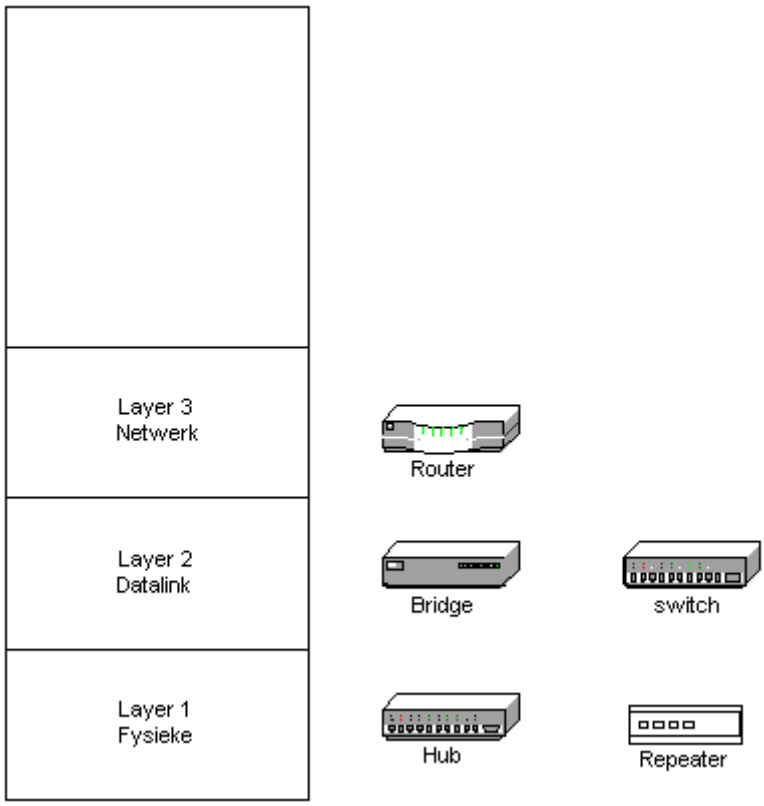
Als de router weet via welke poort de data verstuurd moet worden dan maakt hij van MAC adressen van het , op deze poort aangesloten netwerk, gebruik om het pakket te verzenden.
Evenals bij een hub, bridge en switch hebben de router poorten ook een repeater functie.

Collision en broadcastdomein
Op een netwerk worden niet alleen berichten verstuurd van systeem A naar B maar ook berichten die voor alle systemen bedoeld zijn. Deze berichten worden door de bridges en switches doorgegeven naar alle segmenten van het netwerk. We noemen dit **broadcast** berichten. Wanneer we één groot netwerk maken dan neemt het aantal broadcast berichten sterk toe. Om dit broadcast verkeer te beperken verdelen we grote netwerken in een aantal subnetten of afzonderlijke netwerken. Deze worden onderling verbonden via routers. Een router verdeelt een netwerk dus in meerdere **broadcastdomeinen**. Een broadcast- domein omvat dus een netwerk of subnetwerk
Op een netwerksegment uitgevoerd als een bus of een star topologie met een hub kunnen meerdere systemen gelijktijdig proberen te zenden waardoor **collisions** ontstaan. Zo'n netwerksegment noemen we een **collision domein**. Door bridges en switches toe te passen wordt een netwerk of een subnet verdeeld in meerdere collisiondomeinen.


Hub
Bridge
Router
switch
collision domeinen
Repeater


Hub
Bridge
Router
switch
Repeater
broadcast domeinen

De plaats van de netwerkapparatuur in het OSI-model
Wat is de plaats van de repeater, hub, bridge, switch en router in het OSI model.



De repeater en hub versterken alleen het signaal en hebben dus een layer 1 functie.
De bridge en switch maken gebruik van de MAC-adressering van layer 2 en bezitten ook de layer 1 functie (versterken van het signaal).
Een router maakt gebruik van de logische adressen uit layer 3 voor de route bepaling, de MAC adressen van layer 2 voor het transport en heeft ook de layer 1 functie (versterken van het signaal).

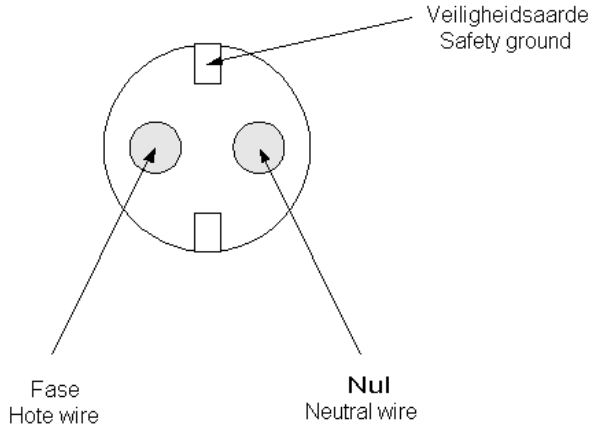
Vragen en opdrachten

1. Wat zijn de belangrijkste eigenschappen van een LAN?
2. Met welke facetten krijg je bij het ontwerp en de installatie van een netwerk te maken?
3. Noem de verschillende topologieën.
4. Noem de verschillende media typen.
5. Wanneer wordt een repeater toegepast?
6. Waar bevindt een hub zich in een star topologie?
7. Waarom wordt een bridge gebruikt?
8. Noem de verschillen tussen een hub en een switch.
9. Noem de verschillende netwerktypen (hoofdstuk 1).
10. Hoeveel collision en broadcastdomeinen zijn er in een LAN met één hub met 8 poorten?
11. Hoeveel collision en broadcastdomeinen zijn er in een LAN met één switch met 8 poorten?
12. Hoeveel collision en broadcastdomeinen zijn er in een LAN dat is opgebouwd uit 4 subnetten met alleen hub's, die onderling verbonden zijn via een router?
13. Van welke OSI lagen voert een hub de functie(s) uit?
14. Van welke OSI lagen voert een bridge en switch de functie(s) uit?
15. Van welke OSI lagen voert een router de functie(s) uit?
16. Geef een omschrijving van de volgende begrippen:
    - Topology, Media,
    - Repeater, hub,
    - Bridge, switch,
    - Router,
    - Half- en Full-duplex,
    - Collision, broadcast,
    - Collision domain, broadcast domain

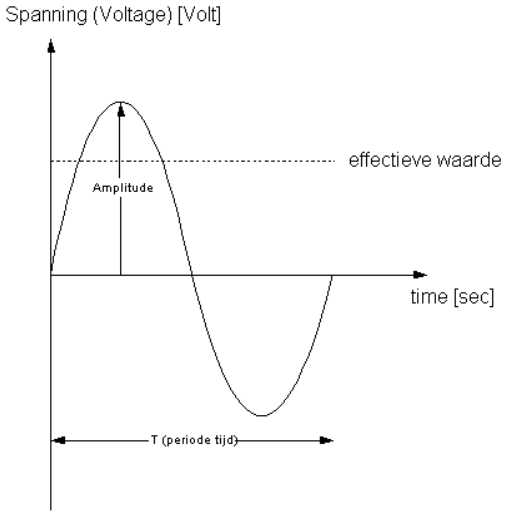
Aantekeningen

1.4 Layer 1, Electronics en Signals

De basisbeginselen van elektriciteit
Een data-netwerk bestaat uit PC's, servers, netwerkapparatuur en netwerkverbindingen. Alle apparaten hebben een hoeveelheid elektronische componenten, zoals; motherboards, microprocessoren, memory en I/O devices.
Al deze onderdelen hebben elektriciteit nodig om te kunnen werken. Deze **elektrische energie** wordt geleverd door **elektriciteitscentrales** en wordt uiteindelijk aangeboden op wandcontactdozen (**wall outlet**) (stopcontact in de volksmond). In sommige gevallen wordt de energie aangeboden in de vorm van **accu's** (voor bv. labtops) en **batterijen** (voor mobiele telefoons ed). In heel kleine elektronische apparaten wordt wel een **zonnecel** als bron gebruikt.

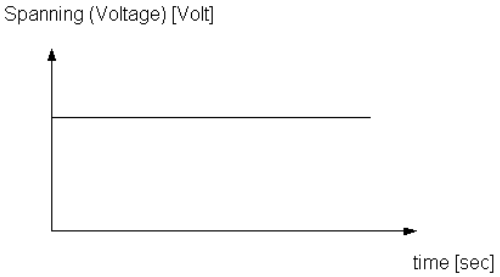


Op de wandcontactdoos wordt een wisselspanning (**Alternating Current AC**) van 220Volt aangeboden. Op de nul staat nul volt en op de fase wisselt de spanning tussen een maximale en minimale waarde. Deze spanning heeft de vorm van een **sinus**. De veiligheidsaarde wordt verbonden met de apparatuurbehuizing om te voorkomen dat deze onder spanning kan komen te staan.



De **amplitude** is de maximale spanning op de fase t.o.v de nul. De effectieve waarde is een rekeneenheid voor wisselstroom. De effectieve waarde van de netspanning die in Nederland gebruikt wordt, is 220Volt.
De **periodetijd T** geeft aan hoelang het duurt voordat de fase een sinus heeft doorlopen.
De **frequentie** van de spanning is het aantal keren dat de sinusvorm zich herhaalt in één seconde.
f = 1/T [Hz]. De frequentie van het 220V signaal is 50 Hz.

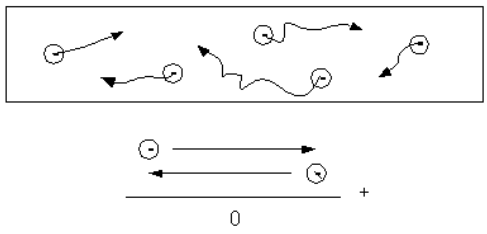
De apparatuur wordt via een aansluitsnoer met stekker (**power cord**) vanuit een wandcontactdoos gevoed. In de apparaten zit een voedingseenheid (**power supply**), die de wisselspanning van 220V omzet naar een aantal gelijkspanningswaarden (**directed current DC**): 5V voor de meeste IC's (**integrated circuits**), 12V voor de motoren van de disks en de elektronica op de video- en soundkaart en 3,3V voor de processor. In een labtop werken de meeste onderdelen op 3,3V of lager.
Een gelijkspanning is een spanning met een gelijkblijvende waarde.

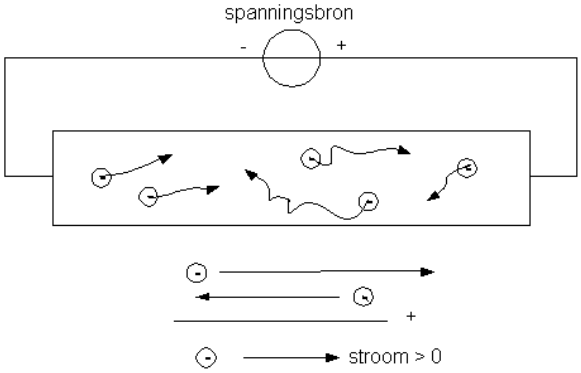


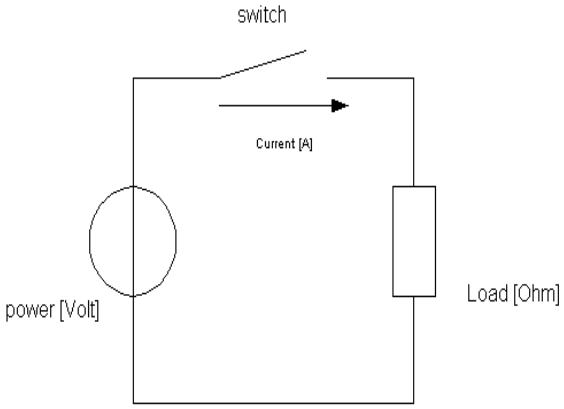
Op de voedingseenheid zit een mogelijkheid om deze in te stellen op een spanning van **110V, 60 Hz**. Dit zijn de spanningswaarde en de frequentie die o.a. in Amerika toegepast worden.

De verbindingen tussen onderdelen op een motherboard bestaan uit kopersporen op een printplaat. Koper is een zeer goede geleider (**conductor**) van

elektrische stroom (**current**). De printplaat zelf is gemaakt van een slecht geleidend materiaal (**insulator**).
De IC's zijn gemaakt van een materiaal dat we een halfgeleider (**semi conductor**) noemen.
Een elektrische stroom is een beweging van **vrije elektronen** in een bepaalde richting door een geleider. We geven de grootte ervan aan met de eenheid **Ampère** (of **mA** als deze heel klein is). De stroom wordt veroorzaakt door de spanningsbron en de grootte wordt bepaald door de belasting (**load**) die er op aangesloten wordt.
De stroom gaat pas lopen als de bron samen met de belasting en bedrading (**wires**) een gesloten stroomkring (**closed circuit**) vormt.

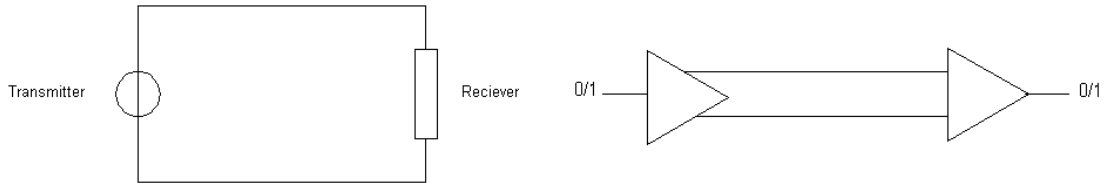






Elektrotechnici gebruiken een **schema** met **symbolen** om stroomkringen aan te geven.
Met een schakelaar (**switch**) kunnen we de stroomkring sluiten (**closed circuit**) of verbreken (**open circuit**).

Als de power een gelijkspanningsbron is (accu of batterij) dan wordt de ene aansluiting de **pluspool** en de andere de **minpool** genoemd. Dit kan omdat de **polariteit** gelijk blijft. Bij een wisselspanningbron is dit niet mogelijk omdat daar de polariteit voortdurend wisselt.



Bij netwerken wordt de stroomkring gevormd door de transmitter, netwerkverbinding en reciever.

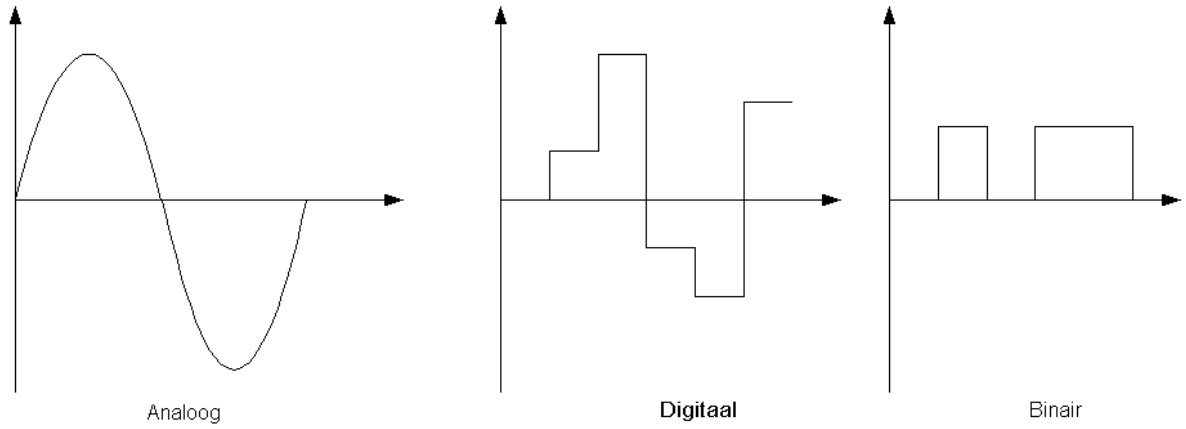
De load of belasting wordt in een DC-kring **weerstand** genoemd. In een AC kring heeft de load naast een weerstand ook frequentieafhankelijke eigenschappen. Dit noemen we **capacitieve** (condensator) en **inductieve** (spoel) eigenschappen. De algemene naam die we voor een AC-load gebruiken is **impedantie** (**Z [Ohm]**). Een coaxkabel en UTP/STP-verbinding bezitten deze eigenschappen ook en we noemen dit de **karakteristieke impedantie**.

Om een spanning-, stroom- of weerstandswaarde te meten gebruiken we een **universeelmeter**. Als we de spanningsvorm willen bekijken hebben we een **oscilloscoop** nodig.

Signalen in een communicatiesysteem
De signalen die gebruikt worden in communicatiesystemen om data te transporteren zijn:

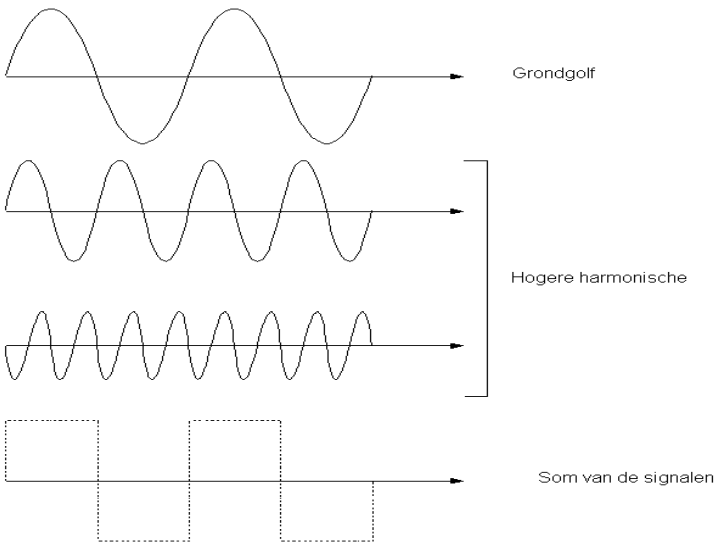
- **elektrische spanning**. Deze wordt toegepast bij koperverbindingen zoals; **coax**, **utp/stp**, waarbij de bron **transmitter** genoemd wordt en de load een **reciever**,
- **licht**. Dit wordt gebruikt bij glasvezelverbindingen. Hierbij is de bron een light emitting diode (**LED)** en de load een **fotocel**,
- **elektromagnetische golven**. Dit komt voor bij **wireless** en **mobiele** communicatie. De bron en de load worden allebei **antenne** genoemd.

Signalen kunnen een analoge-, digitale- of binaire vorm hebben.

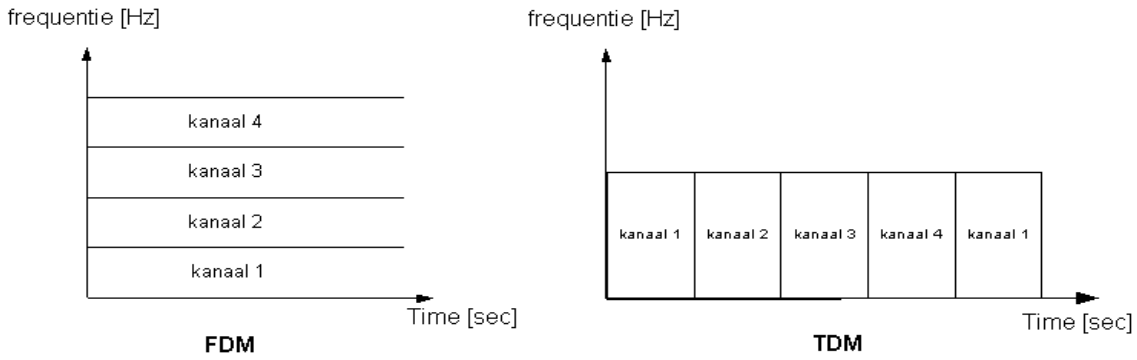


Een **analoog** signaal kan **elke waarde** aannemen tussen een maximum en een minimum.
Een **digitaal** signaal kan een **aantal waarden** aannemen tussen een maximum en minimum.
Een **binair** signaal maakt gebruik van **twee waarden**.

Een niet-sinusvormig signaal is opgebouwd uit de som van een aantal sinusvormen. De laagste frequentie noemen we de **grondgolf** en de andere frequenties zijn de **hogere harmonische**. Als we een binair-signaal gebruiken, dan moet de verbinding de frequenties waaruit het signaal is opgebouwd goed kunnen transporteren. We gebruiken dan de hele **frequentieband** van de verbinding en spreken dan over een **baseband**-verbinding.



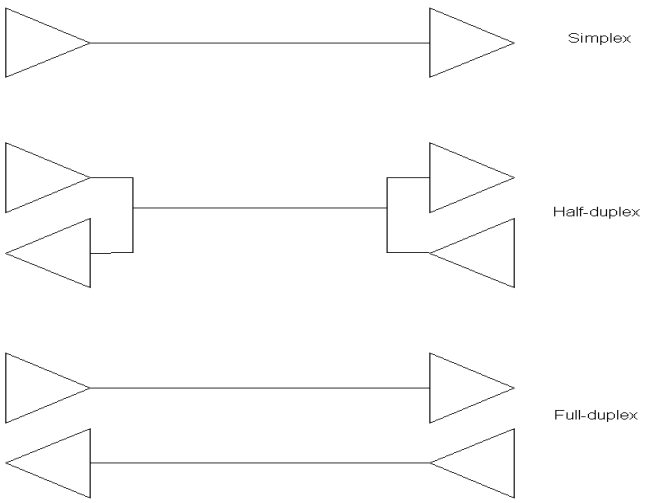
Wanneer we signalen met een aantal frequenties gebruiken om de data te transporteren dan gebruiken we maar een deel van de frequentieband. Door meerdere signalen met verschillende frequenties te gebruiken kan elk signaal data transporteren. Deze signalen kunnen gelijktijdig door de verbinding gestuurd worden. Aan de ontvangstkant worden de afzonderlijke frequenties (signalen) weer uit elkaar gehaald (**filteren**). We spreken dan over een **broadband**-verbinding. Het gelijktijdig verzenden van signalen over een verbinding wordt **multiplexen** genoemd. Als we signalen, die uit een aantal frequenties bestaan, gelijktijdig verzenden wordt dit **frequentie division multiplexing** (**FDM**) genoemd. KabelTV is een goed voorbeeld van FDM.



Binaire signalen kunnen geen gebruik maken van FDM omdat ze de gehele frequentieband van een verbinding gebruiken. We kunnen de verbinding echter wel delen door de verschillende data-signalen in een bepaald **tijdslot** te versturen. We noemen dit **time division multiplexing** (**TDM**).

Bij lichtsignalen kunnen we multiplexing toepassen door voor elk kanaal een andere **golflengte** te kiezen. We noemen dit **dence wavelength division multiplexing** (**DWDM**)

Wanneer we een signaal alleen van A naar B kunnen verzenden en niet terug dan spreken we over een **simplex**-verbinding. De oude centraal antenne systemen werkten zo. Hierbij was geen Internet via de kabel mogelijk.Wanneer we wel van A naar B en terug kunnen, dan spreken we van een **duplex** verbinding. Wanneer dit om en om gebeurt, noemen we dit **half-duplex** en wanneer dit gelijktijdig kan, heet het **full-duplex**.



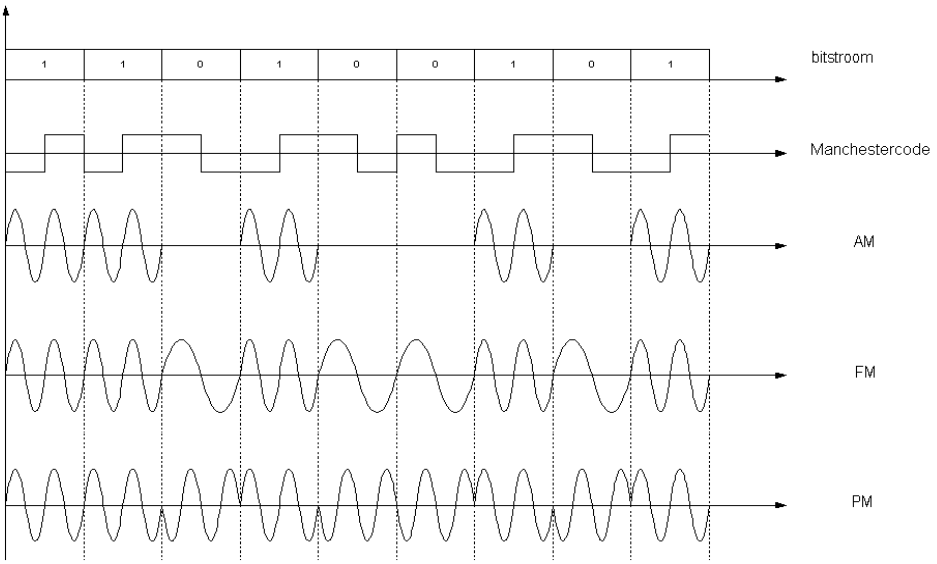
Coderen van netwerksignalen
De signalen die over een netwerkverbinding getransporteerd worden, worden binnen de systemen gezien als logische nullen en enen (bits). De omzetting van nullen en enen in een fysieke signaalvorm noemen we **encoding** of **modulatie**. Het omgekeerde proces heet **decoding** of **demodulatie**. De data worden als bitstroom verzonden. Een groep bij elkaar horende bits noemen we een **frame**.

We kunnen de logische bits encoderen en verzenden via:
- een elektrische puls of frequenties door een koperdraad;
- een lichtpuls door een glasvezel;
- een elektromagnetische golf door de ether;
- een lichtpuls (infra rood) door de ether.

Een bitstroom kan omgezet worden in een binair-signaal waarbij de overgang van laag naar hoog een "1" voorstelt en een overgang van hoog naar laag een "0". We noemen deze methode **Manchestercode**. Deze methode wordt toegepast bij ethernet.

Wanneer voor de omzetting naar een analoog signaal wordt gekozen dan is er een aantal mogelijkheden:
- **Amplitude-modulatie** (**AM**). Hierbij wordt een "1" voorgesteld door de maximale amplitude en de "0" door een amplitude van 0.
- **Frequentie-modulatie** (**FM**). Hierbij worden de enen en nullen voorgesteld door verschillende frequenties.
- **Fase-modulatie** (**PM**). Hierbij wordt het verschil gemaakt door in de tijd verschoven signalen (fase verschil).

De voorbeelden in de volgende figuur geven de eenvoudigste vormen aan. Door combinaties van AM en FM en door te werken met meer dan 2 fasen bij PM kunnen er door een signaalverandering meerdere bits worden aangeduid.
Als we PM toepassen met 8 fasen dan geeft elke verandering een groep van 3 bits weer. De databandbreedte (bps) wordt 3 maal zo groot, terwijl de signaalbandbreedte (Hz) gelijk blijft.



Propagatie van signalen door een netwerkverbinding en de problemen die kunnen ontstaan.
Een signaal wordt verzonden door de transmitter en beweegt zich door de verbinding (**propagation**) naar de reciever(s). Het signaal verplaatst zich met een snelheid van **180.000 tot 250.000 km/sec** door een verbinding. De snelheid is afhankelijk van de soort verbinding. De tijd die nodig is om van het begin van de kabel naar het eind te komen en terug noemen we de **round trip time** (**RTT**).

Deze energiepuls verliest tijdens het transport energie aan de kabel en reciever(s). We noemen dit **attenuation**. Als de kabel te lang is of er te veel recievers (computers) zijn aangesloten is de attenuation zo groot dat het signaal niet meer herkend wordt als 0 of 1. Dit is een van de redenen waarom aan de lengte en het aantal aangesloten systemen een grens is gesteld. Wanneer de afstand tussen twee systemen groter is dan de toegestane kabellengte dan kunnen we gebruik maken van een **repeater**. Dit apparaat herstelt het signaal weer in zijn oorspronkelijke vorm. De systemen kunnen nu 2 maal de kabellengte van elkaar verwijderd zijn.

Van een signaal, dat op de **lijn** wordt gezet en aan het eind zijn energie niet kwijt kan, wordt het overblijvende deel gereflecteerd. Dit **reflectie**signaal vervormt het echte signaal op de lijn zodat deze niet meer op de juiste manier als 0 of 1 wordt herkend. Dit probleem doet zich voor bij coax-kabels en we lossen dit op door aan de uiteinden een **terminator (**vernietiger, ook wel afsluitweerstand genoemd**)** te plaatsen die de overgebleven energie omzet in warmte. Bij een UTP-kabel treedt dit probleem niet op omdat de reciever zo gebouwd is dat hij alle energie opneemt.

Noise of ruis
Ruis is de algemene naam voor **ongewilde toevoegingen** aan optische of elektromagnetische signalen. Aan het originele signaal worden **stoorsignalen** toegevoegd waardoor het originele signaal vervormd wordt. Deze vervorming kan een juiste herkenning van nullen en enen onmogelijk maken. In de theorie gebruiken we een eenheid die de verhouding aangeeft van de ruis t.o.v. het originele signaal. We noemen dit de signaal/ruis verhouding (**S/N ratio**). Deze waarde geeft aan hoeveel ruis er toegestaan is om het originele signaal nog te kunnen herkennen.

Enkele soorten ruis:
- Thermische ruis (**thermal noise**),
- Overspraak (**near end cross talk of NEXT**),
- Ruis veroorzaakt door de voeding en de aardverbinding (**AC power/reference ground noise**),
- Electromagnetic interference (**EMI**),
- Radio frequency interference (**RFI**),

Thermal noise
Thermische ruis is een verschijnsel dat optreedt in elektronica-componenten en in geringe mate in geleiders. Het wordt veroorzaakt door onverwachte elektronen verplaatsingen. Dit is niet te voorkomen maar heeft in de meeste gevallen bijna geen invloed op het signaal.

Near end cross talk
Overspraak is het verschijnsel dat een signaalverandering in een draad een reactie heeft in de andere draden in een kabel. Dit verschijnsel is te voorkomen of te verminderen door aderparen om elkaar te twisten (**twisted pair**) en door aderparen af te schermen met een geleidend omhulsel (**shielded pair**).
In de draden die behoren tot één stroomkring, is de stroomrichting tegengesteld. Om elke draad vormt zich een magnetisch veld. Wanneer de draden dicht tegen elkaar liggen, dan doven deze velden elkaar uit (**cancellation**). Dit verschijnsel wordt versterkt door de draden te twisten. De aderparen beïnvloeden elkaar nu minder. Ook de magnetische beïnvloeding van buiten wordt door de twisting gedoofd. Overspraak komt vooral voor bij slecht gemaakte connectoren waarbij de twisting te ver verwijderd is!!!

AC power and reference ground noise
De voeding en de bijbehorende aarding kan ook ruis veroorzaken. Dit wordt veroorzaakt door motoren van bijvoorbeeld ventilatoren, TL-armaturen en door blikseminslagen. Dit verschijnsel veroorzaakt vooral problemen in de computers en netwerkapparaten. We kunnen dit verschijnsel verminderen door:
- in de voeding netfilters op te nemen, door apparatuur te voeden met een schone groep (een groep waar geen andere apparaten mee worden gevoed).
- In ruimtes met netwerkapparatuur geen TL-verlichting te plaatsen.

- Netwerkverbindingen die buiten een gebouw door de grond lopen niet van koper te maken maar te kiezen voor een glasvezelverbinding.

EMI/RFI
Elke draad in een verbinding werkt als antenne en is dus gevoelig voor elektromagnetische golven. Elektromagnetische instraling wekt in een verbinding een signaal op dat het signaal, dat door de verbinding loopt, kan vervormen zodat bv. een 0 in een 1 kan veranderen of omgekeerd. Dit signaal wordt daardoor corrupt en is niet meer te gebruiken. Deze verschijnselen noemen we elektromagnetic interference (**EMI**) en radio frequency interference (**RFI**). We kunnen dit verschijnsel bestrijden door om een verbinding een **overall shield** aan te brengen. Dit werkt als een kooi van Farraday.
Optische verbindingen zijn niet gevoelig voor EMI en RFI. In zeer storingsgevoelige omgevingen is het daarom aan te bevelen om glasvezel toe te passen.

Timing problemen
Er is een aantal verschijnselen dat de timing tussen de transmitter en de reciever beïnvloedt. Met timing wordt bedoeld de synchronisatie tussen de zendklok en de ontvangstklok. Het kloksignaal wordt gebruikt om het moment aan te geven waarop het signaal op de lijn wordt gezet en vanaf de lijn wordt ingelezen. Als de timing niet in orde is, kunnen er inlees problemen ontstaan (1 wordt 0 of omgekeerd). Als dit in een frame eenmaal voorkomt, is het hele frame corrupt.
Een verschijnsel dat zich voordoet is het verbreden van een puls (**dispersion**) zodat aan de ontvangstkant opeenvolgende pulsen in elkaar overlopen. Dit verschijnsel neemt toe als de lengte toeneemt.
Een ander verschijnsel is het uit de pas lopen van de kloksignalen, de ene keer komt de flank te vroeg en dan weer eens te laat is (**jitter**).
De verbinding en de elektronische componenten in een verbinding zorgen voor het vertragen van het signaal (**latency**).
Deze problemen worden opgelost door de verbindingen zo kort mogelijk te houden en door een synchronisatie mechanisme in het signaal te verwerken.

Collision
Een ander verschijnsel dat de communicatie nadelig beïnvloedt, noemen we collision. Dit treedt op bij gedeelde media waar 2 of meer systemen een signaal over hetzelfde medium willen verzenden. De verschillende signalen vervormen elkaar en worden daardoor corrupt, zodat het signaal opnieuw verzonden moet worden. Dit verschijnsel doet zich voor bij het logische bussysteem mechanisme van ethernet. Het CSMA/CD protocol regelt de toegang en reageert op een collision. Het verschijnsel neemt sterk toe naarmate er meer systemen op een bus worden aangesloten.

Conclusie
Bij communicatie binnen netwerken kunnen zich allerlei problemen voordoen die het correct functioneren beinvloeden. Deze kunnen ontstaan door:
- de voeding en aarding (AC power and reference ground noise);
- eigenschappen van de verbindingen en de elektronica (Near end cross talk, Termal noise),
- door invloeden van buiten (EMI/RFI).

We kunnen deze nadelige effecten verminderen door te zorgen voor:
- een schone voeding en aarde,
- de keuze van de juiste media en een juiste montage van de aansluitingen,
- afscherming van uitwendige invloeden.

Vragen en opdrachten

1. Wat is het verschil tussen AC en DC?
2. Geef een omschrijving van de begrippen amplitude, periodetijd en frequentie.
3. Hoe groot is de frequentie van een periodieksignaal met een periodetijd van 1nS?
4. Wat is de functie van de voeding (power supply) in een computersysteem?
5. Geef een omschrijving van elektrische stroom.
6. Geef een omschrijving van een stroomkring.
7. Wat is het verschil tussen een analoog-, digitaal- en binair-signaal?
8. Noem het verschil tussen baseband en broadband-verbindingen.
9. Op welke manieren kunnen we meerdere signalen over een verbinding transporteren?
10. Wat is het verschil tussen simplex, half-duplex en full-duplex?
11. Geef een omschrijving van het begrip encoding en noem een aantal manieren.
12. Geef een omschrijving van propagation, RTT, attention en reflection
13. Wat is de functie van een terminator?
14. Welke eigenschappen beïnvloeden de timing?
15. Welke ongewenste toevoegingen kunnen er optreden in een communicatieverbinding?
16. Noem de oplossingen om de ongewenste toevoegingen te voorkomen.
17. Waar treedt het verschijnsel collision op?

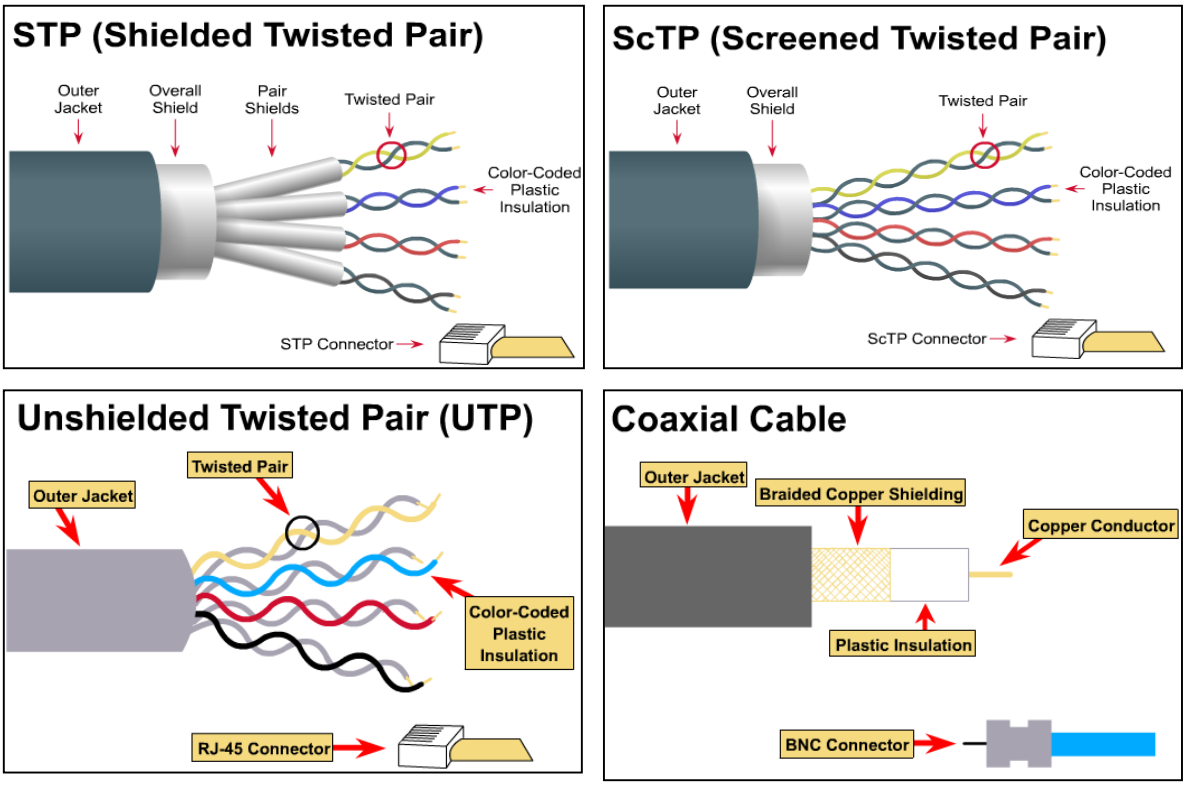
Aantekeningen.

1.5 Layer 1, Media, Connections and Collisions

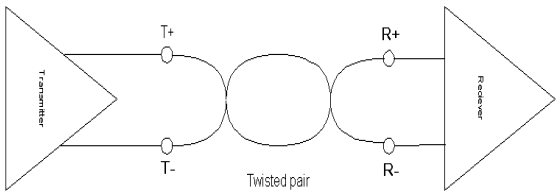
De verbinding tussen netwerkapparatuur onderling en de computersystemen in een LAN netwerk kunnen bestaan uit verschillende media. De functie van elk medium is: "**het foutloos transporten van data**".
Elk medium heeft zijn eigen specifieke eigenschappen, toepassingsgebied en beperkingen.
LAN media:

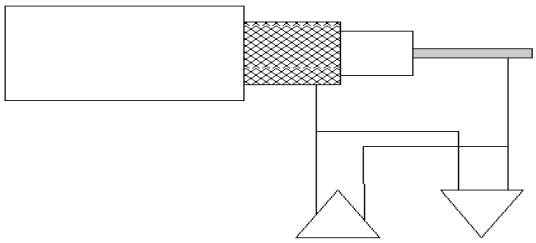
- koperdraden (**coax, UTP, ScTP en STP**),
- glasvezel (**single mode en multimode**),
- ether.

Koper



De twisting wordt gebruikt om het **interferentie** proces te onderdrukken. Interferentie is het verschijnsel dat meerdere signaaldragers elkaar beïnvloeden. Dit kan tot gevolg hebben dat een signaal ontoelaatbaar vervormd wordt. De twisting van de 4 aderparen zijn onderling verschillend van spoed (aantal twisten per centimeter).
De shielding wordt gebruikt om invloeden van buiten (**EMI/RFI**) te onderdrukken.





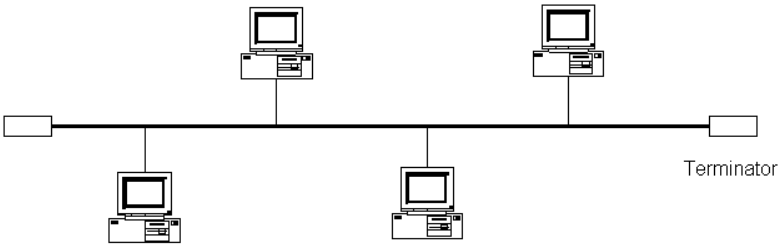
Bij TP kan met 2 aderparen een half- of full-duplex verbinding gemaakt worden. Bij een coaxkabel is alleen een half-duplex communicatie mogelijk.

De samenstelling en de eigenschappen worden beschreven in de normbladen van normalisatie-instituten. Dit zijn de instellingen zoals: IEEE, ANSI, TIA/EIA en AWG (American Wire Group). De EIA/TIA heeft een aantal normen vastgelegd voor bekabeling, patch kasten ed. en installatie van LANs (568, 569, 570, 606 en 607).

Hierin wordt o.a. beschreven:

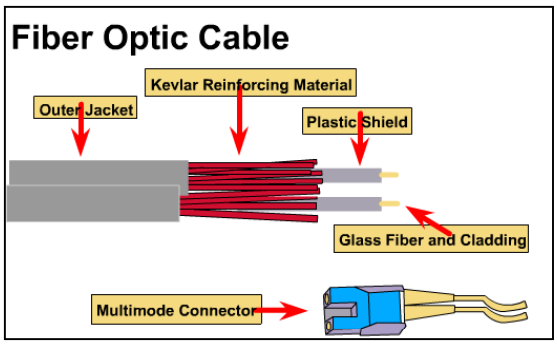
- de karakteristieke impedantie (Z) van de kabels
  UTP = 100 Ohm, ScTP = 100/120 Ohm, STP = 150 Ohm, Thin coax = 50 Ohm en Thick coax = 50 Ohm.
- De lengte
  TP max. 100m, Thin coax 185m en Thick coax 500m
- Connector
  TP via **RJ45**, Thin coax via een **BNC** en Thick coax via een **AUI** (**transiever**).

TP wordt toegepast in een fysieke ster topologie en coax in een fysieke bus topologie.
Bij een coax verbinding moeten de uiteinden worden afgesloten met een terminator om reflecties te voorkomen.

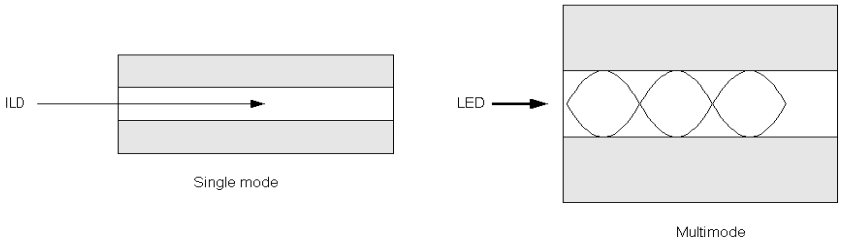


Naast het verschil in eigenschappen is er ook een verschil in kostprijs en montage. De UTP is klein van diameter, soepel en eenvoudig te monteren. Voor STP is meer vakmanschap vereist om de connectoren te plaatsen en de kabel is dikker en stugger. Hetzelfde geld voor thin- en thick coax. Bij thick coax wordt een aansluiting op de kabel geschroefd en met een drop cable op de NIC aangesloten (transiever).

Glasvezel

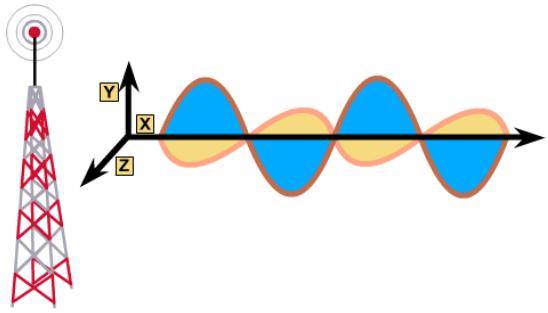


In LANs wordt het multimode type glasvezel toegepast (62,5/125 micrometer). Deze bestaat uit een glaskern van 62,5 micron en een glasbekleding (**cladding**) van 125 micron.



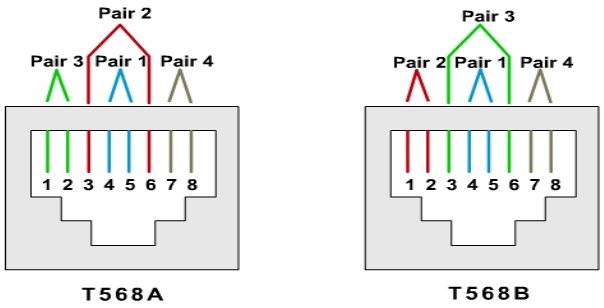
Bij de multimode wordt als lichtbron een LED gebruikt. De lichtbundel gaat onder verschillende hoeken de kern in en de lichtpuls wordt tijdens de loop door de kern steeds breder (dispersion). Hierdoor kunnen de pulsen elkaar gaan overlappen. Om dit te voorkomen zijn er grenzen gesteld aan de snelheid en de lengte. De lengte is **412m** bij een snelheid van **100Mbps**.
Er zijn per verbinding twee vezels nodig, een voor het verzenden en een voor het ontvangen. De verbinding is een point to point link.
Bij de single mode wordt als lichtbron een **injection laser diode** (ILD) gebruikt met licht van één golflengte.
Dit type wordt toegepast bij grote afstanden (WAN).
Als aansluiting wordt een **ST**-connector gebruikt. De montage hiervan vraagt specifieke vaardigheden.

Ether
Draadloze signalen zijn elektromagnetische golven die zich door de lucht maar ook door vaste stoffen kan verplaatsen. Deze signalen worden verzonden en opgevangen door een antenne.



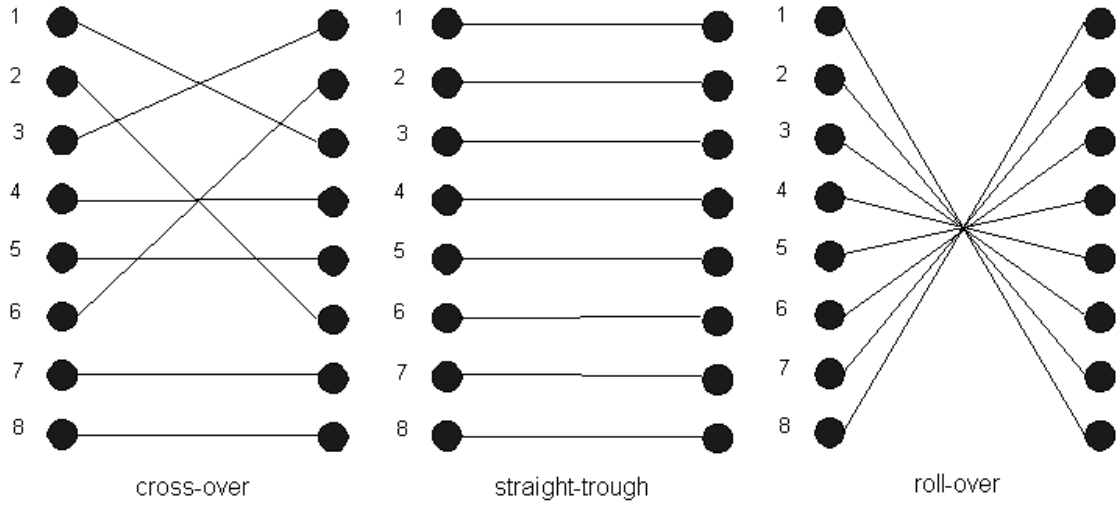
De Lans die met wireless verbindingen werken noemen we WLANs. Hierbij zijn de NIC's voorzien van een antenne en wordt de verbinding met het netwerk verzorgd door wireless accesspoints. De bandbreedte is momenteel 11Mbps. De WLANs worden beschreven door de IEEE 802.11-norm. Het bereik is ongeveer 100m.

Het maken en testen van netwerkkabels
De betrouwbaarheid van een netwerk is een belangrijk punt. Dit is voor een groot deel afhankelijke van het gebruik van de juiste materialen en de kwaliteit van de montage. Een installateur van netwerken moet een certificaat overleggen bij de oplevering. Dit certificaat wordt afgegeven door een keuringsbedrijf dat de installatie inspecteert en door meet.
Een belangrijk punt bij de montage is het aansluiten van de connectoren aan de kabels. Voor een UTP bekabeling zijn dit de RJ45-**pluggen** aan de kabels tussen de computersystemen en de wandaansluiting en de patch kabels en de RJ45-**jackets** in de wand en in de patch pannels.
Voor de bekabeling wordt in de meeste gevallen een **straight-trough** verbinding gebruikt. Dit is een verbinding waarbij de overeenkomstige pennen van de pluggen zijn doorverbonden (1 met 1 , 2 met 2 enz). Hierbij moet wel rekening gehouden worden dat de tranmitters en recievers met elkaar verbonden worden. Dit is geen probleem bij een verbinding tussen een computersysteem en een netwerkapparaat (repeater/hub/enz) omdat in de netwerkapparatuur een kruising van de transmitter- en recieverdraden is opgenomen. We kunnen dit zien aan de **X** achter het poortnummer (6x).
Wanneer we twee gelijke onderdelen moeten koppelen dan moeten we in de kabel zorgen voor en kruising. We noemen zo'n kabel een **cross-over** cable. We gebruiken deze om twee computers te koppelen of om hubs en switches te koppelen. In veel netwerkapparatuur is een poort aanwezig waarbij de kruising in- of uit te schakelen is. Hierdoor wordt het koppelen met een straight kabel mogelijk door op een van de apparaten de kruising uit te schakelen. (MDI of MDIx).
De plaats van het adres in de plug is vastgelegd in de EIA/TIA 568A of B-norm. Bij de montage is het belangrijk om de twisting zoveel mogelijk in tact te laten. Bij het onzorgvuldig onttwisten van een aderpaar kan de twisting ook onder de isolatie verwijderd worden (**let hier goed op!**).



Kleuren:
Pair 1: blauw/blauwwit
Pair 2: oranje/oranjewit
Pair 3: groen/groenwit
Pair 4: bruin/bruinwit

De figuur geeft het vooraanzicht van een jacket aan waar de plug in wordt gestoken. De aders van een aderpaar zijn geheel gekleurd en wit/gekleurd (bv. blauw en wit/blauw).
Voor de montage is een speciale **krimptang** nodig die de pennen door de isolatie drukt. Bij de montage van een jacket wordt een **punch-down** apparaat gebruikt die de ader in de V-opening drukt en direct op lengte afsnijdt.



De **roll-over** kabel is een kabel die gebruikt wordt om de **console** poort van bv. een router aan te sluiten op de **COMx** poort van een PC. We kunnen nu met een terminal programma contact maken met de router om deze te configureren.

Testen van de bekabeling
Het testen van de netwerkbekabeling wordt gedaan om te kijken of een nieuw gemaakte verbinding goed functioneert of om te kijken waar zich eventueel een fout in de bekabeling bevindt.
We gebruiken hiervoor meetinstrumenten die volgende zaken kunnen meten:

- wire map,
- kabellengte,
- near-end crosstalk,
- ruisniveau,
- split pairs,
- signal attenuation.

Met de **wire map** meting wordt onderzocht welke aderparen met welke pennen verbonden zijn. Hiermee kan bepaald worden welk type kabel het is (straight, cross-over of roll-over) en of de aders in een paar niet omgedraaid zijn (reversed order).

Straight	Cross-over	Roll-over	Reversed order 3-2, 6-1	
1 2 3 6 4 5 7 8	**3 6 1 2 4 5 7 8**	**1 2 3 4 5 6 7 8**	**3 6 1 2 4 5 7 8**	**← ene uiteinde**
1 2 3 6 4 5 7 8	**1 2 3 6 4 5 7 8**	**8 7 6 5 4 3 2 1**	**2 1 3 6 4 5 7 8**	**← andere uiteinde**

De kabellengte wordt gemeten door een puls in een aderpaar te sturen en de tijd te meten tussen het verzenden van een signaal en het ontvangen van de gereflecteerde puls De verzonden puls wordt gedeeltelijk gereflecteerd aan het uiteinde van de kabel omdat de kabel wordt afgesloten met een weerstandsnetwerkje die niet gelijk is aan de impedantie van de kabel (misaanpassing). We noemen dit een **time domain refection** meting (TDR). De meting wordt per aderpaar uitgevoerd omdat een storing veroorzaakt kan worden door één aderpaar.
Deze meting is ook uit te voeren met een open- of kortgesloten kabel. Hierdoor kan de plaats van een fout in een bestaande installatie opgespoord worden.

Near-end crosstalk kan veroorzaakt worden door het te ver verwijderen van de twisting en door een te scherpe knik in de kabel. We kunnen dit onderzoeken door de aansluitingen en de kabelloop te inspecteren of door gebruik te maken van een meetinstrument dat een pulstrein in een aderpaar stuurt met een oplopende frequentie en meet of er op de andere paren een reactie voorkomt.

Het ruisniveau (**noise level**) is de mate van invloed van externe stoorbronnen op de kabel. We meten dit door de kabel los te koppelen van de computer en de netwerkapparatuur. Als het niveau te hoog is kunnen we proberen om mogelijke stoorbronnen in de omgeving één voor één uit te schakelen om zo de oorzaak op te sporen.

Split pairs is het verkeerd aansluiten van een connector. Hierbij worden twee draden van twee verschillende aderparen verwisseld. We kunnen dit onderzoeken door de aansluitingen visueel te inspecteren of door een near-end crosstalk meting uit te voeren.

Signal attenuation is de verzwakking van het signaal van het begin tot het eind van de kabel. We meten dit met op het ene eind een apparaat aan te sluiten die een signaal levert met een bepaald energie niveau en aan de andere zijde met een meter het ontvangen niveau te meten.

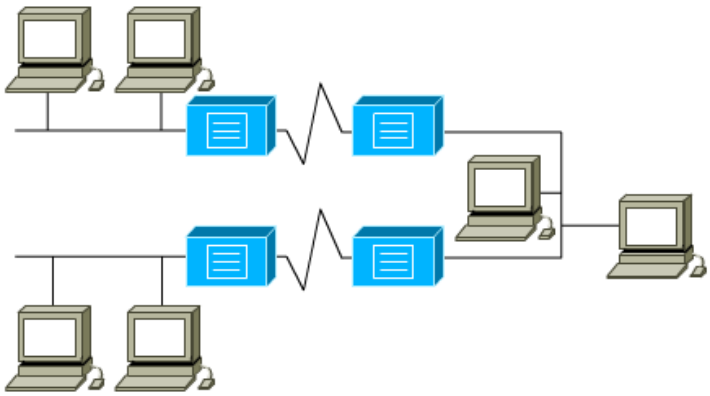
De metingen en de meetinstrumenten zijn afhankelijk van het te meten kabeltype.

Layer 1 netwerkapparatuur
Naast de bekabeling en de connectoren zijn er nog een aantal onderdelen die in layer 1 hun werk doen. Op de eerste plaats is het de interface elektronica zoals die voorkomt op een NIC. Dit onderdeel voert naast layer 1 functies ook layer 2 functies uit.
De onderdelen die zich alleen op layer 1 bevinden zijn de **repeater** en de **multiport repeater of hub**. Dit zijn onderdelen die het ontvangen signaal versterken (terugbrengen in de oude staat) en doorsturen naar alle aanwezige poorten. Niet alleen de datasignalen maar ook alle storingen worden doorgegeven. Op een netwerkdeel wat bestaat uit kabels, repeaters en hubs zijn alle elektrische signalen op elk punt aanwezig. We spreken voor dit netwerkdeel over een collision domein als het een ethernet is.
De repeater wordt gebruikt om de afstand tussen de transmitter en de reciever te vergroten. De hub wordt toegepast in een fysieke ster topologie waarbij de hub het sterpunt inneemt. De afstand van een systeem tot de hub is gelijk aan de maximale lengte van de bekabeling. De afstand tussen twee systemen via een hub kan nu groter zijn dan de maximale lengte van één kabel.

Er kunnen tussen twee systemen meerdere kabels en repeaters of hubs voorkomen. Hiervoor moet, voor de 10basex, de 12345 regel in acht genomen worden.

12345 regel

- 5 verbindingen
- 4 repeaters/hubs
- 3 verbindingen met hosts
- 2 verbindingen zonder hosts
- 1 collision domain



De fysieke typologieën worden ook beschreven in layer 1 evenals het voorkomen van collisions in een ethernet.
Het beheer van de toegang en het afhandelen van de collisions is een taak van layer 2. Met layer 2 en 3 apparatuur (bridges, switches en routers) kunnen we een netwerk in meerdere collision domeinen opdelen (**segmentation**). Dit wordt gedaan als de collisions het netwerkverkeer te veel beïnvloeden.

Layer 1 is het onderdeel dat voor een installateur van computernetwerken het belangrijkste is. Hierin worden de fysieke typologieën, kabeltypes, connectoren, afstanden, signaalvormen, mogelijke fysieke stoorbronnen ed. beschreven. Het is belangrijk dan de montage vakkundig plaatsvindt en dat men weet hoe men storingen opspoort en kan verhelpen.

In IEEE 802.3 worden een aantal ethernet-technologieën beschreven. In de volgende tabel is een overzicht van een aantal specificaties.
De snelheden (**transfer rates**) die gebruikt worden zijn: 10Mbps, 100Mbps, 1000Mbps en 10Gbps (is in ontwikkeling). Alle vormen gebruiken het medium als **baseband**.
De logische topologie van ethernet is een bus.

Table. Ethernet technology

	10base2	**10base5**	**10baseT**	**100baseTx**	**100baseT4**	**100baseT2**	**100baseFx**
Cabling	Thin coax RG58 50Ω	Thick coax RG8 50 Ω	TIA/EIA UTP Cat3, 4 5, 2 pairs	TIA/EIA UTP Cat5, 5e, Type 1 STP, 2 pairs	TIA/EIA UTP Cat 3, 4, 5, 4 pairs	TIA/EIA UTP Cat3, 4 5, 2 pairs	62.5/125 µm multimode fiber
Connector	BNC	AUI/DIX	RJ45	RJ45	RJ45	RJ45	ST
Max. length	185m	500m	100m	100m	100m	100m	412m
Physical topology	Bus	Bus	Star	Star	Star	Star	Point to Point

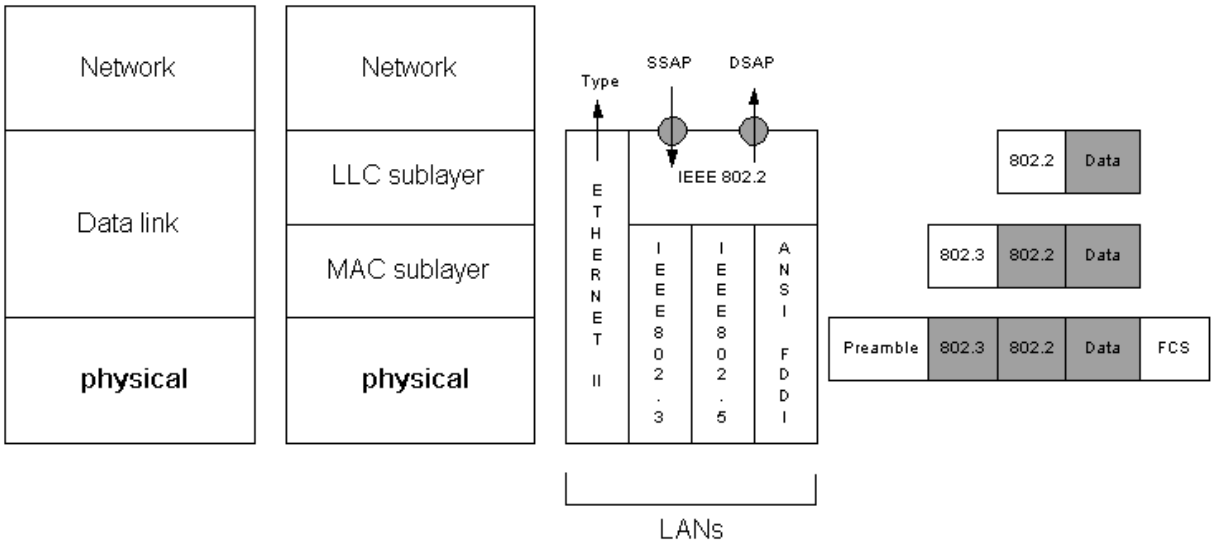
Vragen en opdrachten

1. Wat is de hoofdfunctie van een netwerkmedium?
2. Welke drie media worden er gebruikt?
3. Wat is de reden dat aderparen getwist zijn in een TP kabel?
4. Wat is de reden van pair shielding en wat die van overall shielding?
5. Welk bedrijvenpaar heeft normen gemaakt voor de fysieke laag?
6. Wat is de maximale lengte van UTP, Thin coax en Thick coax?
7. Welk glasvezeltype wordt toegepast in LANs?
8. Welke connectoren worden toegepast bij de verschillende netwerkverbindingen?
9. Wanneer gebruiken we een straight-trough, cross-over en roll-over kabeltype?
10. Waarom kunnen we een straight kabel gebruiken om een PC aan een hub te koppelen?
11. Welke zaken kunnen gemeten worden aan een netwerkverbinding?
12. Wat is het probleem bij een reversed order fout?
13. Wat is TDR en hoe werkt dit?
14. Wat wordt bedoeld met de 12345 regel?

Aantekeningen

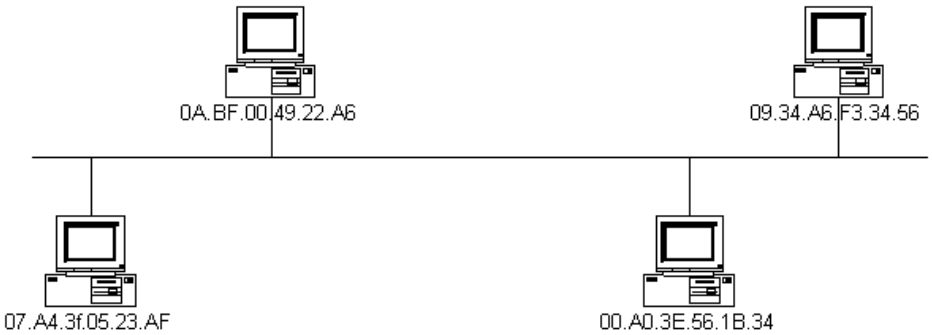
1.6 Layer 2, Concepts

De fysieke laag specificeert de elektrische, mechanische, procedurele en functionele eisen voor het activeren, beheren en deactiveren van een fysieke verbinding tussen systemen.
Dit zijn de specificaties zoals spanningniveaus, data rate (bps), encoding methode, maximale kabellengte en connectortype (bv RJ45).
De LAN-standaarden die gebruikt worden, zijn gemaakt door het **Institute of Electrical and Electronic Engineers (IEEE)** en het **American National Standards Institute (ANSI)**. Deze beschrijven de fysieke en data link laag.



De data link laag

- communiceert met de verschillende LAN-standaards en de protocollen in de network layer (laag 3) via de **Logical Link Control** (**LLC**) sublayer (802.2) met uitzondering van de oude **ethetnet II**-standaard. De koppeling met het protocol uit de netwerklaag wordt gemaakt met een type-nummer (ethernet II) of de DSAP en SSAP nummers (802.2).
- maakt gebruik van een plat (**flat**) adresseringsysteem (flat: geen hiërarchische of plaatsgebonden structuur).

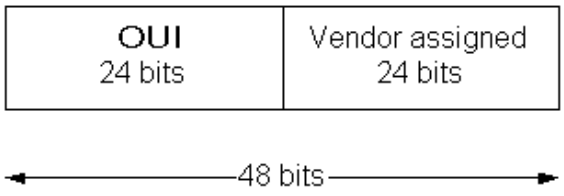


De MAC-nummers hebben een willekeurige waarde (flat). Er zit dus geen hiërarchie in zoals bij de laag 3 adressen die bestaan uit een netwerknummer+hostnummer.

- maakt gebruik van een **frame** bestaande uit een 802.3/802.5/FDDI header en trailer met daarin een 802.2 header en data van de hogere lagen. Ethernet II gebruikt alleen een header en trailer met daartussen de data van layer 3 t/m 7,
- maakt gebruik van **Media Access Control** om te bepalen welke computer bits over de fysieke verbinding mag versturen en controleert (MAC trailer) en analyseert de binnenkomende frames (MAC header).

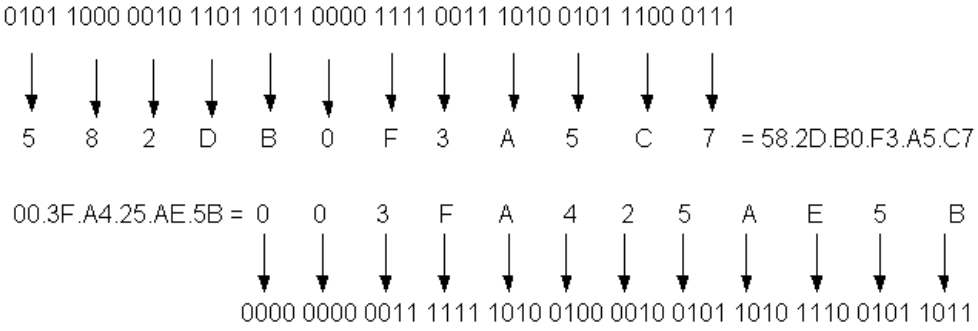
Logical Link control
Deze laag verzorgt dat de invulling van de hogere lagen, onafhankelijk van het gebruikte LAN-type.
Het LLC-protocol is afgeleid van het HDLC-protocol.

Flat addressing system
Elke netwerkinterface in een LAN heeft een uniek adres dat gebruikt wordt om aan te geven voor wie het frame bedoeld is (ontvanger of destination) en van wie het frame afkomstig is (afzender of source). Het adressenbestand wordt, voor ethernet, beheerd door het bedrijf Xerox. Een bedrijf dat netwerkinterfaces maakt, koopt een reeks adressen bij Xerox.
Het adres bestaat uit een 48-bits getal, waarvan de eerste 24bits als **Organizational Unique Identifier** (OUI) dienst doen. Hieraan is dus de maker van de interfaces te herkennen. De laatste 24-bits worden door de maker van de interfaces zelf ingevuld (binnen de gekochte reeks), voor elke interface een ander nummer.

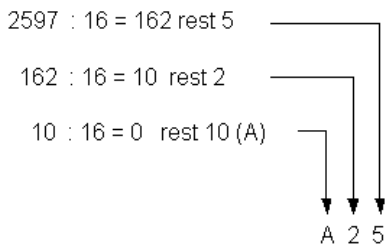


Het nummer wordt door de fabrikant in de interface-elektronica geplaatst (**Burned in**).
Elke interface heeft dus een uniek nummer en kan op elke plaats in de LAN toegepast worden.

Het adres bestaat uit een bitreeks van 48 nullen en enen. Bitreeksen worden weergegeven door middel van hexadecimale getallen om de notatie in te korten en om de kans op fouten te verkleinen.
Een hexadecimaal- of 16 tallig talstelsel (**base 16**) maakt gebruik van de symbolen 0..9,A..F. Met een 4-bits binair (**base 2**) getal kunnen 16 verschillende getallen weergeven (0000 = 0, 0001 = 1, …., 1010 = A, …, 1111 = F). Deze reeks noteren we met een hexadecimaal symbool. Voor een bitreeks van 8-bits gebruiken we dus twee hexadecimale symbolen ($1101\ 0011_{bin} = D3_{hex}$)
Voor het omzetten van een binaire getal naar een hexadecimaal getal of omgekeerd vertalen we steeds 4 binaire bits naar één hexadecimaal symbool of we vertalen een hexadecimaal symbool naar 4 binaire bits.



Voor het converteren van hexadecimale getallen naar decimale getallen (**base 10**) gebruiken we de volgende methode.

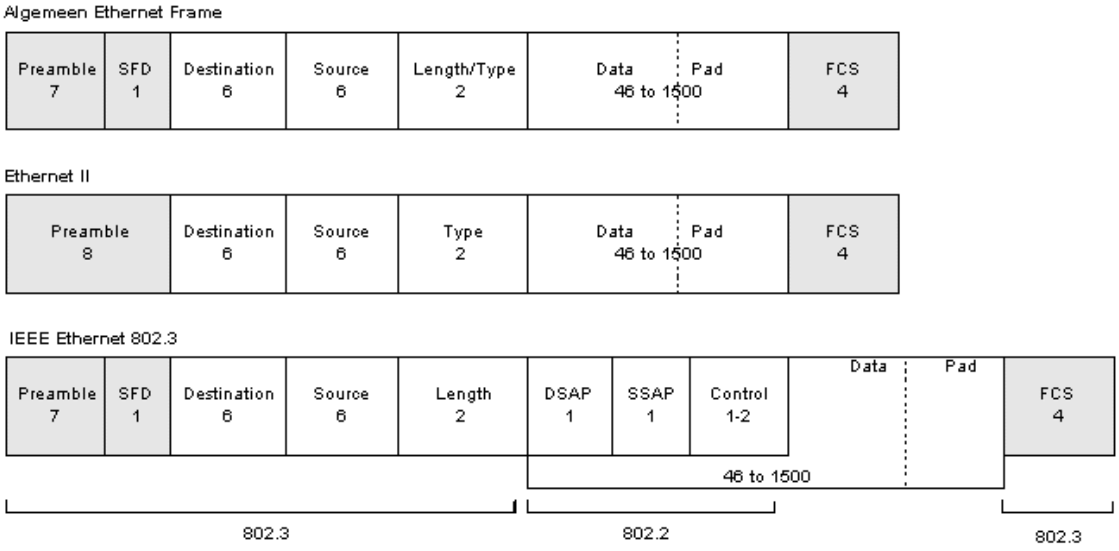


$\mathbf{2597_{dec}} = \mathbf{A25_{hex}}$

$\mathbf{D2E_{hex}} = D(13)x16^2 + 2x16^1 + E(14)x16^0$
$= 13x256 + 2x16 + 14x1$
$= \mathbf{3374_{dec}}$

Een MAC-adres wordt ook wel layer2-adres, hardware-adres of NIC-adres genoemd. We spreken over een **flat** systeem omdat in het adres geen plaatsbepalend element zit. Het logische adres dat in layer 3 toegepast wordt, is een **hiërarchisch** adres omdat dit bestaat uit een netnummerdeel en een hostnummerdeel. (Dit komt in H10 aan de orde).

Framing
Framing is het proces om de data van laag 3 verder in te pakken. Het frame wordt samengesteld door de data link layer die de data uit de hogere lagen voorziet van sublayer headers (802.2 en 802.3).De **transmiter** elektronica begint met het verzenden van het preamble en berekent tijdens het verzenden van het frame de FCS-waarde en voeg deze als laatste toe.
Een frame wordt als een bitstroom verzonden over een synchrone data link. De zendklok en de ontvangklok lopen echter niet constant in de pas. Om deze klokken tijdelijk in de pas te laten lopen begint het frame met 7 bytes (**preamble**) bestaande uit 10101010…. bits, via het 8e byte (**start frame delimitter**) 10101011 herkent de ontvanger het startpunt van het destination MAC-adres. De overige bits in het frame worden gebruikt om de klok in de pas te houden. Nadat het frame gepasseerd is loopt de klok niet meer in de pas. Bij een volgende frame herhaalt het synchroniseren zich weer.
Vanaf het destination adres tot en met de 4 **Frame Check Sequence** (FCS)-bytes wordt, tijdens het inlezen door de **reciever** elektronica, een **CRC checksum** actie uitgevoerd. Als de uitkomst hiervan 0 oplevert, betekent dit dat het frame correct is overgekomen.



Bij een correct frame wordt door de MAC sublayer gekeken of het destination adres een geldig adres is. Als het geen geldig adres is wordt het frame verwijderd (**stripped**). Een geldig adres kan zijn: het adres van de ontvanger, het broadcast-adres of een multicast-adres (niet gebruikt bij token ring).

Als het adres van de ontvanger is, dan spreken we van een **unicast** frame. Dit is een frame dat voor één systeem bedoeld is. Als het adres **FF.FF.FF.FF.FF.FF** is, dan spreken we van een **broadcast** frame. Dit is een frame dat voor alle systemen op het netwerk bedoeld is. Een ander adres wat we **multicast** noemen wordt gebruikt voor frames die bedoelt zijn voor een groep systemen op het netwerk.

Een unicast frame is te vergelijken met een brief.
Een broadcast frame is te vergelijken met een huis aan huis folder.
Een multicast frame is te vergelijken met een krant die bij alle abonnees wordt bezorgd.

De waarde in het **length/type** veld bepaalt of het een ethernet II of IEEE 802.3-frame is. Loopt de waarde van 46 t/m 1500 ($\mathbf{5DC}_{\mathbf{hex}}$ = 5x256 + 13x16 + 12 = 1500_{dec}) dan hebben we te doen met een 802.3 frame en is ook direct de lengte van het data-veld bekend. Is de waarde $\mathbf{600}_{\mathbf{hex}}$ of hoger dan is het een ethernet II-frame. Het typenummer geeft aan voor welk protocol uit de netwerklaag het pakket bestemd is. Voor de lengte bepaling wordt bij een ethernet II-frame het data-veld geanalyseerd.
Bij een 802.3-frame wordt het data-veld met daarin de 802.2 header doorgegeven aan de LLC sublayer. De SSAP geeft aan van welk layer 3 protocol het pakket afkomstig is en DSAP geeft aan voor welk protocol het bestemd is. De controlbits zijn bedoeld voor de diverse functies van het LLC protocol en worden niet verder behandeld.

De data in het data-veld bestaat, inclusief de 802.2 header, uit minimaal 46 bytes en maximaal 1500 bytes. Dit stamt uit het begin van het ethernet. Als het data-veld minder dan 46 bytes bevat dan wordt het veld aangevuld met **padding** bytes. De minimale frame-lengte is 6+6+2+46+4 = 64 bytes of 512 bits. Dit is nodig om in een collision domein een collision nog te kunnen detecteren. Dit geld voor een 10 en 100Mbps netwerk. Voor de 1000Mbps netwerken wordt een minimale frame-lengte van **416…520 bytes** geëist. Als het frame hier niet aan voldoet worden achter de FCS nog bits toegevoegd (**extention bits**) voor collision-detectie. Deze bits bezitten geen informatiewaarde.

Media Access Control
Media access control is het protocol van de MAC-sublayer die te toegang tot het transportmedium regelt en beheert.
Er bestaan twee soorten van media access control:

- **deterministisch** (vastgelegd, bepaald): wachten op je beurt (**taking turns**).
- **non-deterministisch:** wie het eerst komt, wordt het eerst geholpen (**first come, first served**).

Deterministic
Hierbij wordt het medium maar door één zender (transceiver) gebruikt. De verbindingen tussen de systemen vormen een **logische ring**. Token Ring en FDDI maken hier gebruik van. Wanneer er geen communicatie plaatsvindt wordt een "leeg" frame (**token**) van het ene systeem naar het volgende systeem doorgegeven.
Als een systeem wil communiceren, dan wacht deze tot dit token passeert (**token passing**). Het systeem verandert het token in een "bezet" token en voegt zijn data + headers aan het token-frame toe. De andere systemen in de ring kijken of het frame voor hen bedoeld is. Is dit het geval dan kopieert deze het frame en stuurt het vervolgens door naar het volgende systeem. Als het frame weer bij de zender aangekomen is, verwijdert deze het frame en kan opnieuw een frame verzenden. Wanneer het laatste frame verzonden is, wordt het token weer veranderd in een "leeg" token en op de ring gezet.
Een van de systemen in de ring werk als arbiter. Deze regelt het toevoegen van een systeem in de ring en voorkomt dat een systeem te lang het token in bezit houdt.

Non-deterministic
Hierbij wordt het medium gedeeld door meerdere systemen (**shared medium**). We spreken hierbij over een **logische bus**. Ethernet is een logisch bussysteem. Als het stil op de bus is (**carrier sense**), betekent dit, dat er niet gezonden wordt. Alle systemen luisteren of de bus vrij is. Alle systemen die willen zenden, kunnen dit nu proberen (**multi access**). Als één systeem zendt, gaat dit probleemloos.

Proberen er echter meerdere systemen gelijktijdig te zenden dan vermengen deze signalen zich op het medium en zijn daardoor onbruikbaar geworden. We spreken nu van een botsing (**collision**) die herkenbaar is aan een abnormaal spanningsniveau.
De systemen die op de bus zijn aangesloten nemen de botsing waar (**collision detect**) en stoppen met zenden. Na een bepaalde tijd (**back off**) doet men weer een nieuwe poging. We noemen deze access-methode **CSMA/CD**.

LAN topology
Bij LANs spreken we over logische- en fysieke typologieën. De logische topologie geeft de access-methode aan.
De fysieke topologie geeft de manier aan waarop de verbindingen zijn geïnstalleerd.

LAN type	**Logische topologie**	**Fysieke topologie**
Ethernet	Shared (CSMA/CD)(bus)	Bus, star, extended star
Token Ring	Token passing	Ring, star
FDDI	Token passing	Dual ring

Vragen en opdrachten

1. Door welke instituten zijn de OSI layers 1 en 2 voor LANs ingevuld?
2. Wat is de functie van de LLC sublayer?
3. Wat zijn de functies van de MAC sublayer?
4. Wat is de functie van het preamble en de SFD?
5. Wat is de functie van de FCS bytes?
6. Wat zijn padding bytes?
7. Wat zijn extention bits?
8. Wat is het verschil tussen een flat- en een hiërarchisch adresseringssysteem?
9. Maak duidelijk wat er bedoeld wordt met een unicast-, broadcast- en multicast frame.
10. Noteer het hexadecimale getal $A25_{hex}$ als binair getal.
11. Noteer het binaire getal 1011 1000 0001 1010 0111 1111_{bin} als hex. getal.
12. Wat is het verschil tussen token passing en token ring?
13. Beschrijf de begrippen:
    - Framing, preamble, SFD en FCD,
    - Unicast, broadcast, multicast,
    - LLC, MAC,
    - Deterministic, non-deterministic,
    - Logische topologie, fysieke topologie

Aantekeningen

1.7 Layer 2, Technologies

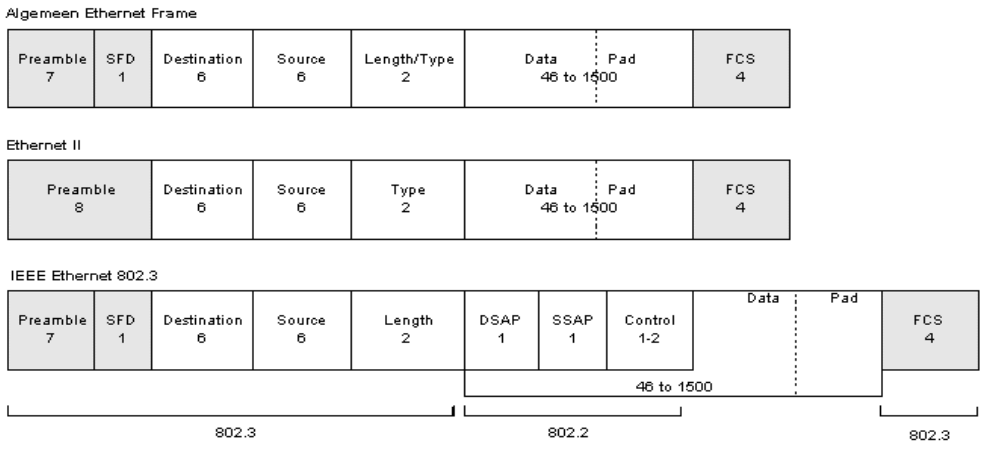
Van de Layer 2 technologieën worden de drie belangrijkste (ethernet, tokenring en fddi) behandeld. Hiervan is ethernet de verreweg meest gebruikte en het cursusmateriaal richt zich hier hoofdzakelijk op. Rond 1997 bestonden 85% van de netwerken uit 10baseT technologie. Token Ring is een ontwikkeling waarvan de toepassing sterk terug loopt en FDDI wordt toegepast als er aan de lengte, snelheid en betrouwbaarheid een hoge eis gesteld wordt. FDDI vindt vooral toepassing als backbone in grotere netwerken.

Ethernet
Ethernet is een ontwikkeling van het bedrijf Xerox en is geïntroduceerd omstreeks 1972. De data rate was 3Mbps en men maakte gebruik van CSMA/CD als access-methode. Door het succes hiervan besloten drie bedrijven in 1980 een tweede versie van ethernet uit te brengen wat Digital-Intel-Xerox (DIX) Ethernet II wordt genoemd.
Het IEEE heeft in 1985 zijn beschrijving van ethernet geïntroduceerd onder het nummer 802.3. Deze uitvoering maakt gebruik van een LLC (802.2). Dit is op dit moment de standaard op ethernet gebied.
Ethernet maakt gebruik van alle mogelijke media als koper (coax, TP), fiber en wireless. De data rate loopt van 10Mbps, 100Mbps (fast ethernet) tot 1000Mbps en de 10 Gbps wordt in 2002 gepresenteerd. De kabellengte is afhankelijk van het gebruikte medium en de data rate. De verbindingen zijn synchroon met manchester encoding.

Lay-out
Stations in een ethernet kunnen op verschillen manieren met elkaar worden gekoppeld. De coax uitvoering wordt als bus gerealiseerd, TP als ster of extended-ster en de fiber als point to point topologie. Als sterpunt worden hubs of switches toegepast. Deze koppelingsmanieren noemen we fysieke typologieën. De frames op een ethernet worden naar alle station op het net verzonden en worden door alle station vrijwel gelijktijdig ontvangen. We noemen dit een **broadcast** systeem. Het medium wordt gedeeld (shared) door alle systemen. We noemen dit een **logisch bus**systeem. De access-methode staat toe dat meerdere systemen gelijktijdig kunnen beginnen met zenden. Als dit het geval is dan treedt er een collision op die door het MAC protocol wordt gedetecteerd en opgelost.

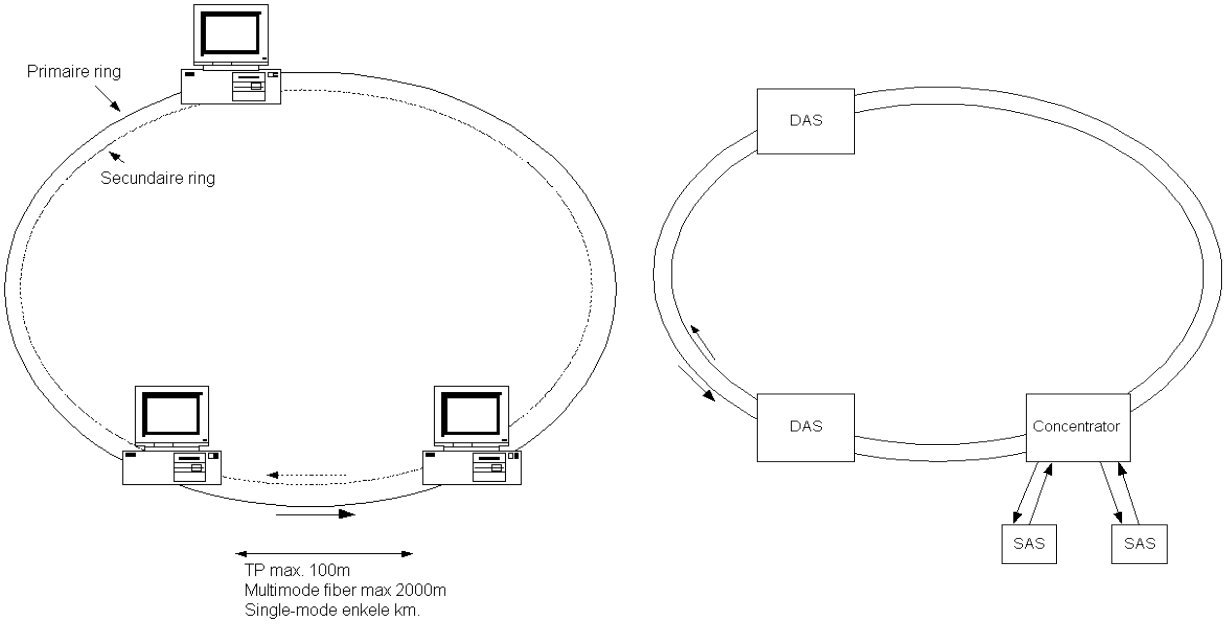
Physical layer
In de physical layer worden een groot aantal media typen beschreven die herkenbaar zijn aan coderingen als 10base2, 10base5, 10baseT, 100baseT, 100baseFx, 100baseT4, 1000baseF enz. De kabellengte loopt van 100m voor TP tot 2km voor fiber toepassingen.

Ethernet MAC sublayer
Hier wordt de framing, error detectie en het access protocol uitgevoerd. In hoofdstuk 1.6 is het een en ander al behandeld.



FDDI
Het **fiber distributed data interface** (**FDDI**) netwerk is ontwikkeld door het ANSI en is in 1986 geïntroduceerd onder de norm **X3T9.5**. Het werd toegepast voor het koppelen van snelle werkstations en LANs. Het in 1997 geïntroduceerde 100BaseT netwerk is een veel goedkopere toepassing voor het koppelen van werkstations zodat de toepassing van FDDI zich nu hoofdzakelijk richt op LAN **backbone**s vanwege de betrouwbaarheid (dual-ring) en de grotere afstanden tussen nodes en in een omgeving met veel EMI/RFI invloeden.
Dit netwerktype is ook uit te voeren met TP kabels. We spreken dan over **copper distributed data interface** (**CDDI**).

Layout
FDDI werkt met een data rate van 100Mbps en twee ringverbindingen (**dual-ring**) een primaire en een secundaire ring waardoor de betrouwbaarheid (**reliability**) hoger is dan bij andere netwerktypen. Er kunnen maximaal 500 nodes in de ring worden opgenomen en de maximale ringlengte voor fibers is 200km.
Dataverkeer kan in beide ringen plaatsvinden. De transportrichting is tegengesteld. Bij een normale werking is de primaire ring actief en de secundaire ring idle.



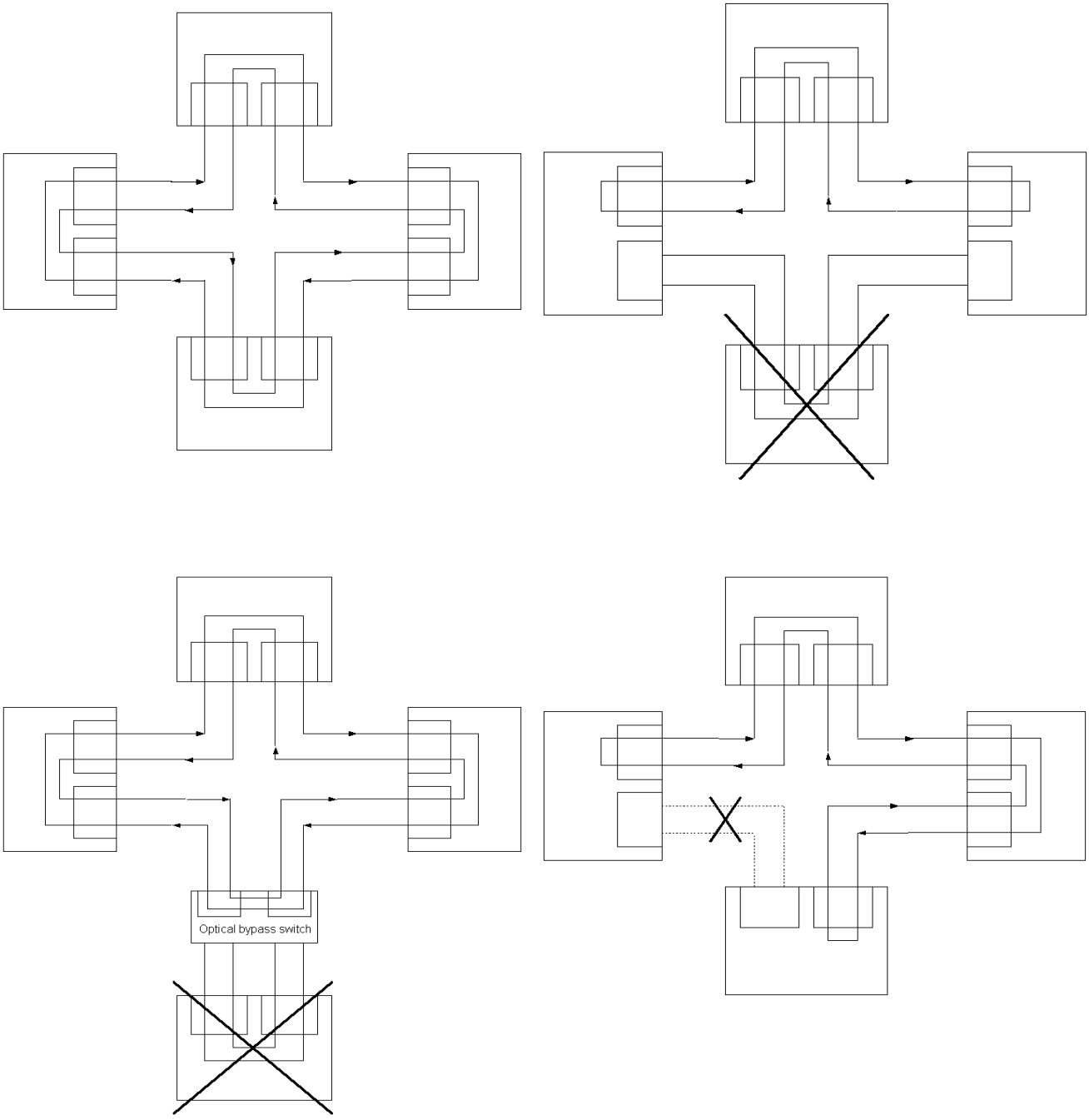
De nodes kunnen een **klasse A of B** interface hebben. Een klasse B betekent dat de node in de primaire- en secundaire ring is opgenomen. Bij een klasse A is de node alleen in de primaire ring opgenomen. Een klasse A node wordt in de ring gekoppeld via een **concentrator**.
De klasse A interface is een single-attachment station (**SAS**) en een klasse B een dual-attachment station (**DAS**).

Men heeft gekozen voor deze opbouw om een hoge betrouwbaarheid te garanderen.
Bij het detecteren van een fout, als het uitvallen van een DAS-, SAS systeem, concentrator of een kabelbreuk, stelt het netwerk zich zo in dat de nog actieve systemen kunnen blijven communiceren.

- DAS systeem valt uit!
  Oplossing 1: Het DAS systeem heeft een optische bypass switch die de ringen doorverbinden.

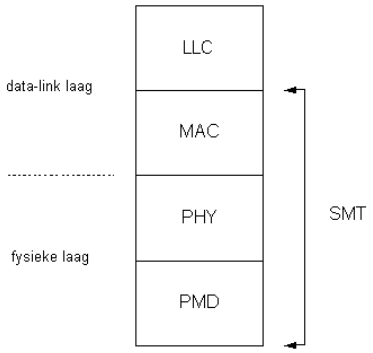
Oplossing 2: Het voorgaande en volgende station koppelen de primaire en de secundaire ring die nu samen
de communicatie ring vormen.

- SAS systeem valt uit!
  Oplossing: De concentrator bypass de interface.
- Concentrator valt uit!
  Oplossingen zijn gelijk aan die bij een DAS, alleen zijn nu de aangesloten SAS systemen uit de ring.
- Kabelbreuk!
  Oplossing: De systemen voor en achter de breuk koppelen de primaire en de secundaire ring die samen de ring vormen.



Een ander mechanisme, wat gebruikt wordt om de betrouwbaarheid te vergroten, is het **dual homing** principe.
Belangrijke systemen zoals servers en routers worden gekoppeld met twee concentrators. De ene verbinding is de actieve link en de tweede is de passieve of stand-by link.
Naast de hoge betrouwbaarheid van FDDI is de fiber uitvoering veel moeilijker af te tappen doordat het maken van een fysieke koppeling moeilijk is en er geen elektromagnetische interferentie voorkomt. Dit is een aspect wat zwaar weegt is het gaat om security. Een aftappunt is met speciale apparatuur (TDR) op te sporen, dit is bij een koperverbinding meestal niet mogelijk.

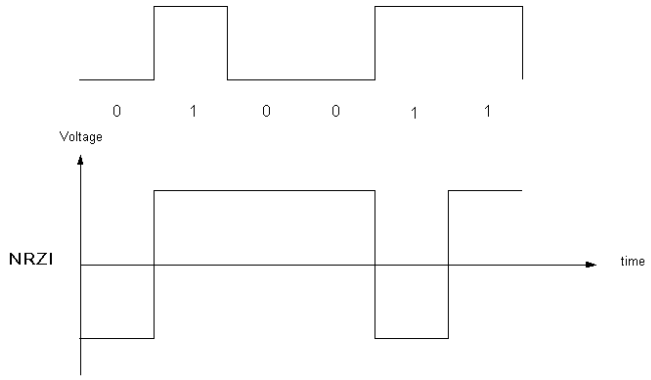
De FFDI standaard omvat de fysieke layer en de MAC sublayer uit het OSI-model. De fysieke laag is nog onder- verdeeld in twee sublayers. De physical medium dependent (**PMD**) sublayer en de physical (**PHY**) sublayer.
Naast de onderverdeling in drie sublayers omvat de standaard ook nog een station management protocol (**SMT**).



In de PMD sublayer komen de verschillende mediumtype en bijbehorende connectoren aan de orde:

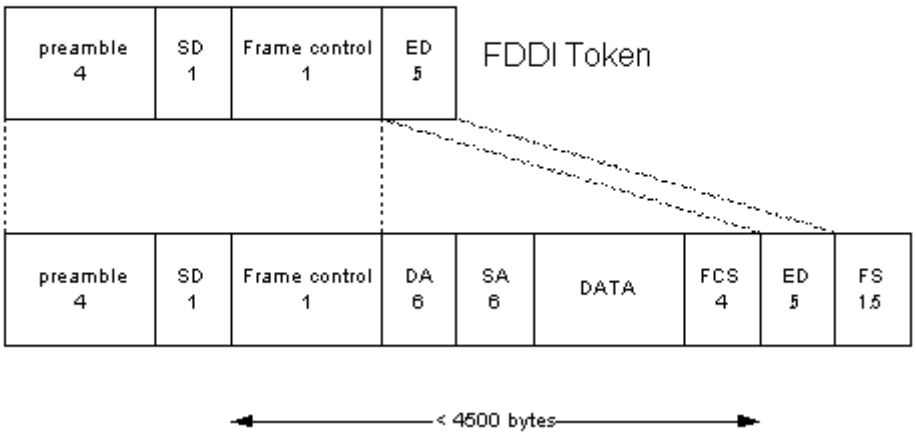
- TP (**CDDI**) met een max. lengte van 100m,
- Multimode fiber (62,5/125µm) met als transmitter een ligth emitting diode (**LED**) met een golflengte van 1,3µm en als reciever een PIN diode. De maximale lengte is 2km.
- Single-mode fiber (8/125µm) met als transmitter een laser diode (**LD**) overbrugt een lengte van enkele kilometers.

In de PHY sublayer wordt de encoding behandeld.
Elke 4-bits uit een FDDI-frame wordt als 5-bits (**4B/5B**) code verzonden via een NRZI signaal. Dit wordt gedaan om voldoende signaalwisselingen te krijgen om de synchronisatie te waarborgen. De codering is zo gekozen dat er nooit meer dan 2 nullen achter elkaar kunnen voorkomen. Om de snelheid van 100Mbps te kunnen halen worden de bits met een kloksnelheid van **125 MHz** verzonden.
De NRZI modulatie is een techniek waar, bij elk begin van een 1 een signaalverandering plaatsvindt en bij een 0 blijft het signaal gelijk.



De FDDI MAC-sublayer.
Door de MAC layer wordt de framing, access-methode en error detectie uitgevoerd.

FDDI frame



De 4 **preamble** bytes worden gebruikt om de zend- en ontvangstklok op elkaar te synchroniseren. Het **start delimiter** (SD) byte zorgt dat de ontvanger het begin van het frame kan bepalen.

Nu volgt het **frame control** (FC) byte dat gebruikt wordt om:

- De lengte van het adresveld aan te geven,
- De verschillende control/test functies aan te geven. Hieronder vallen de ring management functies. Een van die functies is de toegangsmethode. Als een frame een node passeert (**token passing**) dan onderzoekt de MAC layer of het een leeg token is waarna met het verzenden begonnen kan worden. Zo niet dan wordt het frame doorgestuurd naar de volgende node in de ring.
- De datavorm aan te geven. Binnen een FDDI netwerk wordt onderscheid gemaakt tussen audio/video en data. Audio en video gegevens worden **synchrone data** genoemd. De overige frames vervoeren **asynchrone data**. Het delay tussen synchrone frames is belangrijk voor het goed functioneren van de audio/video-applicaties terwijl de delay van algemene data minder van belang is.
  Bij een FDDI netwerk krijgt elke node een bepaalde tijd waarin hij frames kan verzenden. Dit is mede afhankelijk van het aantal nodes in de ring. In de toegekende tijd worden eerst de frames met synchrone data verzonden en als er nog tijd over is kan deze gebruikt worden om asynchrone data te verzenden.

Als het frame een leeg token bevat dan volgt er nu 0,5 bytes als 5-bitscode de **end delimiter** (ED). Dit is een bitcombinatie die niet gebruikt wordt in de omzetting van 4-databits naar een 5-bitscombinatie waardoor de reciever het herkent als ED.

Als het een data/control frame is dan volgt nu het **destination adresveld** (DA). Hierin staat het adres van de node waarvoor het frame bedoeld is (unicast) of een groepsadres (multicast) of een adres voor alle nodes (broadcast). In het volgende adresveld bevindt zich het adres van het station dat het frame verzonden heeft (SA).

Het dataveld bevat control info of upper-layer headers plus data. De lengte van het frame vanaf het FC-veld t/m het FCS-veld dus inclusief het dataveld bedraagt **maximaal 4500 bytes**.

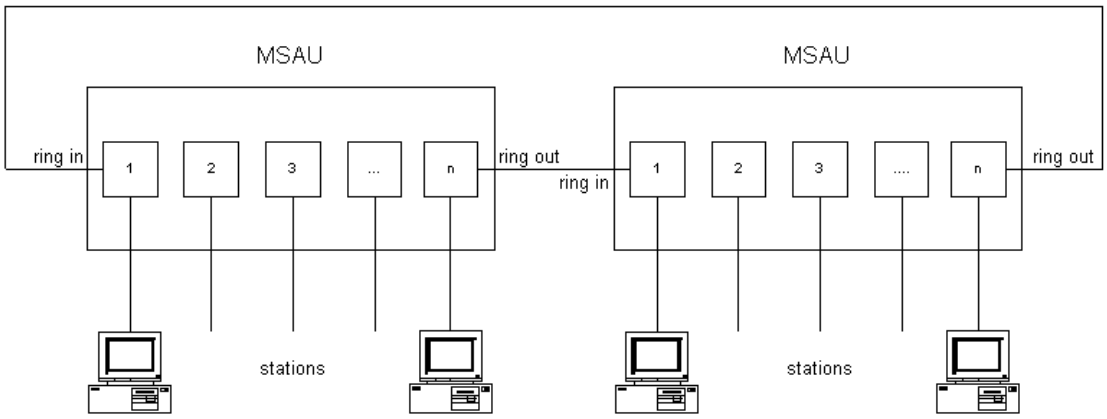
Het FCS-veld wordt tijdens het verzenden door de elektronica berekend en na het dataveld toegevoegd, gevolgd door een 5bitscode (ED).

Als laatste wordt een 1,5 bytes **frame status** (FS) veld toegevoegd die gebruikt wordt voor error meldingen en gebruikt wordt door het **station management protocol** (SMT).

Het SMT detecteert fouten en kiest een oplossing om de ring te repareren. Tijdens de reparatie werkzaamheden is het netwerk even down evenals het moment dat een systeem in de ring wordt ingeschakeld. Tijdens deze downtime repareert het SMT de ring of neemt het nieuwe systeem op in de ring door zijn interface te testen en hem in de administratie op te nemen. Hetzelfde geldt voor defecte onderdelen die vervangen worden zodat de er weer een reparatie actie wordt uitgevoerd om de ring weer in zijn oude staat terug te brengen.
Deze **self-healing** functie is zeer belangrijk voor netwerken die een hoge betrouwbaarheid (**reliability**) vereisen.

Token Ring
Het tokenring-netwerk is een ontwikkeling van IBM uit 1970 dat werk met een data rate van 4- of 16Mbps en werk met STP type 1 bekabeling. Het is een zeer betrouwbaar maar erg dure toepassing, maar wordt steeds minder vaak toegepast vanwege de lage data rate en prijs. De IEEE heeft een beschrijving gemaakt onder nummer 802.5 die vrijwel volledig compatible is met de IBM versie. De IEEE 802.5 maakt gebruik van TP voor de 4Mbps versie en TP of fiber voor de 16Mbps uitvoering. Er kunnen maximaal 250 nodes in een ring worden opgenomen, er wordt gebruik gemaakt van token passing als access-methode en differential manchester-encoding als baseband signalering.

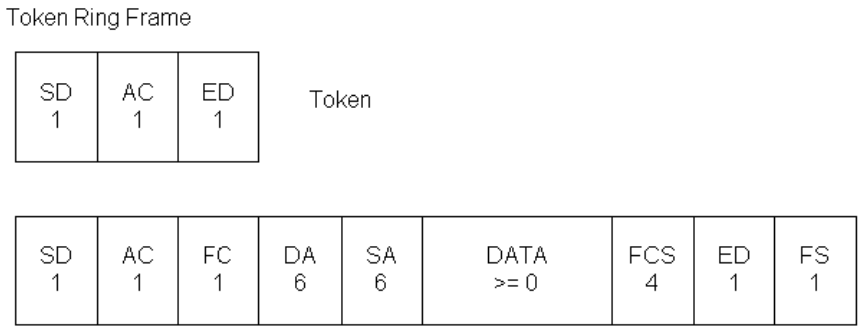
Layout
De bekabeling kan in een ring worden uitgevoerd (van systeem naar systeem) maar meestal wordt een ster topologie gekozen met als sterpunt een **multistation access unit** (MSAU). De systemen worden op een poort van de MSAU aangesloten die intern de aangesloten systemen in een ring schakelt. De niet gebruikte poorten staan in de bypass-mode. Meerdere MSAU's worden met elkaar doorverbonden in en ring.



Physical layer
Een station dat geen frames verzend, zendt de ontvangen frames door naar het volgende station. In elk station bevindt zich een **quartz** gestuurde zendklok. De frequenties van deze klokken zijn niet identiek zodat een frame sneller binnen kan komen dan dat het doorgezonden wordt of omgekeerd. Om dit probleem op te lossen wordt er gewerkt met een **elasticity buffer.** Dit is een buffer waarin binnenkomende bits geplaatst worden en als er enige bits ontvangen zijn start het verzenden ervan. De grootte van de buffer is enkele tientallen bits, groot genoeg om het snelheidsverschil op te vangen. Het protocol is zo, dat tijdens het doorgeven er altijd bits in de buffer staan.

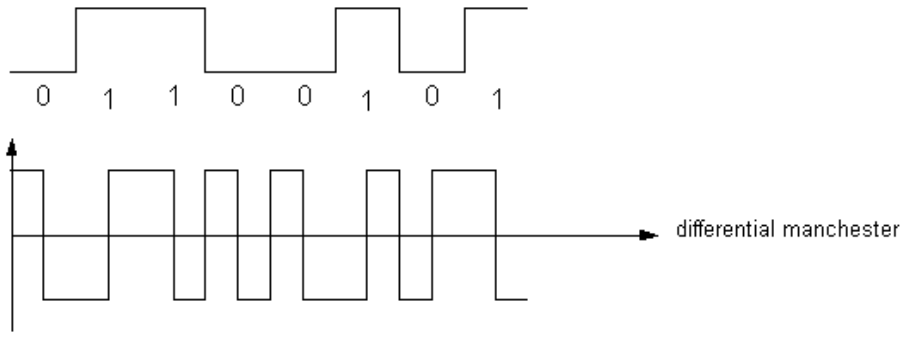
Token Ring MAC sub layer
Deze layer zorgt voor de framing. In de **idle state** van de ring wordt er een token door de ring gestuurd. Als een station wilt zenden wacht hij tot er een token of data-frame passeert. Het station veranderd het token en plaats zijn **prioriteit of reservering** erin. Een station kan een reservering plaatsen als hij een hogere prioriteit heeft dan de prioriteit die in het frame staat vermeld. Met dit

mechanisme is het mogelijk om urgente data sneller te kunnen verzenden dan algemene data. Als er een reservering is geplaatst dan stopt het zendende station met zenden nadat het zijn frame ontvangt. Als er geen reservering is dan kan hij 10ms lang blijven zenden voordat hij het token weer vrij moet geven. In het **access control** (AC) byte wordt ook aangegeven of het frame een data of control frame is.



De start delimiter is een byte die het begin van een token of data/control frame aangeeft. De bitcombinatie van de SD komt, door het gebruik van een coderingsmechanisme, niet voor in de rest van het frame. Het AC bevat 3-bits voor de prioriteit, 3-bits voor reservering, 1-bit voor token/data-control en 1 monitor-bit. Deze laatste wordt gebruikt door het ring management protocol om een frame dat niet van de ring wordt genomen te detecteren en te verwijderen. Eén van de systemen functioneert als ringmanager. Dit kan elk systeem zijn en als een managersysteem wordt uitgeschakeld neemt een ander systeem de functie over. De manager voert ook het managementprotocol uit als een systeem in de ring wordt aan of uitgezet.
Het frame control byte bevat data of control informatie.
De DA en SA bevatten de MAC-adressen. En DA kan zijn een unicast, broadcast of **functional address**. Dit laatste adres wordt gebruikt door een bridge of switch die tokenring-segmenten koppelt.
Het dataveld bevat control informatie of upper-layer headers plus data. De maximale lengte wordt bepaald door de token holding time. Dit is de tijd dat een station een token in zijn bezit mag hebben.
Het FCS-veld bevat het CRC dat tijdens het verzenden berekend wordt en door de ontvanger gebruikt wordt of de geldigheid van een frame te bepalen.
Daarna volgt nog een ED byte en een FS byte dat door het ring management protocol gebruikt wordt.

Token Ring maakt gebruik van differential manchester encoding.



Bij deze encoding vindt er altijd een signaalverandering plaats in het midden van een bit en aan het begin van een 0.

Layer 2 devices (Ethernet)
De onderdelen die hun hoofdfunctie op laag 2 uitvoeren zijn:

- NIC.

Dit is de interface in PC's, servers, netwerkprinters e.d. Er bestaat een NIC voor elk netwerktype. Voor de keuze van een NIC moeten we beschikken over gegevens als; mediumtype, netwerktype, data rate en systeembustype. Bijv. UTP, Ethernet 100baseT (100Mbps) en PCI. Bridges, switches en routers hebben ingebouwde interfaces of wanneer het modulaire systemen zijn kunnen er interfacemodules worden bijgeplaatst.

- Bridges.
  Een bridge heeft als functies:
  - Het koppelen van netwerksegmenten, waarbij de segmentering wordt toegepast om collisions te verminderen en te beperken tot één segment. De bridge geeft een collision niet door aan de andere segmenten die op de bridge zijn aangesloten.
  - Koppelen van netwerksegmenten van verschillende netwerktypen.
    Als we netwerksegmenten van dezelfde technologie koppelen dan noemen we het bridge-protocol **tranparent bridging**. Hierbij worden de frames wel of niet doorgegeven op basis van het MAC destination address. Dit beslissing wordt genomen door een **tabel** te raadplegen waar alle MAC adressen met hun poortnummer staan vermeld. Het frame wordt nu onveranderd doorgegeven.
    In een netwerk worden ook frames verstuurd met een algemeen destination address (broadcast address). Deze frames worden doorgestuurd naar alle andere segmenten. Alle segmenten van het netwerk waar de broadcast-frames naar toe worden gestuurd vormen samen één broadcast-domein. Als het aantal broadcast-frames erg talrijk wordt, spreken we over een broadcast storm. De throughput neemt dan sterk af en wordt het tijd dat we het netwerk opdelen in meerdere netwerken of subneten.. We hebben nu wel een router nodig om deze deelnetten met elkaar te laten communiceren. We hebben nu een internet geconstrueerd.
    Bij een koppeling van verschillende technologieën zorgt de bridge voor frame conversie, buffering en snelheidsaanpassingen. Het bridge-protocol wordt nu **source routing** genoemd.
- Switches.
  Een switch is een nieuwere uitvoering van een bridge met meer functionaliteit en een hogere verwerkings-snelheid. Een switch heeft over het algemeen meer poorten. Elke poort is dan gekoppeld met één systeem zodat er segmenten zonder collisions (**microsegmentering**) ontstaan. Bij een bridged-netwerk bestaan de segmenten meestal uit shared-netwerken als een bus of een ster met een hub als sterpunt. In een switched-netwerk vervangen de switches de bridges plus de hubs. In een switched-netwerk vormen alle microsegmenten samen nog steeds één broadcast-domein.
  Een switch koppelt een source-poort met een destination-poort als deze vrij is. Is dit niet het geval dan buffer de switch een aantal frames. Komt de destination-poort vrij dan worden deze frames doorgestuurd. Dit buffermechanisme geeft een hogere throughput. Er kunnen meerdere source- en destination-poorten gelijktijdig gekoppeld zijn en data uitwisselen. Omdat in de microsegmenten de reciever-lijn niet gebruikt hoef te worden om een collision te detecteren kan een systeem dus gelijktijdig zenden en ontvangen (full-duplex). Dit heeft vooral effect bij systemen zoals servers waar meerdere user-systemen mee willen communiceren.
  De switch haalt veel snelheid uit het feit dat een grootdeel van de functies door speciale poort-hardware (ASIC's) worden uitgevoerd terwijl bij een bridge alle functies door één processor worden geregeld.
  Broadcast-berichten worden standaard naar alle segmenten doorgegeven. Een nieuwe functie van switches is de mogelijkheid om het LAN te verdelen in meerdere virtuele LANs, VLANs genoemd. De broadcast-berichten worden nu alleen naar alle poorten die tot hetzelfde VLAN behoren gestuurd. Om tussen de verschillende VLANs te kunnen communiceren is een apparaat met een routeringsfunctie nodig. Er zijn switches in de handel waar deze functie is ingebouwd de zg'n switch-routers.
  Een switched-netwerk heeft een hogere veiligheidsgraad omdat op de microsegmenten alleen de frames komen die voor het aangesloten systeem bestemd zijn. Op een shared-netwerk of een ring zijn alle frames te zien zodat **snooping** mogelijk is (een systeem met software die alle frames analyseert en bijvoorbeeld user-namen en passwords kan achterhalen). Een switch is een zeer

belangrijk onderdeel in LANs geworden. Op een later moment in het curriculum wordt hier dieper op ingegaan.

Backbone

Een backbone is de bekabeling van afzonderlijke netwerkdelen naar een centraalpunt. Het centrale punt kan zijn een hub die enkele sternetwerken met hubs samenvoegt of een centrale switch die sternetwerken met hubs of switches samenvoegt of een koppeling van verschillende netwerken of subnetwerken via een router.
De bekabeling van een sterpunt naar de computersystemen noemen we **horizotal cables** en de bekabeling van de sterpunten naar een centraal apparaat noemen we **uplinks**.
Een backbone is het bovenste deel van een netwerk. Bij grote netwerken spreekt Cisco over een layer indeling.
De onderste laag noemt men de **access layer**, dit is de laag waar alle computersystemen en hun sterpunten in vallen. De laag daarboven noemt men de **distributie-layer**, dit is het deel waar netwerkdelen uit de access layer worden gekoppeld door switches en/of routers. Bij grote netwerk is er nog een laag boven die de **core layer** genoemd wordt. Hier worden de netwerkdelen of netwerken uit de distributie-layer samengevoegd.

Vragen en opdrachten

1. Noem de drie belangrijkste LAN technologieën.
2. Beschrijf de access-methoden van ethernet, tokenring en FDDI.
3. Noem de encodings-methoden van ethernet, tokenring en FDDI.
4. Op welke manier kan een ethernet opgebouwd worden?
5. Op welke manier wordt een tokenring netwerk geïnstalleerd?
6. Wat is het voordeel van token passing t.o.v. CSMA/CD?
7. Welke voordelen heeft een FDDI netwerk t.o.v. een ethernet?
8. Welke layer 2 devices worden er in een ethernet toegepast?
9. Welk protocol gebruikt een bridge als hij ethernet-segmenten koppelt?
10. Welk protocol gebruikt een bridge als hij segmenten van verschillende technologieën koppelt?
11. Welke apparaten verdelen een ethernet in meerdere collision domeinen?
12. Welke techniek wordt toegepast in een switched ethernet om meerdere broadcast domeinen te creëren?
13. Wat is een broadcast-storm en wat zijn de oplossingen hiervoor?
14. Geef een beschrijving van het begrip intranet.

Aantekeningen

1.8 Design and Documentation

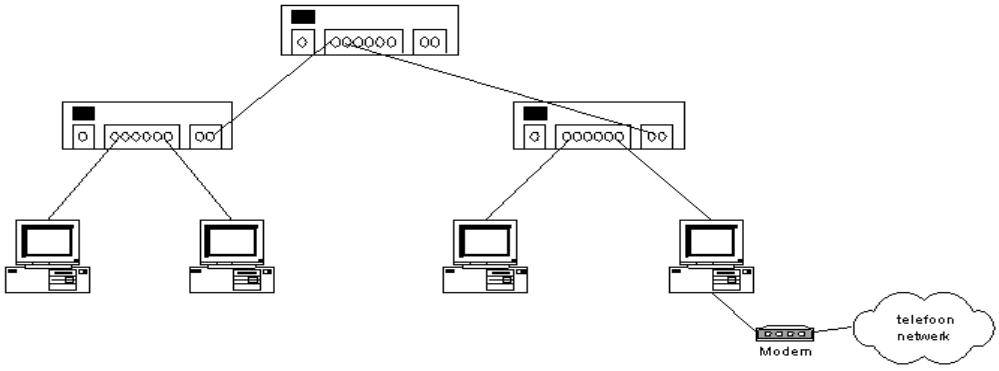
Nu je enige kennis heb opgedaan over het OSI model en de layer 1 en 2 principes en technologieën kunnen we starten met het ontwerpen en documenteren van netwerken. In dit hoofdstuk behandelen we welke logische- en fysieke topologie nodig is en welke kabelsoort gekozen moet worden. Bij de fysieke topologie komen ook aan de orde de eisen die gesteld worden aan de ruimten voor netwerkapparatuur en patching evenals de eisen voor de installatie methoden.

Een ontwerp kan bestaan uit het uitbreiden en/of vernieuwen van een bestaande installatie of uit het volledig nieuw opzetten van een netwerk. De meeste netwerken zijn/worden aangelegd in bestaande gebouwen waar tijdens de bouw nog geen rekening gehouden is met voorzieningen voor een netwerk. Bij nieuwe bouwprojecten worden deze voorzieningen al verwerkt door de architect. In bestaande gebouwen moeten vaak bouwkundige aanpassingen plaatsvinden om ruimten geschikt te maken voor een toepassing als netwerkruimte.
Bij het ontwerp richten we ons alleen op de ethernet-technologie.

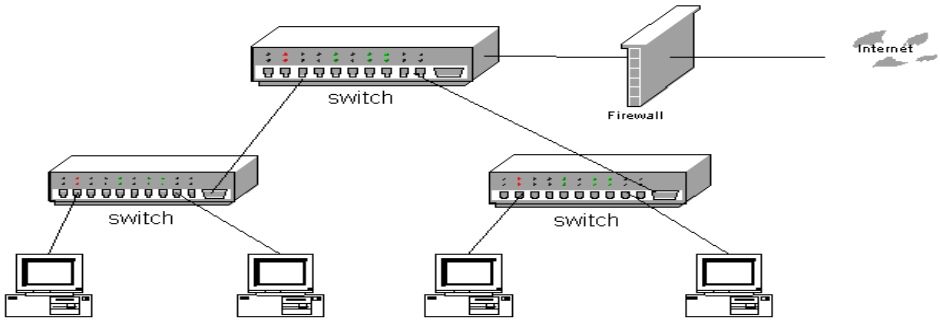
Afhankelijk van de grootte spreken we over een drietal netwerktype. Te beginnen met een **layer 1 netwerk** waarbij er keuzes gemaakt moeten worden als:

- kabeltype (meestal UTP cat 5),
- de fysieke topologie (meestal extended star),
- data rate (meestal 10baseT of 100baseTX),
- de plaats van de netwerkruimten.

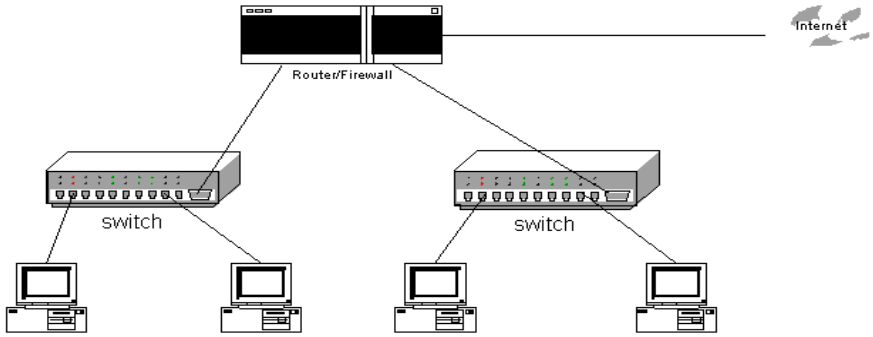
We maken nu gebruik van layer 1 devices als; repeaters, hubs, plugs, jacks en patch panels. Dit wordt toegepast in kleine bedrijven met enkele computers, randapparatuur en een server. Een van de systemen wordt gebruikt om via een modemverbinding en een softwarepakket elektronisch te bankieren en voor een inbelaccount bij een provider voor email.



Daarna gaan we over naar een **layer 2 netwerk** met bridges en switches die het probleem van opstoppingen en te veel collisions kunnen oplossen. We gaan nu over tot het segmenteren van het netwerk. Een layer 1 netwerk kan opgewaardeerd worden naar een layer 2 netwerk door de hubs te vervangen door switches. Dit wordt gebruikt bij kleine en middelgrootte bedrijven met enkele 10tallen computersystemen. Hier wordt meestal gewerkt met een firewall als koppeling naar het Internet voor email, fax en browser diensten. Ook elektronisch bankieren is via het Internet mogelijk. Vanwege de security wordt meestal nog gekozen voor een inbelverbinding naar de bank/giro.



Als laatste kijken we naar een **layer 3 netwerk** waar, naast de segmentering het netwerk opgedeeld wordt in meerdere netwerken of subnetten om, naast het probleem van opstoppingen en collisions, het broadcast probleem op te lossen. Het device dat nu nodig is, is een router. Dit is ook het apparaat wat gebruikt wordt om het netwerk aan een WAN link te koppelen zoals de verbinding naar Internet. Een van de routers wordt dan speciaal ingericht als firewall.C



Ontwerpstappen
Om een netwerk te ontwerpen, dat voldoet aan de eisen van de gebruikers, is het nodig om **systematisch een aantal geplande stappen te volgen**. Om dit proces goed te laten verlopen is het van groot belang dat, tijdens het ontwerp en de installatie, een goede **documentatie** wordt bijgehouden. Dit vergemakkelijkt het, op een later moment, **aanpassen of uitbreiden** van het netwerk en is leerzaam voor volgende projecten.

De eerste stappen die voor een project nodig zijn, zijn:
1. het **verzamelen van informatie** over:
   - de historie en de huidige status van het bedrijf.
   - de te verwachtte groei.
   - de binnen het bedrijf gebruikte regels en afspraken over de gebruik en het beheer van systemen.
   - gebruikte applicaties en de gebruiksregels ervan.
   - kennis van de gebruikers.

2. een **grondige analyse** van de verzamelde gegevens uit stap 1.

3. verzamelen van informatie over de organisatie en de aanwezige hardware en kennis zoals:
   - hoeveel geld is er beschikbaar,
   - hoeveelheid en status van aanwezige apparatuur en infrastructuur (is hergebruik mogelijk?),
   - aantal gebruikers van het netwerk,

- wat is hun kennis (is er bijscholing nodig?, verzorgd men zelf beheer en onderhoud of moet dit uitbesteed worden? enz).

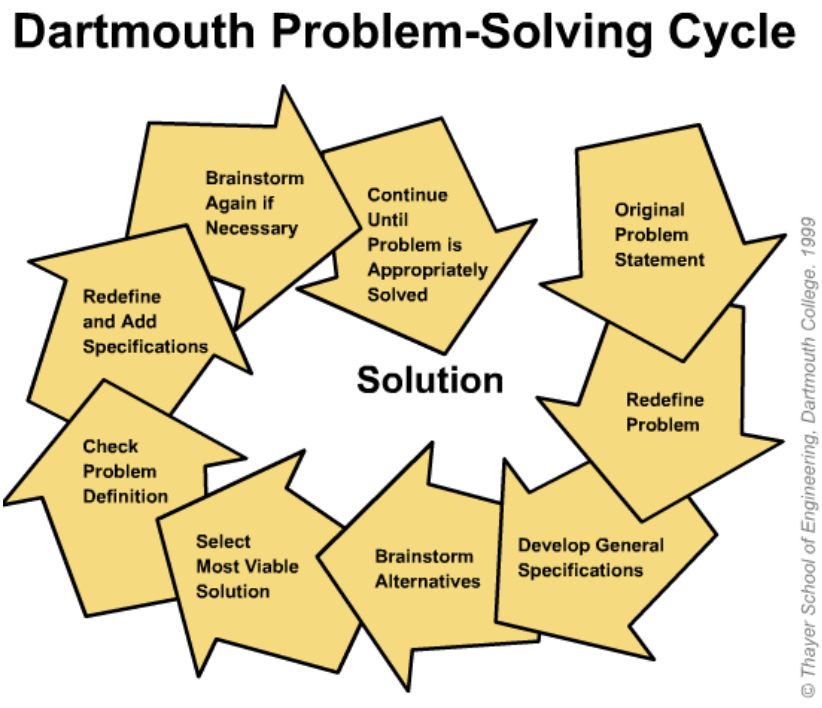
Op dit moment heeft u al een aardige documentatie opgebouwd met gegevens die verwerkt worden m.b.v. een tekstverwerker en spreadsheet-programma.
Dit is meestal een ijkpunt van het project. Samen met de klant worden de verzamelde gegevens besproken en bepaald of het project een vervolg krijgt.

Ontwerpproces
Als het echte ontwerpen begint komen we in dit proces een aantal personen en zaken tegen zoals:

- **Designer**(s). De persoon of personen die het ontwerp uitvoeren,
- **Cliënt**. Dit is de opdrachtgever of de contactpersoon,
- **Users**. De gebruikers van het netwerk,
- **Brainstorming**. Dit is een manier voor de designers om creatieve ideeën voor het ontwerp op te roepen en te bepreken,
- **Specificaties**. Dit is het vaststellen van de eisen waaraan het netwerk moet voldoen. Dit zijn meetbare zaken die de leverancier gebruikt om aan te tonen dat hij geleverd heeft wat er gevraagd is en voor de klant om te reclameren als deze vindt dat dit niet het geval is,
- **Bouwen en testen**. Hierbij wordt aangegeven hoe de montage plaatsvindt en hoe de kwaliteit van de installatie gemeten wordt. De netwerkbekabeling wordt door een onafhankelijk bedrijf getest en zonodig gecertificeerd.

Tijdens het ontwerpproces groeit de hoeveelheid documentatie sterk. Goede afspraken over dit punt is van groot belang voor de kwaliteit van een project en eventuele vervolgopdrachten.

In de ontwerpfase doen zich problemen voor. De eerste stap is nu om te onderzoeken of dit probleem als eens eerder voorgekomen is b.v. in een eerder project en te kijken wat voor oplossing toen gekozen is. Een goede documentatie voorkomt het opnieuw uitvinden van het wiel. Is het een nieuw probleem dan maken de ontwerpers gebruik van een bepaalde oplossingmethode op het probleem te lijf te gaan. B.v. de Dartmouth Problem-Solving Cycle.



Een speciale probleemdocumentatie wordt gebruikt om de problemen en de gekozen oplossing vast te leggen.

Ontwerp en uitvoeringsdocumentatie
Naast de documentatie, die opgebouwd is tijdens de hierboven beschreven projectfasen, bestaat een goede documentatie nog uit de volgende onderdelen:

- Engineering journaal. Dit is een opsomming van de activiteiten en de problemen die zich voordoen met hun oplossing. Hierbij wordt het moment en de persoon vermeld.
- Schema's van de logische topologie. Tekening met algemene symbolen.
- Schema's van de fysieke topologie. Tekening met toegepaste apparatuurgegevens.
- Plattegronden met daarin de apparatuur, verdeelkasten en kabelloop.
- Coderingslijsten van systemen, kabels, patch panels en jacks.
- Overzicht van onderdelen, MAC adressen en IP adressen.

Voor het maken en beheren van de documentatie maken we gebruik van een tekstverwerker, spreadscheet, tekenprogramma en bij grote projecten van een **projectmanagementpakket**. Tijdens de cursus wordt gebruik gemaakt van de **Cisco Network Designer**.

Tijdens het ontwerp en de installatie dient er steeds gewerkt te worden met de plaatselijk geldende normen en regels van de normaliseringinstituten zoals ANSI/EIA/TIA/ISO en in Nederland de NEN eisen.

Een belangrijk deel van het ontwerp is het onderzoek van:

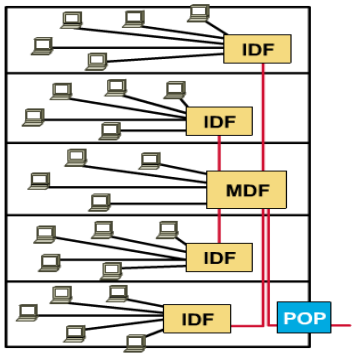
- De plaats van PC's en randapparatuur,
- Een geschikte plaats voor de verdeelkasten (wiring closet),
- Loop van het kabelgootsysteem,
- Serverruimte,
- Elektrische voeding + aarding.

Hiervoor is een plattegrond van het gebouw nodig met daarin alle bestaande leidingen, bekabeling en gootsystemen. Hierin worden de bovengenoemde onderdelen getekend en het gootsysteem uitgebreid als niet van de bestaande voorzieningen gebruik gemaakt kan worden.

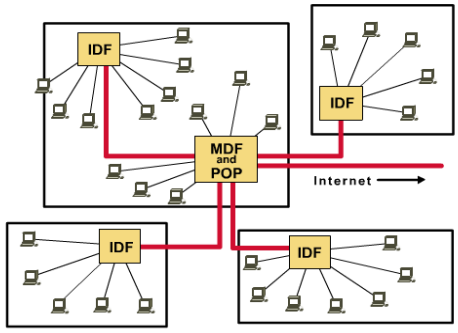
In de plattegrond worden:

- De PC's en randapparatuur getekend,
- De verdeelkasten aangegeven.
  Voor dat dit kan gebeuren moet eerst een keuze gemaakt worden welke aanwezig ruimten gebruikt kunnen worden of geschikt gemaakt moeten worden. Om dit te kunnen bepalen moeten we weten aan welke eisen de ruimten moeten voldoen. Hierbij maken we gebruik van de EIA/TIA normen.
  De gestelde eisen gaan over de vloer, wand en plafondeigenschappen, de ventilatie, luchtvochtigheid en temperatuur, verlichting, aanwezige voeding, toegang tot de ruimte en de aanwezigheid van leidingen.
  In het cursusmateriaal worden deze zaken uitgebreid behandeld.
  De belangrijkste ruimte is de **Main Distribution Facility** (MDF of hoofdverdeelkast). Als één kast niet voldoende is gebruiken één of meer **Intermediate Distribution Facilities** (IDF of secundaire verdeelkast).
  Elk netwerk heeft een MDF waarin een patch panel, netwerkapparatuur als routers en switches, servers en indien mogelijk de telefooncentrale of aansluiting naar de telefoonmaatschappij (**POP**) zijn ondergebracht.

Extended Star Topology in a Multi-Story Building

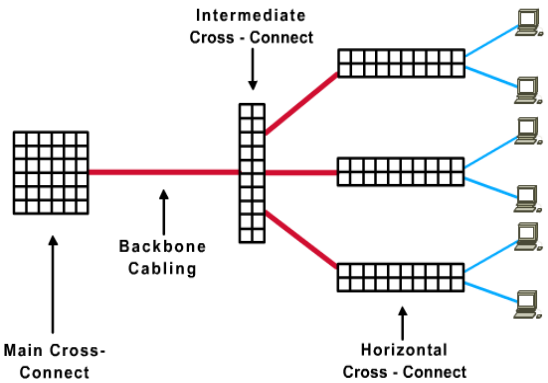


Extended Star Topology in a Multi-Building Campus



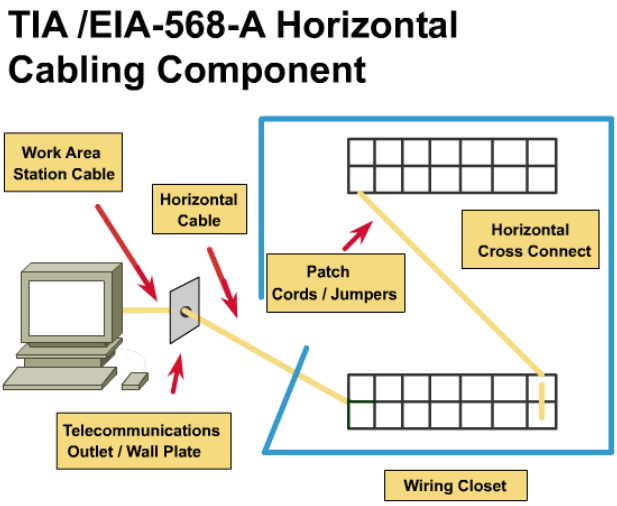
De bekabeling vanaf de wall jacks loopt naar een **Horizotal Cross Connect** (HCC). Deze kan zich bevinden in de MDF, een IDF of in een speciale kast in een ruimte geplaatst worden. Een **HCC** bestaat uit een patch panel en een hub of switch. Vanaf de HCC loopt er een backbone of uplink verbinding naar een **MCC** in de MDF. Als de afstanden te groot worden wordt er een **Intermediate Cross Connect** (ICC) tussen de HCC en de MCC geplaatst. De ICC worden in een IDF geplaatst. Voor de backbone bekabeling wordt gekozen uit Fastethernet UTP of fiber. De ICC bestaat uit een patch panel met hubs en/of switches en in sommige gevallen ook een workgroupserver. Voor de afstanden tussen de wall jackets en de HCC, de HCC in de ICC en de ICC en MDF heeft men maximale lengten vastgelegd. Dit is wel afhankelijk van het gebruikte medium. De afstand tussen een wall jack en een HCC is voor UTP 90 meter. De overblijvende 10 meter wordt gebruikt door de **patch cords** tussen de systemen en de jacks en de patch cords in de HCC.
De overige afstanden lopen van 90 meter tot 3 km.

Type B Backbone Cabling



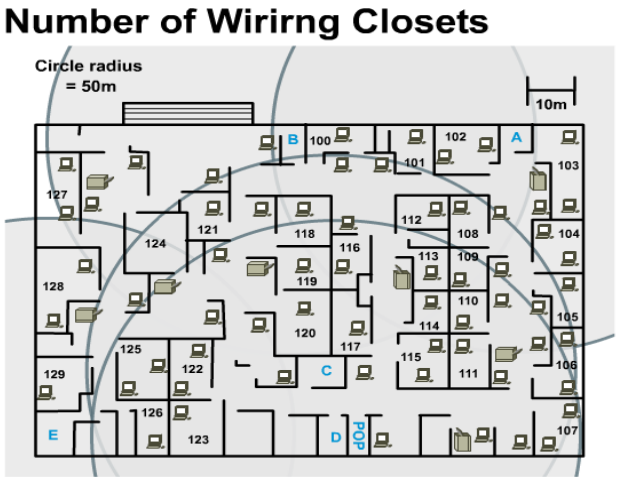
Max. Recommended Distances For Backbone Cabling Runs

Type of Networking Media	Distance From HCC to MCC	Distance From HCC to ICC	Distance From ICC to MCC
62.5/125 fiber-optic cable	2000 meters (6560 feet)	500 meters (1640 feet)	1500 meters (4820 feet)
Single-mode fiber-optic cable	3000 meters (9840 feet)	500 meters (1640 feet)	2500 meters (8200 feet)
UTP (voice)	800 meters (2624 feet)	500 meters (1640 feet)	300 meters (984 feet)
UTP (data)	Data applications, limited to 90 meters (295 feet) total		

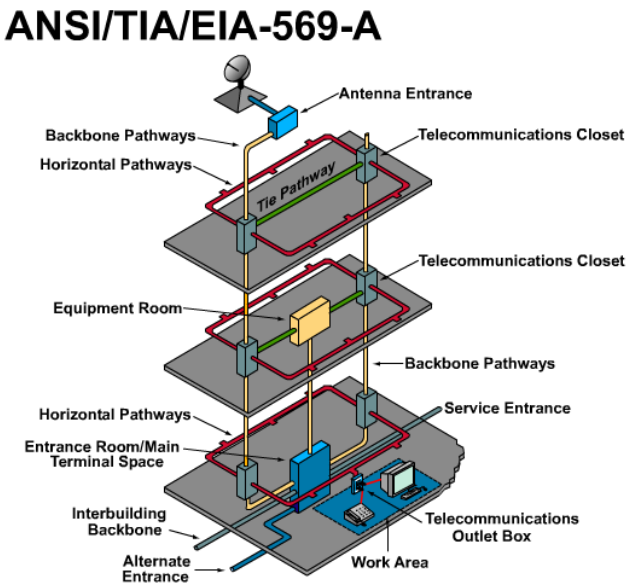


Met de cirkels op de plattegrond kunnen we concluderen dat de plaats C vrijwel volledig wordt afgedekt door de B en D. De overblijvende ruimte bevat maar enkele systemen een IDF in A en E heeft maar een beperkte functie. We kunnen onderzoeken of de systemen zich meer dan 90 meter van B of D bevinden. Als dit niet het geval is kunnen we kiezen voor een extra losse HCC.
In dit geval wordt gekozen voor D als MDF (kort bij de POP), B als IDF en eventueel A en E voor het plaatsen van een losse HCC.

Voor de bepaling van het aantal en de plaats van de verdeelkasten en/of losse HCC's worden vanuit de plaatsen die in aanmerking komen als MDF en IDF cirkels met een straal van 50 meter getrokken. De MDF/IDF zijn de sterpunten in een extanded star topologie. De apparatuur binnen de cirkels wordt met het sterpunt verbonden. Als er enkele of een groep systemen buiten de cirkels vallen kunnen we kiezen voor een extra IDF of een losse HCC en in sommige gevallen alleen een losse repeater.



- Nu wordt het gootsysteem (pathways) bekeken. Men spreek over horizontal pathways voor het gootsysteem in de ruimte voor de aansluiting van de PC's en randapparatuur. Dit gootsysteem wordt tevens gebruikt voor de bekabeling van het telefoonnetwerk. Het patches van deze bekabeling wordt ook in de IDF en MDF gedaan. De pathways tussen de HCC's, ICC's en MCC worden backbone patch ways genoemd. Voor het gootsysteem wordt, indien mogelijk het bestaande systeem gebruikt.



- Bij het installeren van de bekabeling moet er op gelet worden dat er voldoende ruimte in de kabel aanwezig is (niet te strak), dat bochten een voldoende grote straal hebben en dat met tijdens het monteren de kabel niet uitrekt zodat de twisting minder wordt. Scherpe bochten en uitgerekte bekabeling geeft meer kans op ruisverschijnselen.
  Backbone bekabeling tussen gebouwen worden bij voorkeur uitgevoerd met fiber omdat deze ongevoelig zijn voor stoorsignalen als blikseminslag en omdat deze geen aardlussen kunnen creëren.
- Een laatste maar zeer belangrijk punt is de energievoorziening van de netwerkapparatuur en de beveiliging tegen storingen die door de voeding veroorzaakt kunnen worden.
  Belangrijk is dat de apparatuur gevoed wordt via een "schone groep", dit is een groep waar geen apparatuur mee gevoed wordt als liftmotoren, ventilatoren, koelkasten, fotokopieerapparatuur e.d. dit soort apparatuur veroorzaakt spanningsveranderingen tijdens het in- en uitschakelen. De spanning kan tijdelijk in waarde dalen (**Sag**) of stijgen (**Surge**) er kunnen kortstondige pieken/dalen (**Spikes**) ontstaan en er kan ruis optreden. Om de apparatuur tegen surges en spikes te beschermen worden er **filters** in de voeding geplaatst (**surge suppressors**). Om te voorkomen dat bij sags en het volledig wegvallen van de spanning (**brownout**) de netwerkapparatuur en servers uitvallen worden deze onderdelen gevoed via een **Uninterruptible Power Supply** (UPS). Dit zijn apparaten met een accu, waarin, bij het wegvallen van de spanning, de accuspanning wordt omgezet naar 220V AC. Een UPS kan gedurende 15 minuten de energie leveren voor de systemen zodat de gebruikers gemeld kan worden dat problemen zijn en zij hun netwerkacties kunnen beëindigen.
  De problemen die ontstaan tussen de fase (**hot wire**) en nul (**neutral wire**) in de voeding noemen we **normal-mode problems**. Problemen die ontstaan tussen de aarde (**ground**) en de fase of nuldraad noemen we **common-mode problems** . De aardleiding in de voeding wordt gebruikt om te voorkomen dat er gevaarlijke situaties ontstaan als het onderspanning komen van de behuizing van de systemen. Aardingsproblemen kunnen ook zorgen voor beschadiging van de apparatuur of delen ervan. Dit komt als de aardleiding tevens gebruikt wordt door de eerder genoemde apparatuur die veel **lekstromen** veroorzaken en energie pulsen van b.v **blikseminslag**. Om problemen zoveel mogelijk te voorkomen is het nodig dat er gewerkt wordt met een **schone aarde**. Dit wil zeggen dat de aardverbinding niet gebruikt wordt door andere apparaten en door te voorkomen dat aardlussen ontstaan tussen meerdere delen van het netwerk.
  Bij het optreden van problemen of het bepalen van de kwaliteit van de aarding kan een speciaal meetinstrument gehuurd worden dat gedurende enkele dagen tot een week de voeding en aarde meet en waarmee een meetrapport te maken is.
- Nu rest nog het maken van een coderingsplan waarna de labels gemaakt kunnen worden die gebruikt worden om de apparatuur, kasten, patch panels, wall jackets en kabels te merken.

Er is een punt in het ontwerpproces waar voldoende informatie voorhanden is om een **gespecificeerde offerte** uit te brengen. Dit is het document waarop de klant besluit om het project uit te laten voeren door een bedrijf.
Een gespecificeerde offerte bevat de specificaties van de leveren apparatuur en bekabeling, de specificaties van de eisen waaraan het netwerk moet voldoen, de specificaties van werkzaamheden die nodig zijn voor de installatie maar niet voor rekening van de leverancier komen zoals allerlei bouwkundige aanpassingen en uiteindelijk de vraagprijs.
Om een project tot een goed einde te brengen heeft een bedrijf geschoold en ervaren personeelsleden nodig die een ontwerp, het installeren, het inbedrijfstellen en een kostenberekening kunnen verzorgen. In veel gevallen wordt ook het beheer en onderhoud van het netwerk uitbesteed. Dat betekend dat het bedrijf ook moet beschikken over vakbekwaam personeel op dit gebied. Een opleiding die dan vereist is, is vaak het CCNA examen of gelijkwaardig.
Zoals al eerder aangegeven is het van groot belang dat deze mensen doordrongen zijn van het feit dat dit soort werkzaamheden niet mogelijk is zonder een goede en adequate manier van documenteren.

Vragen en opdrachten

1. Geef een korte omschrijving van een layer 1, layer 2 en layer 3 netwerk.

2. Wat zijn de eerste stappen die nodig zijn bij een netwerkproject?

3. Welke personen en zaken kom je tegen in een ontwerpproces? Geef van elk een korte omschrijving.

4. Hoe worden problemen behandeld door de ontwerpers?

5. Geef een overzicht van de documentatie die opgebouwd wordt tijdens het ontwerp en de uitvoering van het project.

6. Geef aan waarom een goede documentatie belangrijk is.

7. Welke instituten zorgen voor normen en regels voor het maken van netwerken?

8. Welke eisen worden er gesteld aan een verdeelruimte?

9. Wat betekent MDF en IDF?

10. Op welke manier wordt bepaald waar en hoeveel verdeelruimten er moeten komen?

11. Wat betekent MCC, ICC en HCC? Waar zijn deze zaken te vinden?

12. Wat zijn de afstanden van de kabels in een netwerk tussen de PC's, HCC's, ICC's en MCC en welke namen worden hierbij gebruikt?

13. Wat zijn pathways en wall jacks?

14. Beschrijf het begrip "schone groep".

15. Wat is een surge, sag, spike en brownout?

16. Waardoor worden de problemen van vraag 15 veroorzaakt?

17. Op welke manier kunnen we het netwerk tegen de problemen van vraag 15 beschermen?

18. Wat wordt bedoeld met normal-mode en common-mode problems?

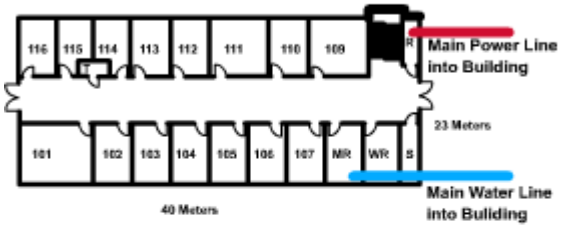
19. Beschrijf de problemen die kunnen optreden door de aardleidingen.

20. Wat is een "schone aarde"?

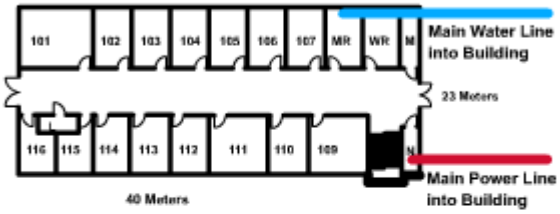
21. Bepaal de plaats van de MDF en IDF's in het gebouw waarvan de plattegronden op de volgende bladzijde zijn te vinden. Teken de backbone bekabeling en maak een voorstel voor de codering. De ruimtes aangegeven met een letter komen in aanmerking voor de functie van verdeelkast. Een aantal voldoen niet aan de eisen als vloer, wand en plafondeigenschappen enz. De ruimtes C, D, E , F, H, I, K, N, O, Q, R, T, W en U kunnen wel gebruikt worden.

Floor Plans

West Building First Floor

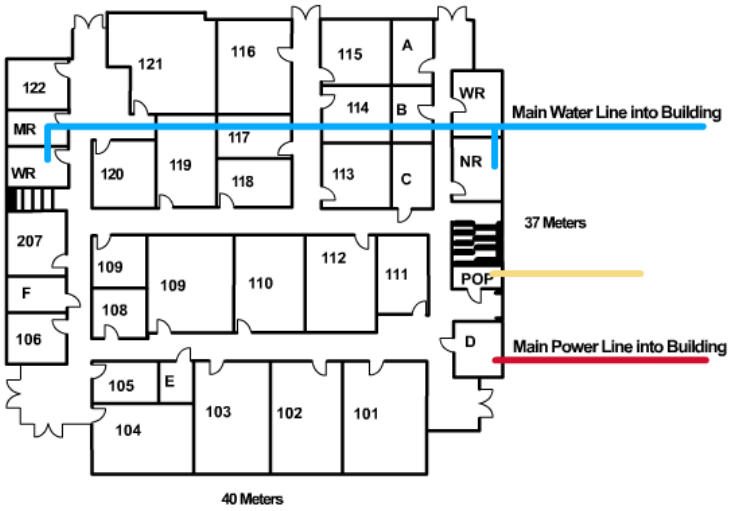


First Floor East Building

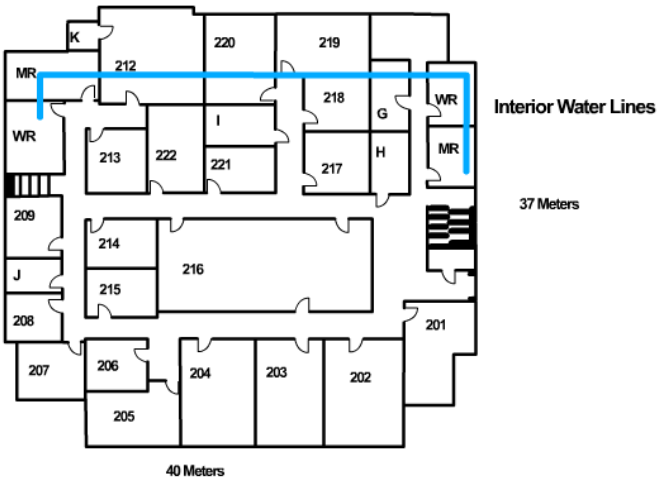


Main Building First Floor

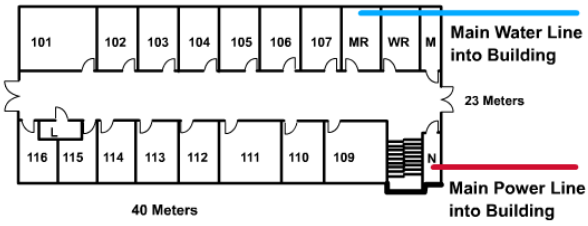
Main Building First Floor



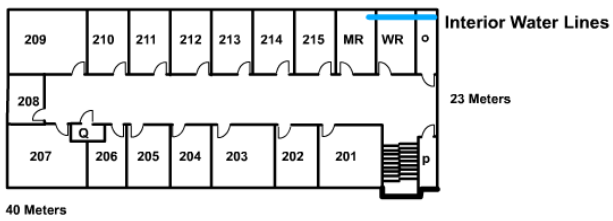
Main Building Second Floor



East Building First Floor

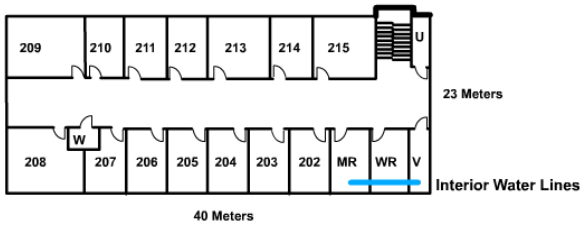


East Building Second Floor



West Building First Floor

West Building Second Floor



Aantekeningen

1.9 Structured Cabeling Project

In hoofdstuk 1.8 hebben we gekeken naar de aspecten van het ontwerpen van netwerken en de noodzaak en wijze van een documentatie maken. In dit hoofdstuk kijken we naar zaken die van belang zijn voor de daadwerkelijke uitvoering van een project.
Als een opdrachtgever na de ontwerpfase, de projectomschrijving en de offerte (kosten) besluit om het project uit te laten voeren, moet er binnen het uitvoerende bedrijf een aantal zaken opgestart worden.
Als eerste wordt er een uitvoerend projectteam samengesteld. Dit team kan (afhankelijk van de omvang van het project) bestaan uit een;

- Coördinerend projectleider,
- Werkvoorbereider,
- Uitvoerend projectleider,
- Installatiemedewerkers,
- Afmontage/Inbedrijfstel-medewerkers.

We zullen nu, aan de hand van deze personen, de aspecten van de uitvoering behandelen.

Coördinerend projectleider
Dit is de persoon die de algemene leiding heeft over het project, de communicatie verzorgt met de opdrachtgever, de voorgang van het werk bewaakt enz. Dit is in de meeste gevallen iemand met een hogere beroepsopleiding (HBO) die ook bij het ontwerp betrokken geweest is.

Werkvoorbereider
Dit is een sleutelfiguur in het project. Deze zorgt voor:
- de bestelling van materialen en apparatuur,
- het tijding afleveren ervan op de werkplek,
- het reserveren van speciale gereedschappen ed. Als er meer projecten lopen, dan kan een speciaal stuk gereedschap niet gelijktijdig voor meer projecten gereserveerd worden,
- het plannen en coördineren van werk dat door derden verricht moet worden. Het moet dus niet zo zijn dat de kabelmonteurs niet verder kunnen omdat het bedrijf die een doorvoer moet boren in een betonnen wand of vloer op een verkeerd moment is ingepland.
- het plannen van de uitvoerende medewerkers (monteurs),

Een werkvoorbereider is meestal een persoon met een middelbare beroepsopleiding (ICT-MBO) met werkervaring in de uitvoering van dit soort projecten.
Hij communiceert met de uitvoerende projectleider over bovenstaande punten en past zijn planningen aan als dit in de loop van het project nodig is.

Uitvoerend projectleider
Deze persoon geeft leiding aan de uitvoerende mensen. Hij is gestationeerd op de werkplek en communiceert met de coördinerend projectleider en de werkvoorbereider van zijn bedrijf en met de medewerkers van de klant die het netwerk gaan beheren. Voorts heeft hij te maken met andere bedrijven die werkzaamheden verrichten op de werkplek. Vooral bij nieuwbouwprojecten zijn er meer bedrijven actief op de werkplek. Hij is dan betrokken bij de coördinatie van de activiteiten van de verschillende bedrijven onderling, zodat de voortgang van werk niet onnodig vertraagd wordt.
Projectleiders (vaak chefmonteur genoemd) zijn meestal personen met veel ervaring in de uitvoerende taken en hebben een MBO-opleiding.

Installatiemedewerkers
Dit zijn mensen die ingezet worden voor de daadwerkelijke montage van;
- bekabeling (UTP, Fiber),
- gootsystemen (cable raceways),

- aansluitdozen (outlets),
- bedradingkasten (wiring closets),
- netwerkapparatuur (NICs, repeaters, hubs, switches, routers enz.),
- serverruimten (MDF, IDF).

Dit zijn over het algemeen beginnende ICT/Telematica-MBO'ers of mensen zonder een specifieke opleiding die getraind zijn in het uitvoeren van bepaalde montagetechnieken.

Zij moeten kennis hebben van onderstaande zaken en moeten die ook kunnen uitvoeren toepassen.
- veilige werkmethoden,
- montagetechnieken,
- het lezen van werktekeningen,
- apparatuur- en bekabelingscodereringen.

Afmontage/Inbedrijfstel-medewerkers
Deze mensen worden ingezet bij de afmontage van RJ-jackets in outlets en in wiring closets en bij het testen van de installatie en het configureren van de netwerkapparatuur.
Dit zijn over het algemeen ervaren ICT/Telematica MBO'ers met aanvullende trainingen op het gebied van de apparatuur.

De medewerkers van een projectteam vervullen een specifieke functie als we kijken naar de grotere projecten. Bij kleine projecten combineren de medewerkers vaak meerdere functies. Een chefmonteur die ook installatie en afmontage werkzaamheden verricht of medewerkers die zowel de installatie als de afmontage en de inbedrijfstelling verzorgen.

Veilige werkmethoden
Het is belangrijk dat de medewerkers hun werkzaamheden uitvoeren volgens de ARBO-regels. Deze beschrijven voorschriften op het gebied van:
- werk- en rusttijden,
- juiste werkkleding en schoeisel,
- omgang met ladders en steigers,
- gebruik van de juiste gereedschappen,
- voorkomen van gevaarlijke situaties (elektriciteit is er een van),
- voorkomen van brandgevaarlijke situaties.

Een algemene regel is om, wanneer er gewerkt wordt aan elektrische leidingen of er bv. gaten geboord moeten worden in een muur waarin zich ook elektrische leidingen bevinden, te weten waar deze leidingen zich bevinden en om te zorgen dat tijdens de werkzaamheden deze leidingen niet onder spanning staan. De spanning moet dus uitgeschakeld worden en men moet voorkomen dat een andere persoon per ongeluk de spanning weer kan inschakelen. Het ophangen van waarschuwingsborden en het verwijderen van zekeringen voorkomt problemen.

Montagetechnieken
Het is belangrijk dat de medewerkers begrip hebben voor en goed getraind zijn in de montage-technieken die ze moeten toepassen.
Bv.
- Bij de montage op een muur met een pleisterlaag is het belangrijk dat het bevestigingsgat voldoende diep geboord wordt, zodat de plug in het achterliggende materiaal hecht in plaats van in de pleisterlaag.
- Kennis en vaardigheid van bevestiging op verschillende ondergronden zoals; gipsplaat, hout enz.
- Tijdens het leggen van UTP-kabel mag er niet onnodig hard aan de kabel wordt getrokken omdat anders de interne twisting wordt opgerekt.
- In de UTP-kabel mogen geen scherpe bochten (5 maal de diameter)of knikken voorkomen.

- Voorkomen dat aansluitpunten op trek belast worden, dus zorgen voor trekontlasting (bevestigen met tire wraps).
- Voorkomen dat verticale bekabeling door zijn eigen gewicht een constante trekkracht uitoefent.
- Zorgen dat voldoende ruimte in de kabel aanwezig is zodat bij de afmontage, bij een foutieve handeling, nog voldoende kabellengte over is om de kabel opnieuw aan te sluiten.
- Het toepassen van een juiste werkvolgorde. Het is niet verstandig om eerst een aantal kabels van A naar B aan te leggen en daarna de codering aan te brengen. Het is nu zeer lastig om er achter te komen welke uiteinden bij elkaar horen.
- Bij het afmonteren van RJ-jackets en patch panels is het belangrijk om goed te letten op de kleuren, de lengte van de onttwiste uiteinden (13 mm), de ruimte in de kabel en de trekontlasting. Voor het monteren wordt gebruik gemaakt van een punch tool.

In het cursusmateriaal wordt uitgebreid ingegaan op de montage van opbouw/inbouw outlets, patch panels, raceways en cable runs. Noteer bij de aantekeningen de gebruikte termen en afmetingen omdat deze in de toetsvragen aan de orde komen.

De installatie moet voldoen aan voorschriften die door landelijke en internationale normalisatie instituten zijn omschreven zoals; IEEE, TIA/EIA 568A/606/enz, NEN, ANSI ed.

Werktekeningen (cut sheets)
Het is belangrijk om een werktekening te kunnen ‘lezen’. Hierop bevinden zich belangrijke gegevens die nodig zijn voor de installatie en afmontage.
Naast het gebruik tijdens de installatie zijn werktekeningen ook belangrijk bij het achterhalen van de kabelloop en de plaats van de apparatuur als zich op een later moment een storing voordoet.
Het is belangrijk dat de beheerder of installateur bij een (latere) wijzing in de installatie deze wijziging ook verwerkt op zijn werktekeningen (revisie). Een werktekening moet altijd up-to-date zijn.

Codering
In de norm TIA/EIA 606 is een manier van het coderen van de bekabeling, outlets, patch panels en netwerkapparatuur beschreven. Deze codering is gekoppeld aan de plaats van de onderdelen in de installatie. Bv. voor een outlet bestaat de codering uit: ruimtenummer+volgordenummer in de ruimte (654-12).

Testen
Een belangrijk en verplicht onderdeel van een installatie is het testen ervan, waarna een certificaat wordt afgegeven.
Getest moet worden;
- Elke kabel afzonderlijk. Met een kabeltester kunnen storingen gemeten worden als; split pairs, attenuation (demping), near-end crosstalk (overspraak), kabelbreuk ed. Met een TDR-meter kunnen deze onderdelen gemeten worden. Als er fouten geconstateerd worden, moeten ze verholpen worden en opnieuw getest.
- Elk computersysteem dat aangesloten wordt op het netwerk.

Van de gehele test wordt een testrapport gemaakt dat aan de documentatie wordt toegevoegd.

Logboek (journal)
Ook tijdens de installatie en de test wordt een logboek bijgehouden waarin alle voorkomende problemen en hun oplossing vermeld worden. Dit kan dienen bij volgende projecten als naslagwerk om de oplossing te hebben voor problemen die zich eerder hebben voorgedaan.

Vragen en opdrachten

1. Maak een schema van personen en hun functie binnen een uitvoerend projectteam.
2. Geef van elke medewerker in het team een functieomschrijving.
3. Welke regels worden er gesteld aan het leggen van UTP-bekabeling?
4. Geef een voorbeeld van een codering en wat is de functie erven?
5. Geef aan wat voor storingen er met een test gemeten kunnen worden.
6. Beschrijf de zin van documenteren tijdens de installatie.

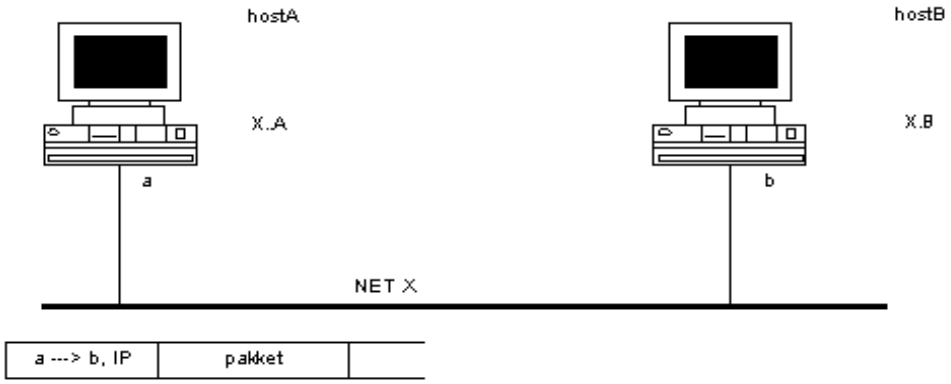
Aantekeningen

1.10 Layer 3, Routing en Addressing

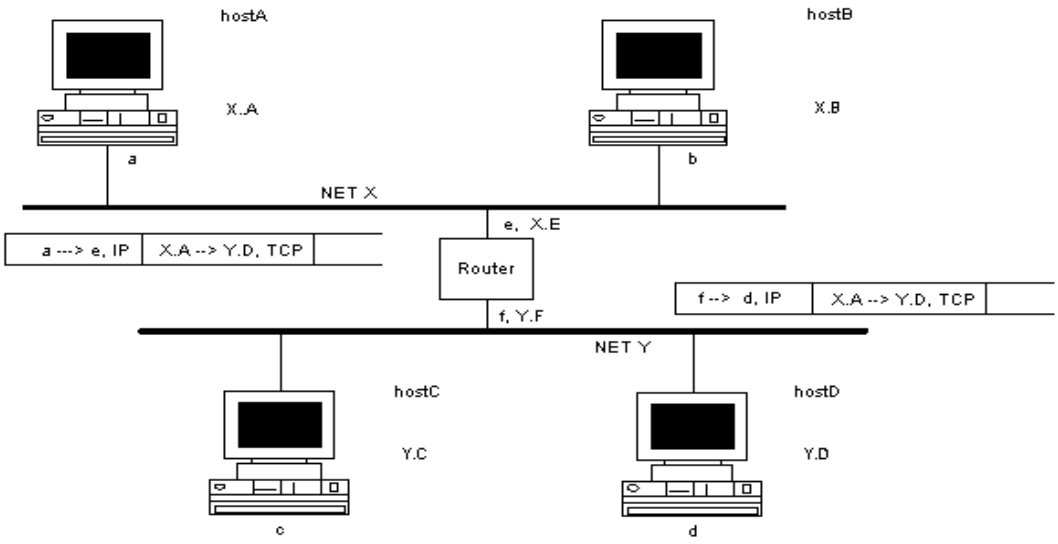
Elke host in een computernetwerk heeft herkenningstekens (**ID's, adressen**). Bij de communicatie tussen hosts wordt gebruik gemaakt van deze ID's.

- **hostname,**
- **logisch adres (IP nummer, layer3 adres),**
- **fysiek adres (MAC nummer, layer2 adres, hardware adres).**

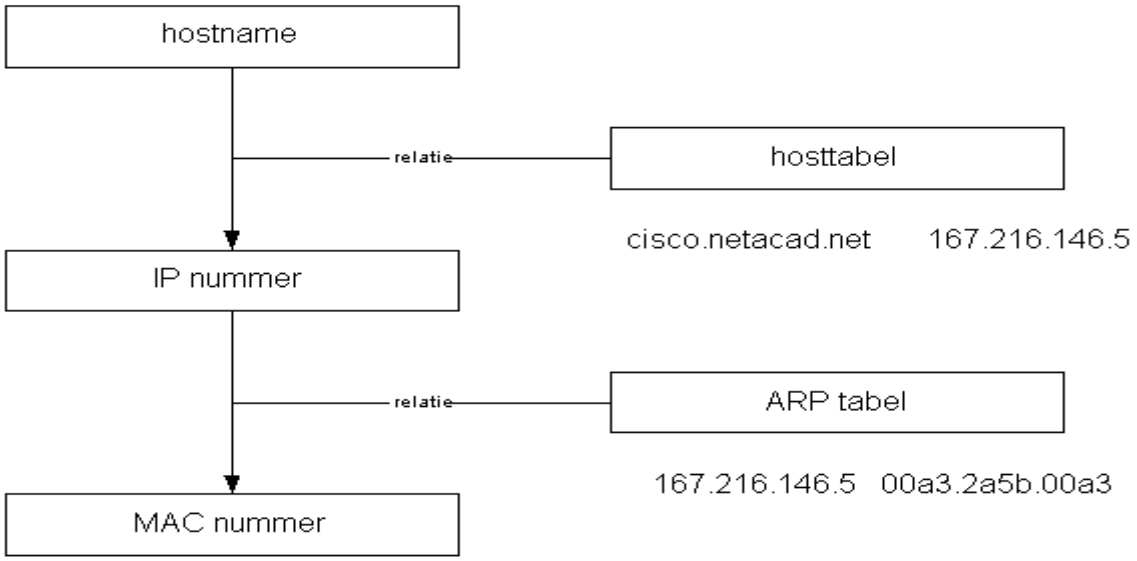
Om te kunnen communiceren moet de source host een ID kennen van de destination host(s). Om een pakket van hostA naar hostB te kunnen verzenden heeft de source het fysieke en logische adres nodig van de destination.
Het fysieke adres is gekoppeld aan het gebruikte type netwerksegment (ethernet/tokenring/fddi). Layer2 is verantwoordelijk voor het versturen van een pakket over een netwerksegment en maakt hierbij gebruik van de MAC nummers (adres en afzender).



Als de source en de destination host niet op hetzelfde netwerk zijn aangesloten, dan wordt een router of een groep routers gebruikt om het pakket van netwerkX naar netwerkY te leiden. De router(s) kennen de weg (route) tussen X en Y. De router(s) bepalen de weg op basis van de netwerk ID's. Dit is verwerkt in het logische adres dat bestaat uit een netwerk ID + host ID (X.A).
Om een bericht van hostA (netX) te verzenden naar hostD (netY), verzendt hostA het bericht naar zijn default gateway (de poort naar andere netwerken). De router(s) leiden het bericht naar netwerkY en de router die gekoppeld aan netY verstuurd het bericht naar hostD.



Het is onmogelijk voor een gebruiker van het netwerk om de layer2 en 3 ID's te kennen. Bij de TCP/IP stack wordt gebruik gemaakt van een hostname, IP nummer en MAC nummer als ID's.
Een gebruiker kent de hostname van de host waarmee een verbinding gemaakt moet worden. Om bijvoorbeeld een verbinding te maken met **cisco.netacad.net** via een browser, onderzoekt de host zijn **hosttabel** om te bepalen welk IP nummer hierbij hoort (**167.216.146.5**). Als de informatie niet in zijn hosttabel staat dan raadpleegt de host een **DNS server** met de vraag om de relatie te achterhalen. Wanneer de host een bericht terug krijgt van deze server dan slaat hij de relatie tijdelijk op in zijn hosttabel.
Vervolgens kijkt de host of het adres deel uitmaakt van zijn netwerk. Als dit het geval is zoekt hij in zijn **ARP-tabel** naar de relatie tussen het IP nummer en het MAC nummer. Als het adres zich op een ander netwerk bevindt kijk hij in zijn ARP-tabel naar de relatie tussen zijn default-gateway IP nummer en het MAC nummer wat hierbij hoort. Als de relatie niet voorkomt in de tabel dan vraagt hij via een broadcast message aan de nodes op zijn net om de relatie aan te geven. Als hij deze ontvangt slaat hij deze weer tijdelijk op in zijn tabel.
Nu is de host klaar om contact te maken met de destination host.



HET INTERNET ADRES (IP nummer)
Elke Internet interface wordt geïdentificeerd door een 32 bits (4 octet's, bytes) Internet adres. Helemaal in het begin van het Internet werkte men met een 8 bits netID en een 24 bits hostID. Dit betekende dat men uitging van niet meer dan 256 afzonderlijke netwerken. Toen bleek dat er veel meer netwerken aan het Internet wilde deelnemen heeft men het klassen systeem ingevoerd.

Classes
In 1981 heeft men de adressering gedefinieerd als een tweedelig object, een netID en een hostID (identifier) binnen dat netwerk, en een verdeling in klassen.

High order bits	Format		Class
0xxx	**7 net bits**	**24 host bits**	**A**
10xx	**14 net bits**	**16 host bits**	**B**
110x	**21 net bits**	**8 host bits**	**C**
1110	**28 multicast bits**		**D**
1111	**gereserveerd voor experimenten**		**E**

NETID	HOSTID

De adressen worden geschreven als decimale getallen gescheiden door punten (**dotted decimal format**).
172.16.0.6 i.p.v 1010110 00010000 00000000 00000110.

De scheiding tussen de net bits en de host bits wordt bepaald door de hoogste bits. De net bits zijn **uniek** binnen het Internet en worden uitgegeven door de Internet nummering autoriteit (**IANA**). De hostnummers worden ingevuld door de netwerkmanager.

In het begin was de **two-level** structuur voor de adressering werkbaar. Door de sterke groei van het aantal computersystemen en de netwerkactiviteit ontstond de behoefte bij netwerkmanagers om de structuur van hun interne netwerken beter te kunnen beheren. In 1984 is daarom een derde level aan het adresobject toegevoegd, het subnetID of de subnet bits.

Subnets

NET ID	HOST ID	Two-level

NET ID	SUBNET ID	HOST ID	Three-level

De netwerkmanagers konden nu hun interne netwerk in meerdere subnetten opdelen . De subnet bits uit de **three-level** structuur bestaan uit **2 t/m het aantal–2** van de host bits uit de two-level structuur. Deze bits worden geleend van de host bits. De overblijvende bits stellen het hostID van systemen binnen een subnet voor.
Het netwerk wordt nu aangegeven met de net bits + subnet bits. Omdat het aantal subnet bits niet vast ligt was er een mechanisme nodig om de scheiding tussen het netwerkdeel en het hostdeel aan te geven.
Men gebruikt hiervoor een 32 bits getal dat op dezelfde manier geschreven wordt als het IP adres en wordt **subnet mask** genoemd. Het subnet mask bestaat uit een aaneengesloten reeks enen overeenkomend met het aantal net- en subnet bits, gevolgd door nullen die overeenkomen met de host bits. Door een logische **AND** bewerking tussen het IP adres en het subnet mask wordt het netwerknummer bepaald. Door het subnet mask te inverteren en nogmaals de AND bewerking uit te voeren vindt men het hostnummer.

Bv. IP adres 192.168.132.54 en subnet mask 255.255.255.240 geeft als netwerknummer 192.168.132.48 en als hostnummer 6.

IP adres	11000000 10101000 10000100 00110110	192.168.132.54
Subnet mask	11111111 11111111 11111111 11110000 AND	255.255.255.240
Netnummer	11000000 10101000 10000100 00110000	192.168.132.48

IP adres	11000000 10101000 10000100 00110110	192.168.132.54
Inv. Subnet mask	00000000 00000000 00000000 00001111 AND	0.0.0.15
Hostnummer	00000000 00000000 00000000 00000110	6

Bij het bepalen van het subnet mask maken we gebruik van de formule: **aantal subnettten = 2^x-2** (x is het aantal subnet bits). De twee netnummers die we niet kunnen gebruiken zijn het adres van de groep subnetten (klasse adres) en het broadcast adres van de groep subnetten. Het aantal subnet bits moeten er dus minimaal 2 zijn om twee subnetten te kunnen maken.
Bij het bepalen van het aantal hosts maken we gebruik van de formule: **aantal hosts = 2^y-2** (y is het aantal host bits). Hostnummer 0 is niet te gebruiken omdat deze gereserveerd is voor subnet ID en het hostnummer met allemaal enen is gereserveerd voor het boardcast nummer van het subnet.

Bv.
Het klasse B netwerk 182.244.0.0 moet verdeeld worden in 8 subnetten.
Met de formule 2^x-2 >= 8 wordt de waarde x bepaald. X krijgt de waarde 4, want wanneer we 3 zouden kiezen dan kunnen er maar 6 subnetten gemaakt worden (2^3-2 = 6).
Het subnet mask bevat nu 20 enen gevolgd door 12 nullen (255.255.240.0 of /20).
Het aantal hosts dat per subnet kan worden toegepast is 2^{12}-2 = 16382.

Door de zeer sterke groei van het Internet ontstond een volgend probleem. De vraag naar middelgrootte netwerken werd veel groter dan de 16384 klasse B netwerken die hiervoor bedoeld zijn. Een klant die een netwerk van bv. 6000 hosts wilde maken, kon dit alleen doen door een groep klasse C netwerken aan te vragen.
Dit betekende wel dat deze voor elk netwerk een interface naar het Internet moest maken die ook individueel beveiligd moesten worden.
Dit leverde veel extra beheersactiviteiten en een kwetsbare beveiliging op, buiten nog de extra interface hardware. Het zeer grote aantal netwerken waaruit het Internet dreigde te gaan ontstaan zou zeer veel routeringdata op het net veroorzaken. Om dit probleem op te lossen heeft men het systeem van **classless** netwerken ontworpen wat in 1993 is ingevoerd.

Classless
Men heeft een systeem gemaakt waarbij een groep klasse C netwerken als één geheel (**supernet**) konden worden gezien binnen het Internet.

Bv.
De klant met de behoefte aan een netwerk voor 6000 hosts krijgt als netwerkadres bv. 204.204.64.0 en als subnet mask 255.255.224.0 of /19 (11111111 1111111 11100000 00000000 dus 19 opeenvolgende enen).

IP adres	11001000 11001000 010xxxxx xxxxxxxx
Subnet mask	11111111 11111111 11100000 00000000

Dit netwerk omvat de klasse C netwerken 204.204.65.0 t/m 204.204.94.0. het subnet mask wijkt af van de klasse structuur dat bij een klasse C minimaal 24 enen bevat. We noemen dit ook wel een **supernet mask.**
Dus de klasse aanduiding via de hoogste bits en de lengte van de reeks enen in het subnet mask geven aan dat het hier over een supernet gaat.
De netwerkmanager kan lokaal het supernet verdelen in meerdere subnetten.

Gereserveerde IP adressen.
Voor het Internet worden door het IANA adressen uitgegeven. Dit gaat in de vorm van een klasse A of B netwerkadres of één of een groep klasse C netwerken. Een aantal nummers worden nooit uitgegeven omdat deze een speciale functie hebben.

Geldige netwerkadressen:

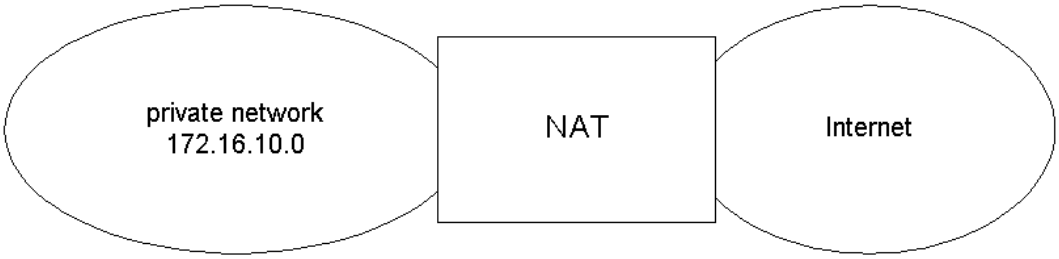
Classe A	1.0.0.0 .. 126.0.0.0
Classe B	128.0.0.0 .. 191.0.0.0
Classe C	192.0.0.0 .. 223.0.0.0

Gereserveerde netwerkadressen:

0.0.0.0	deze host,
0.hostnummer	willekeurige host van dit netwerk,
127.x.x.x	gebruikt voor het testen van de host netwerkinterface (loopback adres),
224.x.x.x .. 239.x.x.x	gebruikt voor multicast in de hogere lagen van het Internet, (classe D)
240.x.x.x .. 254.x.x.x	gebruikt voor experimenten, (classe E)
255.255.255.255	broadcast adres op dit netwerk.

Private addresses
Van de geldige netwerkadressen zijn er een aantal die niet op het Internet toegelaten worden. Deze worden gebruikt binnen netwerken die geen deel uitmaken van het Internet, de zg'n private networks.
10.0.0.0 .. 10.255.255.255
172.16.0.0 .. 172.31.255.255
192.168.0.0 .. 192.168.255.255

Dit zijn de meest gebruikte IP nummers omdat de hosts binnen bedrijfsnetwerken maar zelden rechtstreeks op het Internet toegang hebben. Toch kunnen deze hosts wel gebruik maken van de Internet diensten. Dit wordt mogelijk door een koppeling te maken via een systeem dat **NAPT** (**network address and port translation**) toepast.
De private host is de cliënt en een public host is de server van de dienst.
Dit systeem zet een private adres om in een geldig Internet adres. Er is echter maar één Internet adres en meerdere private adressen. Het onderscheid tussen de diverse private hosts wordt gemaakt met het source port nummer van de cliënt applicatie. Bv. de Web browser die contact met een Web server heeft.

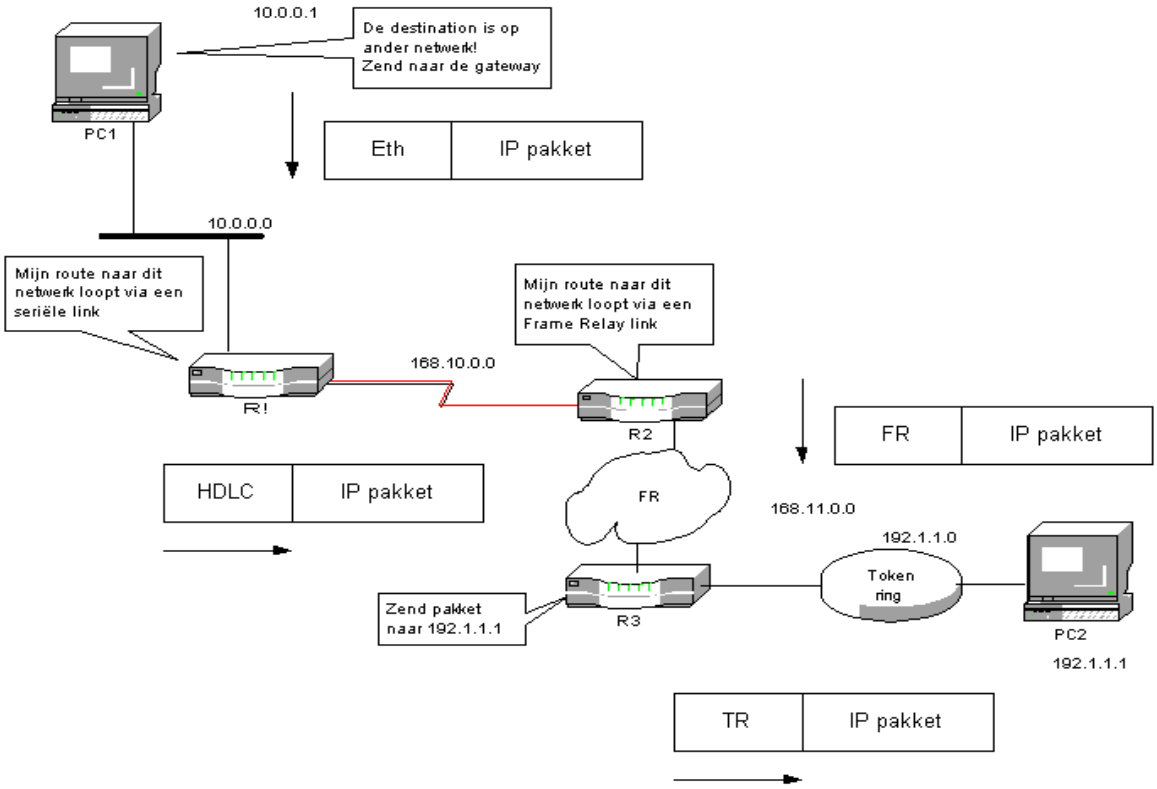


Het systeem heeft een gateway functie, agent (vertegenwoordiger) functie en maak gebruik van NAT.
NAT heeft een tabel met de relatie:

Private IP adres + source port nummer → public IP adres + source port nummer.
Bv

172.16.10.6	5678	→	204.127.212.8	61234
172.16.10.6	15789	→	204.127.212.8	54123
172.16.10.12	3498	→	204.127.212.8	33456

Headers
Als een pakket verzonden wordt, dan plaats een laag in het OSI model er informatie voor (header). Voor de headers wordt vaak een naam gebruikt die verwijst naar de layer en/of het protocol (MAC header, IP header, layer2 header, transport header, TCP header enz). Het proces van het plaatsen van informatie headers en bij de MAC header ook nog een trailer, wordt **encapsulation** genoemd.
De fysieke en logische adressen bevinden zich in deze headers (zie Appendix). De MAC adressen in de MAC header en de IP adressen in de IP header.
De logische adressen van de source en de destination zijn de echte adressen van de hosts en de header blijft tijdens het transport gelijk. Een router maakt gebruik van deze header om een beslissing te nemen voor de te kiezen route.
De fysieke adressen van de source en destination zijn de echte adressen als ze beide tot hetzelfde netwerksegment. Wanneer dit niet het geval is, dan is het destination adres, het adres van de gateway naar andere netwerken. De router(s) passen de inhoud van de MAC header aan en versturen het pakket over een ander netwerksegment. De router die gekoppeld is met het destination netwerk plaatst in de header als source adres het adres van de gateway en als destination het echte adres van de ontvangende host.



Het NAT systeem maakt gebruik van de IP adressen en de source portnummers (uit de layer4 header). Het NAT systeem verander deze headers door er een ander adres en portnummer in te plaatsen. Bij een uitgaand pakket zijn eigen public IP adres en een random portnummer en voeg een regel toe aan zijn tabel. Bij een inkomend pakket wordt de header weer aangepast aan de private gegevens.
Omdat een NAT systeem tevens een router functie heeft worden ook de MAC headers aangepast.
De veranderingen die door routers en het NAT systeem worden aangebracht zorgen ervoor dat ook de controle bits in headers en de trailer opnieuw bepaald moeten worden.

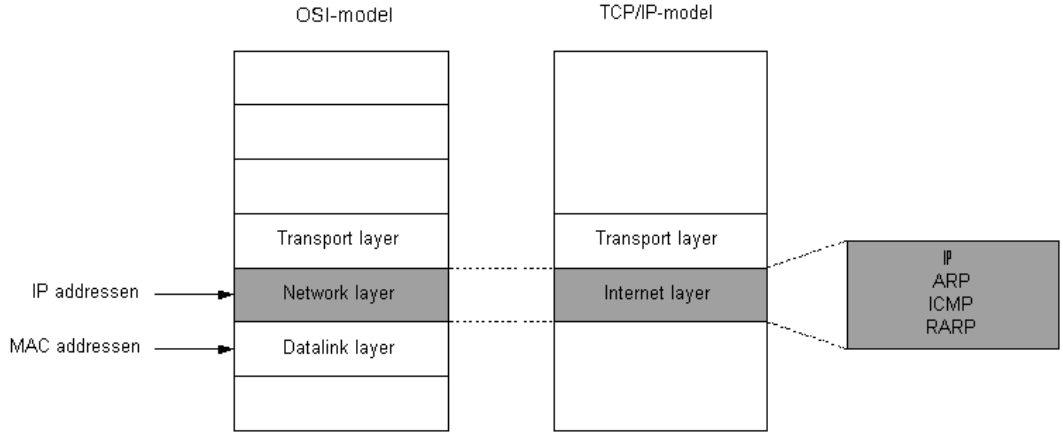
Vragen en opdrachten

1. Welke herkenningstekens heeft een host in een IP netwerk?
2. Uit welke twee delen bestaat een IP adres en welk deel gebruikt een router voor routing?
3. In welke tabel is de relatie tussen een hostnaam en zijn IP adres opgeslagen?
4. In welke tabel is de relatie tussen een MAC adres en zijn IP adres opgeslagen?
5. Verklaar de naam gateway?
6. Waaraan is de klasse van een IP adres te herkennen?
7. Welke IP adressen zijn geldig voor klasse C?
8. Waarmee wordt bepaald wat het netwerk ID is bij een subnet adres?
9. Met welke subnet mask waarde kunnen we een klasse C netwerk in 6 subnetten verdelen?
10. Hoeveel host systemen kunnen aangesloten worden op IP netwerk 192.16.1.96 met een subnet mask 255.255.255.240?
11. Geef het verschil aan tussen een private adres en een public adres.
12. Waarvoor wordt het NAT systeem gebruikt?
13. Geef een andere naam voor een fysiek en logisch adres.
14. Welke header waarde wordt door een router veranderd?

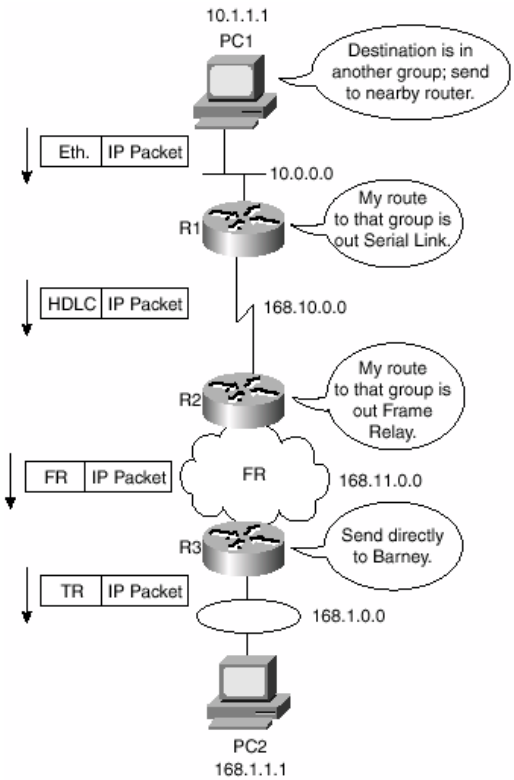
Aantekeningen

1.11 Layer 3, Protocols

Layer 3 is de network layer van het OSI-model. Deze komt overeen met de Internet layer van het TCP/IP-model. Deze lagen zijn verantwoordelijk voor het transport van packets van een **source-netwerk** (waarop zich de zendende host bevindt) naar een **destination-netwerk** (waarop zich de ontvangende host bevindt).
De datalink layer is verantwoordelijk voor het transport van frames van een **source host** naar een **destination host** binnen een netwerk (host – host, host – router, router – router en router – host). Het **MAC-protocol** maakt hierbij gebruik van MAC-adressen.
Het **network-protocol** (layer 3) maakt gebruik van **logische adressen** die bestaan uit een **netwerknummer** en een **hostnummer**. De netwerknummers worden gebruikt om de packets naar het destination-netwerk te leiden.
In network layer zijn een aantal protocollen aanwezig die gebruikt worden om het transport te regelen.



Communicatie tussen hosts op verschillende netwerken



Als een frame naar een ander netwerk moet worden gestuurd dan plaats het MAC-protocol, het MAC-adres van de **gateway** (poort naar andere netwerken) in de MAC header. Bij de source host moet het IP-nummer van de gateway bekend zijn (**default-gateway**), anders is er geen communicatie met een ander netwerk mogelijk.
De gateway is een poortinterface van een **router** (layer 3 device) waarmee een netwerk verbonden is.
De router verwijderdt de MAC-header en vergelijkt het netwerknummer van het destination IP-adres uit de IP-header van het packet, met de netwerknummer uit zijn **route-tabel**.
Als het netwerk in de tabel voorkomt, dan staat daar ook in via welke poort de router het packet moet doorgeven naar een volgende router. Het MAC-protocol in de router verzorgt het transport van het frame naar de volgende router. Hierin wordt door het netwerk-protocol het vervolg van de route bepaald. Dit proces herhaalt zich totdat het packet bij de router arriveert met de gateway naar het destination-netwerk. Het MAC-protocol bezorgt het frame bij de destination host.
Tijdens het transport verandert steeds de frame header met als source MAC-adres de poort waarvan het frame verzonden wordt en als destination het MAC-adres waar het frame naar toe gezonden wordt.

Routers kunnen alleen packets verwerken die werken met een logisch adres dat bestaat uit een netwerk- en een hostdeel. Protocollen die met deze adressering werken zijn o.a; IP, IPX en Appletalk DDP. We noemen deze protocollen **routed protocols**.
De routers sturen hun route-tabellen naar de routers waarmee ze direct verbonden zijn (**neighbours**).
Het protocol, dat zorgt voor het uitwisselen van de tabellen en het bepalen van de route als er meer mogelijkheden zijn, noemen we **routing protocols**. Een aantal van deze protocollen zijn; RIP, OSPF, IGRP, BGP en EIGRP.

Wat is er nodig om over een IP-netwerk te communiceren?
Om te kunnen communiceren over een IP-netwerk moet een host beschikken over:

- Een layer2-adres. (Het MAC-nummer)
- Een layer3-adres. (Het IP-nummer en subnet mask)
- Een gateway-adres. (Het IP-nummer)

Hoe komt de zendende host aan zijn eigen IP-adres?
Het MAC-nummer is door de fabrikant in de NIC geplaatst.
De IP-nummers kunnen op verschillende manieren bij de host bekend worden.

- **Statisch**. De netwerkbeheerder vult handmatig het host IP-nummer en het IP-nummer van de default-gateway in. Deze gegevens worden in de Registry opgeslagen. Tijdens het opstarten test de host of er op het netwerk al een systeem bestaat met dit IP-nummer. Als dit het geval is, dan wordt de netwerkpoort niet geactiveerd en volgt er een foutmelding (IP conflict).
- **Dynamisch**. Tijdens het opstarten van de host worden de IP-nummers, via het netwerk, door de host opgevraagd.

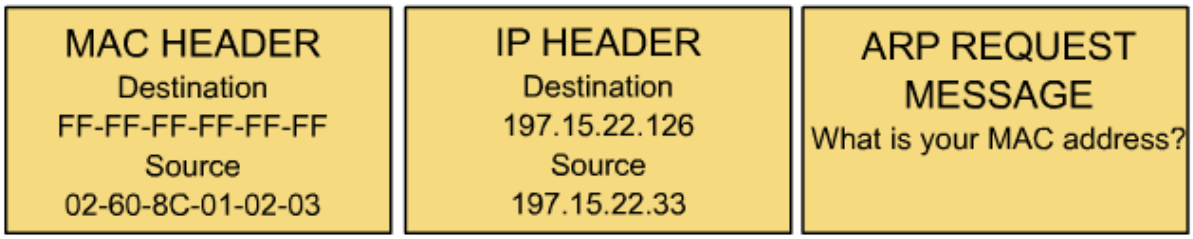
De dynamische toekenning van IP-adressen kan op verschillende manieren plaatsvinden.

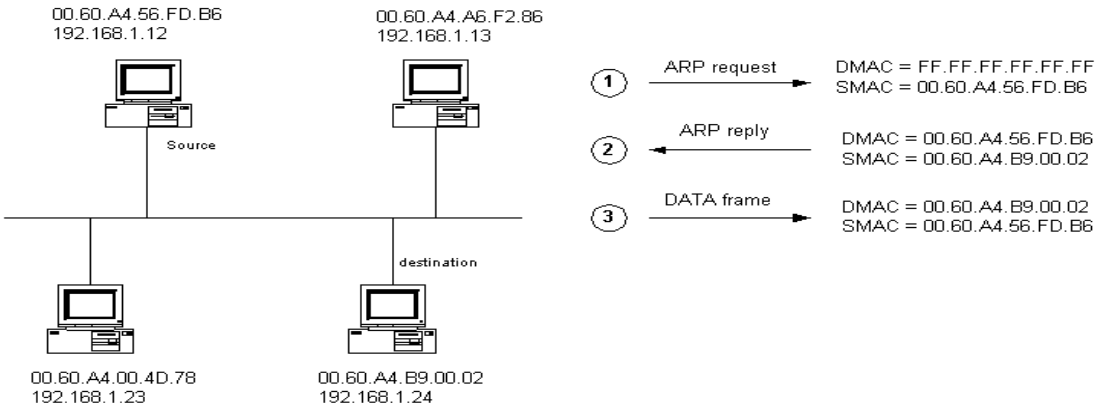
- Bij een diskless-systeem is het mogelijk om via het netwerk op te booten van een netwerkserver. In de bios is een protocol aanwezig (**reverse address resolution protocol RARP**) dat een broadcast bericht (**RARP request**) verstuurt met zijn eigen MAC-nummer en met een leeg source IP-veld. De RARP server ontvangt het bericht en zoek in zijn tabel naar het MAC-nummer en stuurt daarna een bericht terug (**RARP reply**) met het gevraagde IP-nummer.
- Het **Bootstrap protocol** (**BOOTP**) is vergelijkbaar met RARP. Het verschil is, dat RARP alleen een host IP-nummer verstrekt en BOOTP ook het IP-nummer van de default-gateway en van een server doorgeeft. In beide gevallen zijn het vaste nummers die uit een tabel gehaald worden. De tabel moet door de netwerkbeheerder gemaakt worden. Een ander verschil is, dat BOOTP wordt geactiveerd door een systeem dat boot van een lokale disk/cd. Als tijdens het booten blijkt dat enkele netwerkparameters via het netwerk moeten worden opgevraagd, dan wordt het Bootstrap Protocol gebruikt.
- Het **Dynamic Host Configuration Protocol** (**DHCP**) is de opvolger van BOOTP. De DHCP-server kiest de IP-nummers uit een reeks nummers. Een host krijgt dus niet altijd hetzelfde nummer. De DHCP server biedt, naast het host IP-nummer ook het subnet mask, de default-gateway, het IP-nummer van de DNS server en andere configuratie informatie aan.

Communicatie tussen hosts
Een host moet niet alleen over de IP-adressen van zichzelf en de bestemming kunnen beschikken, maar ook over het MAC-adres waar het frame naar toe gestuurd moet worden.
Als een host de benodigde netwerkgegevens heeft, dan kan een communicatie met een andere host gestart worden. De netwerk-layer krijgt van de transport-layer een **datagram** met een destination IP-adres. Het IP-protocol van de zendende host kijkt eerst in zijn **ARP-tabel** (een tabel in het **ramgeheugen** met IP-nummers en bijbehorende MAC-nummers) of het IP-nummer daarin voorkomt. Als het IP-nummer daarin staat, dan geeft de netwerk-layer een **data-packet** met het destination MAC-nummer door aan de datalink layer die hier een **frame** van maakt en dit via de fysieke layer op de lijn zet.

Als het IP-nummer niet in de ARP-tabel staat dan wordt de hulp van het Address Resolution Protocol (ARP) ingeroepen om het MAC-nummer te achterhalen. ARP stuurt een **request-packet,** met als destination adres het MAC broadcast-nummer (FF.FF.FF.FF.FF.FF), naar de datalink layer. Dit packet wordt door alle systemen op het netwerk (broadcast domein) gelezen en het systeem met als IP-adres het IP-nummer uit het packet stuurt een **reply-packet** terug met zijn MAC-nummer. Het zendende systeem plaats nu een extra regel in zijn ARP-tabel met het IP-nummer en het MAC-nummer van het destination-systeem.

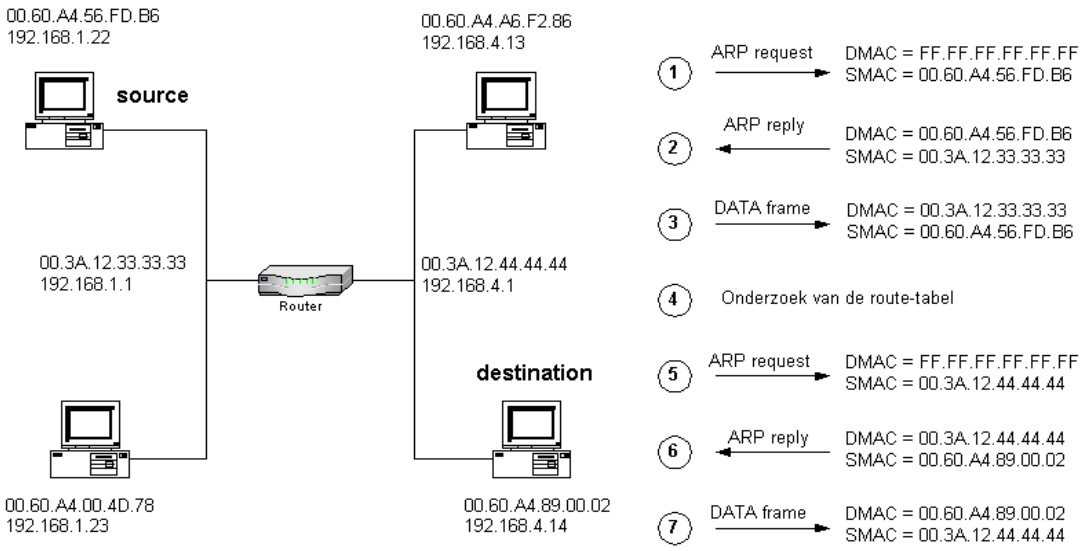
ARP request (host 197.15.22.33 vraagt om het MAC-adres van host 197.15.22.126).





Na stap 2, voegt het source-systeem een regel toe aan zijn ARP-tabel.
Het destination-systeem voegt een regel toe aan zijn ARP-tabel met het IP- en MAC-nr uit het request-packet. De entries in de tabellen worden na 100sec weer verwijderd als er binnen deze tijd geen gebruik van gemaakt is.

Als het destination-systeem zich op een ander netwerk bevindt, dan kijkt het IP-protocol van de zendende host in zijn route-tabel naar het IP-nummer van de default-gateway. Vervolgens zoekt hij in zijn ARP-tabel naar dit nummer. Als dit niet aanwezig is, volgt de ARP request/reply actie. Nu wordt het data-frame verzonden en de router gebruikt het destination IP-nummer en zijn route-tabel om de weg naar het destination-netwerk te bepalen. Als het packet bij de gateway van het destination-netwerk is aangekomen wordt de ARP-tabel van deze poort doorzocht naar het MAC-nummer van de destination host. Eventueel gebruikt de router ARP om dit nummer te achterhalen en stuurt tenslotte het frame naar deze host.



In de ARP-tabellen van de source, de router-poorten en de destination is tijdelijk één regel toegevoegd Het ARP dat de router gebruikt noemt men **proxy ARP**. De router vertegenwoordigt het destination-systeem en het source-systeem op de verschillende netwerken (192.168.1.0 en 192.168.4.0).

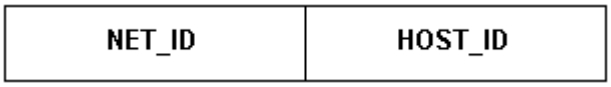
ARP-tabel van het source-systeem.

IP-adres	**MAC-adres**	**Type**
192.168.1.1	00.3A.12.33.33.33	dynamic
192.168.1.23	00.60.A4.00.4D.78	dynamic

Dit geeft aan dat er contact geweest is met systeem 192.168.1.23 en één of meer systemen op een ander netwerk (minder dan 100 sec. geleden).

We kunnen de inhoud van de ARP-tabel bekijken en bewerken met het commando '**arp –option**' in een dos-box. Voor het ARP frame zie Hoofdstuk 6.

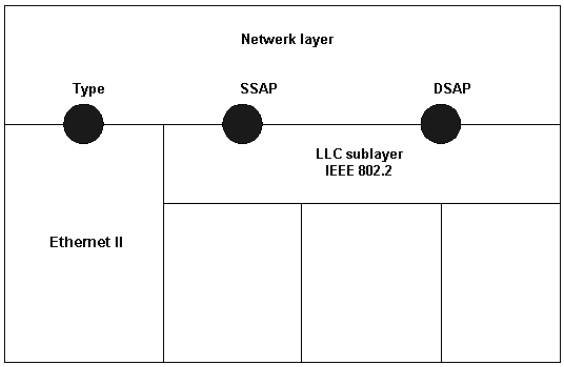
Routed protocol
Een routed protocol is een layer 3 protocol dat de communicatie tussen verschillende netwerken regelt. Deze protocollen werken met adressen die uit een netwerk- plus een host-nummer bestaan.



Het netwerk_id wordt bepaald door een AND-bewerking uit te voeren met het adres en het subnet mask.

192.168.4.23 AND 255.255.255.0 = 192.168.4.0

Het netwerknummer identificeert het netwerk binnen een intranet of het Internet en het hostnummer identificeert de systemen binnen een netwerk. De netwerknummers zijn uniek binnen het intranet of het Internet en de hostnummers zijn uniek binnen het netwerk.
Routed protocollen zijn o.a; IP, IPX en Apple DDP. We kijken in dit semester naar het IP-protocol en op een later moment naar IPX (Novell).
Een layer 3-protocol heeft een header in het data-packet dat volgt op de layer 2 header uit een data-frame (ethernet II of IEEE 802.2). In de layer 2-header wordt de koppeling gemaakt met het layer 3-protocol. Ethernet II doet dit met een typenummer (0x0800 = IP) en IEEE 802.2 doet dit met de SSAP en DSAP nummers.



De IP header heeft de volgende samenstelling.

IP Header

Type in MAC header = 0x0800

0 3	4 7	8 15	16 31
Version	Header Length	Type of Service	Total length
Identifier		Flags	Fragment Offset
Time to Live	Protocol	Header Checksum	
Source IP Address			
Destination IP Address			
Options + Padding			

- **Version.** De gebruikte IP-versie.
- **IP Header Length.** Hierin wordt de lengte van de IP header aangegeven in een aantal 32-bits words (minimaal 5 tot maximaal 15).
- **Type of service.** De hogere lagen geven hierin service parameters aan die o.a. gebruikt worden door routing protocollen.
- **Total Length.** Hierin wordt het aantal bytes aangegeven waaruit het IP-packet bestaat (header + data).
- **Identification, Flags and Fragment offset.**
  Dit zijn parameters die nodig zijn om het transport van data-blokken, die meer bytes bevatten dan de grootte van de MTU (Maximum Transport Unit), te kunnen regelen. Als een PC een data-blok wil verzenden die groter is dan de MTU, dan wordt door het layer 4 protocol de data gefragmenteerd in segmenten die passen in een MTU. Deze segmenten worden door het ontvangende layer 4 protocol weer samengevoegd tot één blok en doorgegeven naar de hogere lagen.
  Als de segmentering plaatsvindt voor een 100Mbps FDDI-netwerk, dan is de MTU 4096 bytes. Wanneer dit FDDI-frame naar een router verzonden wordt die deze door moet geven aan een 10Mbps ethernet-netwerk dan wordt het FDDI-frame gefragmenteerd in blokken van maximaal 1500 bytes. De genoemde velden in de IP-header zijn bedoeld om dit te kunnen regelen. Het layer

3-protocol van het ontvangende systeem voegt de fragmenten weer samen tot één segment voordat hij het doorgeeft aan het layer 4-protocol.

- **Time to Live.**
  Dit geeft aan hoe lang een packet zich in een netwerk mag bevinden tijdens het transport van de zender naar de ontvanger. Een router verlaagt de teller afhankelijk van de tijd dat het packet zich in de router bevindt en de snelheid van de verbinding waarover het frame wordt geleid. In moderne routers en verbindingen is dit meestal minder dan 1 sec. De router verlaagt de teller met 1 ook al is de tijd minder dan 1 sec. De functie van het TTL-veld is dus veranderd in een **hop counter**. Als de teller op nul staat wordt het packet niet verder doorgegeven en verdwijnt van het net. Hiermee wordt voorkomen dat een frame in een loop zou kunnen blijven rondlopen zonder ooit zijn bestemming te bereiken.
- **Protocol.** Hierin wordt het layer 4 protocol aangegeven (6 = TCP en 17 = UDP) of het layer 3 sub-protocol (1 = ICMP).
- **Header Checksum.** Dit zijn twee controle-bytes om te bepalen of de IP-header correct is ontvangen. Een router wijzigt het TTL-veld en soms ook nog andere velden, zodat de checksum opnieuw berekend moet worden en toegevoegd aan de header van het door te zenden packet.
- **Source- and Destination address.** Hierin staan de IP-adressen van de zender en de ontvanger. Het source-adres wordt door de ontvanger gebruikt om een packet terug te kunnen zenden en het destination-adres wordt door de routers gebruikt om de route door het netwerk te bepalen en om het packet bij de destination af te kunnen leveren.
- **Options.** Dit veld kan wel of niet aanwezig zijn. Als het bestaat, dan wordt het gebruikt voor parameters en data voor diverse IP-functies (o.a. ICMP) en voor routing protocollen.

Een layer 3-protocol dat geen communicatie tussen netwerken ondersteunt (**non-routed protocol**) is **NETBEUI.** Dit protocol gebruikt de computernamen en MAC-adressen om de communicatie te regelen op een netwerk.

Routing protocol
Als een netwerk bestaat uit een groep netwerken dan zijn er routers nodig om deze netwerken te koppelen en verkeer tussen deze netwerken mogelijk te maken. Routers zijn netwerkapparaten die hun werk op layer 3 uitvoeren (layer 3 device).
Als een router op één van zijn poorten een frame binnen krijgt, dan wordt de MAC-header verwijderd. Daarna vergelijkt de router het destination-adres uit de layer 3-header met zijn route-tabel. Als een entry overeenkomt, dan staat hierin via welke poort het packet doorgestuurd moet worden. Als er geen entry voorkomt in de tabel, dan wordt het frame verwijderd. Als het packet doorgestuurd kan worden, plaats de datalink layer in de router hier een nieuwe MAC-header voor en verstuurt het frame.

Route-tabel van een host-systeem met IP-adres 192.168.1.6.

Network address	Subnet mask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.6	1
192.168.1.0	255.255.255.0	192.168.1.6	192.168.1.6	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.6	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.1.255	255.255.255.255	192.168.1.6	192.168.1.6	1
224.0.0.0	224.0.0.0	192.168.1.6	192.168.1.6	1
255.255.255.255	255.255.255.255	192.168.1.6	192.168.1.6	1

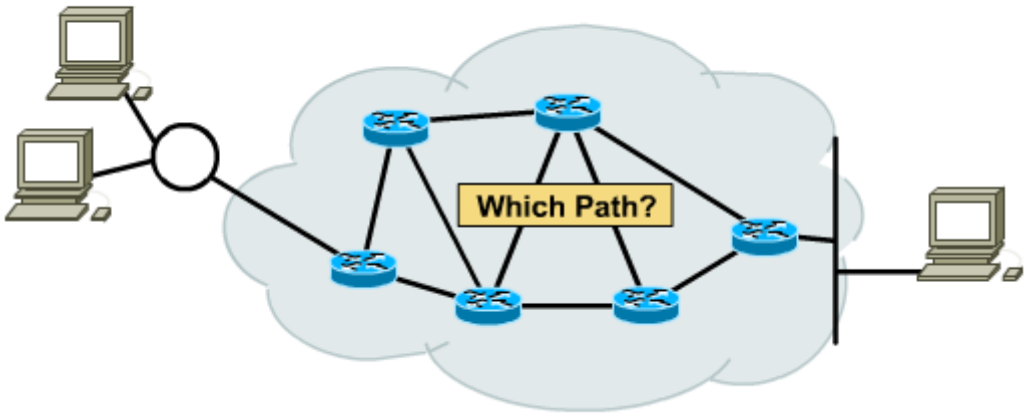
default-gateway 192.168.1.1

Route-tabel van een router met twee ethernetpoorten en twee seriële poorten (Cisco 2514).

	Network address	Subnet mask	
C	192.5.5.0	default	via e0
C	205.7.5.0	default	via e1
C	205.100.11.0	default	via s0
R	219.17.100.0	default	naar 205.100.11.2 via s0
R	199.6.113.0	default	naar 205.100.11.2 via s0
R	223.8.115.0	default	naar 205.100.11.2 via s0
R	204.204.7.0	default	naar 205.100.11.2 via s0
R	210.93.105.0	default	naar 205.100.11.2 via s0

IP-adres 205.100.11.2 is het adres van de seriële poort op de volgende router. De "**C**" staat voor direct verbonden (connected) met de router en de "**R**" staat voor routing-protocol **RIP**. Alle andere netwerken zijn via s0 te bereiken.

Hoe wordt de route (which path) van de source naar de destination bepaald?



In de routers draait een routing-protocol, dat bepaalt welke route een binnenkomend frame moet nemen om bij zijn bestemming te komen. Hiervoor gebruikt het protocol zijn route-tabel. Als het netwerk niet voorkomt in de tabel dan wordt het frame verwijderd. Het protocol stuurt zijn tabel via zijn poorten het netwerk in. Dit arriveert dus bij de routers die direct gekoppeld zijn (neighborhood routers). De ontvangende routers passen hun tabel aan met de routes naar netwerken die hij nog niet kent. Als er een route naar een reeds bekend netwerk wordt aangeboden onderzoek hij of deze route beter is dan de bestaande. Als dit het geval is wordt de route vervangen. Na verloop van tijd heeft elke router een tabel met de beste route naar alle aangesloten netwerken. Het proces om te komen tot een juiste tabel in elke router noemen we **convergention**. Er is dus altijd maar één beste route van A naar B. In het netwerk zijn er wel meerdere wegen van A naar B mogelijk. De route wordt via een andere weg geleid als een verbinding uitvalt of verstopt raakt (**congestion**). Als er een verbinding uitvalt worden de tabellen aangepast en na enige tijd (**convergention time**) zijn alle tabellen weer oké.
We kunnen een router ook dwingen een vaste route te kiezen om een ander netwerk te bereiken. We doen dit door een route handmatig in te geven (**static route**). Deze route heeft altijd voorrang op een **dynamic route.** Dit zijn de routes die door een andere router worden aangeboden.

Het protocol dat de tabel samenstelt, de beste weg bepaalt en zijn tabelinformatie doorgeeft aan zijn buren noemen we een **routing-protocol**. Er zijn verschillende protocollen die onderling verschillen in toepassing en werking.
Een netwerk met een groep routers noemen we een **autonomous system.** Hiervoor gebruiken we een protocol dat alleen route-informatie uitwisselt tussen de routers binnen dit systeem en we spreken dan over een **Interior Gateway Protocol** (**IGP**).

Wanneer we autonomous systemen koppelen via een backbone-netwerk dan gebruikt de backbone een **Exterior Gateway Protocol** (**EGP**). De routers die de koppeling met de backbone verzorgen maken gebruik van een **Border Gateway Protocol** (**BGP**) Deze wisselen route-informatie uit met het backbone-netwerk.

De IGP's die in het Cisco-progamma aan de orde komen zijn;
- **Routing Information Protocol** (RIP),
- **Interior Gateway Routing Protocol** (IGRP),
- **Enhanced Interior Gateway Routing Protocol** (EIGRP),
- **Open Shortest Path First** (OSPF).

Het bepalen van de beste route gebeurt op basis van de **Metric-waarde**. Dit verwijst naar de 'afstand' (**distance**) tot het target-netwerk. **De laagste waarde geeft de beste weg aan**.
De Metric-waarde wordt bepaald door,
- het aantal routers dat gepasseerd moet worden om het destination-netwerk te bereiken (**hop count**),
- de bandbreedte van een link (**bandwidth**),
- de tijd die nodig is om een packet van de source naar de destination te vervoeren (**delay**),
- het aantal packets dat een router of link verwerkt (**load**),
- de **error rate** van een link (hoe vaak treedt er een fout op) (**reliability**),
- het delay van een verbinding in een aantal maal 35msec (**ticks**),
- de kosten van een verbinding (**cost**); een willekeurige waarde die door een netwerkbeheerder kan worden toegekend.

De verschillende protocollen gebruiken één of meerdere van bovengenoemde punten om de metric-waarde te bepalen. De verschillende werkwijze geven we aan met:
- **Distance-vector**.
- **Link-state**.
- **Balance hybrid**.

De distance-vector methode wordt toegepast door RIP en IGRP.
RIP versie 1 bepaalt de metric-waarde door het aantal hops te bepalen. Als een router, routes krijgt aangeboden van een neigborhood router, dan wordt de metric-waarde met één verhoogd omdat de route via één hop meer loopt, dan vanaf de router die de route aanlevert.
IGRP kan de hop counter met meer dan 1 verhogen. Dit gebeurt als de netwerkbeheerder, voor de route naar de volgende router, meer dan 1 hop heeft ingesteld. Hierdoor kan de netwerkbeheerder het verschil in links mee laten wegen voor het bepalen van de beste route.
RIP versie 1 en IGRP zijn alleen te gebruiken in niet in subnetten verdeelde netwerken of met subnetten van gelijke grootte. Het subnet mask wordt niet doorgegeven. Deze protocollen maken gebruik van de één subnet mask of het default mask.
RIP versie 2 geeft wel de subnet masks door zodat deze gebruikt kunnen worden in netwerken met subnetten.

OSPF gebruikt een link-state methode. Hierbij wordt gebruik gemaakt van de **Shortest Path First** methode die ontwikkeld is door de **Nederlander E.W. Dijkstra**.
Dit is een methode die de metric-waarde berekent aan de hand van de parameters van de verbindingen zoals; bandwith, load, delay, reliability en cost. Elke keer dat er een tabel-update van een neighbour ontvangen wordt, wordt de tabel opnieuw berekend.

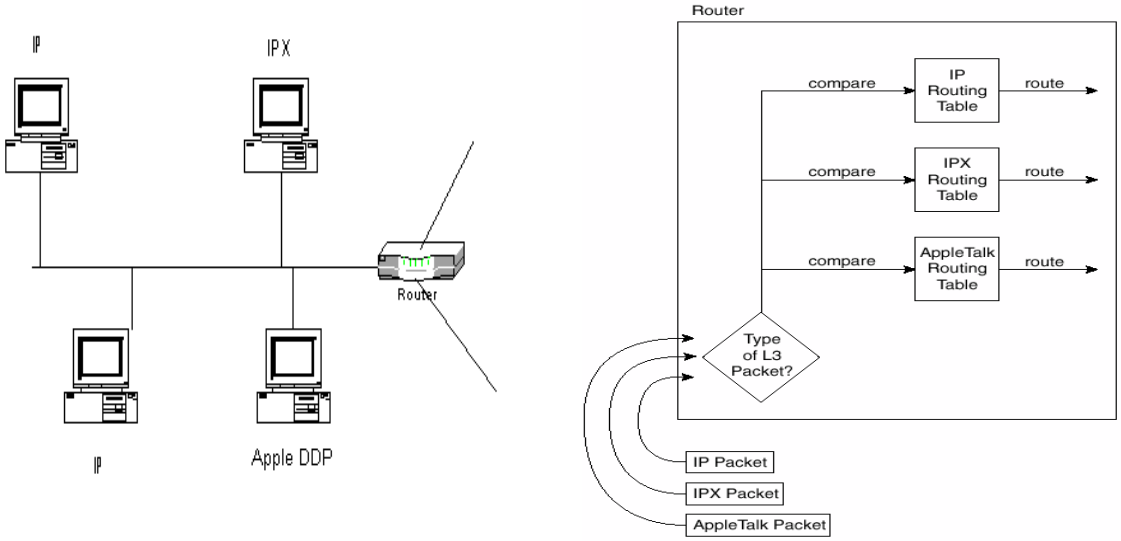
De balance hybrid methode wordt gebruikt door EIGRP. Deze uitgebreide (enhanced) versie van IGRP gebruikt een combinatie van distance-vector en link-state om de beste route te bepalen.

Default route
Als een aantal of alle netwerken maar via één weg te bereiken is, is het niet nodig om van al deze netwerken een tabel te onderhouden. Door het handmatig toevoegen van een **default route** wordt het verkeer naar de overige netwerken geregeld.
We passen dit toe als een router maar met één link verbonden is met het gehele netwerk (**Stub netwerk**) en bij een groep routers die via één link (bv. WAN link) verbonden is met een andere groep routers. De afzonderlijke groepen kennen dus elkaars netwerken niet, maar gebruiken de default route om deze te kunnen benaderen. De route bepaling is nu sneller maar heeft als nadeel dat een packet eerst een aantal routers passeert voordat bekend is of een netwerk wel bestaat of te bereiken is.

Connectionless en Connection-oriented
De meeste netwerk-services zijn verbindingsloze bezorgingssystemen. Dit betekent dat contact gemaakt wordt met de bestemming en dat er geen controle op de bezorging van de packets plaatsvindt. Dit is te vergelijken met het post bezorgingsysteem. IP is een connectionless systeem. Een layer 4-protocol kan de bezorging eventueel controleren. TCP is zo'n protocol dat eerst contact legt met de ontvanger en daarna de bezorging controleert (connection-oriented) omdat hij een bevestiging verwacht van de ontvanger dat het packet goed is aangekomen. UDP is een layer 4-protocol dat geen overleg heeft met de ontvanger en de bezorging niet controleert (connnectionless). E-mail maakt hiervan gebruik.

Bij fysieke netwerken spreken we ook over connectionless en connection-oriented.
Bij een connection-oriented netwerk wordt eerst een circuit opgebouwd en daarna worden alle packets via dezelfde weg naar de ontvanger gebracht. Dit is te vergelijken met een telefoonnetwerk (circuit switched).
Connection-oriented netwerken zijn WAN netwerken zoals ISDN en ATM. Hierin wordt eerst een virtueel circuit opgebouwd en daarna worden de packets verzonden via een vaste weg. Binnen deze netwerken worden dus geen route-tabellen gebruikt.
Connectionless netwerken zijn WAN netwerken zoals Frame Relay en X25.

Multi Protocol Routing
Over een netwerk worden frames vervoerd. De frame header wordt gebruikt om het frame, binnen een netwerk bij de bestemming af te leveren. Wat er in het frame zit is hiervoor niet belangrijk. Dit kunnen dus packets zijn van verschillende netwerk-protocollen (bv. IP, IPX, Apple DDP).
Om deze packets via een router te kunnen laten verwerken, moet de router voor elk type een routing-protocol geactiveerd hebben. We noemen dit **mullti protocol routing**.



Vragen en opdrachten

1. Wat is de functie van een netwerkprotocol bij het transport van data-packets en welke functie heeft de datalink layer hierbij?

2. Wat is de functie van een router en in welke layer is hij werkzaam?

3. Geef het verschil aan tussen een routed-protocol en een routing-protocol. Geef van beide enkele voorbeelden.

4. Op welke manieren kan een PC aan zijn netwerkparameters komen?

5. Op welke laag bevindt het ARP zich en waarvoor is deze nodig?

6. Wat wordt bedoeld met proxy ARP?

7. Welke gegevens bevinden zich in een ARP-tabel, hoe kunnen we die bekijken en hoe lang blijft de inhoud geldig?

8. Wat is de functie van de identification, flags en fragment offset velden in een IP-header?

9. Welke waarde bepaald de beste weg naar een destination-netwerk?

10. Welke gegevens bepalen de grootte van de metric-waarde?

11. Noem enkele IGP protocollen.

12. Noem de manieren waarop deze protocollen het beste weg bepalen.

13. Wat is een static-route en wat een default-route?

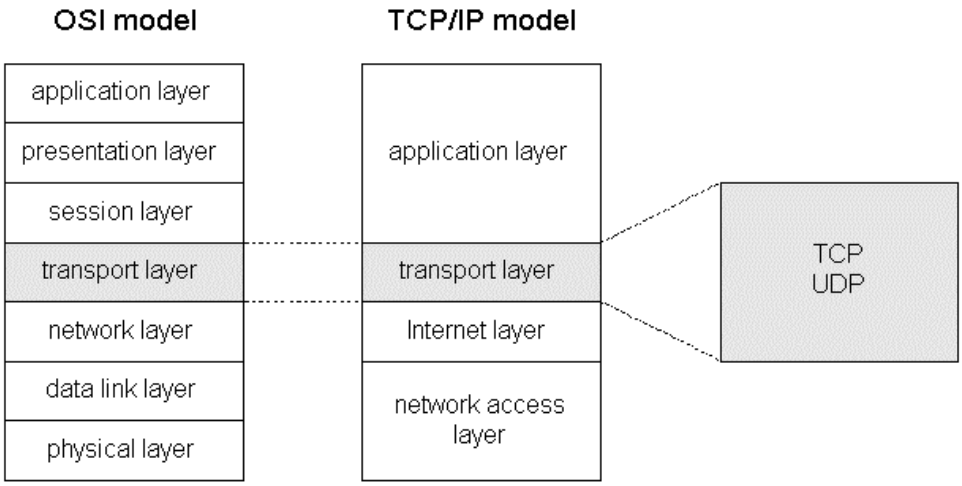
14. Beschrijf een connectionless en een connection-oriented netwerk service.

15. Wat wordt verstaan onder multi protocol routing?

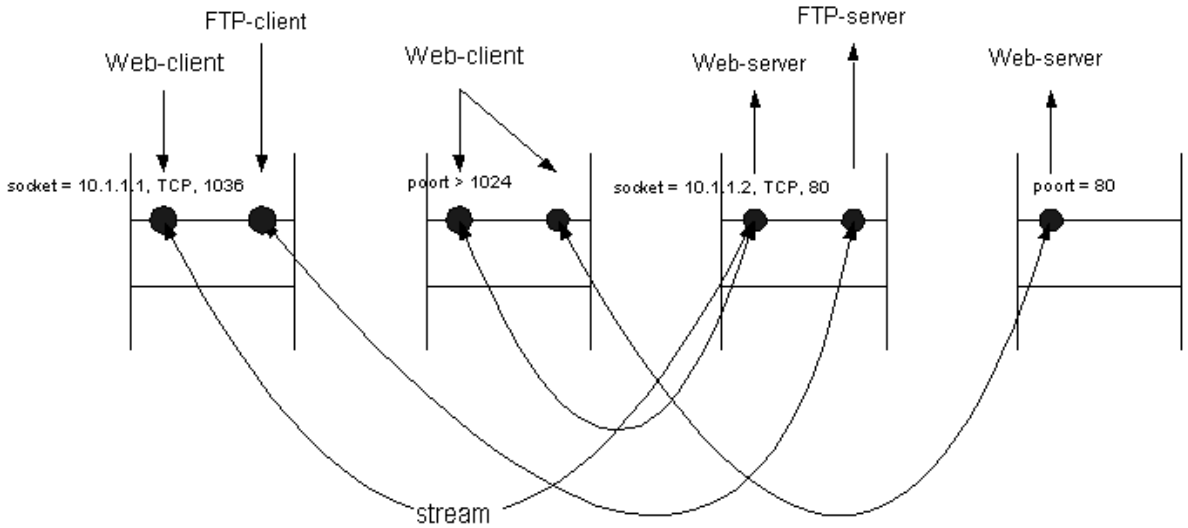
Aantekeningen

1.12 Layer 4, Transport Layer

De protocollen van layer 4 voeren de opdrachten uit van de hogere lagen en gebruiken daarvoor de functies van de onderste lagen.



Het transport-protocol krijgt opdracht van de hogere lagen om een data-block te verzenden.
De hogere lagen geven naast de data, het protocol-type, het destination-adres de source- en destination-poortnummers door. De koppeling tussen de hogere lagen en de transportlaag noemt men een **socket**. Een socket bestaat uit het IP-nummer van het systeem, het gebruikte protocol en het poortnummer van de applicatie (bv. 10.1.1.1, TCP, 1036 of 10.1.1.2, TCP, 80). De poortnummers worden centraal geregeld (te vinden in RFC 1700). Hierdoor is het bekend welke applicatie gebruik maakt van welk nummer.
Nummers tussen 1 en 1024 zijn bedoeld voor server-applicaties. De client-applicaties gebruiken de nummers boven 1024 tot 64k (16bits getal). Een web-browser wordt gekoppeld aan poort 1036 op systeem 10.1.1.1 en communiceert met poort 80 van de web-server op systeem 10.1.1.2.
De protocollen in de TCP/IP stack kunnen een connectionless (UDP) of connection-oriented (TCP) verbinding gebruiken. De verbinding tussen twee sockets noemen we een **stream**.



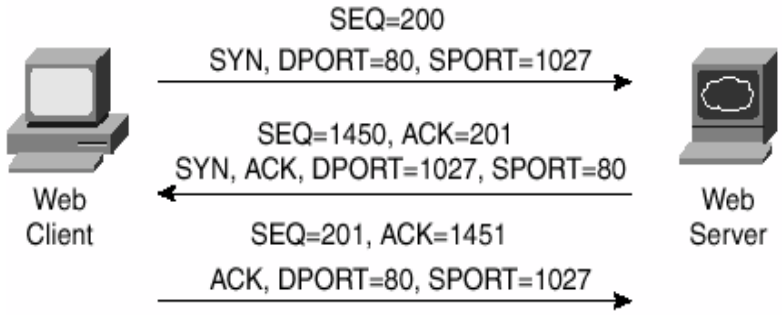
Een client-applicatie kan meerdere sockets gebruiken (verschillende nummers) en een server kan op zijn socket, packets van verschillende clients ontvangen. We noemen dit **multiplexing**. Een verbinding wordt gekarakteriseerd door de combinatie van twee sockets. Hierdoor kan in het multiplexing-systeem de verschillende streams onderscheiden worden.

De functies van de transport-protocollen worden door de hogere lagen gebruikt om;

- Een verbinding op te bouwen (**connection establishment**),
- De data te verzenden/ontvangen via de connection (stream) (**data transfer**),
- Het data-verkeer te regelen (**flow control**),
- De betrouwbaarheid van het data-vekeer te garanderen (**error recovery, reliability**),
- Een verbinding weer vrij te geven (**connection termination**).

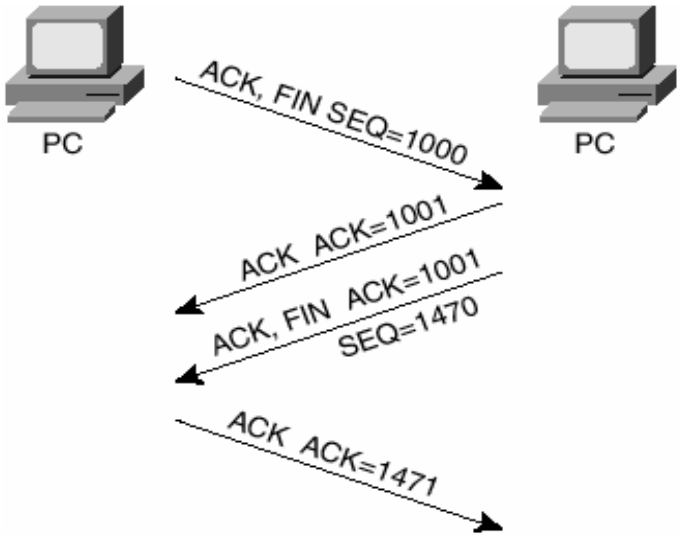
Connection establishment (TCP)
Een transport via het TCP-protocol kan alleen plaatsvinden als de verbinding eerst is opgebouwd. Hiervoor wordt door het client-systeem contact gemaakt met het server-systeem. De systemen wisselen gegevens uit over hun ontvangstbuffers (window size), synchroniseren hun sequence- en acknowlegement-velden in de TCP-header en hun poortnummers.

Het opbouwen van de verbinding gebeurt in drie stappen (**three-way** connection establishment).

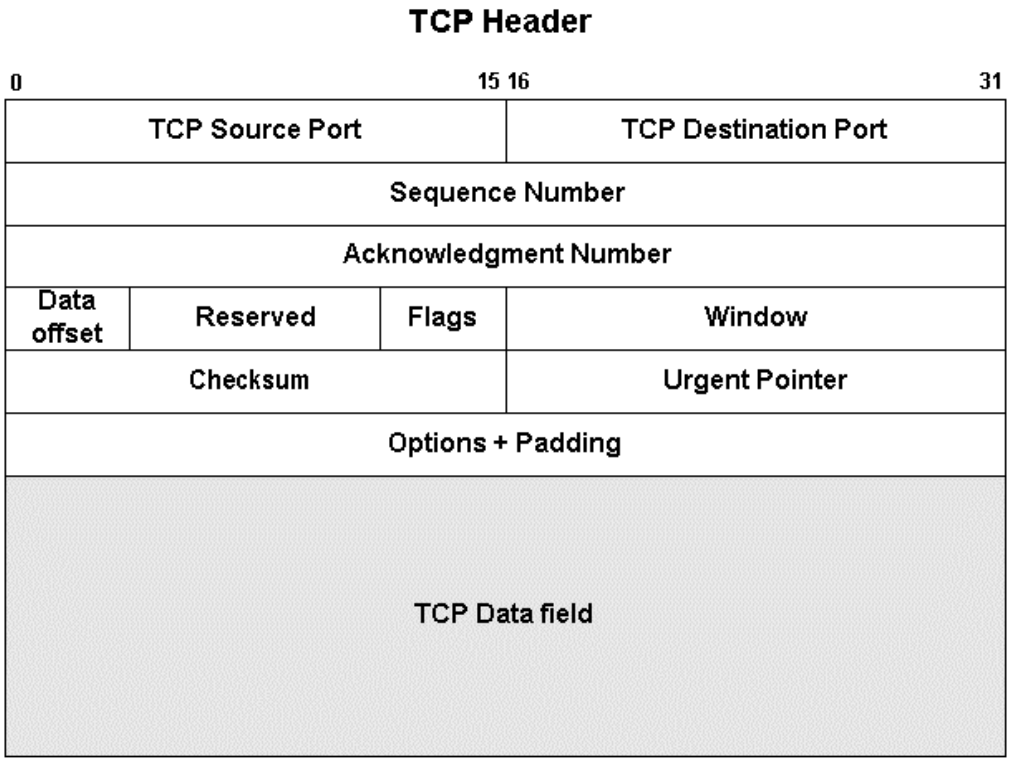


De SYN en ACK-flags worden aangegeven in het flags-veld van de TCP-header.

Connection termination (TCP)
Wanneer de data-uitwisseling heeft plaatsgevonden neemt het cliëntsysteem het initiatief om de verbinding te verbreken. Dit is een actie in vier stappen (**four-way handshake**). Hiervoor worden de **ACK** en **FIN**-flags gebruikt.

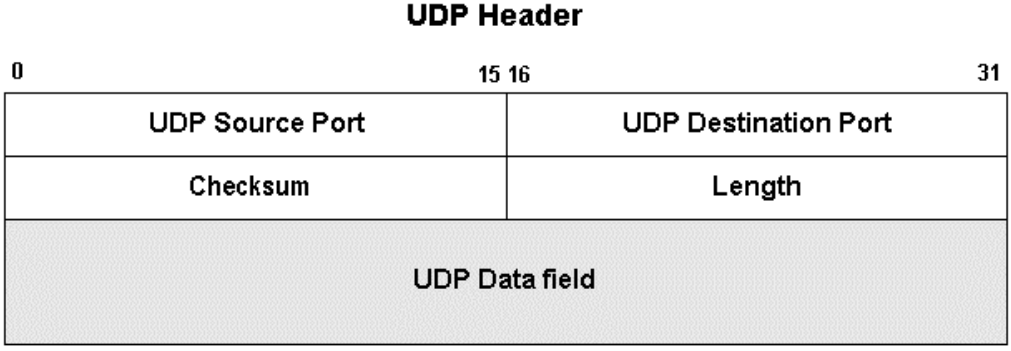


TCP-header



- **Source- and Destination Port**. Dit zijn de koppelingen naar de applicaties op de systemen. Source voor de zendende applicatie en destination voor de ontvangende applicatie.
- **Sequence Number**. Dit is het nummer van het eerste byte in het data-segment.
- **Acknowledgement Number**. Het eerste byte nummer van het te verwachten data-segment.
- **Data offset**. Dit geeft de lengte van de TCP header aan of ook wel het begin van het data-veld.
- **Reserved**. Set to zero. (reserved betekent dat het gebruik er van niet bekend is)
- **Flags**. Veld voor de SYN, ACK en FIN flags voor het establishment en termination proces van de connection.
- **Window**. Het aantal bytes dat het systeem kan ontvangen. Deze waarde kan tijdens het data-transport wijzigen.
- **Checksum.** Controle bytes voor de header + het data-veld.
- **Urgent pointer.** Indicator om aan te geven dat dit het einde van de urgente data is.
- **Options.**
- **Data**. Data voor de hogere lagen.

UDP header



- **Source- and destination port**. Dit zijn de koppelingen naar de applicaties op de systemen. Source voor de zendende applicatie en destination voor de ontvangende applicatie.
- **Checksum.** Controle bytes voor de header + het data-veld.
- **Length**. De lengte van het data-veld.

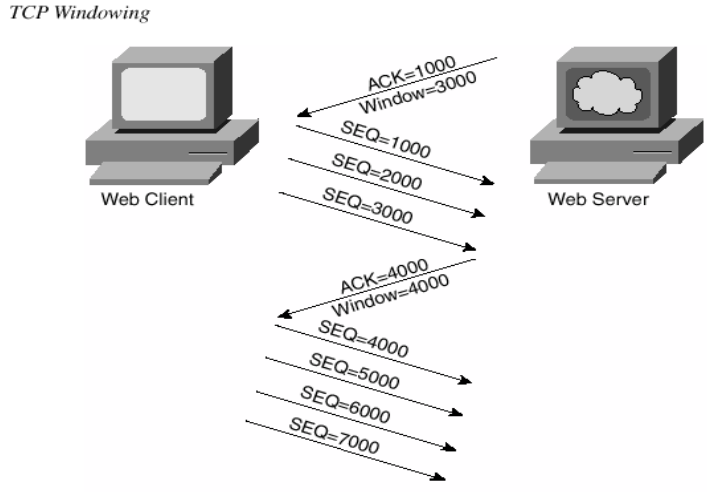
Het UDP-protocol bouwt geen verbinding op met de destination (connectionless) maar stuurt ongevraagd data. Dit zijn data, die niet meer dan een segment omvatten. De controle op de bezorging (flow control) wordt overgelaten aan de hogere lagen.

Data transfer (TCP)
Het data-block dat het TCP-protocol krijgt aangeboden om te verzenden wordt in segmenten verdeeld. De grootte van de segmenten wordt bepaald door het te gebruiken MAC-protocol en de window size van het ontvangende systeem. De maximale grootte wordt bepaald door MTU van de MAC layer en werkelijke grootte door de window size. Een segment voor een ethernet (MTU = 1500) en een window size van 3000 is 1500bytes. Voor een window size van 4000 wordt de segment grootte 1000 bytes. We spreken hier ook wel over een window size van 4 segmenten.
De sequentie-nummers geven het begin van een segment aan. Hiermee kan de ontvanger de segmenten in de juiste volgorde plaatsen en controleren of er een of meerdere segmenten ontbreken. Met het acknowlegement-nummer wordt om het volgende of het ontbrekende segment gevraagd.

Error recovery (Reliability)

In het bovenstaande voorbeeld is de window size 3000. tijdens het transport is er iets misgegaan met het segment met sequence-nummer 2000 en via ACK=2000 wordt deze nogmaals opgevraagd.

Flow control met windowing



De window size begint met 3000 en tijdens het data-transport wordt hij vergroot naar 4000. De size kan ook kleiner worden.
Een probleem dat zich voor kan doen is, dat de ontvanger niet snel genoeg zijn buffer data kan verwerken. De ontvanger stuurt nu een bericht met een **not ready flag**. De zender stop nu het zenden van segmenten ook al heeft hij nog niet een volledig window size verzonden. De ontvanger wacht op een bericht met een **ready flag** om het transport te hervatten.

Port numbers
Met de poortnummers worden de applicaties aan de communicatie verbinding gekoppeld. Er is een centrale administratie waarin de poortnummers van de verschillende applicaties zijn opgeslagen.
Een poortnummer is een 16 bits binair getal.

- De nummers 0 t/m 254 zijn toegewezen aan algemene applicaties.
- De nummers 255 t/m 1023 zijn bedoeld voor commerciële applicaties (gekoppeld aan een bedrijf). De applicaties zijn server-applicaties waarmee een client-applicatie kan communiceren.
- De nummers 1024 t/m 65536 zijn niet gedocumenteerd. De session layer software kiest een nummer en koppelt deze aan een client-applicatie.

Op de site http://www.rfc-editor.org kan je een lijst met nummers vinden onder RFC 1700.

Enkele voorbeelden.
TCP port numbers

Nummer	Afkorting	Applicatie
20	ftp	File transfer protocol (data)
21	ftp	File transfer protocol (control)
23	telnet	Terminal connection
25	smtp	Simple Mail Transfer Protocol
80	http	Www-server

UDP port numbers

Nummer	Afkorting	Applicatie
53	dns	Domain Name Server
67	bootp	Bootstrap Protocol Server
69	tftp	Trivial File Transport Protocol

Vragen en opdrachten

1. Wat is de functie van de transport layer?

2. Welke parameters karakteriseren een socket?

3. Wat wordt bedoeld met de multiplex-functie van transport layer?

4. Uit hoeveel stappen bestaat de connection establishment actie? Welke gegevens worden tijdens deze actie uitgewisseld? Hoe worden deze stappen genoemd?

5. Uit hoeveel stappen bestaat de connection termination actie? Hoe worden deze stappen genoemd? Welke flags worden hierbij gebruikt?

6. Geef het verschil tussen TCP en UDP aan.

7. Waarvan is de segmentgrootte afhankelijk?

8. Waardoor wordt de window size bepaald? Wat is de functie van een window?

9. Welke functies hebben de sequence- en acknowlegement-nummers?

10. Beschrijf het mechanisme van error recovery.

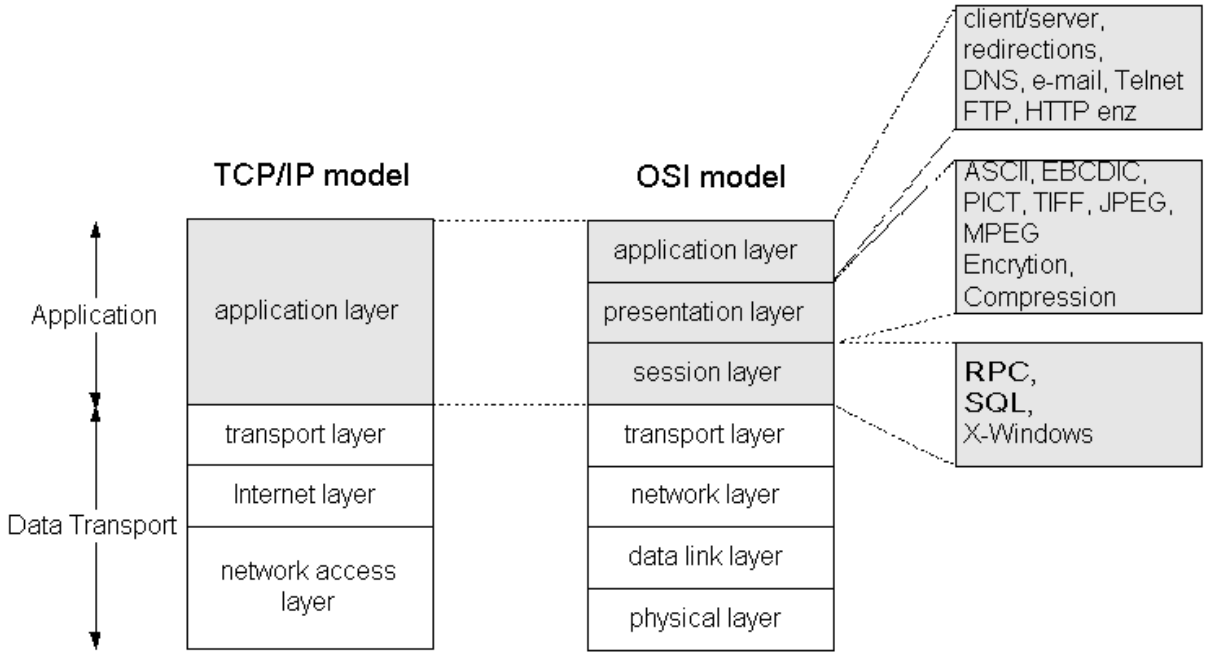
11. Hoe kan de ontvanger voorkomen dat zijn buffer overloopt?

12. Beschrijf het gebruik van de poortnummers.

Aantekeningen

1.13..15 Layer 5, 6 and 7 The Session, Presentation and Application Layers

De bovenste drie layers van het OSI-model en de bovenste layer van het TCP/IP-model worden de application layer(s) genoemd. De layers eronder noemen we de data transport layers.
In de application layer(s) bevinden zich ondersteunende diensten (services) voor applicaties, die via een netwerk met andere systemen communiceren. Bijv. een webbrowser met webserver, een database-applicatie met een database-server of een tekstverwerker met een file-server.
De session service beheert de koppeling tussen de applicaties op de verschillende systemen. Er kunnen meerdere koppelingen gelijktijdig actief zijn die gemultiplexed informatie kunnen uitwisselen. De koppelingen (sessions) worden herkend aan hun socket-informatie.
De presentation services bieden functies die op de data betrekking hebben zoals; de data opbouw (**formatting**), de manier van beschermen van data (**encryption**) en het indikken (**compression**) van de data.
De application services zijn diensten die door applicaties gebruikt kunnen worden. De programmeur hoeft deze services niet zelf te programmeren maar koppelt ze met een Application Programming Interface (API) aan zijn applicatie.

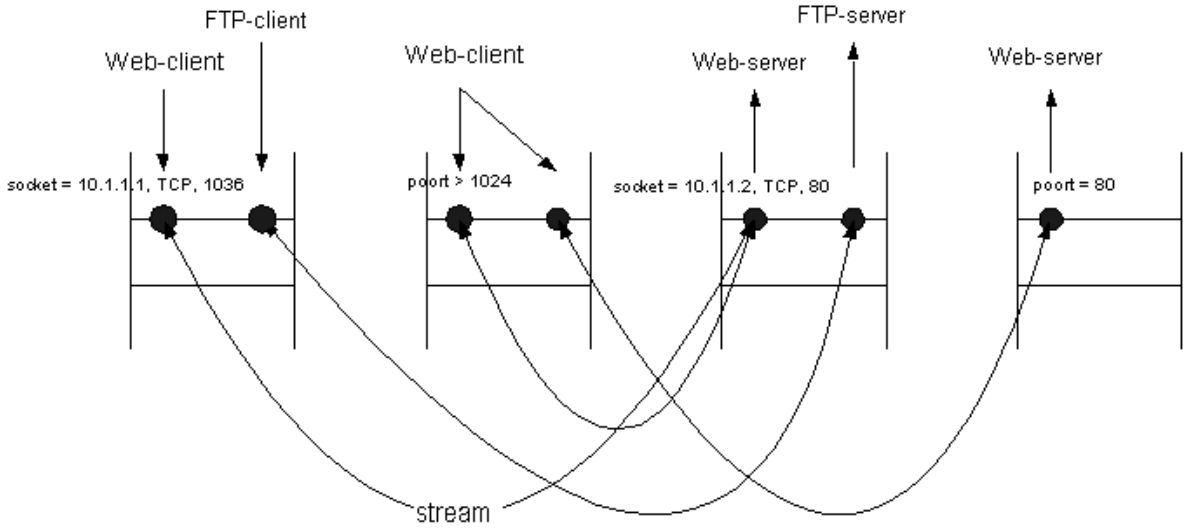


Session layer (chapter 13)
De session layer beheert de sessions.
Een session is een complete communicatie-actie tussen twee hosts. Dit houdt in:

- starten van de session,
- data uitwisseling en session control,
- stoppen van de session.

De informatie uitwisseling loopt via een stream met aan beide uiteinden een socket. Een socket bevat drie parameters; het IP-nummer, het protocoltype van de tranport layer en het poortnummer van de applicatie (10.16.1.1, TCP, 2067). Bij een stream horen dus twee socketrecords zodat de sessionsoftware kan herkennen voor welke stream de inkomende data bestemd is.
De sessionsoftware kan meerdere streams beheren waarvan de data, in de tijd gemultiplexed, over hetzelfde netwerkmedium kunnen worden verzonden.
Een session wordt gestart door een cliënt die in de meeste gevallen geen vast poortnummer heeft. De sessionsoftware kiest een poortnummer (boven 1024) om het socketrecord te maken. Het socketrecord

op het remote systeem is ook te maken omdat hiervoor een vast poortnummer gebruikt wordt, dat aangeeft met welke server-application (webserver gebruikt poort 80) de session moet worden gestart.
De cliënt heeft dus, na het openen van de sessie, beide sockets van de stream.
Het server-systeem haalt de socket-gegevens van de cliënt uit het ontvangen packet. Zijn eigen socket-gegevens zijn bekend. Na het openen van de sessie kent het server-systeem dus ook beide sockets van de stream tussen de client- en de server-applicatie. Als een packet op een van de systemen binnen komt wordt aan de hand van de socket-gegevens (beide) in het packet (IP-adres, protocol type en poortnummer) bepaald voor welke stream het packet bestemd is.



De session-software bepaalt ook hoe de dialoog tussen de beide uiteinden van een stream verloopt (**dialog control**). Mogen beide kanten op eigen initiatief data verzenden (full-duplex) of is er maar één zijde instaat om te zenden en moet de andere zijde wachten tot hij de zendmachtiging ontvangt (half-duplex)? Voor de laatste manier is protocol nodig om de zendrichting te sturen.
Dit is te vergelijken met een communicatie via een mobilofoon.
Bij een communicatie via een mobilofoon staan de systemen default op ontvangen. Als een gebruiker wil communiceren met een andere gebruiker dan drukt hij op zijn systeem de zendknop in en vraagt aan de andere gebruiker om zich te melden. Hij zet zijn systeem nu weer terug op ontvangen. De oproep kan nu beantwoord worden. De afspraak bij deze manier van communiceren is, dat de gebruiker die van zenden terug wil schakelen naar ontvangen dit doet door zijn zin te beëindigen met de kreet ‘OVER’. Dit is een sein voor de andere partij dat hij over kan schakelen van ontvangen naar zenden. Om het gesprek te beëindigen gebruikt men de kreet ‘OVER EN SLUITEN’.

Een andere functie van de sessionsoftware is om de dialoog in meerdere stukjes op te delen (**dialog separation**). Dit wordt vooral gedaan bij uitgebreide sessions om tussentijds te controleren of alle informatie tot dan toe goed verwerkt is. Er kan nu tussentijds besloten worden om een aantal stappen terug te gaan in de dialoog (**rolled back**) en vanaf dit punt de communicatie voort te zetten.
Dit is te vergelijken met de dialoog die je voert met een ‘flappentapper’. Wanneer je tijdens de dialoog opgeeft dat je een bedrag wil opnemen waarvoor het apparaat op dat moment niet de juiste bankbiljetten bezit dan zal hij dit melden en je vragen om opnieuw een bedrag in te geven (een stap terug in de dialoog).

Presentation layer (chapter 14)
In deze laag bevinden zich alle data-manipulatie functies.
De data (of een deel ervan) kunnen in een onleesbare vorm worden omgezet (**encryption**) die alleen door de ontvanger weer leesbaar gemaakt kan worden. Dit vindt plaats bij elektronisch betalingsverkeer en wanneer een username + password moet worden opgegeven (veiligheid).

In deze laag bevinden zich ook de **data-formating** functies. Hier worden de formaten herkend zoals; TIFF, JPEG, MPEG ed.
Een andere functie van deze laag is het **comprimeren/decomprimeren** van de data. Dit wordt gedaan om de data die getransporteerd moet worden tot een minimum te beperken.

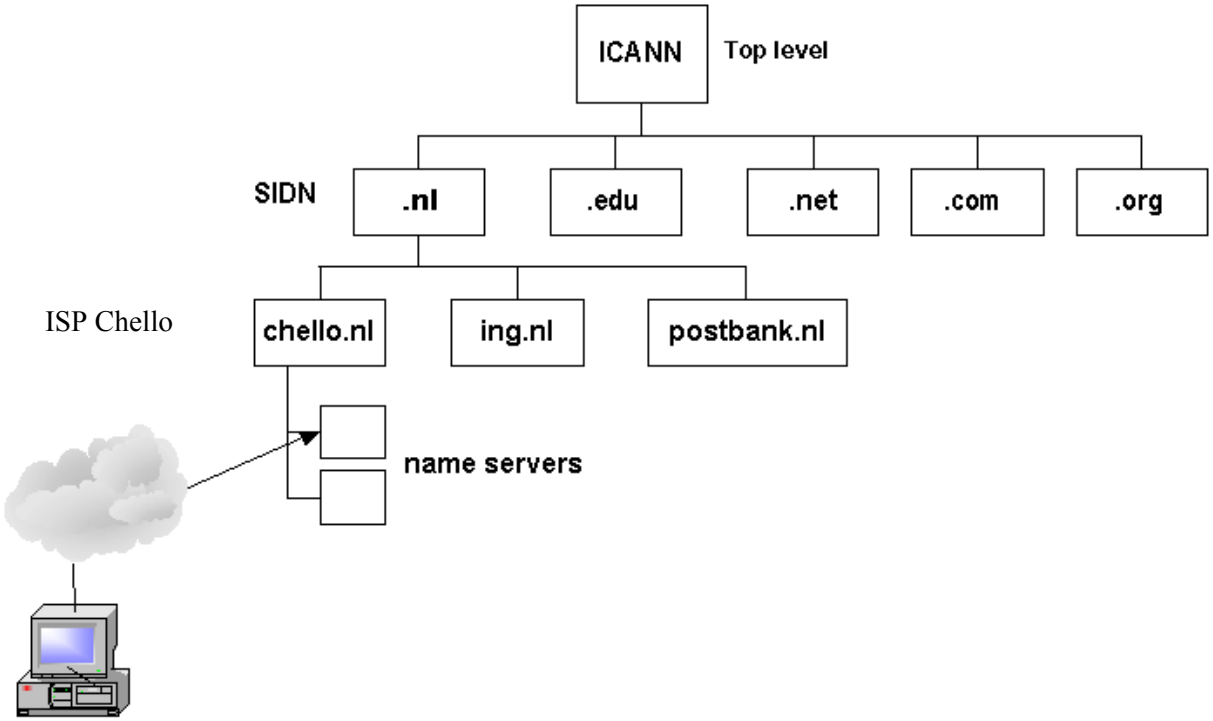
Application layer (chapter 15)
In deze laag zijn de koppelingen (**interfaces**) tussen de netwerk services en applicaties vastgelegd. Zo'n interface noemt men een **Application Programming Interface** (**API**). Veel problemen die bedrijven met Microsoft hebben gaan over deze APIs. Microsoft gebruikt naast algemene APIs een groot aantal APIs die veel beter (sneller) samenwerken met hun Windows systemen. Microsoft geeft deze echter niet vrij voor gebruik door derden.

Applicaties kunnen we verdelen in twee typen; **netwerkapplicaties** en **stand alone-applicaties**.
Netwerkapplicaties bestaan uit een cliënt- en serverdeel. Het cliëntdeel draait op een andere computer dan het serverdeel. Enkele bekende netwerkapplicaties zijn; Webbrowser, FTP, Telnet, E-mail en netwerkbeheerssoftware. We noemen netwerkapplicaties ook wel **direct network applications**.
Stand alone-applicaties draaien meestal op één systeem. Wanneer deze gebruik willen maken van centrale filesystemen, databases ed. dan wordt een **redirector** gebruikt om de locale applicatie te koppelen met een remote filesysteem of database. We noemen dit applicaties met **indirect network support**. Applicaties als officepakketten, tekenprogramma's en database-toepassingen maken hier gebruik van.
Bij een redirector dient de netwerkbeheerder de toegang te regelen tot de remote resources zoals het delen van file maps, printers, databases ed.

Een belangrijk punt om bij stil te staan is de manier waarop de cliënt en server communiceren. Een webbrowser (cliënt) zoekt contact met een webserver en vraagt om een html-file op te sturen. Als de file ontvangen is wordt de verbinding verbroken. Wanneer je nu naar een andere pagina wil, dan moet er eerst weer contact gemaakt worden.
Een Telnet- en FTP-session daaren tegen houden de verbinding open totdat er opdracht gegeven wordt om de session te beëindigen.
E.e.a is van belang bij het installeren van ISDN-routers om te voorkomen deze steeds de verbinding verbreekt en daarna opnieuw in moet bellen om weer verbinding te maken.

Hoe maakt de cliënt verbinding met de server?
We kunnen een cliënt verbinden met een server door het IP-adres, de computernaam of de DNS-naam op te geven. We kunnen echter van een gebruiker niet verwachten, dat deze IP-adressen kent. In intranetten en het Internet gebruikt men een **domain name system** (DNS) om de namen met de bijbehorende IP-adressen van de systemen te beheren. Dit zijn database-systemen die over een groot aantal name servers opgedeeld zijn.
Voor een intranet is de netwerkbeheerder verantwoordelijk voor deze database.
Voor het Internet is een aantal organisaties verantwoordelijk voor het DNS systeem. Aan het hoofd hiervan staat '**The Internet Corporation for Assigned Names and Numbers**' (**ICANN**)
http://www.icann.org
Deze organisatie beheert een aantal servers met een database met daarin gegevens over de beheerders van domain servers (.com, .edu, .org, .net, .nl enz) en de IP-adressen van deze servers. Als er een toplevel domain name toegevoegd moet worden dan kan alleen deze organisatie dat doen.
Voor het beheer van de locale domain namen (.nl, .uk, .de enz) bestaan er drie organisaties. Voor Europa is dat het **RIPE Network Coordination Centre** (**RIPE, Réseaux IP Européens**).
http://www.ripe.net
Voor Nederland heeft het RIPE het beheer overgedragen aan de **Stichting Internet Domeinregistratie Nederland** (**SIDN**). http://www.domain-registry.nl/sidn/flat/home/
Deze organisatie beheert de name servers waarin de subdomain namen zijn opgenomen met de provider die deze beheert en de IP-adressen van de name servers van deze providers.
De name servers gebruiken een **cache** om tijdelijk gegevens van andere name servers op te slaan.

Een Internet gebruiker is gekoppeld met de name server of de proxy server van zijn provider.



Als een webbrowser contact wil maken met www.postbank.nl, dan wordt aan de name server van zijn provider gevraagd of deze het IP-adres van de www server van de postbank kent. Als dit het geval is geeft deze het nummer door en kan de browser kontact maken. Als hij dit adres niet kent dan zoekt de name server naar het IP-adres van de SIDN (.nl) name server en vraagt aan hem het IP-adres van de postbank, hij slaat dit op in zijn cache en stuurt het door naar de gebruiker.
Als het nummer van .nl ook niet bekend is dan neemt de name server contact op met de name server van ICANN om het .nl IP-adres op te vragen en vraagt daarna aan de .nl server naar het IP-adres van de postbank.
Een DNS naam noemen we een Universal Resource Locator (URL). Toevoegingen achter de DNS naam verwijzen naar locaties en/of bestanden binnen de www server.
b.v.
http://cisco.netacad.net/
http://cisco.netacad.net/cnacs/prot-doc/index.shtml

Protocollen
De service software die de netwerkapplicaties ondersteunt, wordt protocol genoemd.

E-mail applicaties maken gebruik van het Simple Mail Transfer Protocol (SMTP) om mail te versturen naar een mail server. Dit is in eerste instantie de mail server van de provider. Deze mail server gebruikt DNS om het IP-adres van mail server te achterhalen waarvoor de mail bestemd is. Hij gebruikt ook SMTP om de mail te bezorgen. Dus mail servers onderling gebruiken SMTP. Als een gebruiker contact maakt met zijn mail server dan gebruikt zijn e-mail-applicatie het Post Office Protocol (POP3) om zijn post op te halen. Mail applicaties maken gebruik van een adres dat bestaat uit de naam en de DNS naam van een mail server gescheiden door het @ teken. Bijv. j.jansen@chello.nl
Het deel achter @ wordt gebruikt door het DNS en de naam voor @ is de naam van de postbus in de mail server van chello.nl. Naast het adres moet de brief ook een naam (subject) hebben. De naam geeft aan wat de inhoud van de brief is, zodat niet alleen de afzender met de datum en de tijd in de mailling-list te zien is.
Een webbrowser maakt gebruik van het Hypertext Tranfer Protocol (HTTP) om met de www-server te communiceren. Files met een Hypertext Markup Language (HTML)-formaat kunnen door de browser

verwerkt worden. In het HTML kunnen verwijzingen naar andere bestanden staan die door de server daarna verzonden worden. Het verzenden van de overige files kan tussentijds gestopt worden door bijvoorbeeld naar een andere pagina over te schakelen.
Over het maken van web pagina's en het beheren van webservers is veel te vertellen en te leren. Een groot aantal mensen heeft hier zijn beroep van gemaakt. Het is dus een vak op zich.

Het File Transfer Protocol (FTP) wordt gebruikt om bestanden te up- en downloaden. De FTP cliënt maakt contact met een FTP server en geef daarna de opdrachten en verbreek tenslotte de session.
Voor de commando's en de data worden door de FTP cliënt/server twee poortnummers gebruikt. Er zijn dus bij een FTP session twee streams actief. De data kan in ASCII of binaire vorm verzonden worden. Bij een FTP session moet een username en password opgegeven worden of er kan gekozen zijn voor alleen een password bestaande uit het e-mail-adres van de cliënt (anonymous).

Voor het beheer van netwerken wordt, zeker bij grote netwerken, gebruik gemaakt van beheers-software (bijv. OpenView van HP of Network Inspector van Fluke). Dit is een systeem met een console op een van de beheerssystemen en met agents in de netwerkapparatuur en computersystemen.
Deze communiceren onderling via het Simple Network Management Protocol (SNMP)

Vragen en opdrachten

1. Welke lagen van het OSI-model behoren tot de application-layers en welke tot de data transport-layers?

2. Welke lagen zijn dit bij het TCP/IP-model?

3. Hoe heet de logische verbinding tussen een client- en een server-applicatie en waaraan wordt deze verbinding herkent?

4. Wat is het verschil tussen een half- en een full-duplex dialoog?

5. Wat is het doel van dialog separation?

6. Geef een omschrijving en de reden van gebruik van; encrytion en compresion.

7. Noem een aantal data-formats uit de presentatielaag.

8. Wat is een API?

9. Geef het verschil aan tussen een netwerk- en een stand alone-applicatie.

10. Geef het verschil aan tussen een Web- en een FTP session.

11. Wat is de functie van DNS?

12. Waar bevinden zich de gegevens van het DNS systeem en door wie worden die beheerd?

13. Wat is de functie van de organisaties; ICANN, RIPE en SIDN?

14. Welke applicaties maken gebruik van de protocollen; HTTP, FTP, SMTP, POP3 en SNMP?

Aantekeningen