



Busleyden | Atheneum
Campus Zandpoort

CREËREN DENKEN DOEN **ONDERNEMEN** ZORGEN

Networking



N. Robyn – BA Campus Zandpoort

6 Information Technology

2019 - 2020

Inhoudsopgave

1	Inleiding: algemene begrippen	7
1.1	Het doel van computernetwerken.....	8
1.2	Schema van zenden en ontvangen	9
1.3	Telecommunicatienetwerken	12
1.3.1	Geografische spreiding	12
1.3.2	Schakeltechnieken	12
1.3.3	Datacommunicatietechnologieën.....	14
1.3.4	Hiërarchie tussen netwerkcomponenten	19
1.4	Datatransmissie	21
1.5	Transmissietypes.....	23
1.6	Transmissiesnelheden.....	25
2	Opbouw en werking van netwerken.....	27
2.1	Netwerktopologieën	28
2.1.1	Maasnetwerk	28
2.1.2	Ringnetwerk	28
2.1.3	Busnetwerk	29
2.1.4	Sternetwerk.....	30
2.1.5	Huidige situatie	30
2.2	Het OSI reference model.....	31
2.2.1	Communiceren in lagen	31
2.2.2	Het OSI reference model.....	31
2.3	Communicatieprotocollen	34
2.3.1	Toegangsprotocollen	35
2.3.2	Overdrachtsprotocollen	37
2.3.3	Toepassingsprotocollen	46
3	Netwerkhardware	50
3.1	Netwerkkarten	51
3.2	Transmissiemedia en connectoren.....	52
3.2.1	Kenmerken van netwerkbekabeling	52
3.2.2	Coaxiale kabel	53
3.2.3	Twisted pair.....	54
3.2.4	Glasvezelkabel.....	55
3.2.5	Powerline communicatie	57

3.2.6	WiFi	57
3.2.7	Alternatieve draadloze verbindingen	59
3.3	Netwerkverdeeldozen.....	61
3.3.1	Repeater en hub.....	61
3.3.2	Switch.....	62
3.3.3	Bridge	63
3.3.4	Router	64
3.3.5	(Wireless) Network Access Point	65
4	Servers.....	67
4.1	Client/server-verwerking	68
4.2	Serverhardware	72
4.3	Serverdiensten in een lokaal netwerk	73
4.3.1	DHCP-server	74
4.3.2	Domeincontroller.....	78
4.3.3	Fileserver (bestandsserver).....	79
4.3.4	Mailserver	80
4.3.5	Printserver.....	81
4.3.6	Application server (toepassingsserver).....	81
4.3.7	Webserver (informatieserver)	82
4.4	Netwerkbesturingssystemen	84

Voorbehouden voor inhoudsopgave

Voorbehouden voor inhoudsopgave

1 Inleiding: algemene begrippen

Waarin je leert dat het ene computernetwerk het andere niet is.

In dit hoofdstuk leer je dit:

- ◆ Het doel van computernetwerken
- ◆ Het schema van zenden en ontvangen
- ◆ De indeling van telecommunicatienetwerken op basis van geografische spreiding, schakeltechnieken, datacommunicatietechnologieën en hiërarchie tussen netwerkcomponenten.
- ◆ De verschillen tussen analoge, digitale en binaire datatransmissie.
- ◆ De verschillen tussen modulatie technieken: amplitudemodulatie, frequentiemodulatie en fasemodulatie.
- ◆ Het verschil tussen parallelle en seriële gegevensoverdracht.
- ◆ De manier om transmissiesnelheden uit te drukken.

1.1 Het doel van computernetwerken

Gemeenschappelijk gebruik van gegevens

Vanop een computer in een netwerk kunnen gegevens beschikbaar worden gesteld voor andere computers. Omdat die gegevens centraal bewaard worden, werken alle gebruikers steeds met de meest recente gegevens en bestaan er geen conflicten met verschillende versies van bijvoorbeeld een centraal gegevensbestand.

Gemeenschappelijk gebruik van apparatuur

Scanners, printers en andere randapparaten kunnen door meerdere computers in een netwerk gebruikt worden.

Gemeenschappelijk gebruik van software

Programma's kunnen beschikbaar gemaakt worden op een server. Andere computers op het netwerk kunnen van deze programma's gebruik maken zonder ze lokaal moeten geïnstalleerd zijn. Op deze manier kan bespaard worden op schijfruimte en verwerkingscapaciteit van werkstations maar het veronderstelt wel een voldoende krachtige server.

Eenvoudig systeembeheer

Via een netwerk is het makkelijker om als systeembeheerder de software op computers up-to-date te houden, om back-ups te maken, enz. Door een efficiënte planning kan een systeembeheerder veel tijd besparen.

Beveiliging

Via een netwerk kan een systeembeheerder gegevens centraal beveiligen, toegangen aanmaken en gebruikersrechten bepalen voor de gebruikers van het netwerk. Ook de beveiliging tegen virussen en hackers is makkelijker in een netwerk dan in computers die elk apart op het internet zijn aangesloten.

Elektronische communicatie

Via een netwerk kunnen gebruikers elektronisch communiceren, of dat nu via e-mail is, al chattend of via voice-over-IP (netwerktelefonie).

Gemeenschappelijk gebruik van een internettoegang

Via een netwerk kan een internettoegang worden gedeeld voor meerdere computers op het netwerk.

Financiële besparing

Met behulp van een computernetwerk kan een bedrijf veel efficiënter werken. Bovendien kunnen ICT-middelen efficiënter worden beheerd. Dat levert een besparing op die al snel heel wat groter is dan de investeringskost in een computernetwerk.

Rekenkracht verhogen

In sommige omgevingen, zoals universiteiten en andere onderzoekscentra, kunnen computers via een netwerk hun rekencapaciteit bundelen voor rekentaken die te complex zijn voor een enkel computersysteem.

1.2 Schema van zenden en ontvangen

Alle communicatie verloopt steeds volgens dit schema:



Als A en B mensen zijn, dan is het **communicatiekanaal** de *gemeenschappelijke taal*. Als A een computer is en B is een printer, dan is het communicatiekanaal een printerkabel.

Vaak staan er tussen A en B hindernissen in de weg die rechtstreekse communicatie onmogelijk maken. Een hulpmiddel dat deze hindernissen opheft, wordt een **medium** genoemd. Zo kunnen mensen die zich niet in elkaars buurt bevinden geen gesprek voeren. Maar met een telefoon wordt dat wel mogelijk. In dat geval is de telefoon het medium. Op dezelfde manier hebben computers een netwerkkaart nodig als medium voor onderlinge communicatie. Het communicatieschema ziet er dan zo uit:



De communicatie tussen A en B op het communicatiekanaal kan verlopen in verschillende richtingen en al dan niet tegelijkertijd. We onderscheiden de volgende drie mogelijkheden:



Wanneer er slechts communicatie mogelijk is in één richting, spreken we van een **simplex** communicatie. Een voorbeeld van simplex communicatie zijn radio- of televisie-uitzendingen.



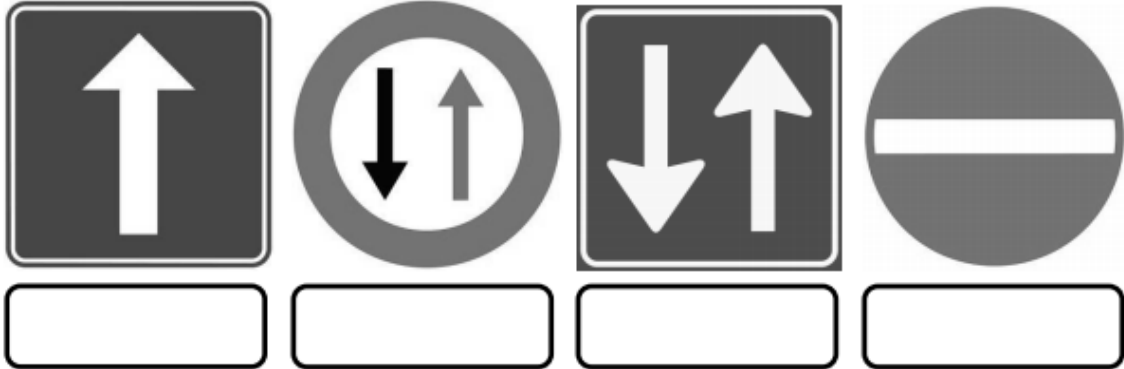
Soms is communicatie mogelijk in twee richtingen, maar niet tegelijkertijd. Dat noemen we **half-duplex** communicatie en dat is bijvoorbeeld het geval bij het communiceren via walkietalkies.



Meestal kan er tegelijk in beide richtingen gecommuniceerd worden. Dat heet dan **duplex** communicatie. Telefoneren of chatten zijn vaak gebruikte vormen van duplex communicatie.

OPDRACHT

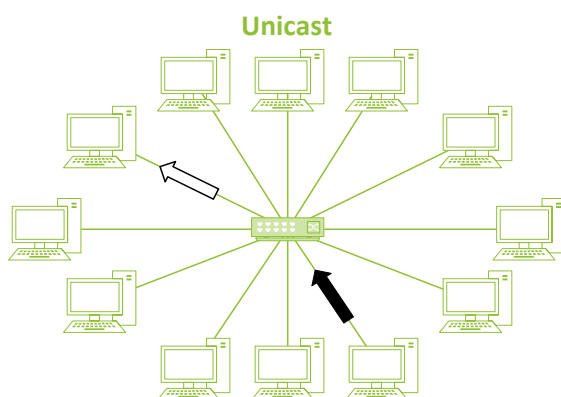
Vergelijk communicatiemethodes met situaties in het verkeer. Noteer onder elk verkeersbord de juiste term: simplex, half-duplex, duplex:



Randapparaten communiceren met de computer. Noteer welke vorm van communicatie er bestaat voor de volgende randapparaten: simplex, half-duplex of duplex?

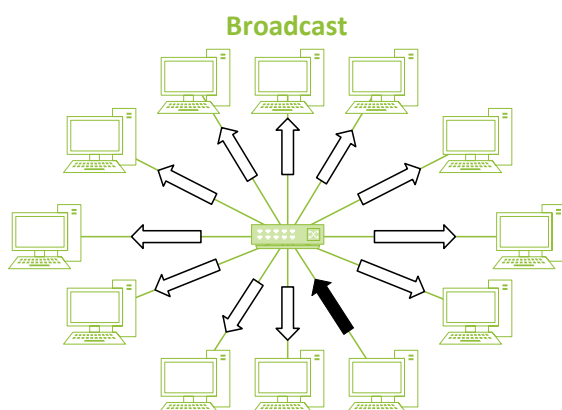
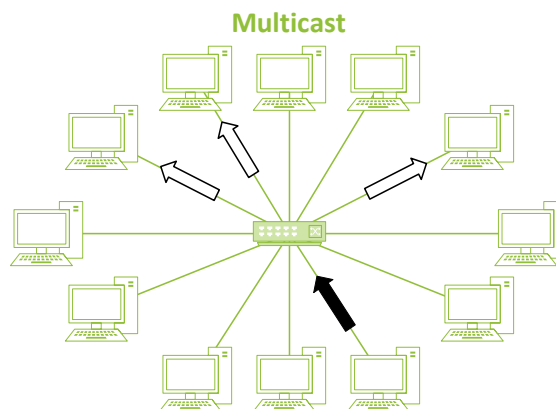


Wanneer een bericht wordt verzonden in een netwerk kan het zijn dat er één of meerdere ontvangers zijn. De verschillende manieren hoe een bericht wordt verzonden kunnen we als volgt omschrijven:



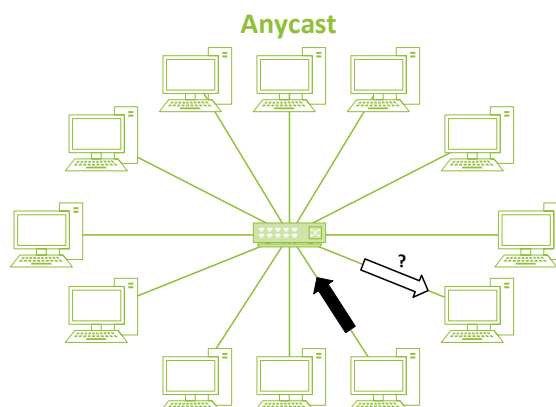
Een bericht wordt verzonden van een computer in een netwerk naar een andere, specifieke computer.

Een bericht wordt verzonden van een computer in een netwerk naar verschillende andere, specifieke computers tegelijk.



Een bericht wordt verzonden van een computer in een netwerk naar alle andere computers tegelijk.

Een bericht wordt verzonden van een computer in een netwerk naar de gemakkelijkst te bereiken computer met een bepaalde functie.



OPDRACHT

Zoek wel op van welke communicatietechniek ze gebruik maken en leg de juiste verbinding met de rechterkolom.

ARP-request
DHCP-request
DNS-request
Afdrukopdracht naar een netwerkprinter

Unicast
Multicast
Broadcast
Anycast

1.3 Telecommunicatienetwerken

Computernetnetwerken kunnen op verschillende manieren ingedeeld worden:

- ♦ op basis van geografische spreiding
- ♦ op basis van de gebruikte schakeltechniek
- ♦ op basis van de gebruikte datacommunicatietechnologie
- ♦ op basis van de hiërarchie tussen de gebruikte netwerkcomponenten

1.3.1 Geografische spreiding

Een computernetwerk dat zich beperkt tot een klein geografisch gebied wordt een **LAN** (*local area network*) genoemd. Veruit de meeste computernetwerken zijn van dit type: je thuisnetwerk, het netwerk op je school of het netwerk op de campus van een bedrijf, een ziekenhuis, enz.

Een computernetwerk dat zich uitstrekt over een groot geografisch gebied wordt een **WAN** (*wide area network*) genoemd. Het bekendste WAN is het internet, maar ook een bedrijfsnetwerk dat verschillende vestigingen over een grote afstand met elkaar verbindt, kan een WAN genoemd worden.

Tot voor een aantal jaren bestond er nog een tussenweg tussen een LAN en een WAN. Een **MAN** (*metropolitan area network*) was een netwerk dat zich uitstreckte over het grondgebied van een stad. Dit begrip dateert nog uit de tijd dat sommige grote steden hun inwoners via een eigen netwerk diensten wilden aanbieden. Met de doorbraak van het internet werd het MAN overbodig en verdween.

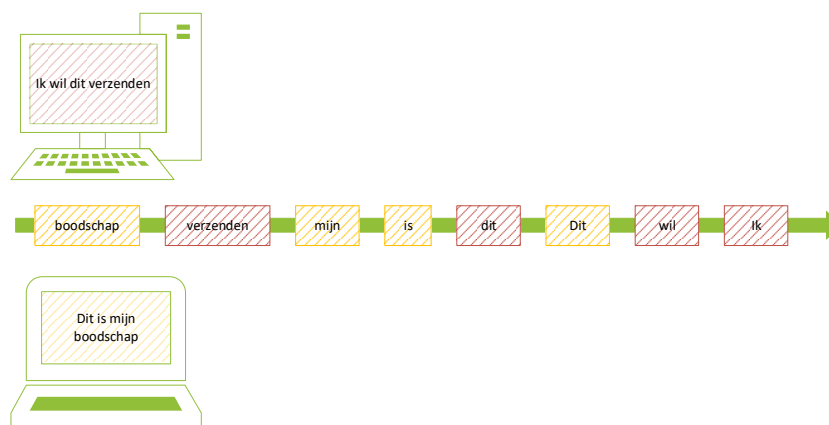
1.3.2 Schakeltechnieken

Digitale informatie die via computernetwerken worden doorgestuurd, wordt opgedeeld in **pakketjes**. De manier waarop die pakketjes over datacommunicatielijnen worden doorgegeven, heet **switching**. Daarvoor bestaan verschillende technieken:

a) Packet switching

Wanneer een computer alle pakketjes in één onafgebroken stroom zou verzenden over het netwerk, wordt het netwerk tijdelijk onbeschikbaar voor de andere computers. Die moeten dan wachten tot die ene computer klaar is met het verzenden.

Packet switching maakt het mogelijk dat de pakketjes van verschillende computers door elkaar heen kunnen worden verstuurd over hetzelfde netwerk. Gezien elk pakketje voorzien is van een tag, waarin onder meer het adres van de ontvanger zit, komen alle pakketjes bij de juiste ontvanger aan.



Over een groter netwerk hoeven alle pakketjes die verstuurd worden tussen twee computers niet noodzakelijk eenzelfde route te volgen over het netwerk. Sterker nog: ze hoeven niet eens in dezelfde volgorde aan te komen als ze verstuurd zijn. Software zorgt ervoor dat de pakketjes correct worden opgesplitst en weer samengesteld. Bij oudere netwerken moesten de pakketten allemaal exact even groot zijn. Men sprak dan van **cell-switching**. Moderne packet switching netwerken laten een variabele pakketgrootte toe.

De techniek om het verzenden van verschillende pakketten over eenzelfde datacommunicatielijn mogelijk te maken wordt **multiplexing** genoemd:

- ◆ **FDM (Frequency Division Multiplexing)**

De verschillende verbindingen gebruiken verschillende frequenties die ver genoeg uit elkaar liggen om elkaar niet te storen.

- ◆ **STDM (Synchronous Time Division Multiplexing)**

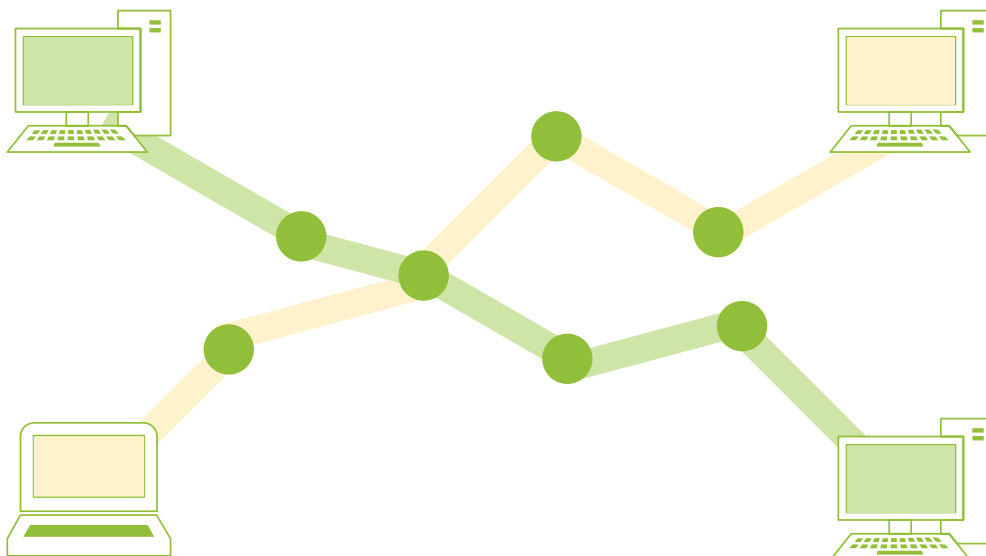
De verschillende verbindingen wisselen elkaar af op een vast tijdsinterval.

- ◆ **ATDM (Asynchronous Time Division Multiplexing)**

De verschillende verbindingen wisselen elkaar af, maar op een variabel tijdsinterval. Zo kan er een langere tijd toebedeeld worden aan een verbinding waarbij meer gegevens moeten doorgestuurd worden dan bij een andere verbinding.

b) Circuit switching

Dit is het tegenovergestelde van packet switching. De zender opent een speciaal toegewezen communicatiekanaal met de ontvanger voor er gegevens verzonden worden. Wel kunnen verschillende communicatielijnen gebruik maken van dezelfde knooppunten op een netwerk. De verbinding tussen zender en ontvanger blijft open, ook als er even geen informatie wordt verstuurd, tot een signaal wordt gegeven om de verbinding af te sluiten.



Deze techniek is vooral geschikt voor interactieve communicatie die niet onderbroken mag worden, zoals bij telefoonverbindingen. Voorwaarde is wel dat de snelheid van het zenden en ontvangen op elkaar afgestemd is.

c) Message switching

Bij message switching wordt een bericht wel opgedeeld in pakketjes, maar die worden als één bericht aangezien en in één geheel verzonden. Doorgaans verloopt de verzending niet rechtstreeks: het bericht wordt eerst van de zender naar een knooppunt gestuurd, waar het tijdelijk wordt opgeslagen (**gebufferd**). Pas nadat het volledig bericht ontvangen werd, wordt het doorgestuurd naar het volgende knooppunt, waar het eveneens gebufferd wordt alvorens het weer door te sturen. Bij elk knooppunt kan een controle gebeuren om na te gaan of er onderweg geen pakketjes van het bericht verloren gegaan zijn. Dit gaat zo verder tot de informatie bij de ontvanger terecht komt. Die manier van verzenden van informatie wordt ook wel **store-and-forwarding** genoemd.

Het voordeel is dat dezelfde informatie op die manier naar verschillende ontvangers kan gestuurd worden, maar het nadeel is dat interactieve communicatie niet mogelijk is omdat de vertragingstijd tussen verzenden en ontvangen te groot is.

Deze manier van werken wordt tegenwoordig niet meer op fysiek niveau toegepast. Op applicatieniveau werkt het versturen en ontvangen van e-mail wel op deze manier.

OPDRACHT

Zoek op welke manier de communicatie op deze netwerken verloopt en verbind ze met de juiste schakeltechniek.

telefoonnetwerk

internet

ISDN

ATM-netwerk

WiFi-netwerk

packet-switching

cell-switching

circuit-switching

message-switching

1.3.3 Datacommunicatietechnologieën

Er zijn verschillende datacommunicatietechnologieën doorheen de geschiedenis tot stand gekomen. We beschrijven hieronder de voornaamste technieken om een verbinding te maken van een computersysteem of een lokaal netwerk met een WAN. Technologieën om computers in lokale netwerken te verbinden worden besproken in hoofdstuk 3.2.

a) Het telefoonnetwerk

Het telefoonnetwerk bestaat uit telefooncentrales, telefoontoestellen en de bekabeling. De telefooncentrale zorgt voor het starten en verbreken van verbindingen tussen twee abonnees. Wanneer die abonnees op verschillende centrales zijn aangesloten, bestaat de totale verbinding uit een keten van centrales die met elkaar verbonden worden. De centrales zorgen er ook voor dat de opgebouwde verbindingen in stand worden gehouden zolang de abonnees die wensen en registreren de aard en de duur van de verbindingen. Dat is belangrijk om achteraf de kosten van de verbinding aan de gebruikers te kunnen aanrekenen.

Het telefoonnetwerk was oorspronkelijk ontwikkeld als een analoog netwerk. De akoestische spraaksignalen worden door de microfoon in het telefoontoestel omgezet in een elektrisch signaal. Aan de ontvangerskant wordt dat elektrisch signaal door de luidspreken weer omgezet in een akoestisch signaal. Digitale communicatie via een klassieke telefoonlijn veronderstelt dus dat digitale gegevens eerst moeten worden omgezet naar analoge gegevens en bij de ontvanger opnieuw moeten worden omgezet naar digitale gegevens. Dit proces wordt **moduleren** en **demoduleren** genoemd en wordt uitgevoerd door een modem.

Abonnees kunnen kiezen tussen geschakelde of kieslijnen (*dial-up lines*) en gehuurde lijnen (*leased lines*). De eerste soort is interessant voor wie slechts af en toe gebruik maakt van een telefoonnetwerk, zoals thuisgebruikers. Grote bedrijven die intensief gebruik maken van de telefoon kiezen beter voor een gehuurde lijn.

De frequentie op een telefoonlijn is beperkt (tussen 300 en 3400 Hz), waardoor de gegevensoverdracht erg traag loopt. Datacommunicatie via een klassieke telefoonlijn is bovendien niet erg betrouwbaar: storingen op de telefoonlijn komen vaak voor en zorgen er regelmatig voor dat verbindingen plots uitvallen. Het klassieke telefoonnet wordt vaak aangeduid met de afkorting **PSTN** (*public switched telephone network*), of wat meer spottend **POTS** (*plain old telephone system*).

b) Het ISDN-netwerk:

ISDN (integrated services digital network) was een uitbreiding op het bestaande telefoonnet. Hier wordt het signaal – zowel spraak als data – in digitale vorm verstuurd in plaats van analoog. De telefooncentrales werden daarvoor speciaal aangepast in de jaren 1980 en 1990.

Met ISDN gaat de gegevensoverdracht een stuk sneller dan via een klassieke telefoonlijn. Bovendien is de verbinding stabiel: ze valt dus minder makkelijk weg. ISDN maakte ook nieuwe diensten op het telefoonnetwerk mogelijk:

- ◆ **Conference call:** bellen met meer dan één persoon tegelijk.
- ◆ **Tweede beller-signaal:** een waarschuwing wanneer je tijdens een gesprek wordt opgebeld.
- ◆ **Caller identification:** het bekend maken van het nummer en de naam van de correspondent.
- ◆ **Hogere bandbreedte:** doorgaans het dubbele van een gewone telefoonverbinding.

ISDN-verbindingen waren geen erg lang leven beschoren omdat met ADSL de mogelijkheden nog veel groter werden.

OPDRACHT

ISDN bestaat in verschillende vormen. Verklaar het verschil tussen bijvoorbeeld 2B + D en 30B + D.

.....

.....

.....

.....

.....

c) Het ADSL-netwerk

ADSL (*asymmetric digital subscriber line*) is een technologie die door middel van een **splitter** je analoge telefoonlijn in twee opsplitst: de lage frequenties dienen voor spraak, de hoge voor datacommunicatie. De bandbreedte is veel hoger dan bij klassieke telefoonlijnen of ISDN-lijnen en de verbinding is stabiel, op voorwaarde dat de aansluiting zich niet verder dan 5km van de telefooncentrale of een **repeater** bevindt. De snelheid van de verbinding is niet afhankelijk van het aantal actieve gebruikers, wel van de afstand tussen de gebruiker en de centrale.

ADSL-verbindingen worden asymmetrisch genoemd omdat de bandbreedte in de twee richtingen van de verbinding niet dezelfde is: **downstream** (van het netwerk naar de gebruiker) is de bandbreedte beduidend groter dan **upstream** (van de gebruiker naar het netwerk). Oorspronkelijk was het een technologie om bedrijven een snelle, permanente toegang tot het internet te verschaffen. Tegenwoordig kunnen ook particuliere gebruikers zich een ADSL-internetabonnement aanschaffen.

Verwante netwerktechnologieën zijn **SDSL** (*symmetric digital subscriber line*), **HDSL** (*high bit rate digital subscriber line*) en **VDSL** (*very high bit rate digital subscriber line*).

OPDRACHT

Wat is het wezenlijke verschil tussen ADSL en SDSL?

.....

.....

.....

.....

.....

d) Het glasvezelnetwerk

In Vlaanderen en Nederland ligt een glasvezelnetwerk voor TV- en radiodistributie langs de meeste bewoonde wegen. De volledige bandbreedte van dit netwerk wordt hiervoor echter niet gebruikt. Met een speciale **splitter** is het mogelijk om ook datacommunicatie te laten verlopen via dit glasvezelnetwerk. In Vlaanderen was Telenet vroeger het enige bedrijf dat een internettoegang via glasvezel mogelijk maakt, ondertussen zijn meerdere aanbieders actief. In bedrijven wordt glasvezeltechniek gebruikt om afstanden tussen bedrijfsgebouwen in een bedrijfsnetwerk te overbruggen.

Het grote verschil met telefoon-, ISDN- en ADSL-netwerken is de manier waarop de signalen overgedragen worden. Dat gebeurt niet met elektrische maar met optische signalen. Hoe dat precies in z'n werk gaat, leer je in hoofdstuk 3.2. Bovendien is de overdrachtssnelheid niet afhankelijk van de afstand tot de centrale maar wel van het aantal actieve gebruikers.

e) Het GPRS-netwerk

GPRS (*general packet radio service*) is een techniek die een uitbreiding vormt op het bestaande gsm-netwerk. Met deze technologie kan digitale informatie verzonden en ontvangen worden.

Bij GPRS betalen gebruikers niet voor de tijd dat ze aangemeld zijn, maar voor de hoeveelheid gegevens die ze downloaden of versturen. Technisch gezien houdt de gebruiker de verbinding ook alleen maar bezet op momenten dat er daadwerkelijk gebruik van wordt gemaakt. Daardoor wordt de capaciteit van het netwerk optimaal benut en kan de beschikbare bandbreedte al naar gelang de behoefte over de actieve gebruikers gedeeld worden. De afstand tot een gsm mast is een erg belangrijke factor voor de kwaliteit van het signaal.

Hoewel GPRS specifiek voor mobiele telefoons bedoeld was, bestaan er GPRS-adapters voor laptops. De bandbreedte van GPRS blijkt in de praktijk vrij laag om vlot op het internet te surfen.

f) 3G en 4G

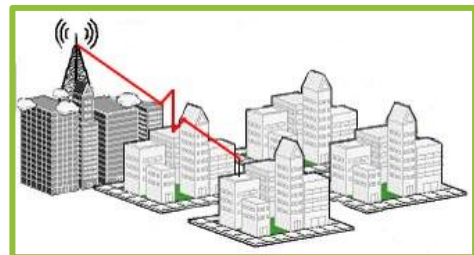
UMTS (*universal mobile telecommunication system*) wordt ook de derde generatie (3G) mobiele communicatie genoemd. UMTS biedt een grotere verbindingssnelheid tegenover andere mobiele systemen, die wel aanvaardbaar is voor het klassieke surfen zolang je niet teveel multimedia-geweld verwacht.

HSDPA (*high-speed downlink packet access*) is een doorontwikkeling met een transmissiesnelheid van 5 tot 10 keer de UMTS-snelheid. Daarmee is het wel mogelijk om vlot mobiel te surfen, hoewel de maximale snelheid van HSDPA de maximale snelheid van een glasvezel- of een ADSL-verbinding nog niet benadert. Net zoals bij GPRS bestaan er adapters om ook laptops toe te laten op dit draadloos netwerk.

De meest recente ontwikkeling op dit gebied wordt HSDPA+ genoemd, maar kennen we beter onder de verzamelnaam **4G** of **LTE** (*long term evolution*). Deze technologie laat mobiel surfen toe aan dezelfde snelheden als bekabeld breedband internet. In stedelijke gebieden waren 4G-toegangen het eerst beschikbaar. De technologie vereist immers relatief veel zendmasten om het netwerk volledig dekkend te maken en in landelijke gebieden is het aantal gebruikers voorlopig te laag om de investeringen voor de providers te verantwoorden.

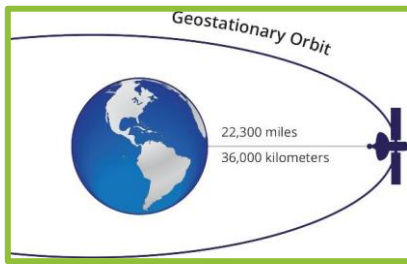
g) Straalverbindingen

Voor straalverbindingen worden paraboolvormige schotelantennes gebruikt, die elkaar moeten kunnen zien om contact te maken. Hindernissen zoals gebouwen, beplanting of heuvels tussen de antennes maken de communicatie onmogelijk. Ook zware mist of hevige sneeuwval vormen een probleem.



Meestal wordt deze techniek gebruikt voor het verbinden van computernetwerken in verschillende gebouwen, waar het leggen van kabel te moeilijk is (bijvoorbeeld twee filialen van eenzelfde bedrijf in een stad). Om een straalverbinding te installeren heeft men in België wel de toelating nodig van het **BIPT** (*Belgisch Instituut voor Post en Telecommunicatie*). In Nederland is dat het Agentschap Telecom.

h) Satellietverbindingen



Voor dataverbindingen over zeer lange afstand (zelfs intercontinentaal) kunnen satellietverbindingen worden gebruikt. Satellieten bevinden zich op ongeveer 36.000 km boven de aarde in een **geostationaire** baan, waardoor zo'n satelliet een vaste plaats heeft ten opzichte van de aarde. Satellietverbindingen worden gebruikt voor zowel datacommunicatie als voor telefoonverbindingen of het

doorsturen van radio- en televisiesignalen. Ook **GPS** (*Global Positioning System*) maakt gebruik van satellietverbindingen.

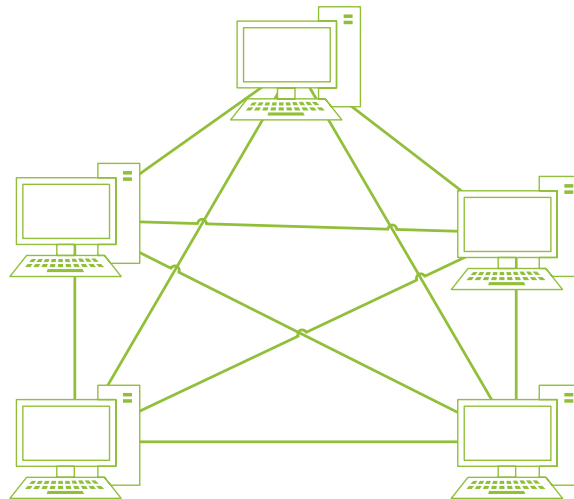
Wie internettoegang wil via satelliet dient een schotelantenne te installeren die zo precies mogelijk naar de satelliet gericht staat. Nadeel van internetten via satelliet zijn de vertragingen omwille van de grote afstand. Vooral voor realtime toepassingen (zoals internettelefonie of gamen via het internet) is een satellietverbinding dus minder geschikt. Belangrijke voordelen zijn de permanente beschikbaarheid van het satellietnetwerk op de meest afgelegen plaatsen en tijdens periodes van overbelasting van de klassieke communicatienetwerken, zoals bijvoorbeeld bij rampen. Bovendien maken satellieten ook internetverbindingen mogelijk in lijnvliegtuigen. Sommige vliegtuigmaatschappijen bieden dit reeds aan.

1.3.4 Hiërarchie tussen netwerkcomponenten

De verschillende netwerkcomponenten in een netwerk kunnen op twee manieren opgezet worden: een peer-to-peer netwerk en een servergestuurd netwerk. Peer-to-peernetwerken worden zelden toegepast in professionele omgevingen. Ze zijn hooguit geschikt voor kleine thuisnetwerkjes waar slechts enkele computers actief zijn. In professionele omgevingen zal altijd gebruik gemaakt worden van een servergestuurd netwerk.

a) Peer-to-peer netwerk

In een peer-to-peer netwerk (in het Nederlands sporadisch een evenknie-netwerk genoemd) nemen alle computers een evenwaardige plaats in tegenover elkaar. De werkstations communiceren rechtstreeks met elkaar zonder tussenkomst van een server. In een dergelijk netwerk vervult elke computer een deel van de netwerktaken. Zo kan eender welk workstation diensten aanbieden aan andere computers in het netwerk, zoals het toegang geven tot een gedeelde printer of opslagcapaciteit delen. We spreken hier van een **gedecentraliseerd** netwerktype.



De voordelen:

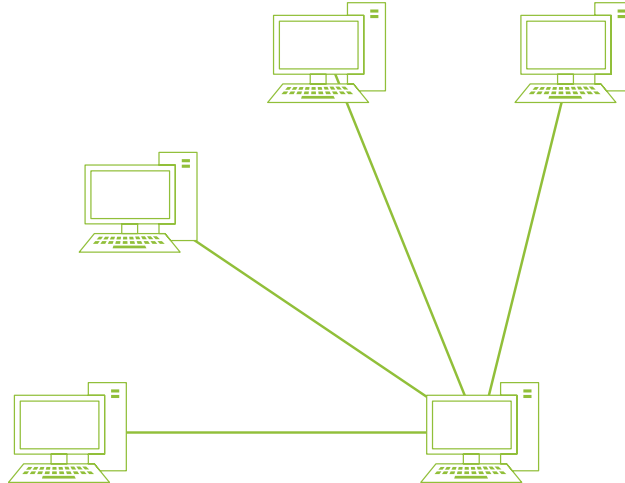
- ☑ Relatief goedkoop, want geen dure netwerkapparatuur nodig.
- ☑ Wanneer één computer uitvalt, blijft het netwerk operationeel.
- ☑ Eenvoudig te realiseren

De nadelen:

- ☒ Moeilijker te onderhouden.
- ☒ Beveiliging moet op elke computer apart worden ingesteld.
- ☒ Consistentie van gegevens is moeilijker te waarborgen.
- ☒ Doorgaans minder stabiel.
- ☒ Enkel geschikt voor zeer kleine netwerkjes.

b) Servergestuurd netwerk

In een servergestuurd netwerk is er een duidelijke hiërarchie tussen werkstations en servers. Een krachtige computer, die server wordt genoemd, beheert hier het hele netwerk. Alle communicatie tussen de werkstations vindt steeds plaats via die server. Die dient daarvoor te beschikken over een netwerkbesturingssysteem. Dit soort netwerken maken een centraal netwerkbeheer en een centrale beveiliging een stuk makkelijker dan in een peer-to-peer netwerk. We spreken hier van een **gecentraliseerd** netwerktype.



De voordelen:

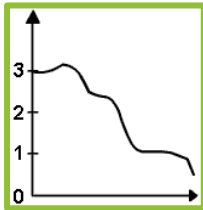
- ☒ Onderhoud kan centraal gebeuren.
- ☒ Netwerkdiensten zijn makkelijker op te zetten en te controleren.
- ☒ Consistentie van gegevens is makkelijker te waarborgen.
- ☒ Geschikt voor zowel grote als kleine netwerken.

De nadelen:

- ☒ Relatief duur.
- ☒ Onderhoud vergt meer specifieke kennis van netwerken.
- ☒ Als de server uitvalt, is het ganse netwerk onbeschikbaar.

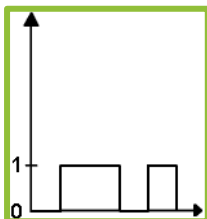
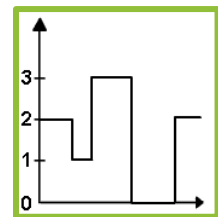
1.4 Datatransmissie

Datatransmissie, het verzenden en ontvangen van informatie over een communicatiekanaal, bestaat uit analoge, digitale of binaire signalen.



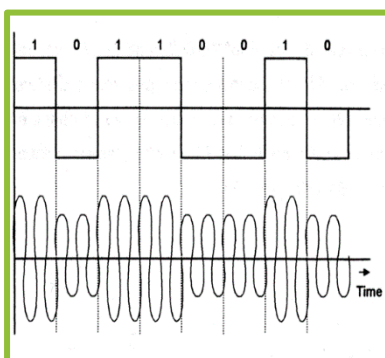
Een **analoog** signaal kan oneindig veel waarden tussen het minimum en maximum signaal aannemen. Het vormt een continu signaal dat erg in sterkte kan wisselen. Geluid plant zich op deze manier voort in de lucht. Toonhoogte en geluidsterkte kunnen traploos wisselen. Ook over klassieke telefoonlijnen worden signalen analoog overgedragen.

Een **digitaal** signaal kent een beperkt aantal mogelijke waarden tussen het minimum en maximaal signaal. Zo'n signaal kent een getrapt verloop. Hoe minder trapper er zijn, hoe minder zo'n signaal onderhevig is aan de invloeden van vervorming en verzwakking tijdens het verzenden ervan. De reconstructie van een digitaal signaal is dan ook betrekkelijk eenvoudig.



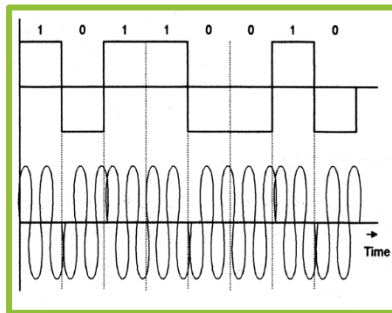
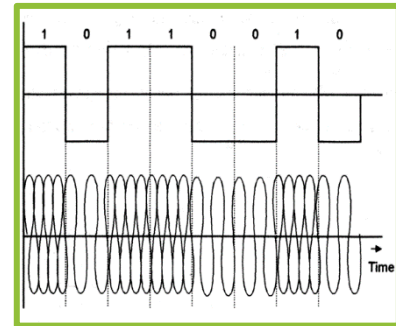
De meeste digitale signalen kennen slechts twee niveaus: 1 en 0. Die worden dan **binaire** signalen genoemd. Ze zijn de signalen bij uitstek waarmee computers kunnen communiceren.

Het omzetten van digitale signalen naar analoge signalen wordt **moduleren** genoemd; het omgekeerde heet **demoduleren**. Zo kan een analoog telefoonsignaal omgezet worden in een digitaal signaal van maximum 64000 bits. Voor het moduleren en demoduleren van signalen wordt gebruik gemaakt van een modem - de naam van het toestel is trouwens van de begrippen **moduleren** en **demoduleren** afgeleid.



Amplitudemodulatie is een van de oudste modulatie technieken en is gekend van de zogenaamde lange golf radio-uitzendingen. Daarbij levert een grote amplitude een 1 op, en een kleine amplitude een 0. Ze levert een grote vervorming van het signaal op en is weinig geschikt voor datatransmissie.

Frequentiemodulatie is een meer populaire modulatietechniek, die gebruikt wordt voor gewone radio-uitzendingen op de FM-band. Ze levert relatief weinig vervorming van het signaal op, maar heeft dan weer het nadeel dat de overbrugbare afstand voor radio-uitzendingen beperkt is. Deze modulatietechniek is ook niet geschikt voor datacommunicatie.



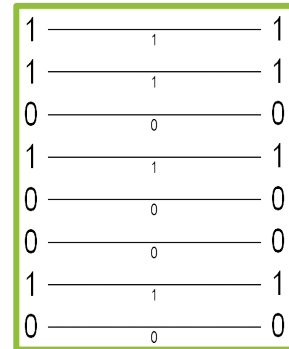
Bij **fasemodulatie** wordt gekeken naar de oriëntatie van elke fase – dat is een volledige analoge golf. Begint de fase opwaarts, dan wordt een 1 gegenereerd. Een fase die neerwaarts start krijgt de waarde 0. Het grote voordeel van deze manier van moduleren is dat ze minder problemen oplevert bij een eventueel vervorming van het signaal. Bovendien laat ze geen twijfel toe tussen een 1 en een 0. Daarom is dit de meest geschikte modulatietechniek voor datatransmissie.

1.5 Transmissietypes

Als gegevens over een transmissiemedium getransporteerd worden, kan dat bit na bit, ofwel met een aantal bits tegelijk. Worden ze één na één verzonden, dan spreken we van **seriële** gegevensoverdracht, worden ze met een aantal bits gelijktijdig verzonden, dan spreken we van **parallele** gegevensoverdracht.

a) Parallele gegevensoverdracht

Een te verzenden bitreeks van een aantal bits wordt een **block** genoemd. Bij parallele gegevensoverdracht worden de bits aan de zenderkant van de communicatielijn klaargezet. De zender verstuurt nu een **request**-signaal (**REQ**) naar de ontvanger, om aan te geven dat de bits klaar staan om verzonden te worden. De ontvanger zal een **acknowledge**-signaal (**ACK**) terugsturen om aan te geven dat de gegevens binnengekomen zijn en dat de ontvanger klaar is om een volgend block te ontvangen. Deze werkwijze wordt het **handshake-mechanisme** genoemd.



Voor parallele gegevensoverdracht heb je in de kabel voor elke tegelijk te versturen bit een draad nodig. Bovendien zijn er nog enkele bijkomende draden nodig voor de besturingssignalen REQ en ACK.

b) Seriële gegevensoverdracht

Hier worden de bits één na één verzonden over één enkele lijn. Parallele signalen van bijvoorbeeld het bus systeem op het moederbord moeten daarvoor omgezet worden naar een serieel signaal. Die omzetting gebeurt door de **DCC** (*data communications controller*), een chip die zich op het moederbord bevindt.

De ontvanger moet weten waar een teken begint en waar het eindigt. Daarom wordt er aan elk gegeven een afzonderlijk kop- en staartinformatie (de **start- en stopbit**) toegevoegd. Bovendien wordt nog een **pariteitsbit** meegestuurd waardoor kan nagegaan worden of het karakter correct werd ontvangen. De zender moet aan de ontvanger vooral wel duidelijk maken hoeveel bits één teken precies telt, anders weet de ontvanger niet welke de start- en stopbits zijn. Ook de snelheid van de gegevensoverdracht moet op elkaar worden afgestemd. Als de zender de gegevens bijvoorbeeld aan 1200 bps zou verzenden maar de ontvanger zou ze slechts aan 300 bps ontvangen, dan gaat drie vierde van de informatie verloren. Deze werkwijze wordt **asynchrone seriële gegevensoverdracht** genoemd.

Bij **synchrone gegevensoverdracht** worden gegevens in grotere blocks verstuurd. Nu hoeven niet de afzonderlijke tekens de kop- en staartinformatie te krijgen, maar wel het block in z'n geheel. De zender stuurt met de informatie een kloksignaal door, waarmee de communicatie gesynchroniseerd wordt. De kans op foute gegevensoverdracht is veel kleiner dan bij asynchrone communicatie en daarom wordt deze manier van gegevensoverdracht gebruikt in computernetwerken.

Tussen zender en ontvanger moet een afspraak worden gemaakt op welke manier de ontvanger kan weten dat het verzenden van de informatie beëindigd is. Daarvoor bestaan drie methoden:

Time-out methode

Wanneer er gedurende een vooraf vastgelegde tijd geen informatie meer wordt doorgegeven, wordt aangenomen dat het verzenden van de boodschap beëindigd is.

Byte-count methode

Bij aanvang van de communicatie geeft de zender aan de ontvanger het aantal bytes van het bericht door. De ontvanger telt het aantal ontvangen bytes. Wanneer het vooraf opgegeven aantal bytes bereikt is, wordt het bericht als beëindigd beschouwd.

End-of-message-teken methode

Er wordt vooral een bepaalde bitcode afgesproken, die aangeeft dat het bericht ten einde is. De zender geeft als laatste teken die afgesproken bitcode door, zodat de ontvanger weet dat het bericht beëindigd is.

Het geheel van afspraken over de manier waarop een teken begint of eindigt, hoe het doorsturen van een bericht wordt beëindigd of hoe de snelheid van zender en ontvanger gesynchroniseerd worden, wordt vastgelegd in een **communicatieprotocol**. Die standaarden zijn daardoor wereldwijd dezelfde zodat computers van over de hele wereld probleemloos met elkaar kunnen communiceren. Voor elke specifieke netwerkdienst wordt een specifiek protocol gebruikt. Je leert meer over communicatieprotocollen in het volgende hoofdstuk.

Je zou kunnen verwachten dat parallelle gegevensoverdracht een stuk sneller is dan seriële gegevensoverdracht, omdat in het eerste geval een aantal bits tegelijk kunnen worden doorgestuurd. Dat was zeker zo in de begintijden van de personal computers, maar tegenwoordig is de technologie van DCC's zo hoogwaardig dat moderne seriële verbindingen vele malen sneller zijn dan traditionele parallelle verbindingen. Bovendien is bekabeling voor seriële gegevensoverdracht veel eenvoudiger en dus goedkoper te produceren. Daarom zijn alle externe verbindingen van en naar de computer tegenwoordig serieel, of het nu om verbindingen met randapparaten (zoals USB of FireWire) of om netwerkverbindingen gaat.

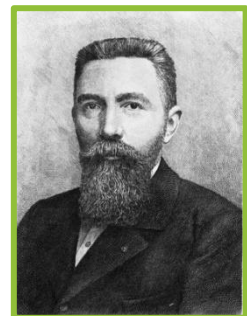
1.6 Transmissiesnelheden

De snelheid waarmee gegevens verstuurd worden over een netwerk, wordt uitgedrukt in bits per seconde (bps). Snellere verbindingen worden dan uitgedrukt in kilobits of megabits per seconde. De afkortingen voor die laatste zijn soms verwarrend. Kbps staat dan voor kilobits per seconden, maar dat durft men ook wel eens foutief kilobytes per seconde noemen, een eenheid die bij parallelle gegevensoverdracht wordt gebruikt. Om zeker geen verwarring mogelijk te maken worden daarom ook de afkortingen Kbit/s en Mbit/s gebruikt – ook in deze cursus trouwens. In tegenstelling tot gegevensopslag zijn de eenheden van gegevensoverdracht verder niet op het binair talstelsel gebaseerd. 1 Kbit/s betekent dus 1000 bits per seconde en geen 1024. 1Mbit/s is dus precies 1 miljoen bits per seconde.

a) Baud rate

De snelheid van gegevensoverdracht via datacommunicatielijnen werd vroeger **baud rate** genoemd. De transmissiesnelheid van een verbinding werd dan uitgedrukt in het aantal signalen per seconde. Een baud rate van 1200 wil zeggen dat er per seconde 1200 signalen kunnen verstuurd worden.

Als elk signaal precies één bit is, dan is de baud rate precies gelijk aan het aantal bits per seconde, maar als er meer bits in één signaal worden gestopt, klopt dit niet meer. Wanneer in één signaal bijvoorbeeld 4 bits tegelijk worden verstuurd, dan verkrijgt je een gegevensoverdracht van 4800 bps bij 1200 baud. Gezien alle communicatie over een computernetwerk serieel verloopt en de informatie bit per bit wordt verstuurd, is in computernetwerken baud altijd gelijk aan bits per seconde.



Aangezien voor de reële snelheid van gegevensoverdracht bps een correctere waarde is, is de baud rate in onbruik geraakt. Het gaat ook al om een erg oude eenheid: ze werd al gebruikt voor het aanduiden van de transmissiesnelheid over telegraaflijnen. De naam van de eenheid is afkomstig van de Franse telegraafingenieur Jean-Maurice-Emile Baudot (1845 - 1903).

b) Bandbreedte

In verband met de snelheid van gegevensoverdracht wordt vaak het begrip **bandbreedte** gebruikt. Daarmee wordt het verschil aangeduid tussen de hoogste en de laagste frequentie op een transmissiemedium. Niet alleen het type transmissiemedium (dus het soort kabel) is daarbij van belang, maar ook de lengte ervan. Daarom kent elk kabeltype een maximale lengte die moet gerespecteerd worden. In te lange kabels kunnen immers de hoogste frequenties afzwakken, waardoor er fouten in de gegevensoverdracht kunnen optreden. Strikt genomen gaat bandbreedte dus over frequentie. De eenheid van bandbreedte wordt uitgedrukt in Hz, KHz of Mhz.

Het spreekt voor zich dat een grotere bandbreedte een snellere **gegevensdoorvoersnelheid** mogelijk maakt. Bandbreedte uitdrukken in frequentie-eenheden als Hz heeft voor computergebruikers weinig concrete betekenis, omdat ze niet uitdrukt hoe snel de gegevens daadwerkelijk verzonden worden. Daarom wordt bandbreedte ook wel eens uitgedrukt in bps, hoewel dit niet correct is. Niet altijd wordt de maximale bandbreedte van een verbinding immer benut. De doorvoersnelheid is dan variabel, terwijl de bandbreedte van het transmissiemedium natuurlijk altijd dezelfde is.

Een datacommunicatie-verbinding is vaak samengesteld uit een aantal **links**, verbonden met knooppunten. Het spreekt voor zich dat de traagste link de snelheid bepaalt van de ganse verbinding.

De volledige bandbreedte van de snellere links wordt dan niet benut. Dit wordt de **transmissie-bottleneck** genoemd.

De capaciteit van een transmissiemedium kan op twee manieren worden toegekend. Bij **baseband** wordt de volledige bandbreedte toegekend aan één communicatiemedium. Bij **broadband** (in het Nederlands **breedband**) wordt de bandbreedte gedeeld door twee of meer verbindingen. De meeste lokale netwerkverbindingen werken in baseband modus, maar verbindingen tussen netwerken, zoals het internet, zijn vaak breedbandverbindingen.

De distributiekabel is een typisch voorbeeld van een broadband-verbinding: ze kan immers verschillende signalen dragen, gaande van televisie- en radiosignalen, over telefoonverbindingen tot een snelle internettoegang.

Modems kennen eigen standaarden die de bandbreedte en dus ook de snelheid van de gegevensoverdracht bepalen. In de loop van de jaren werden nieuwe standaarden ontwikkeld om steeds hogere snelheden mogelijk te maken. Die zogenaamde **V-standaarden** werden ontwikkeld door het CCITT (*Comité Consultatif International de Téléphonie et Télégraphie*), een organisatie die werkt onder de vleugels van de Verenigde Naties. In de tabel staan de voornaamste V-standaarden.

Standaard	Snelheid
V.21	300 bps
V.22	1200 bps
V.22bis	2400 bps
V.32	9600 bps
V.32bis	14400 bps
V.34	28800 bps
V.90/V.92	56600 bps

OPDRACHT

Waarom wordt er voor het uitdrukken van de snelheid van gegevensoverdracht gebruik gemaakt van bits (bijvoorbeeld in “megabits per seconde”) en niet van bytes?

.....

.....

.....

.....

.....

Waarom worden de eenheden voor gegevensoverdracht niet gebaseerd op het binair talstelsel, zoals bijvoorbeeld bij het uitdrukken van opslagcapaciteit? Met andere woorden: waarom is 1 Kbit/s gelijk aan 1000 bps en niet aan 1024 bps?

.....

.....

.....

.....

.....

.....

2 Opbouw en werking van netwerken

Waarin je een computernetwerk laagje per laagje leert kennen.

In dit hoofdstuk leer je dit:

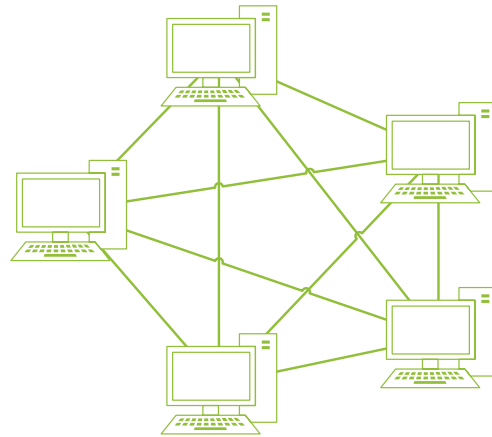
- ◆ De opbouw van de verschillende logische en fysieke netwerktopologieën.
- ◆ De functie van het OSI reference model verklaren.
- ◆ De functie van elke laag in het OSI reference model verklaren.
- ◆ De functie en werking van de toegangsprotocollen token passing bus / token passing ring, ATM, Ethernet en PPP.
- ◆ De functie en werking van de overdrachtsprotocollen TCP/IP (IPv4, ARP, IPv6) en IPX/SPX.
- ◆ De netwerkinstellingen van een computer nagaan.
- ◆ De functie en werking van de toepassingsprotocollen HTTP, SMTP, POP3, IMAP, FTP, Telnet, SSH, RDP en SNMP

2.1 Netwerktopologieën

In een computernetwerk staan de computers met elkaar in verbinding. De manier waarop dat gebeurt, wordt de **topologie** van een netwerk genoemd.

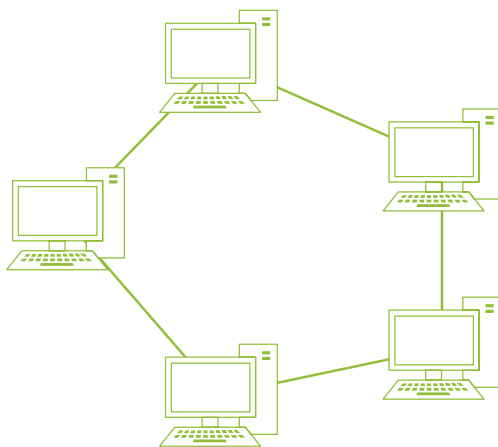
2.1.1 Maasnetwerk

In maasnetwerken is elke computer verbonden met alle andere, al hoeven er niet effectief tussen alle computers verbindingen te bestaan. In functie van de te verwachten verkeerspatronen kunnen een deel van de verbindingen worden weggelaten. Communicatie tussen computers die niet rechtstreeks met elkaar verbonden zijn, kan dan nog altijd via een tussenliggende computer gebeuren. Een netwerkontwerper zal echter altijd proberen directe verbindingen aan te brengen tussen computers met de meest intensieve onderlinge communicatie.



Je kan een maasnetwerk vergelijken met ons wegennet: er bestaan rechtstreekse verbindingen tussen belangrijke steden, maar je kan ook van de ene stad naar de andere rijden via een stad ergens tussenin.

2.1.2 Ringnetwerk



In een ringnetwerk staan de computers met elkaar in contact via één verbinding die van computer naar computer loopt. Doorgaans wordt daarbij gebruik gemaakt van een coaxiale kabel. Wanneer een computer een bericht wilt doorgeven aan een andere computer in het netwerk, zullen alle computers één na één dat bericht ontvangen. Samen met het bericht wordt ook het netwerkadres van de bestemming meegestuurd. Enkel de computer met dat netwerkadres zal het bericht ook effectief kunnen inlezen. De andere computers sturen het bericht gewoon verder naar de volgende computer op het netwerk. Het bericht wordt op die manier langs het hele netwerk gestuurd tot het weer bij de zender aankomt, die daarmee weet dat het bericht alle computers – en dus ook de bestemming – heeft bereikt.

Het verkeer over een ringnetwerk verloopt **unidirectioneel** (simplex, in één richting). Een bericht dat van de eerste naar de laatste computer moet worden verstuurd, zal dus verplicht de langste weg moeten nemen. Omdat elke computer het bericht moet verder sturen naar de volgende computer op het netwerk, spreken we van een **actieve topologie**.

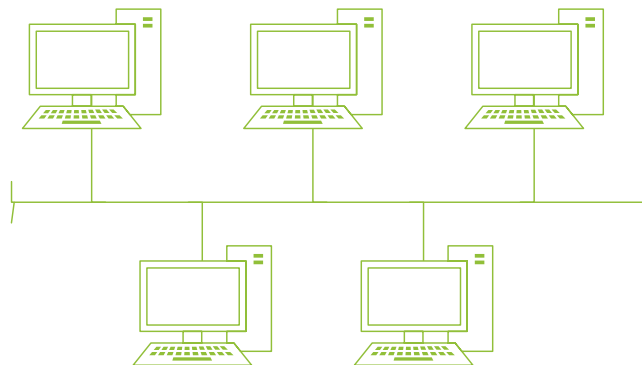
Een van de grootste nadelen van ringnetwerken is dat slechts één computer tegelijk gegevens kan verzenden. De andere computers moeten wachten tot die ene computer klaar is met zenden. Hoe meer computers er deel uitmaken van het netwerk, hoe groter de gemiddelde wachttijden zullen worden. Het aantal computers op een ringnetwerk is in de praktijk dan ook beperkt. Nog een nadeel is wanneer de netwerkkaart van één computer defect is, of wanneer er een breuk in de kabel voorvalt, het volledige netwerk wordt lam gelegd.

De bekendste ringnetwerken zijn de **token passing ring** netwerken. Die worden zo genoemd, omdat op regelmatige tijdstippen een signaal (token) over het netwerk wordt gestuurd om het netwerk te synchroniseren. Daarmee wordt de snelheid van zenden en ontvangen van alle computers op elkaar afgestemd. Enkel wanneer het token langskomt, kan een bericht verzonden worden. Dat maakt een ringnetwerk bedrijfszekerder. Bij niet-gesynchroniseerde ringnetwerken kan er immers gegevensverlies optreden omdat het zenden en ontvangen tussen verschillende computers niet aan dezelfde snelheid gebeurt. Dat fenomeen wordt **jitter** genoemd.

Ringnetwerken zijn over het algemeen weinig stabiel en worden in de praktijk nog zelden toegepast.

2.1.3 Busnetwerk

In een busnetwerk worden de computers eveneens met elkaar verbonden door één lijn die van computer naar computer loopt, maar die een begin en een einde heeft. Aan het begin en het einde van die centrale lijn wordt een weerstand geplaatst die men **terminator** noemt en die het signaal moet neutraliseren (absorberen). Zonder terminator zou het signaal immers voortdurend heen en weer worden gekaatst, waardoor geen enkele computer nog zou kunnen beginnen zenden.



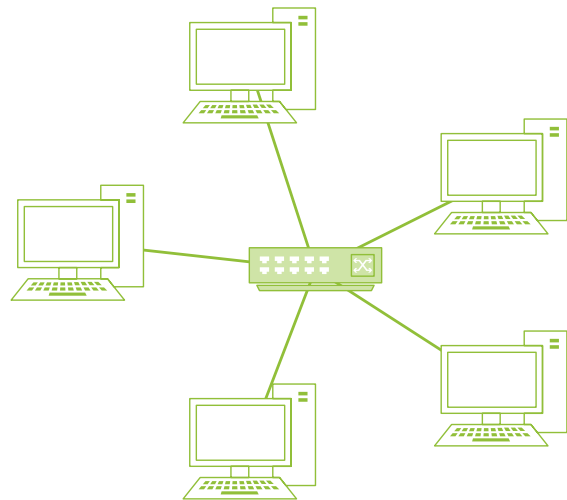
Een busnetwerk werkt **bidirectioneel**: gegevens kunnen in twee richtingen over de kabel worden gestuurd. Een busnetwerk is bovendien een **passieve topologie**: de computers hoeven het bericht niet zelf verder te sturen. Wanneer een computer defect is, heeft dit dus geen invloed op de rest van het netwerk. Een breuk in de kabel zal het netwerk wel plat leggen.

De **head-end-topologie** is een alternatieve vorm van bustopologie. Daarbij wordt gebruik gemaakt van twee communicatielijnen: eentje voor het zenden (**up-link**) en eentje voor het ontvangen (**down-link**). Zo'n netwerk bestaat dus uit twee unidirectionele lijnen, waardoor de capaciteit per lijn aanzienlijk kan verhoogd worden.

2.1.4 Sternetwerk

In sternetwerken worden de computers met elkaar verbonden door middel van een of meer netwerkverdeeldozen - hubs of switches. Daarbij wordt doorgaans gebruik gemaakt van UTP-bekabeling.

Het bericht van een computer komt in de hub aan en die stuurt het signaal verder. Passieve hubs geven het bericht door naar alle aangesloten computers. Elke computer controleert of het bericht voor hem bestemd is. Het bericht hoeft niet verder gestuurd te worden, want elke computer is als het ware een eindpunt. Een sternetwerk is daarom een **passieve topologie**.



Indien gebruik gemaakt wordt van actieve switches wordt het bericht enkel doorgestuurd naar de computer voor wie het bedoeld is. Het verschil tussen passieve hubs en actieve switches leer je in hoofdstuk 3.3.

De zwakste schakel in een sternetwerk is de hub of de switch. Als die het begeeft, wordt het hele netwerk onklaar gemaakt. Anderzijds heeft een sternetwerk wel het voordeel dat wanneer één computer uitvalt of een kabel onderbroken wordt, dit de rest van het netwerk niet beïnvloedt.

Lokale sternetwerken worden op hun beurt vaak in stervorm met elkaar verbonden. We spreken dan van een **boomtopologie** of een **hiërarchische stertopologie**.

2.1.5 Huidige situatie

In de loop van de geschiedenis verdwenen maas-*, ring- en bustopologieën volledig ten voordele van de stertopologie. Sternetwerken beantwoorden veel meer aan de behoeften van moderne netwerken. (*zie uitleg Mesh Networking)

Vroeger bestonden ook combinaties van verschillende fysieke netwerktopologieën. Een bekend voorbeeld is het **ster-busnetwerk**. Daarbij zijn meerdere hubs aanwezig die met elkaar verbonden zijn door middel van één kabel zoals in een busnetwerk. Rond elk van de hubs is een stertopologie opgebouwd. Deze combinatie van twee verschillende topologieën kwam typisch voor in kantoren met verdiepingen. Horizontaal op elke verdieping was er een hub voorzien en had je dus een sternetwerk. Verticaal over de verdiepingen heen is er een kabel, die de hubs verbindt in busvorm.

In dit hoofdstukje werden vier verschillende **fysieke netwerktopologieën** besproken. De wijze waarop berichten over de bekabeling worden gestuurd, vormt **de logische netwerktopologie**. De logische en fysieke netwerktopologie zijn doorgaans dezelfde, hoewel dat niet noodzakelijk is. Zo is het bijvoorbeeld mogelijk een logisch ringnetwerk in te stellen op een fysiek sternetwerk of een fysiek busnetwerk.

2.2 Het OSI reference model

Met het ontstaan van netwerken drong zich de noodzaak op om internationale afspraken te maken over de manier waarop computers met elkaar moesten communiceren. Dat resulteerde in het wereldwijd aanvaarde en gebruikte **OSI reference model** (*open systems interconnection*).

2.2.1 Communiceren in lagen

Het staatshoofd van China en zijn collega van Peru willen een geheime afspraak met elkaar maken. Hierbij doen zich enkele prangende problemen voor: beide staatshoofden spreken een verschillende taal en begrijpen elkaar dus niet. Bovendien gaat het om een boodschap die gevoelige informatie betreft. Als ze onderschept wordt, mag ze dus niet ontcijferd kunnen worden.

Eerst deelt het Chinese staatshoofd zijn boodschap mee aan een tolk. Die spreekt met zijn Peruviaanse collega een gemeenschappelijke taal af. Het probleem is immers dat de Chinese tolk geen Spaans kent en de Peruviaanse kent geen Chinees. Gelukkig kennen beide tolken wel Engels. Ze spreken dus af om elkaars berichten in het Engels te vertalen.

De tolken spreken niet rechtstreeks met elkaar. Iedereen die het bericht onderschept en Engels kent, zou de geheime boodschap zo kunnen lezen. Daarom wordt het bericht eerst door een cryptograaf in geheimschrift omgezet. De Chinese noch de Peruviaanse cryptograaf begrijpt Engels, maar dat geeft niet. Met de inhoud van de boodschap hebben zij immers niets te maken. Belangrijk is uiteraard wel dat ze gebruik maken van dezelfde code, zodat ze boodschappen correct kunnen encrypteren en ontcijferen.

Ten slotte wordt het bericht doorgegeven aan de operatoren die het bericht naar elkaar doorsturen. Zij spreken af via welk gemeenschappelijk communicatiemedium dat moet gebeuren.



Het valt op dat hoe hoger in deze hiërarchie, hoe meer je te maken hebt met de inhoud van een bericht; hoe lager de functie, hoe “technischer” de taak. In dit voorbeeld wordt in vier lagen gecommuniceerd en elke laag maakt gebruik van de diensten van de onderliggende laag.

2.2.2 Het OSI reference model

Voor computers werd er ook een **lagen-model** ontworpen: het OSI reference model, dat reeds in 1977 werd ontwikkeld. Het is een theoretisch model dat fabrikanten van netwerkapparatuur en softwareontwikkelaars in staat stelt om vlot met elkaar samen te werken en compatibele apparatuur en programma’s te ontwikkelen. Net zoals in het voorbeeld met de twee staatshoofden bestaan er tussen de verschillende lagen van zender en ontvanger gemeenschappelijke afspraken die **protocollen**

worden genoemd. Die protocollen zijn openbaar zodat alle ontwikkelaars er vrij gebruik van kunnen maken. Het OSI reference model bevat volgende lagen die elk specifieke diensten leveren:



1

Toepassingslaag (application layer)

In deze laag zijn de toepassingsprogramma's actief waarmee computergebruikers met elkaar communiceren. Deze laag levert geen diensten aan andere OSI-lagen – er zijn immers geen bovenliggende lagen – maar levert wel diensten aan computertoepassingen zoals browsers of e-mail clients.

De toepassingslaag zorgt er ook voor dat de juiste protocollen worden geactiveerd voor een bepaalde verbinding. Zo wordt het verzenden van een e-mail bericht met een heel ander protocol behandeld dan bijvoorbeeld het plaatsen van een bestand op een fileserver.

2

Presentatielaag (presentation layer)

Niet alle computers werken met dezelfde bestandsformaten en bestandssystemen. Er bestaan vaak nogal verschillen in de manier waarop gegevens weergegeven worden tussen verschillende computers in een netwerk.

In deze laag wordt alle in- en uitgaande informatie getransformeerd naar een vooraf vastgesteld standaardformaat dat door alle elementen van het netwerk aanvaard wordt. Zo kan bijvoorbeeld een bericht dat in Unicode werd opgesteld, in ASCII-code omgezet worden voor het verzonden wordt.

Andere taken die in de presentatielaag worden uitgevoerd zijn gegevenscompressie en – decompressie (hoewel dit ook in de applicatielaag kan gebeuren), encryptie en decryptie, en netwerkbeveiliging.

3

Sessiel laag (session layer)

Deze laag zorgt ervoor dat een gebruiker zich bij een andere gebruiker of server slechts één keer hoeft aan te melden voor de ganse duur van de verbinding. Wanneer de verbinding wegvalt, zal opnieuw een beroep gedaan worden op de sessiel laag om weer aan te melden. Om te vermijden dat een verbinding te vaak zou worden verbroken of dat bij het verbreken van de verbinding alle gegevens opnieuw moeten worden verzonden, zal de sessiel laag de verbinding tussen de twee computers synchroniseren.

Samengevat kan je zeggen dat de sessiel laag instaat voor het maken van een verbinding, het onderhouden en het synchroniseren ervan, en het correct afsluiten van de verbinding aan het einde van de communicatie.

4

Transport laag (transport layer)

De belangrijkste functie van de transport laag is het op splitsen van de gegevens in segmenten om ze geschikt te maken voor het netwerk waarover ze verzonden worden. Die taak wordt **segmenteren** of **fragmenteren** genoemd. Daardoor zijn alle bovenliggende lagen totaal onafhankelijk van hardware of netwerktopologie. Je zou kunnen zeggen dat de transport laag de eerste laag is, die zich werkelijk met het datatransport tussen computers bezighoudt, terwijl de activiteiten van de bovenliggende lagen zich enkel afspelen in de verzendende of ontvangende computer zelf.

Tevens zorgt de transport laag voor een betrouwbaarheidsgarantie (**QOS** of *quality of service*): ze zorgt ervoor dat de gegevens zonder wijzigingen bij de ontvanger aankomen. Daarvoor bestaan 5 transportklassen, waarbij de laagste klasse geen foutcontrole voorziet terwijl de hoogste klasse de meest doorgedreven foutcontrole kent.

Ten slotte worden binnen de netwerkl laag ook afspraken gemaakt tussen de verbonden computers met betrekking tot de doorvoersnelheid van de gegevens. Dat is een ingewikkeld proces dat **option negotiation** wordt genoemd.

5

Netwerkl laag (network layer)

Deze laag verpakt de informatie in pakketjes. Elk pakketje wordt voorzien van de adresinformatie van het bericht, zodat geen enkel pakketje onderweg verloren kan gaan. Tevens regelt deze laag de doorstroming van de pakketjes over het netwerk (**routing**) zodat er geen oververzadiging van de datacommunicatielijnen ontstaat.

Op het niveau van de netwerkl laag worden computers op een netwerk herkend aan de hand van een IP-adres. Dit logische adres wordt volledig softwarematig toegekend aan een computer en is onafhankelijk van de hardware. Je leert meer over IP-adressering in hoofdstuk 2.3.2.1.

Het IP-adres van de zender en dat van de ontvanger zijn noodzakelijk voor het bepalen van de route die een pakketje zal afleggen. Het bepalen van die route wordt **path determination** genoemd en gebeurt door routers.

6

Verbindingslaag (datalink layer)

In deze laag worden de pakketjes opgedeeld in of samengevoegd tot frames. Zo'n frame kan dus meerdere pakketjes bevatten, die zelfs van verschillende zenders afkomstig zijn maar gebruik maken van dezelfde route. Terwijl een pakketje uit de netwerklaag een **logische eenheid** is, vormt een frame een **fysieke eenheid**. De manier waarop frames worden samengesteld, is afhankelijk van het netwerktype en de netwerktopologie waarover de informatie moet worden verstuurd.

De verbindingslaag bestaat zelf uit twee deellagen: de MAC-laag en de LLC-laag. In de MAC-laag communiceren de computers met elkaar door middel van een **MAC-adres** (*media access control*). Dat is een 48 bits lang uniek identificatienummer van de netwerkkaart en bevindt zich in een ROM-chip. De **LLC-laag** (*logical link control*) is niet afhankelijk van de hardware en communiceert met de bovenstaande lagen van het OSI reference model. Binnen de verbindingslaag worden het MAC-adres en het IP-adres aan elkaar gekoppeld.

7

Fysieke laag (physical layer)

Deze laag vervoert de bits zonder zich van de inhoud of de foutcontrole iets aan te trekken. Hierin worden de verschillende componenten beschreven die belangrijk zijn voor de manier waarop de gegevens moeten doorgestuurd worden, zoals het soort bekabeling, de maximale kabellengte, de gebruikte modulatie- en codeertechniek, connectortypes, enz.

Belangrijke variabelen die bij een verbinding tussen twee netwerkcomponenten gelegd zijn de hoogte van de spanning om een 1 en een 0 uit te drukken, hoe lang het doorsturen van één bit duurt, in welke richting er gecommuniceerd wordt, hoe de verbinding tot stand komt en hoe ze wordt onderbroken, hoeveel contacten een netwerkconnector heeft en waarvoor elk contact gebruikt wordt.

2.3 Communicatieprotocollen

Het hele OSI reference model werd bedacht om hard- en software van zender en ontvanger op elk niveau van de communicatie vlot met elkaar te laten samenwerken. De afspraken die de basis vormen van die samenwerking worden **protocollen** genoemd. Ze worden ingedeeld op basis van de OSI-laag waarbinnen ze actief zijn.

Er bestaan bijzonder veel communicatieprotocollen. Die allemaal bespreken is weinig zinvol. We beperken ons hier dus tot de netwerkprotocollen die belangrijk zijn voor moderne computernetwerken en voor de ontwikkeling van het internet. We doen dat van onder in het OSI reference model naar boven.

Hier kan je een overzicht terugvinden van de belangrijkste netwerkprotocollen:

OSI-laag	Protocollen	
Toepassingslaag	Toepassingsprotocollen	<i>http, SMTP, POP3, IMAP, FTP, Telnet, SSH, RDP, SNMP</i>
Presentatielaag		
Sessiel laag		
Transportlaag	Overdrachtsprotocollen	<i>TCP/IP, IPX/SPX</i>
Netwerklaag		
Verbindingslaag	Toegangsprotocollen	<i>Token passing ring / token passing bus, ATM, Ethernet, PPP, ARP*</i>
Fysieke laag		

(*) ARP zal pas bij de overdrachtsprotocollen besproken worden, hoewel het eigenlijk actief is in de verbindingslaag. Maar om de werking van ARP te begrijpen, heb je eerst de kennis nodig van het IPv4-protocol en dat is een overdrachtsprotocol.

2.3.1 Toegangsprotocollen

Toegangsprotocollen zijn actief in de verbindingslaag van het OSI reference model. Ze bepalen de manier waarop de informatie in frames wordt verpakt en over het netwerk wordt gestuurd.

a) Token passing ring / token passing bus

Token passing ring is het toegangsprotocol dat gebruikt wordt voor de meeste ringnetwerken. Een speciaal **bitpatroon** (het **token**) wordt verstuurd door de eerste computer die wordt ingeschakeld. Wanneer een computer geen informatie te verzenden heeft, geeft die het token gewoon door aan de volgende computer. Wanneer die computer wel een bericht wil versturen, dan wordt dat in de plaats van het token op het netwerk gezet, het werkadres van de bestemming wordt erbij geplaatst en doorgestuurd over het netwerk.

De computers voor wie het bericht niet is bestemd, geven het gewoon door over het netwerk. Wanneer het de bestemming bereikt, kopieert die het bericht en stuurt het ongewijzigd verder tot het weer bij de zender aankomt. De zender stuurt vervolgens een vrij token door op het netwerk, dat dan door een ander werkstation kan worden gebruikt. Aangezien er maar één token over het netwerk circuleert, kan er steeds maar één computer tegelijk informatie verzenden.

Er ontstaat echter een probleem wanneer een computer informatie verstuurt waarin eenzelfde bitpatroon voorkomt als het token. De andere computers in het netwerk zouden dat patroon kunnen interpreteren als het token, wat niet is. Om dat probleem op te lossen, wordt het principe van **bitstuffing** toegepast: er wordt aan die bitreeks in het bericht een extra bit toegevoegd, zo gekozen dat het nieuwe patroon bitpatroon altijd verschillend is van het token. De ontvanger herkent de toegevoegde bit en zal die bij de verwerking van de informatie verwijderen, zodat het bericht opnieuw de bitreeks bevat die op het token lijkt. Maar dat gebeurt lokaal bij de verwerking door de ontvangende computer. De andere computers worden er niet door beïnvloed.

Token passing bus is een alternatief verbindingsprotocol voor ring- en busnetwerken, dat op het gebied van werking gelijkaardig is aan token passing ring.

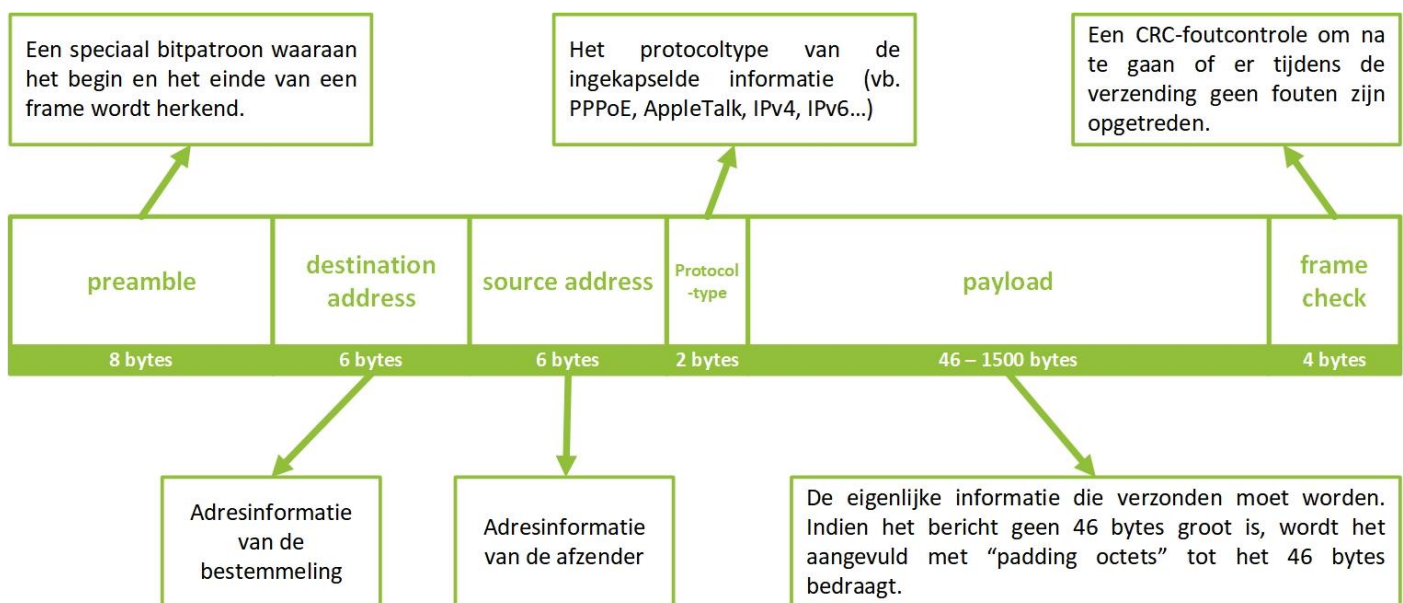
b) ATM (Asynchronous Transfer Mode)

ATM (*asynchronous transfer mode*) werd door telefoonmaatschappijen ontwikkeld voor het versturen van digitale gegevens over backbones van telefoonlijnen. ATM is ontworpen voor hoge bandbreedte en wordt tegenwoordig nog gebruikt bij ADSL-verbindingen. Voor lokale netwerken wordt het haast nooit toegepast.

Bij ATM worden berichten opgedeeld in frames met een gelijke omvang die men cells noemt. Elke cell bestaat uit 53 bytes, waarvan 48 databytes bedoeld zijn voor de inhoud van het bericht (de **payload**). De overige vijf bytes zijn bedoeld voor informatie om het bericht bij de juiste ontvanger te doen terechtkomen.

c) Ethernet

Het Ethernet-protocol is het toegangprotocol voor de meeste moderne netwerken. Het kan toegepast worden in alle netwerktopologieën en laat breedbandtransmissie toe. Elke computer in het netwerk kan op eender welk ogenblik een bericht verzenden. Om te verhinderen dat er conflicten op het netwerk ontstaan, moet er voor het verzenden van het bericht eerst nagegaan worden of de lijn beschikbaar is. Dat principe wordt **lijnraftasting** genoemd en wordt mogelijk gemaakt door het **CSMA/CD**-protocol (*Carrier Sense Multiple Access with Collision Detection*). Met dit protocol kunnen bovendien conflicten (**collisions**) op het netwerk opgespoord worden.



De stukjes informatie die voor de payload worden toegevoegd, worden **headers** genoemd. Het deel achter de payload noemt men **footers** of **trailers**. Het hele proces van het toevoegen van headers en footers, wordt **inkapseling** of **encapsulation** genoemd.

Ethernet werd al in 1973 ontwikkeld door Xerox. Ondertussen is Ethernet het meest verspreide toegangprotocol voor computernetwerken en voor het internet. Bovenop het Ethernet-protocol zijn tal van andere protocollen actief, waarvan het bekendste het TCP/IP-protocol is.

d) PPP (Point-to-Point Protocol)

PPP (*point-to-point protocol*) is een veel gebruikt toegangsprotocol voor inbelnetwerken waarbij authenticatie nodig is, met andere woorden, waarbij de echtheid van de inbeller moet worden vastgesteld alvorens die toegang verkrijgt tot het netwerk. Indien dat netwerk gebaseerd is op Ethernet spreken we van **PPPoE** (*PPP over Ethernet*). Bij ATM-gebaseerde netwerken wordt dat dan **PPPoA** (*PPP over ATM*).

PPP maakt gebruik van frames met een variabele lengte. Die moeten bij de ontvanger arriveren in dezelfde volgorde waarin ze verzonden werden. Om de performantie van hun internetverbinding te verhogen maken sommige bedrijven gebruik van twee of meer communicatielijnen voor dezelfde verbinding. Daarbij kan de volgorde van het ontvangen van de frames niet gegarandeerd worden.

Multilink PPP, een toevoeging aan het oorspronkelijke PPP, nummert de frames zodat ze aan ontvangerszijde in de juiste volgorde kunnen worden teruggezetzet.

2.3.2 Overdrachtsprotocollen

Overdrachtsprotocollen zijn actief in de netwerklaag en de transportlaag van het OSI reference model. Ze bepalen de manier waarop berichten geadresseerd en opgedeeld worden in pakketjes. Deze protocollen zijn actief boven een toegangsprotocol (meestal Ethernet).

2.3.2.1 TCP/IP

TCP/IP (*Transmission Control Protocol / Internet Protocol*) is veruit het bekendste overdrachtsprotocol. Het werd al in de jaren 1960 ontwikkeld en was het voornaamste overdrachtsprotocol bij het koppelen van Unix-mainframes aan het voormalige ARPAnet, de voorloper van het internet. Later is het TCP/IP-protocol eveneens de basis gebleven voor de gegevensoverdracht op het internet.

TCP/IP is een open standaard. Alle eigenschappen, definities, concepten en werkwijzen zijn openlijk op het internet gepubliceerd in zogenaamde **RFC's** (*Request for Comments*). Dit maakt het mogelijk voor veel software-firma's uitbreidingen op de standaard te ontwikkelen en zelfs voorstellen tot wijzigingen in te dienen. Omdat TCP/IP niet toebehoort aan een of andere producent, kan het protocol overal gebruikt worden zonder licentierechten te moeten betalen. Dat was een erg belangrijke factor in de snelle ontwikkeling van het internet.

TCP/IP is een samenvoeging van twee belangrijke protocollen. TCP regelt de segmentering van de informatie (het opdelen van de informatie in kleinere pakketjes), terwijl IP instaat voor de adressering van die pakketjes.

a) IPv4

Iedere component op een netwerk (server, werkstation, netwerkprinter, switch, router, ...) beschikt over een eigen **logisch identificatienummer**: het **IP-adres**. Dat nummer identificeert niet een computer zelf, maar een netwerkinterface. Een computer die beschikt over twee netwerkkaarten, zoals een computer die een knooppunt vormt in een netwerk of een router beschikt dus over minstens twee IP-adressen.

Een IPv4-adres bestaat uit vier getallen van elk 8 bits. Ze worden in decimale code weergegeven, van elkaar gescheiden met een punt. Elk getal tussen de puntjes wordt een **octet** genoemd en kan een 8 bits-waarde bevatten. Daarmee kunnen dan 2^8 of 256 waarden gemaakt worden. De waarde van een octet bevindt zich altijd tussen 0 en 255. Een IP-adres ziet er zo uit:



Het gedeelte van het IP-adres dat voor alle componenten in het netwerk identiek is, wordt het **netwerknummer** genoemd. Het gedeelte van het IP-adres dat voor elke computer verschillend is, wordt het **computernummer** genoemd. Er bestaan drie klassen van netwerken op het internet:

♦ Klasse A-net

Het eerste octet heeft een vastgestelde waarde tussen 1 en 126 in het ganse netwerk. De laatste drie octetten kunnen vrij gebruikt worden voor het adresseren van 256^3 of 16.777.214 verschillende netwerkcomponenten op het netwerk te adresseren.



74.125.136.94
65.55.58.201

♦ Klasse B-net

Het eerste octet heeft een vastgestelde waarde tussen 128 en 191. Ook het tweede octet krijgt een vaste waarde. Er zijn dan nog 256^2 of 65.536 beschikbare IP-adressen voor de verschillende netwerkcomponenten op het netwerk.



180.200.45.6
131.20.128.128

♦ Klasse C-net

Het eerste octet krijgt een vastgestelde waarde tussen 193 en 223. De twee volgende octetten krijgen eveneens een vaste waarde. Er blijven nog 256 IP-adressen over voor de netwerkcomponenten op het netwerk.



193.168.200.254
202.106.192.12

Netwerkadressen waarvan het eerste octet begint met een hogere waarde dan 223 behoren toe aan klasse D of klasse E-netwerken. Dat zijn netwerken die gereserveerd zijn voor specifieke diensten op het internet en worden niet vrijgegeven voor netwerkbeheerders.

Je hebt misschien opgemerkt dat de hoogste klasse A-netwerken beginnen met 126 als eerste octet en dat de laagste klasse B-netwerken beginnen met 128 als eerste octet. Waarom beginnen netwerkadressen niet met 127?

Dat komt omdat het **loopbackadres** (*local host*) altijd begint met 127 in het eerste octet. Meestal wordt enkel het adres 127.0.0.1 gebruikt. Dit IP-adres verwijst altijd naar de eigen computer om die in staat te stellen gebruik te maken van eigen serverdiensten. In de praktijk maak je er zelden bewust gebruik van, maar software doet dat soms wel.

De netwerkadressen binnen het bereik van de klasse A, B of C netwerken zoals op de vorige pagina aangegeven, zijn **publiek**. Dat wil zeggen dat je een computer door middel van zo'n IP-adres rechtstreeks via het internet kunt benaderen. Veel lokale netwerken hebben slechts één toegang tot het internet via een router. Zo'n netwerk heeft dus slechts één publiek IP-adres. De computers in het achterliggende lokale netwerk moeten uiteraard ook kunnen geadresseerd worden. Daarbij worden best geen publieke IP-adressen gebruikt. Wanneer een computer uit het lokale netwerk hetzelfde IP-adres heeft als bijvoorbeeld een webserver op het internet, dan wordt die webserver vanuit het lokale netwerk onbereikbaar.

Om dat probleem te vermijden, gebruiken systeembeheerders IP-adressen die speciaal voor lokale netwerken zijn gereserveerd:

- ◆ Klasse A-netwerken: 10.x.x.x
- ◆ Klasse B-netwerken: 172.16.x.x - 172.31.x.x
- ◆ Klasse C-netwerken: 192.168.0.x - 192.168.255.x

Wanneer je vanuit een lokaal netwerk met een computer op het internet wil communiceren, moet er een bruggetje gemaakt worden tussen het IP-adresseringsbereik van het lokale netwerk en het internet. De techniek die daarvoor gebruikt wordt, heet **NAT** (*network address translation*). Je leert er meer over in hoofdstuk 6.2.1 in deze cursus.

Zelfs binnen een lokaal netwerk met private adressering zijn er enkele speciale IP-adressen die nooit kunnen gebruikt worden, aangezien ze een speciale functie hebben:

◆ Netwerkadres

Dat is het IP-adres dat het netwerk zelf adresseert en bestaat doorgaans uit het adres dat toegekend wordt binnen een klasse, gevolgd door allemaal nullen in de volgende octetten:

Klasse A:	10. <u>0.0.0</u>
Klasse B:	bijvoorbeeld: 172.20. <u>0.0</u>

◆ Broadcastadres

Dit is het hoogste IP-adres in een netwerk. Pakketten die naar dat IP-adres worden verstuurd, worden ontvangen door alle netwerkcomponenten in dat netwerk.

Klasse A:	10. <u>255.255.255</u>
Klasse B:	bijvoorbeeld: 172.20. <u>255.255</u>

Hierin mogen we besluiten dat in een klasse C-netwerk niet echt 256 netwerkcomponenten kunnen geadresseerd worden, maar slechts 254. Ook in klasse B en klasse A-netwerken nemen het netwerk- en broadcast-adres twee IP-adressen in.

Wanneer een bedrijf niet voldoende heeft aan de 254 IP-adressen van een publiek klasse C-netwerk, maar lang niet de behoefte heeft aan de meer dan 65000 IP-adressen van een klasse B-netwerk, kan

het een deel van een klasse-B netwerk huren. Deze manier van het indelen van bedrijfsnetwerken wordt **CIDR** (*classless interdomain routing*) genoemd. Om dat volledig te begrijpen, moeten we even naar de binaire notatie van IP-adressen kijken.

Nemen we als voorbeeld het IP-adres 185.200.24.0. Dan ziet er in binaire notatie zo uit:

10111001 11001000 00011000 00000000

In plaats nu van gebruik te maken van de vier vaste octetten, wordt afgesproken dat een willekeurig maar vooraf bepaald aantal bits samen het netwerknummer bepalen. Dat moet dan wel expliciet worden genoteerd: 185.200.24.0/21 betekent dat het netwerk begint bij IP-adres 185.200.24.0 en dat voor alle computers in dat netwerk de eerste 21 bits hetzelfde zijn:

10111001 11001000 00011000 00000000

Het onderlijnde gedeelte van het IP-adres is nu het netwerknummer, terwijl de resterende 11 bits het computernummer vormen. Daarmee kunnen 2^{11} of 2048 netwerkcomponenten geadresseerd worden, min twee voor het netwerk- en broadcast-adres, natuurlijk.

Aan elk TCP/IP-netwerk wordt standaard een **subnetmasker** toegekend. Met zo'n subnetmasker kan een fysiek computernetwerk opgedeeld worden in afzonderlijke logische netwerken, die dan subnetwerken worden genoemd. Netwerkbeheerders doen dat om het netwerk overzichtelijker te maken. Meestal is dat enkel zinvol in omvangrijke netwerken.

Het subnetmasker bestaat net als een IP-adres uit een reeks van 4 getallen van elk 8 bits. De standaard subnetmaskers zijn:

- ♦ Klasse A-netwerken: 255.0.0.0
- ♦ Klasse B-netwerken: 255.255.0.0
- ♦ Klasse C-netwerken: 255.255.255.0

We kijken even hoe subnetting precies in z'n werk gaat aan de hand van een voorbeeld. Daarbij gaan we uit van een klasse B-netwerk met het IP-bereik 172.16.0.1 tot en met 172.16.255.254.

1

We noteren het standaard subnetmasker (255.255.0.0) in binaire vorm:

11111111.11111111.00000000.00000000

2

Als we het netwerk in subnetten willen onderverdelen, wijzigen we de waarde van het derde octet. Dit is het eerste octet met een nulwaarde. We maken van de eerste drie nulletjes eentjes (255.255.224.0):

11111111.11111111.11100000.00000000

3

Omdat we de eerste drie bits van het eerste octet met een nulwaarde hebben gewijzigd, wordt dit een 3-bits subnetmasker genoemd. Daarmee kan je in principe 2^3 of 8 subnetten maken, maar aangezien de laagste (000) en de hoogste (111) waarde als subnet wegvallen, kan je het netwerk slechts opdelen in 6 echte subnetten:

00100000.00000000 (16.0)
 01000000.00000000 (32.0)
 01100000.00000000 (96.0)
 10000000.00000000 (128.0)
 10100000.00000000 (160.0)
 11000000.00000000 (192.0)

4

Om te weten tot welk subnetwerk een bepaalde computer behoort, moet je de bits in het IP-adres en de bits in het subnetmasker, die precies boven elkaar liggen, met een logische AND-functie verbinden:

10101100.00010000.10111101.11001000	(172.16.189.200)
11111111.11111111.11100000.00000000	(255.255.224.0)
10101100.00010000.10100000.00000000	(172.16.160.0)

Het netwerkadres van de computer in dit subnetwerk is dus 172.16.160.0. De computer zal dus deel uitmaken van het vijfde subnet.

Let op: het subnetmasker dat je bij alle computers in het ingeeft, moet dan wel 255.255.224.0 zijn en niet het netwerknummer van het subnetwerk.

Je kan een subnet ook aangeven door het netwerkadres van het subnet te geven, gevolgd door het aantal eentjes dat je gebruikt in je subnetmasker – in ons voorbeeld: 172.16.160.0/19

Een klein nadeel van het opdelen van een netwerk in subnetten, is dat je daarmee in he totaal minder werkstations kan adresseren. Je verliest immers een aantal adressen, niet alleen omdat er nu meer netwerkadressen zijn, maar ook omdat er een aantal bereiken wegvallen. Het aantal werkstations dat je nog kan adresseren, is afhankelijk van het aantal subnetten en dat is op zijn beurt weer afhankelijk van het aantal bits dat je aan het subnet toekent (in ons voorbeeld 3 bits = 6 subnetten). Hieronder vind je de schema's voor netwerken van klasse B en klasse C, hoewel subnetten in klasse C-netwerken zelden worden toegepast.

Netwerk klasse B: subnetten				
Bits	Subnetmasker	Aantal subnetten	Componenten per subnet	Totaal aantal componenten
2	255.255.192.0	2	16382	32764
3	255.255.224.0	6	8190	49140
4	255.255.240.0	14	4094	57316

5	255.255.248.0	30	2046	61380
6	255.255.252.0	62	1022	63364
7	255.255.254.0	126	510	64260
8	255.255.255.0	254	254	64516
9	255.255.255.128	510	126	64260
10	255.255.255.192	1022	62	63364
11	255.255.255.224	2046	30	61380
12	255.255.255.240	4094	14	57316
13	255.255.255.248	8190	6	49140
14	255.255.255.252	16382	2	32764

Netwerk klasse C: subnetten				
Bits	Subnetmasker	Aantal subnetten	Componenten per subnet	Totaal aantal componenten
2	255.255.255.192	2	62	124
3	255.255.255.224	6	30	180
4	255.255.255.240	14	14	196
5	255.255.255.248	30	6	180
6	255.255.255.252	62	2	124

b) ARP (Address Resolution Protocol)

Een IP-adres is een logisch adres, wat wil zeggen dat het adres softwarematig wordt toegekend aan een netwerkinterface. Dat kan ook niet anders, aangezien een fabrikant uiteraard niet kan voorzien in welk netwerk de hardware zal worden ingeschakeld. Wel krijgt elke netwerkcomponent van de fabrikant een hardware-adres mee. Dat adres wordt vastgelegd in een ROM-chip en wordt het **MAC-adres** (*media access control*) genoemd. Fabrikanten maken onderling afspraken zodat twee verschillende netwerkcomponenten nooit eenzelfde MAC-adres kunnen hebben. Het MAC-adres is samengesteld uit zes (in de toekomst acht) groepjes van acht bits. Meestal worden ze geschreven in hexadecimale vorm, van elkaar gescheiden door een dubbele punt:

00 : 64 : 22 : 15 : D7 : 8A

Aangezien computers op een netwerk met elkaar communiceren door middel van een IP-adres, maar de netwerkinterface fysiek enkel beschikt over een MAC-adres, moet het IP-adres aan het MAC-adres gekoppeld worden. Daarvoor wordt gebruik gemaakt van het **ARP-protocol** (*address resolution protocol*).

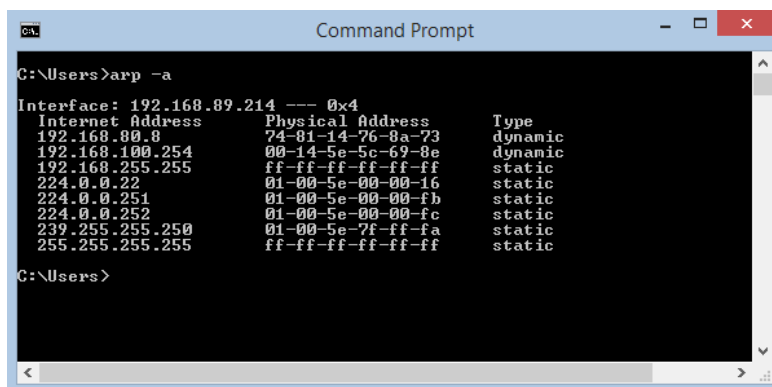
Wanneer computer A een verbinding wil maken met computer B op hetzelfde netwerk, moet computer A het MAC-adres van computer B te weten komen. Computer A kent wel het IP-adres van computer B en heeft in een speciaal deel van het geheugen (de **ARP-cache**) een tabel staan waarin aan alle gekende IP-adressen het MAC-adres gekoppeld staat. Die tabel wordt de **mappinglijst**

genoemd. Indien het MAC-adres van computer B op dat ogenblik al gekend is, staat die bij het juiste IP-adres in de mappinglijst en kan er onmiddellijk een verbinding worden gemaakt.

Indien het MAC-adres nog niet gekend is, stuurt computer A een **ARP-request**. Dat is een broadcast-bericht – een bericht dat naar alle computers in het netwerk wordt gestuurd – met de vraag om het MAC-adres te verkrijgen van computer B. Die herkent het IP-adres in het bericht als het zijne en zal een bericht terugsturen naar de afzender met het MAC-adres erin. De andere computers negeren het broadcast-bericht. Vanaf dan wordt het MAC-adres van computer B bewaard in de mappinglijst in de ARP-cache van computer A en kan ook in de toekomst makkelijker een verbinding worden gelegd.

De mappinglijst kan zowel statische als dynamische entries bevatten. Statische entries zijn entries die permanent bewaard blijven. Entries van computers waarmee zeer veel wordt gecommuniceerd, blijven op deze manier bewaard. Dynamische entries zijn entries die na een ARP request bewaard worden. Deze entries hebben een levensduur van slechts enkele minuten. Zo wordt er voorkomen dat de ARP-cache niet overvol geraakt.

Bij een Windows-computer kan je met het commando `arp -a` in de command prompt de entries in het ARP cache zien. Met het commando `arp -s [ip adres] [mac-adres]` kan je handmatig een statische entry invoeren in de ARP-cache van je computer.



```
C:\Users>arp -a
Interface: 192.168.89.214 --- 0x4
Internet Address      Physical Address      Type
192.168.80.8          74-81-14-26-8a-73    dynamic
192.168.100.254       00-14-5e-5c-69-8e    dynamic
192.168.255.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
C:\Users>
```

Wanneer computer A en computer B niet tot hetzelfde netwerk behoren, gebeurt eigenlijk hetzelfde, al zal het dan in verschillende tussenstappen gebeuren met een of meer routers als tussenstations. Computer A herkent het IP-adres van computer B als eentje van een extern netwerk en zal dan contact zoeken met de router, die het ARP-request van de standaard gateway van het lokale netwerk beantwoordt en het pakket via andere routers zal doorgeven tot het computer B bereikt heeft. Over IP-routing leer je meer in hoofdstuk 6.2.1 van deze cursus.

c) IPv6

De ontwikkeling van IPv4 dateert uit de jaren 1970. Toen werden voornamelijk mainframes aan elkaar gekoppeld. Van personal computers was op dat moment zelfs nog geen sprake. Met een theoretisch bereik van meer dan vier miljard IP-adressen zal men destijds wel aangenomen hebben dat er tot in de eeuwigheid voldoende IP-adressen ter beschikking zouden staan.

De gigantische vlucht die het internet enkele decennia later nam, creëerde een niet te stillen honger naar IP-adressen. In 2011 raakten de IPv4-adressen uitgeput. Gelukkig hebben het **IANA** (*Internet Assigned Numbers Authority*) en het **IETF** (*Internet Engineering Task Force*) dit probleem tijdig voorzien. Vanaf 1994 begonnen ze met de ontwikkeling van een nieuwe IP-generatie. Ongeveer tien jaar later stond IPv6 op punt. Fabrikanten maakten nieuwe netwerk hardware onmiddellijk compatibel

met deze nieuwe standaard. Toen op 6 juni 2012 een groot aantal internet service providers tegelijk overschakelden op IPv6 was alle apparatuur daar reeds op voorzien. De omschakeling gebeurde probleemloos en zonder dat het grote publiek er iets van merkte. Hoewel IPv6 nu de standaard is op het internet, blijven het overgrote deel van de internethosts eveneens via een IPv4-adres bereikbaar. Ook de adressering van computers in lokale netwerken blijft vaak nog op IPv4 gebaseerd.

IPv6-adressen zijn 128 bits lang. Daarmee kunnen 2^{128} verschillende adressen worden gemaakt – een onuitspreekbaar hoog getal. IPv6-adressen worden geschreven als acht groepen van vier hexadecimale cijfers, van elkaar gescheiden met een dubbele punt:

fe80:bdb2:b9ff:d165:2001:3090:a55c:9c47

Indien een groep de waarde 0 heeft, kan dit op drie manieren geschreven worden: als 0000, als 0 of gewoon helemaal niet:

fe80:bdb2:0000:d165:2001:3090:a55c:9c47

fe80:bdb2:0:d165:2001:3090:a55c:9c47

fe80:bdb2::d165:2001:3090:a55c:9c47

Ook meerdere opeenvolgende groepen met de waarde 0 kunnen gewoon weggelaten worden:

fe80:bdb2:0000:0000:0000:0000:a55c:9c47

fe80:bdb2:0:0:0:0:a55c:9c47

fe80:bdb2::a55c:9c47

Dit kan je wel slechts met één reeks groepen binnen een IPv6-adres doen. Het volgende adres is dus fout, omdat je nooit kan weten hoeveel groepen van nullen er op elke plaats moeten komen:

fe80::bdb2::a55c:9c47

Wanneer een groep begint met een waarde 0, mag die gewoon weggelaten worden:

fe80:bdb2:0e13:d165:0001:3090:a55c:9c47

fe80:bdb2:e13:d165:1:3090:a55c:9c47

IPv4 adressen kunnen op een eenvoudige manier geconverteerd worden naar een IPv6-adres. Je zet de vier decimale waarden uit het IPv4-adres om naar een hexadecimale schrijfwijze en groepeer die in twee groepjes van vier hexadecimale tekens. Je laat ze voorafgaan door vijf groepen met de waarde 0 en één groep met de waarde FFFF:

172.16.189.200



0000:0000:0000:0000:0000:ffff:ac10:bdc8

::ffff:ac10:bdc10

Zolang de twee IP-versies naast elkaar bestaan zal het converteren van adressen tussen beide versies noodzakelijk blijven. Het ziet er naar uit dat dat nog wel een tijdje nodig zal zijn. Het tegelijk werken met de twee IP-versies wordt **dualstack** genoemd.

Het toewijzen van IP-adressen in een lokaal computernetwerk en de omzetting naar een MAC-adres verlopen bij IPv6 heel wat eenvoudiger dan bij IPv4. De eerste 64 bits – dit zijn de eerste vier groepen – van het IPv6-adres vormen het netwerknummer. Dat deel van het adres is dus hetzelfde voor elke component in het netwerk. Het laatste deel van het adres vormt het computernummer en daarvoor wordt gewoon het MAC-adres gebruikt, voorafgegaan door een groep. Dat is immers sowieso uniek voor elke netwerkcomponent.

fe80:db2:0000:d165:0001:3090:a55c:9c47

netwerknummer

computernummer

Op deze manier bestaat er in feite geen limiet op het aantal netwerkcomponenten in een lokaal computernetwerk. Bovendien zullen er geen private IP-adressen meer voorzien hoeven te worden – elke computer in een computernetwerk heeft dankzij het gebruik van het MAC-adres een identificatienummer dat uniek is in de wereld. Dat wil zeggen dat elke computer in een netwerk dat geconfigureerd is volgens het IPv6-protocol rechtstreeks toegankelijk is vanuit het internet. Een degelijke beveiliging van de toegang tot het lokale netwerk wordt daardoor alsmaar belangrijker.

IPv6 kent geen verschillende klassen van netwerken. Wel kan een netwerkbeheerder een bedrijfsnetwerk opdelen in verschillende segmenten. In dat geval vormen de eerste 48 bits (de eerste drie groepen) het netwerknummer en worden de volgende 16 bits (de vierde groep) gebruikt om het segment aan te geven.

2.3.2.2 IPX/SPX

IPX/SPX (*internetwork packet exchange / sequenced packet exchange*) was een van de belangrijkste overdrachtsprotocollen, ontwikkeld door de software-firma Novell. Omdat Novell een erg groot marktaandeel had in netwerkbesturingssystemen, groeide het protocol uit tot een standaard. Het protocol bleek echter onvoldoende flexibel voor het gebruik op een niet-hiërarchisch netwerk zoals het internet en werd zo goed als volledig verdrongen door TCP/IP.

Het protocol bestaat uit twee delen:

◆ IPX

IPX zorgt voor de adressering en het versturen van de gegevenspakketten. IPX-adressen voor werkstations op een computernetwerk zijn 32 bits groot en worden hexadecimaal geschreven (bijvoorbeeld 0x48C6D80A). Hosts zoals routers en servers gebruiken een 48-bits adres dat standaard bestaat uit het MAC-adres. Verder lijkt de manier van communiceren via IPX heel erg op IPv4.

◆ SPX

SPX zorgt voor het opdelen van een bericht in gegevenspakketten bewaakt de correcte overdracht ervan. Je kan de functie van het SPX-protocol min of meer gelijk stellen met die van het TCP-protocol van TCP/IP.

SPX is ingekapseld in IPX, dat op zijn beurt is ingekapseld in een toegangsprotocol (meestal Ethernet).

2.3.3 Toepassingsprotocollen

Toepassingsprotocollen zijn actief in de toepassingslaag van het OSI reference model. Ze geven aan voor welke toepassing een ontvangen informatiepakket bedoeld is. In TCP/IP-netwerken wordt daarbij gebruik gemaakt van **poortnummers**. Zo verwijst het poortnummer 80 altijd naar HTTP en poort 23 naar Telnet.

a) HTTP

HTTP (*hypertext transfer protocol*) is het toepassingsprotocol waarmee informatiepagina's (webpagina's) kunnen worden opgevraagd van een webserver op het internet of op een intranet. In TCP/IP-netwerken krijgt dit protocol standaard de poort 80 toegewezen. Wanneer een gebruiker een webpagina wil raadplegen, zal de computer een HTTP-request versturen naar de **URL** (*uniform resource locator*), het webadres van de webpagina. Om dat informatieverzoek bij de juiste webserver te laten terechtkomen, moet die URL eerst nog worden omgezet naar een IP-adres. Dat gebeurt met **DNS** (*domain name system*). Hoe dat precies in z'n werk gaat, leer je in hoofdstuk 6.2.2 van deze cursus.

Wanneer de webserver een HTTP-request ontvangt, zal die de webpagina voor de aanvrager opzoeken. Indien de webpagina gevonden werd, stuurt de webserver een response met daarbij alle informatie van die webpagina: tekst, afbeeldingen, scripts, enz. Die informatie wordt vervolgens weergegeven in de browser van de gebruiker. Soms kan de webserver aan de informatievraag niet voldoen. In dat geval stuurt de webserver een foutcode naar de aanvrager. Ontwikkelaars van websites kunnen voor zo'n foutcode een eigen pagina ontwerpen die de gebruiker van de fout informeert. Als zij dat niet doen, wordt de standaard foutcode weergegeven in de browser. De meest voorkomende fouten in HTTP-communicatie zijn:

◆ 403 Forbidden

De webpagina bestaat wel maar kan niet worden getoond omdat ze zich bijvoorbeeld bevindt in een map die niet publiek is.

◆ 404 Not Found

De gevraagde webpagina bestaat niet op de website. Mogelijk heeft de gebruiker een fout gemaakt in de URL of heeft de beheerder van de website de pagina verwijderd.

◆ 405 Not Allowed

De gebruiker is niet gemachtigd om de pagina te raadplegen omdat die bijvoorbeeld deel uit maakt van een deel van de website waarvoor autorisatie vereist is.

◆ 500 Internal Server Error

Er is een fout opgetreden in de verwerking van de actieve inhoud van de pagina, bijvoorbeeld omdat er een fout staat in een script.

HTTPS (*hypertext transfer protocol secure*) is een doorontwikkeling van HTTP met het doel om informatiepakketjes die via het HTTP-protocol over het internet verstuurd worden te beveiligen met **encryptie**. Op die manier kunnen pakketjes die onderweg onderschept worden niet gelezen worden. Dat was een noodzakelijke voorwaarde om op een veilige manier betalingen uit te voeren via websites, of om gegevens te beveiligen op websites waarop informatie staat met een erg persoonlijk karakter, zoals sociale media of webgebaseerde e-mail diensten.

Voor de encryptie van beveiligde websites wordt het **SSL**-protocol (*secure socket layer*) gebruikt. SSL is een protocol uit de presentatielaag van het OSI reference model. Beveiligde webpagina's zijn eigenlijk gewone HTTP-informatiepagina's die door het onderliggende SSL-protocol worden versleuteld. Zo herken je een beveiligde website:

Een icoontje met een hangslot wordt getoond in de buurt van de adresregel van je browser of in de statusbalk. Wanneer je op dit icoontje klikt worden de details van de gebruikte encryptietechniek en het beveiligingscertificaat weergegeven.



Soms wordt ook de eigenaar van het beveiligingscertificaat weergegeven.

De URL begint met *https* in plaats van *http*.

HTTP is al vrij oud. De eerste versie dateert van 1991, de meest recente van 1999. Ondertussen zijn websites heel wat complexer geworden, zonder dat het HTTP-protocol mee geëvolueerd is. Zo kan een webpagina samengesteld zijn uit informatie die in verschillende bestanden bewaard worden (tekst, afbeeldingen, scripts, css, bewegende beelden...). Voor elk apart stukje informatie moet een aparte HTTP-verbinding worden gemaakt. Dat zorgt voor een grote overhead aan verstuurd informatie die niet rechtstreeks met de inhoud te maken heeft. Bovendien vertraagt dat het inladen van de webpagina.

Sinds enkele jaren werkt het internetbedrijf Google daarom aan een nieuwe protocol met de naam **SPDY** (geen afkorting, spreek uit als het Engelse woord *speedy*). Daarmee is zelfs voor complex samengestelde webpagina's slechts één verbinding nodig. Dat is efficiënter en gaat sneller. SPDY is voornamelijk nog geen officiële standaard maar wordt toch al op beperkte schaal geïmplementeerd. Je kan gebruik maken van SPDY wanneer de beheerder van een website die mogelijkheid aanbiedt en wanneer je browser het nieuwe protocol ondersteunt. In dat geval zal automatisch voor het snelste protocol gekozen worden. Als computergebruiker merk je daar niets van.

b) SMTP, POP3 en IMAP

SMTP (*simple mail transfer protocol*) is een protocol dat standaard gebruikt wordt voor het verzenden van e-mail. In TCP/IP-netwerken gebruikt dit protocol standaard de poort 25. Het is een erg eenvoudig en behoorlijk oud protocol, dat gebaseerd is op de ASCII-code – niet-opgemaakte tekst dus. In de beginnende jaren van het internet was dat ook voldoende, maar ondertussen al lang niet meer. Voor het versturen van een e-mail met tekst of afbeeldingen of van een bijlage bij een e-mail wordt gebruik gemaakt van **MIME** (*multipurpose internet mail extensions*), een techniek die opmaakmerken en niet-ASCII-tekens converteert naar ASCII-tekens vooraleer een bericht wordt verzonden. Bij de afzender worden

die geconverteerde tekens dan weer omgezet naar hun oorspronkelijke vorm. Op die manier kunnen toch bijlagen en tekstopmaak verzonden worden via het tekstgebaseerd SMTP-protocol.

Een ander nadeel van SMTP is dat het de betrouwbaarheid van de afzender niet controleert. Daardoor kan een fictief e-mailadres worden gebruikt bij het verzenden van een bericht, en dat is de reden waarom spam zo'n plaag is geworden. Men zou kunnen opperen dat het mogelijk moet zijn om al die nadelen op te lossen met de ontwikkeling van een nieuw, moderner protocol, maar SMTP is al te wijd verspreid en te goed ingeburgerd om gemakkelijk vervangen te worden.

E-mail is een combinatie van push en pull: de verzender neemt het initiatief en verzendt het bericht (**push**). Omdat het nooit zeker is of de computer van de bestemming ingeschakeld en verbonden is met het internet, wordt het bericht afgeleverd op de mailserver van de ontvanger. Daar wordt het bericht bewaard tot de ontvanger zelf het initiatief neemt om het bericht op te halen (**pull**). SMTP staat in voor het push-gedeelte van de communicatie. Berichten lezen doe je via POP3 of IMAP.

Van die twee is **POP3** (*post office protocol versie 3*) veruit het meest gebruikte. In TCP/IP-netwerken gebruikt dit protocol standaard de poort 110. Het protocol werd zo ontworpen dat de ontvanger van e-mail niet permanent met de mailserver van zijn provider in verbinding moet staan. De ontvanger maakt slechts even een verbinding en controleert of er nieuwe berichten klaarstaan. Die berichten worden dan opgehaald en lokaal opgeslagen op de computer van de ontvanger. Op de mailserver kunnen de opgehaalde berichten daarna verwijderd worden, alhoewel sommige providers ze om wettelijke redenen nog een beperkte tijd bewaren.

Bij **IMAP** (*internet message access protocol*) verloopt dat anders: daar worden berichten niet eerst lokaal gedownload, maar leest de ontvanger ze rechtstreeks op de mailserver. Dat heeft als grote voordeel dat je de berichten vanuit eender welke locatie kan lezen, een mailbox met meerdere mensen kan delen en dat je geen actie moet ondernemen om een nieuwe e-mail te zien verschijnen in je mailbox - die verschijnt immers automatisch. IMAP is een veel complexer protocol dan POP3 en de meeste providers bieden die mogelijkheid niet aan. In TCP/IP-netwerken gebruikt dit protocol standaard de poort 143 (onbeveiligd) en poort 993 (beveiligd).

c) FTP

Met **FTP** (*file transfer protocol*) kan je bestanden versturen van en naar een FTP-server op het internet. Dat kunnen eender welke soort bestanden zijn, zolang de FTP-server ze maar aanvaardt. FTP maakt in TCP/IP-netwerken gebruik van poort 20 voor de gegevensoverdracht en poort 21 voor het beheer van de verbinding. FTP bestaat zowel anoniem als met authenticatie. In het tweede geval moet de gebruiker een inlognaam met een paswoord hebben op de FTP-server. Bij anonieme FTP hoeft dat niet, maar dat geeft meestal slechts beperkte toegang tot het systeem.

Voor de komst van *bittorrent*-websites werd FTP vaak gebruikt om bestanden al dan niet illegaal van het internet te downloaden. Dat gebeurde doorgaans anoniem. Web ontwikkelaars gebruiken FTP om de bestanden van hun website te uploaden naar de webserver. Computerprogramma's die men hiervoor gebruikt, worden FTP-clients genoemd.

Standaard gebruikt FTP geen beveiliging. Communicatie via FTP kan dus onderschept en gelezen worden door derden. Met **FTPS** (*file transfer protocol secure*) kan een verbinding wel beveiligd worden met encryptie. In feite gaat het dan om een gewone FTP-verbinding die bovenop het **SSL**-protocol (*secure sockets layer*) draait.

d) Telnet, SSH, RDP

Telnet (*teletype network*) is een protocol dat het mogelijk maakt om vanop afstand toegang te krijgen tot een computersysteem op het netwerk en de besturing van dat systeem over te nemen. Het is een van de oudste communicatieprotocollen op het internet. In TCP/IP-netwerken maakt Telnet gebruik van poort 23. Omdat het protocol geen enkele vorm van beveiliging kent, wordt het nog weinig gebruikt, tenzij door netwerkbeheerders bij het uittesten van bepaalde netwerkfuncties.

SSH (*secure shell*) is een moderner protocol uit de UNIX/Linux-wereld met dezelfde functie, maar met de mogelijkheid om de verbinding te beveiligen met encryptie. Standaard maakt dit protocol gebruik van poort 22 in TCP/IP-netwerken. Toch wordt voor remote login – het op afstand besturen van een computer – tegenwoordig veel vaker gebruik gemaakt van **RDP** (*remote desktop protocol*), een niet-openbaar protocol dat door Microsoft werd ontwikkeld. Andere softwareontwikkelaars hebben RDP ook gebruikt, waardoor het protocol tegenwoordig ook clients kent voor andere besturingssystemen dan Windows.

e) SNMP

SNMP (*simple network management protocol*) is een veel gebruikt protocol voor netwerkbeheer en maakt in TCP/IP-netwerken gebruik van poort 161. Met behulp van dit protocol kunnen netwerkbeheerders elke netwerkcomponent met een IP-adres controleren om met die informatie het netwerk te optimaliseren. Het programma dat de beheerder daarvoor gebruikt wordt de SNMP-manager genoemd, de netwerkcomponenten heten dan agents.

De SNMP-manager verzamelt voortdurend gegevens over het netwerkverkeer van en naar de agents. Die gegevens worden ingedeeld volgens een gegevensbestand dat de **MIB** (*management information base*) wordt genoemd. De gegevens zelf worden in logbestanden bewaard. Al naargelang de instellingen en de mogelijkheden maakt de SNMP-manager grafieken of slaat alarm.

Het uitwisselen van informatie tussen de SNMP-manager en de agents gaat door middel van **requests** (verzoeken). Op een request van de manager zal de agent antwoorden met een **response** met daarin de gevraagde gegevens. In de meeste SNMP-omgevingen loopt een manager met een zekere interval (bijvoorbeeld elke twee minuten) alle agents af. Een agent hoeft echter niet altijd te wachten op de request van de manager om zelf bijvoorbeeld een fout te melden. Dat gebeurt met SNMP trap-commando's.

Een van de grootste nadelen van SNMP is dat het protocol niet erg goed beveiligd is. De SNMP-requests zelf zijn wel beveiligd met een wachtwoord, maar de requests kunnen door hackers gekaapt worden, waarna de hacker ze kan vervangen door zijn eigen requests. Op die manier kunnen hackers de werking van een volledig netwerk ontregelen.

3 Netwerkhardware

*Waarin je leert dat er heel wat apparatuur nodig is
om een werkbaar netwerk aan te leggen.*

In dit hoofdstuk leer je dit:

- ◆ De kenmerken van netwerkkarten
- ◆ De algemene kenmerken van netwerkbekabeling
- ◆ De bouw en kenmerken van een coaxiale kabel
- ◆ De bouw en kenmerken van een twisted pair kabel
- ◆ Een netwerkkabel zelf op maat maken
- ◆ De bouw en werking van WiFi (draadloos netwerk)
- ◆ De kenmerken van alternatieve draadloze verbindingen: IrDA, SWAP, bluetooth en WUSB.
- ◆ De kenmerken en werking van een repeater
- ◆ De kenmerken en werking van een hub
- ◆ De kenmerken en werking van een switch
- ◆ De configuratie van een switch controleren en aanpassen
- ◆ De kenmerken en werking van een bridge
- ◆ De kenmerken en werking van een router
- ◆ De kenmerken en werking van een network access point
- ◆ De configuratie van een NAP controleren en aanpassen
- ◆ Een netwerkdiagram opstellen

3.1 Netwerkkarten

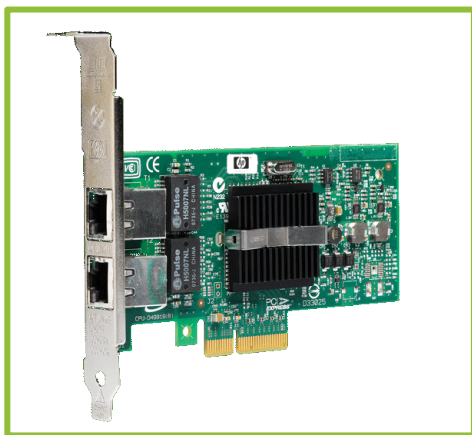
De netwerkkart (ook: network adapter, **NC**, *network card*, networking interface, **NIC**, *network interface card*) vormt de brug tussen een computer en het netwerk. Niet alleen zorgt de netwerkkart voor een fysieke aansluiting, maar ook voor de identificatie van de computer op het netwerk. Het MAC-adres, het unieke identificatienummer van een netwerkcomponent, bevindt zich immers op een ROM-chip van de netwerkinterface. Dat betekent dat een computer die beschikt over twee netwerkkarten twee MAC-adressen heeft.

Desktopcomputers beschikken standaard over een netwerkaansluiting voor een bekabeld netwerk. Laptops hebben die meestal ook maar beschikken bovendien over een ingebouwde draadloze netwerkmodule. In beide gevallen zijn de netwerkinterfaces op het moederbord geïntegreerd. Je hebt dan geen aparte netwerkkart meer nodig.

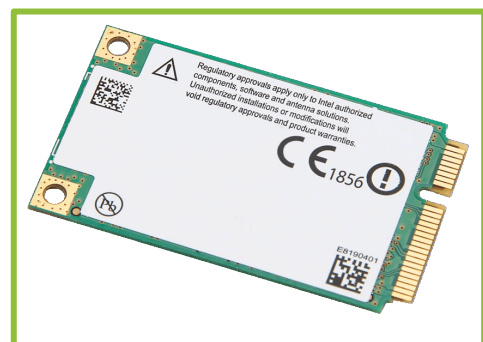
Wanneer je desktop computer standaard niet over een netwerkaansluiting beschikt of indien je een tweede netwerkaansluiting nodig hebt, kan je gebruik maken van een aparte **netwerkinterface**. Die bestaan in verschillende vormen:

♦ Uitbreidingskaarten

Zowel draadloze netwerkkarten als netwerkkarten voor bekabelde netwerken bestaan in de vorm van standaard insteekkaarten voor **PCI-express**. Voor oudere computers bestonden ook uitbreidingskaarten voor klassieke PCI-sloten. Insteekkaarten voor draadloze netwerken beschikken doorgaans over een externe antenne om een betere ontvangst van de draadloze signalen te bekomen.



Moderne laptops beschikken steeds over een draadloze netwerkkart, maar indien dat niet het geval is, of indien die ingebouwde draadloze netwerkkart stuk is, kan je gebruik maken van kleine insteekkaartjes voor **mini-PCI** en **mini-PCI-express** sloten. De laptop moet dan wel uitgerust zijn met een interne antenne – dit zijn een of twee kabeltje die in de behuizing van het beeldscherm zijn weggestoken en die je kan verbinden met het netwerkkartje.



♦ USB-adapters

Indien je draadloze verbinding wil maken met een computer die niet over een geïntegreerde draadloze netwerkkaart beschikt, kan je gebruik maken van een **USB-adapter**. Dat is een klein stickje dat je in een USB-poort kan steken. Voordelen zijn dat dit past op zowel laptops als desktops en dat een computer niet moet openmaken om een insteekkaart te monteren. Het nadeel is dat zo'n USB-adapter niet uitgerust is met een degelijke externe antenne. In vergelijking met een insteekkaart is de ontvangst van het draadloze signaal daarom doorgaans zwakker. Bovendien neem je met zo'n adapter een USB-poort op je computer in.



Een nieuwe ontwikkeling is een **SD-geheugenkaartje** met een ingebouwde draadloze adapter. Daarmee kan je foto's of andere bestanden van een digitale camera draadloos overbrengen naar een computer die ook over een draadloze netwerkadapter beschikt. Het is zelfs mogelijk om ze rechtstreeks vanuit je camera te uploaden naar het internet, bijvoorbeeld naar Facebook. De instellingen daarvoor kan je naar je hand zetten met je computer via een USB-adapter waarin je het kaartje kan schuiven.

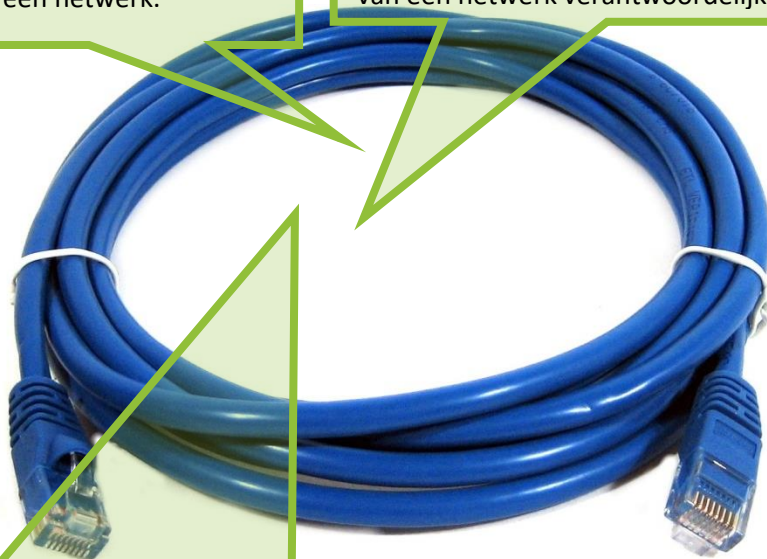
3.2 Transmissiemedia en connectoren

3.2.1 Kenmerken van netwerkbekabeling

De bekabeling in een netwerk zorgt voor het overbrengen van de gegevens. Het ganse netwerk wordt meestal opgebouwd met dezelfde kabelsoort, maar noodzakelijk is dat niet.

De bekabeling beslaat slechts 5 tot 10 procent van de totale kost voor het uitbouwen van een netwerk.

Toch wordt geschat dat fouten in de bekabeling voor meer dan de helft van de tijd van inactiviteit van een netwerk verantwoordelijk is.



De bekabeling is de component die het minst aan slijtage onderhevig is en dus ook het langst meegaat. Dat kan belangrijk zijn bij de keuze van de kabel wanneer je een netwerk aanlegt.

Plenum

Kabels worden vaak getrokken door verluchttingsholtes in gebouwen. Wanneer zo'n kabel verbrandt, kunnen de giftige gassen die vrijkomen bij de verbranding van het isolatiemateriaal in en rond de kabel zich via die holtes makkelijk verspreiden doorheen het hele gebouw. Daarom wordt voor kabels die in dergelijke holtes worden aangebracht materiaal gebruikt dat bij verbranding geen giftige gassen vrijgeeft. Dergelijke kabels zijn een flink stuk duurder dan niet-plenum kabels.

Niet-plenum

Dit soort kabels geeft wel giftige gassen vrij bij verbranding, omdat er materialen gebruikt worden als PVC. Ze worden echter vaker gebruikt als losse netwerkkabels omdat ze flink goedkoper zijn. Bovendien zijn ze buigzamer dan plenum-kabels.

Sinds 1991 bestaat er een internationaal aanvaarde standaard voor de kwaliteitsnormen en werkingseisen waaraan de verschillende bekabelingstypes moeten voldoen voor netwerken. Die norm werd in 1995 herzien en staat bekend onder de naam **Commercial Building Telecommunications Cabling Standard (ANSI/TIA-568-A)**. Bekabeling die aan deze norm voldoet, garandeert een levensduur van minstens 10 jaar.

3.2.2 Coaxiale kabel

Vanwege de lagere transportsnelheid en de kwetsbaarheid wordt coaxiale kabel (meestal afgekort tot coax-kabel) niet meer vaak gebruikt.

Een coaxiale kabel bestaat uit een koperen kern, omgeven door isolatiemateriaal (PVC of Teflon) waarrond een geleidende mantel is aangebracht. Deze isolatie is gevat in een geleider in de vorm van een dicht vlechtwerk. Dit vlechtwerk voorkomt **elektromagnetische interferentie** van verlichting, motoren, computers, elektrische toestellen, enz.

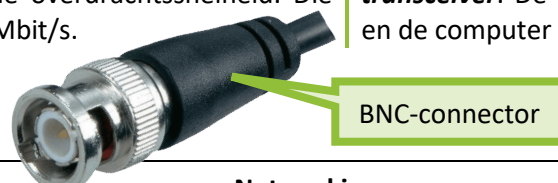


Thinnet coax

Thinnet coax (technische specificatie 10Base-2) is een buigzame RG-58-kabel met een doorsnede van 0,25 inch (6,35mm). Met behulp van een T-stuk en **BNC**-stekker (*British Naval Connector of Bayonet-Neill-Cancelman*) wordt de coaxiale kabel rechtstreeks aangesloten op de netwerkkaart. Zonder versterking is het maximale bereik van de kabel 185 meter. De maximale overdrachtssnelheid is afhankelijk van de lengte van de kabel. Hoe korter de kabel, hoe groter de overdrachtssnelheid. Die bedraagt maximaal 10 Mbit/s.

Thicknet coax

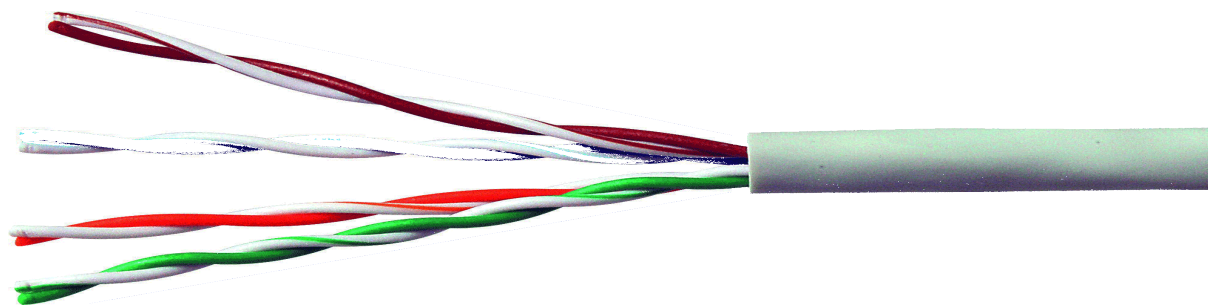
Thicknet coax (10Base-5) is een onbuigzame RG-62-kabel van 0,5 inch (12,7mm). Deze kabelsoort wordt vooral gebruikt als backbone om verschillende netwerken over een afstand van enkele kilometers met elkaar te verbinden. De maximale overdrachtssnelheid bedraagt 500 Mbit/s. Zo'n kabel kan je niet rechtstreeks verbinden met een computer. Dat gebeurt met een **transceiver**. De kabel tussen de transceiver en de computer wordt **dropcable** genoemd.



Indien verschillende coax-kabels tegen elkaar aan worden gelegd, kan **crosstalk** optreden. Dat is een probleem waarbij het signaal van de ene kabel de andere beïnvloedt. Soms wordt dit wel eens voorgesteld alsof het signaal van de ene kabel volledig wordt overgenomen door de andere, maar dit klopt niet. Wel leidt crosstalk tot een vervorming van het signaal, wat bij overdracht van digitale gegevens tot gegevensverlies leidt.

3.2.3 Twisted pair

Twisted Pair bestaat uit twee geïsoleerde koperdraden van ongeveer 1 mm dikte, die **spiraalsgewijs** om elkaar gewonden om zijn om elektromagnetische interferentie tegen te gaan. Het aantal omwindingen per meter is afhankelijk van de categorie van de kabel. Hoe groter dat aantal, hoe kleiner de kans is op crosstalk. In een twisted pair kabel voor computernetwerken zijn er vier paren van twee draden voorzien. Gegevenstransport over een dergelijke kabel is beperkt tot 100 meter.



UTP	FTP
UTP (<i>unshielded twisted pair</i>) is een niet-afgeschermd gevlochten koperdraad, vergelijkbaar met een gewone telefoondraad. Ze is de algemeen gebruikte standaardkabel voor lokale netwerken.	FTP (<i>foiled twisted pair</i>) is een gewone UTP-kabel waarbij rond de vier aderpairs samen een beschermende folie is aangebracht om magnetische interferentie van buitenaf tegen te gaan – iets minder efficiënt dan bij STP, maar ze kunnen goedkoper geproduceerd worden.

STP
Bij STP (<i>shielded twisted pair</i>) zijn de aderpairs afgeschermd door een metalen mantel, vervaardigd uit een soort aluminiumfolie. Dit voorkomt storingen op de pairs door bronnen buiten de kabel. Deze soort kabel is duurder dan UTP en wordt vooral gebruikt in omgevingen waar er heel wat interferentie mogelijk is, zoals in ziekenhuizen en in industriële omgevingen. Dit type van kabel werd eveneens gebruikt in token-ring netwerken.

De verschillende snelheden die met twisted pair kabels kunnen bereikt worden, werden vastgelegd in Ethernet-specificaties:

10BASE-T	Overdrachtssnelheden tot 10 Mbit/s (<i>voice-grade Ethernet</i>)
100BASE-T	Overdrachtssnelheden tot 100 Mbit/s (<i>fast Ethernet</i>)
1000BASE-TX	Overdrachtssnelheden tot 1 Gbit/s (<i>gigabit Ethernet</i>)
10GBASE-TX	Overdrachtssnelheden tot 10 Gbit/s (<i>10 gigabit Ethernet</i>)

Twisted pair-kabels zijn in verschillende kwaliteitsklassen of categorieën beschikbaar, afhankelijk van het gebruik en van de overdrachtssnelheid. De standaarden voor die verschillende klassen werden vastgelegd door de **EIA** (*Electronic Industries Association*) en de **TIA** (*Telecommunications Industries Association*).

CAT1	Kabels voor het transport van spraaksignalen in oude telefoonsystemen. Kabels van deze categorie zijn niet geschikt voor datacommunicatie.
CAT2	Kabels die geschikt zijn voor gegevensoverdracht aan een relatief lage snelheid (4 Mbit/s) en gebruikt op oudere token-ring en token-bus netwerken.
CAT3	Kabel die beter gekend is voice-grade. Ze is geschikt voor overdrachtssnelheden tot 10 Mbit/s en werd veel gebruikt voor oudere Ethernet 10-base T-netwerken.
CAT4	Kabel die geschikt is voor overdrachtssnelheden tot 16 Mbit/s en eveneens in oudere Ethernet en token-based netwerken gebruikt werd.
CAT5	De standaard kabel voor Ethernet 100Base-T met overdrachtssnelheden tot 100 Mbit/s.
CAT5E	Een op categorie 5 gebaseerd kabeltype dat aangepast werd om ook gigabit Ethernet toe te laten.
CAT6	Speciaal ontwikkeld voor gigabit Ethernet met minder signaalverlies dan de categorie 5E op langere afstanden.
CAT6A	Een op categorie 6 gebaseerd kabeltype dat aangepast werd om ook 10 gigabit Ethernet toe te laten.
CAT7	Speciaal ontwikkeld voor 10 gigabit Ethernet waarbij de vier paren apart afgeschermd worden (STP).

Een twisted pair-kabel wordt met een netwerkcomponent (netwerkaart, hub, switch...) verbonden door middel van een RJ-45 stekker. RJ staat voor "*Registered Jack*", een benaming die gebruikt wordt voor stekkers voor telecommunicatiedoeleinden.

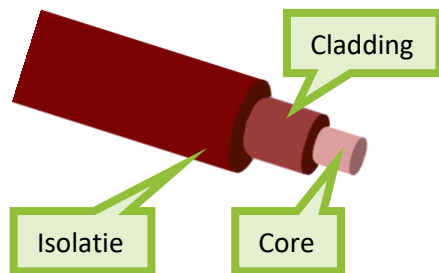


3.2.4 Glasvezelkabel

Bij glasvezelkabel (*fiber optic cable*) wordt er geen elektrisch signaal over de kabel verstuurd, maar worden de binaire waarden 1 en 0 omgezet in **optische signalen** – licht dus. Daardoor is glasvezelkabel ongevoelig voor elektromagnetische interferentie en wordt ze vaak ingezet in industriële omgevingen waar de kans op dergelijke interferentie groot is, zoals in de buurt van hoogspanningscabines. Er kunnen overdrachtssnelheden tot 10 Gbit/s over afstanden van enkele kilometers ver bereikt worden.

Een laatste, niet onbelangrijk voordeel is de veiligheid die glasvezelkabel biedt tegenover bekabeling gebaseerd op koper. Het is immers fysiek onmogelijk om illegaal gegevens af te tappen van een glasvezelkabel omdat die daarvoor zou moeten onderbroken worden, wat onmiddellijk opgemerkt wordt.

Nadelen van glasvezel zijn de hoge productiekostprijs en het feit dat een kabelbreuk zeer moeilijk te herstellen is. Werken aan een glasvezelkabel is trouwens echt specialistenwerk, dat niet voor de doorsnee netwerkbeheerder weggelegd is.



Een glasvezelkabel bestaat uit een dunne cilinder van glas (*de core of kern*), die op zijn beurt door glas of plastic omgeven is (*de cladding of mantel*). Daarrond zit een *isolatie* van Kevlar. Om gegevensverkeer in twee richtingen mogelijk te maken, moet een glasvezelkabel voorzien zijn van minstens twee cilinders. Meestal beschikt een glasvezelkabel over meerdere cilinders, die men dan samen een **bundel** noemt.

Het gebruik van glas voor kabels lijkt een beetje vreemd. Normaal is glas erg broos, maar wanneer het gesmolten is en er dunne draden van getrokken worden (zoals glasvezel) dan is het sterk en buigzaam.

Er bestaan twee manieren om lichtsignalen door een glasvezelkabel te sturen:

♦ Single mode fiber

Het optische signaal beweegt zich lineair in de as van de kabel voort. Hierbij wordt meestal een **ILD** (*injection laser diode*) als lichtbron gebruikt.



Dit soort glasvezelkabel staat hogere overdrachtssnelheden toe dan multimode kabels en kan grotere afstanden overbruggen, maar de kabel is aanzienlijk duurder. De cilinders in single mode kabels zijn veel dunner dan in multimode kabels. Ze worden voornamelijk gebruikt als backbone voor langeafstandsverbindingen.

♦ Multimode fiber

Hierbij worden meerdere optische signalen onder verschillende hoeken door de kabel gestuurd. Het lichtsignaal plant zich voort door te reflecteren tegen de wanden van de cilinder. Meestal wordt hierbij gebruik gemaakt van een **LED** (*light emitting diode*) als lichtbron.



Multimode kabels hebben een hogere bandbreedte dan een single mode kabel, maar een lagere overdrachtssnelheid. Ook de overbrugbare afstand is kleiner. Vanaf een bepaalde afstand (hooguit een kilometer) kunnen verschillende lichtpulsjes elkaar immers beginnen verstoren. Dat fenomeen wordt **straalverstrooiing** of *modal dispersion* genoemd. Bovendien wordt de intensiteit van het signaal door het reflecteren tegen de wand verzwakt. Daarom wordt multimode glasvezelkabel enkel gebruikt voor kortere verbindingen, zoals tussen twee bedrijfsgebouwen op dezelfde campus.

In Vlaanderen en Nederland bestaat een sterk uitgebouwd glasvezelnetwerk en is het medium erg populair voor breedband internetverbindingen. De glasvezelkabel wordt doorgaans niet tot aan de abonnees gelegd, maar vormt de verbinding tussen een node – een centraal distributiepunt in een wijk – en de provider. Van uit de nodes wordt het signaal verder naar de individuele gebruikers getransporteerd via een gewone distributiekabel. Omdat de vraag naar supersnel internet voortdurend toeneemt, bieden enkele providers toch al glasvezelverbindingen aan tot bij de deur. Dat wordt dan **FTTH** (*fibernet to the home*) genoemd.

3.2.5 Powerline communicatie

Powerline communicatie (kortweg **PLC**, ook **BPL**, *Broadband over Powerline* of Homeplug) staat voor het overdragen van netwerksignalen over het elektriciteitsnet binnen een gebouw. Daarvoor werden adapters ontwikkeld die je in het stopcontact kan steken en via USB, met een UTP-kabel of draadloos met de computer verbindt.

Elk gebouw is voorzien van stopcontacten in de verschillende ruimtes. Door gebruik te maken van de **vrije frequenties** op het stroomnet, vermijd je dat je doorheen het hele gebouw netwerkbekabeling moet leggen. Om geen interferentie met de elektrische stroom over het stroomnet te krijgen, wordt het digitale signaal opgesplitst in verschillende parallelle banden, die gebruik maken van frequenties die weinig beïnvloed worden door de elektrische stroom. De modulatietechniek die daarvoor gebruik wordt heet **OFDM** (*orthogonal frequency division multiplexing*). Powerline communicatie vormt eveneens de basis voor vele domotica-systemen – dat zijn systemen waarmee je allerlei functies in je huis, zoals verwarming, verlichting en verluchting, vanop een computer kunt besturen.



De maximale doorvoersnelheid voor powerline communicatie is aanzienlijk lager is dan die voor UTP-netwerken. Toch is dat ruim voldoende voor gewone thuisnetwerken en daarvoor is PLC in de eerste plaats bedoeld. Fabrikanten van PLC apparatuur beloven vaak snelheden van enkele honderden Mbit/s, maar in de praktijk valt dat toch erg tegen. Dat heeft vooral te maken met netspanningsvervuiling op het elektriciteitsnet, de te

overbruggen afstand en het gebruikte netwerkprotocol.

De maximale afstand die door de ontwikkelaars wordt opgegeven bedraagt 200 meter, al is het zelfs mogelijk om grotere afstanden te overbruggen indien de kwaliteit van de elektrische installatie in het gebouw goed genoeg is. Nog een beperking is het aantal aansluitbare netwerkapparaten. In theorie is het mogelijk tot 253 apparaten in het netwerk te brengen, maar in de praktijk houdt het op bij een tiental.

De beveiliging van een powerline netwerk is erg belangrijk, aangezien een hacker zou kunnen inbreken door in eender welk stopcontact in te pluggen. Voor de beveiliging van de communicatie via stroomkabels wordt encryptie gebruikt. Bovendien stopt het signaal in principe aan de elektriciteitsmeter, zodat het netwerkverkeer het gebouw niet verlaat – dat houden de fabrikanten van powerline adapters toch voor.

3.2.6 WiFi

Radiofrequenties zijn erg dankbaar voor het opzetten van draadloze netwerken. Ze worden weinig gehinderd door obstakels en afhankelijk van het vermogen van de zender en de gevoeligheid van ontvanger varieert het bereik van enkele tientallen tot enkele honderden meters. De overdrachtssnelheid komt tegenwoordig in de buurt van bekabelde netwerken maar is sterk afhankelijk van de afstand tussen zender en ontvanger. Wireless LAN maakt gebruik van een licentievrije frequentie van 2,4 GHz (**UHF**, *ultra high frequency*), al bestaat er ook apparatuur die gebruikt van de 5 GHz band (**SHF**, *super high frequency*). Moderne apparatuur voor draadloze netwerken zijn meestal dualband. Ze kunnen dus met beide frequenties overweg.

Wireless LAN maakt het mogelijk om met dezelfde protocollen te werken als een bekabeld netwerk, waardoor beide perfect geïntegreerd kunnen worden. De standaarden voor draadloze communicatie

werden internationaal vastgelegd in de **IEEE 802.11** norm. Deze norm staat in de computerwereld beter bekend onder de naam WiFi – hoewel nooit officieel een letterwoord, tegenwoordig algemeen aanvaarde afkorting voor *Wireless Fidelity* – en er ontstonden in de loop van ren verschillende standaarden:

802.11	2 Mbit/s	Eerste versie, gestandaardiseerd in 1997.
802.11b	11 Mbit/s	Eind 1999 goedgekeurde standaard op 2,4 GHz en de eerste die algemene verspreiding kende. Ondanks standaardisatie was het nog niet vanzelfsprekend dat apparatuur van verschillende fabrikanten met elkaar kon communiceren.
802.11a	54 Mbit/s	Deze standaard zag samen met 802.11b het levenslicht maar werkt op 5 GHz. Bovendien wordt het signaal gemakkelijker verstoord door obstakels tussen zender en ontvanger. Wellicht daardoor werd de standaard nooit erg populair.
802.11g	54 Mbit/s	In 2003 de opvolger van de 802.11b standaard voor hogere snelheden. Werkt met de apparatuur die compatibel is met 802.11b.
super-g	108 Mbit/s 125 Mbit/s	Technologie verwant aan de 802.11g-standaard, maar met een dubbele bandbreedte dankzij een techniek die channel bonding wordt genoemd (het koppelen van verschillende kanalen). Helaas is het niet altijd compatibel met bestaande apparatuur.
802.11n	300 Mbit/s 600 Mbit/s	Opvolger voor 802.11g vanaf 2009, compatibel met oudere standaarden en werkend zowel op 2,4 GHz als 5 GHz.
802.11ac	> 1 Gbit/s	Nieuwe standaard in 2013, die enkel werkt op 5 GHz.

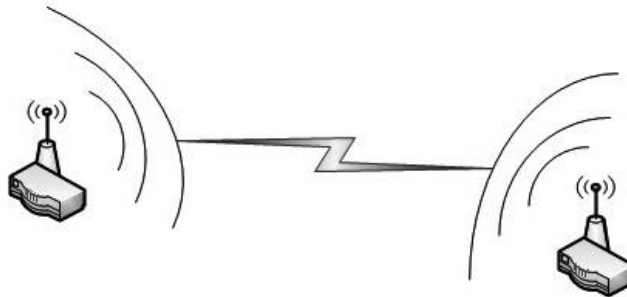
De snelheden die in de tabel vermeld staan zijn theoretische snelheden: in de praktijk worden ze nooit gehaald. Vaak liggen de reële doorvoersnelheden ver beneden de helft van deze theoretische snelheid omwille van afstand, obstakels, interferentie met andere apparatuur (zoals microgolfovens of draadloze binnenhuistelefoons) en protocol-overhead. Met dat laatste worden de signalen bedoeld die zender en ontvanger voortdurend met elkaar uitwisselen om een verbinding te onderhouden. Die signalen nemen een deel van de bandbreedte van de verbinding in beslag en beperken dus de reële overdrachtssnelheid. Een plaats in een gebouw waar de signalen zo zwak zijn dat je geen werkbare communicatie meer tot stand kunt brengen, wordt een **deadspot** genoemd.

Om gebruik te maken van draadloze netwerken, dienen de aangesloten computers uitgerust te zijn met een netwerkkaart met een WiFi-chip. Om het draadloze signaal zo goed mogelijk te kunnen opvangen, is zo'n netwerkkaart meestal uitgerust met een antenne. Dat kan een externe antenne zijn zoals bij in steekkaarten voor desktop computers, maar bij draagbare apparatuur zoals laptops, tablets en smartphones is zo'n antenne intern. De draadloze netwerkkaart ontvangt het signaal van een basisstation dat verbonden is met een bekabeld netwerk. Zo'n basisstation wordt een **NAP** (*network access point*) genoemd. Je leert er meer over in hoofdstuk 3.3.5 van deze cursus.

Vaak vind je draadloze toegangen in bedrijven, openbare gebouwen, scholen en universiteiten, zodat werknemers, klanten of studenten met hun laptop rechtstreeks op het internet kunnen. Openbare plaatsen waar dit kan worden **hotspots** genoemd.

Draadloze netwerken geven hackers de mogelijkheid om van op afstand toegang te krijgen tot het netwerk. Daarom is een degelijke beveiliging van een draadloos netwerk erg belangrijk. Je leert meer over het beveiligen van draadloze netwerken in hoofdstuk 5.2 van deze cursus.

Het bereik van een draadloos netwerk is beperkt. Wanneer je een grotere afstand wil overbruggen, kan dat eventueel met **WDS** (*wireless distribution system*, ook wireless bridge genoemd), waarmee verschillende draadloze basisstations aan elkaar gekoppeld kunnen worden. WDS kent echter geen universele standaard, waardoor basisstations van verschillende merken vaak niet met elkaar kunnen communiceren. Bovendien zijn de goedkopere access points niet uitgerust om WDS te ondersteunen. Tenslotte heeft een WDS doorgaans ook een negatief effect op de beschikbare bandbreedte.



Een aparte discussie met betrekking tot draadloze netwerken is het gezondheidsdebat. Er bestaan vermoedens dat de WiFi-straling op lange termijn schadelijk kan zijn voor de gezondheid, hoewel dit voorlopig nog door geen enkele studie onomstotelijk kon worden bewezen. Dat deelt deelnemers aan dit debat al snel op in "*believers*" en "*non-believers*". De waarheid ligt vermoedelijk ergens in het midden: een grote meerderheid zal nooit gevolgen ondervinden van WiFi-straling, maar voor wie erg gevoelig is aan straling valt het wellicht af te raden om lang in de buurt van een access point voor draadloos netwerk te verblijven.

3.2.7 Alternatieve draadloze verbindingen

Om apparaten lokaal met elkaar te laten communiceren bestaan er nog tal van andere draadloze technieken. Die zijn minder geschikt voor het verbinden van computers met een lokaal netwerk – niet alleen omdat de overdrachtssnelheden veel lager liggen, maar ook omdat de gebruikte protocollen niet compatibel zijn met de heersende communicatieprotocollen. Voor draadloze computernetwerken blijft WiFi dus aangewezen.

f) IrDA (infrared direct access)

IrDA (*infrared direct access*) maakt gebruik van infrarood lichtpulsen om apparaten met elkaar te laten communiceren. Theoretisch zijn snelheden tot 4 Mbit/s mogelijk.

Het grootste probleem voor deze technologie is dat de zender en ontvanger visueel contact moeten houden. Indien een obstakel tussen zender en ontvanger komt te staan, valt de verbinding weg. Bovendien is de overbrugbare afstand beperkt tot slechts enkele meters en werkt het enkel tussen twee apparaten, niet voor een uitgebreid netwerk. Er werd wel geëxperimenteerd met infrarood peer-to-peer netwerkes in de jaren 1990, maar het leverde nooit echt stabiele verbindingen op. De enige toepassing die het nog kent zijn afstandsbedieningen.

g) SWAP (shared wireless access protocol)

SWAP (*shared wireless access protocol*) staat ook bekend onder de naam **HomeRF** en werd vooral ontwikkeld voor thuisgebruik. Het werd ontwikkeld op basis van de **DECT**-standaard (*Digital European Cordless Telecommunication*) die bedoeld is voor draadloze telefoontoestellen.

SWAP maakt gebruik van de techniek van **frequentie-hopping**: het voortdurend wijzigen van de gebruikte frequentie binnen de frequentieband. Daardoor wordt de maximale bandbreedte benut en

wordt afluisteren bemoeilijkt. De maximale gegevensoverdrachtssnelheid bedraagt 1,6 Mbit/s, al is in theorie 20 Mbit/s mogelijk. Het bereik is beperkt tot enkele tientallen meters en er kunnen tot 127 toestellen in één netwerk worden opgenomen. Obstakels tussen zender en ontvanger maken de communicatie niet onmogelijk, maar verzwakken wel het signaal.

Rond de millenniumwisseling leek het er even op dat SWAP een ernstige concurrent zou worden van WiFi, maar vooral toen Intel eind 2000 aankondigde volledig in te zetten op de toen nog gloednieuwe WiFi-standaard, verloor de SWAP-technologie erg snel terrein. Nu wordt het protocol enkel nog gebruikt voor binnenhuistelefonie.

h) Bluetooth

Bluetooth is bedoeld voor goedkope radiolinks tussen draagbare computers, handhelds, PDA's, organizers, smartphones... De technologie maakt gebruik van microgolffrequenties om gegevens over een korte afstand (tot 10 meter) en aan een vrij lage snelheid (maximaal 2 Mbit/s) te versturen. De naam verwijst naar de Viking koning Blauwtand – niet verwonderlijk als je weet dat de technologie ontwikkeld werd door het Zweedse bedrijf Ericsson. Toen het bedrijf in 1998 de Bluetooth Special Interest Group oprichtte, waarbij zich zowat alle grote bedrijven uit de IT-wereld aansloten, werd Bluetooth een internationaal verspreide standaard.

Bluetooth creëert een lokaal netwerkje waarvan maximum acht andere apparaten deel kunnen uitmaken. Het eerste apparaat dat een Bluetooth-verbinding aangaat, wordt de beheerder van dat netwerk (**master**), alle andere apparaten zijn dan slaven (**slaves**). Binnen een Bluetoothnetwerk kun je zowel peer-to-peer communiceren als gecentraliseerd via de master.



Het voordeel van Bluetooth is dat het bijzonder energiezuinig is, wat het uitermate geschikt maakt voor mobiele toestellen waarbij batterijautonomie belangrijk is. Voor het opzetten van een echt computernetwerk is Bluetooth te beperkt. Daarom wordt Bluetooth voornamelijk gebruikt voor het overbrengen van bestanden tussen mobiele apparaten onderling of als verbinding tussen een mobiel apparaat en een randapparaat, zoals een headset of een printer.

i) WUSB (wireless universal serial bus)

WUSB (*wireless universal serial bus*) werkt gecentraliseerd, wat wil zeggen dat één toestel dienst doet als WUSB-host waarlangs alle verbindingen met WUSB-apparaten wordt geregeld. Zo'n **sterverbinding** wordt een **WUSB-cluster** genoemd en kan tot 127 randapparaten met een computer verbinden, evenveel als bij een gewone VSB-verbinding.

Voorlopig werd met WUSB een bereik van 10 meter opgemeten maar de prestaties zijn erg afstandsgevoelig. De hoogste transmissiesnelheid wordt enkel bereikt indien het toestel minder dan 2 meter van de host verwijderd is. Grote merken als HP, Microsoft, NEC, Philips en Samsung hebben de krachten gebundeld in de "*Wireless USB Promotor Group*" en beloven dat WUSB volledig neerwaarts compatibel blijft met bekabelde USB-apparaten.

WUSB is de eerste toepassing van de nieuwe *ultrawideband*-toekomst (**UWB**). UWB verschilt van het klassieke WiFi doordat het niet gebruik maakt van één enkele frequentie, maar een breder deel van het radiospectrum (van 3,1 GHz tot 10,6 GHz) benut. Zo kan er dus meer informatie verzonden worden in een korte tijd.

UWB is een ingewikkelde standaard en het voortdurend wisselen tussen frequenties gebeurt met **OFDM** (*orthogonal frequency division multiplexing*), een moderne modulatietechniek die onder meer

ook bij powerline communicatie gebruikt wordt. Het spectrum dat UWB ter beschikking heeft wordt in een aantal banden gesplitst die elk 528 MHz breed zijn. Een actief UWB-apparaat gebruikt drie van die banden en springt 3 miljoen keer per seconde tussen die drie banden heen en weer. Door een andere selectie aan frequentiebanden of door een andere sequentie voor het verspringen tussen de frequentiebanden te kiezen, kunnen meerdere UWB-clusters in eenzelfde omgeving parallel actief zijn zonder elkaar te storen.

3.3 Netwerkverdeeldozen

Met “*verdeeldozen*” worden alle toestellen in een netwerk bedoeld, die erop gericht zijn om de verschillende apparaten van het netwerk met elkaar te verbinden. In zo’n netwerkverdeeldoos worden de netwerkkabels van computersystemen op het netwerk ingeplugd in contacten, die men poorten noemt.

Vaak worden de begrippen repeater, hub, bridge, switch, router en gateway losjes door elkaar gebruikt. Toch bestaan er duidelijke verschillen en heeft elk type netwerkverdeeldoos specifieke functies.

3.3.1 Repeater en hub

j) Repeater

Gegevens worden door de kabels getransporteerd via een **elektrisch signaal** dat verzwakt over een grotere afstand. Wanneer afstanden moeten overbrugd worden die groter zijn dan het maximale bereik van een kabelsoort, wordt er gebruik gemaakt van een repeater. Dat is een elektronische schakeling die het elektrische signaal op de netwerkkabel in beide richtingen opvangt, regeneert om eventuele storingen weg te halen, versterkt en weer doorgeeft.

Een repeater is het eenvoudigste toestel om een lokaal netwerk uit te breiden. Ze hebben geen controlefunctie en zullen corrupte informatiepakketten of foutieve transmissies gewoon doorgeven. Ze hoeven daarom ook niet als dusdanig herkend of aangesproken te worden door de andere actieve netwerkcomponenten en krijgen geen eigen IP-adres. Ze zijn enkel werkzaam op de fysieke laag in het OSI reference model.

Het aantal repeaters dat tussen twee uiterste werkstations van een Ethernet-netwerk kan geplaatst worden is beperkt tot vier.



k) Hub

Het begrip hub verwees aanvankelijk naar een centraal punt in het netwerk waar netwerkbekabeling samenkwam. In die tijd deden hubs niet veel meer dan het doorgeven van het signaal op alle poorten. Tegenwoordig hebben netwerkverdeeldozen veel meer intelligentie in huis dan dat. Die worden dan switches genoemd. Omdat hub en switches uiterlijk sterk op elkaar lijken, worden beide vaak door elkaar gehaald.

Vanaf iedere computer in het netwerk vertrekt een kabel naar de hub die dan de onderlinge verbindingen tussen de computers regelt. Wanneer er een slechte verbinding ontstaat tussen de hub en één computer hebben de andere computers in het netwerk daar verder geen last van.

Kenmerkend voor een hub is dat de gegevensstroom van een computer doorgestuurd wordt naar alle aangesloten toestellen. De beschikbare bandbreedte wordt gewoon gedeeld door het aantal aangesloten werkstations, ongeacht de behoefte. Wanneer een hub louter fungeert als verbindingsstuk tussen de computers, dan spreekt men van een **passieve hub**. Heeft de hub ook de mogelijkheid om het signaal te versterken zoals een repeater, dan noemen we dat een **actieve hub**.

De meeste hubs beschikken over 4 tot 24 poorten, maar er bestaan ook exemplaren met meer poorten. Je kan ze met elkaar verbinden door middel van een speciale **uplink**-poort om op die manier meerdere poorten ter beschikking te hebben. Net als bij repeaters is het maximaal aantal hubs tussen twee computers in een netwerk beperkt.



Een 5-poorts hub

3.3.2 Switch

Een switch (kort voor switching hub) lijkt uiterlijk erg op een gewone hub, maar zal de informatie enkel doorgeven aan de geadresseerde computer. De andere computers worden dus niet belast met overbodig netwerkverkeer dat niet voor hen bestemd is. Bovendien verdeelt een switch de beschikbare bandbreedte niet gelijkmatig over alle werkstations, maar wel naargelang de behoefte. Zo kan een computer bij het downloaden van een bestand over het netwerk gebruik maken van de volledige bandbreedte van de switch, als er op dat ogenblik geen enkele andere computer informatie verstuurt of ontvangt van het netwerk. Dat verhoogt de overdrachtssnelheid over het hele netwerk en verkleint de kans op botsingen. Een switch is actief in de verbindingslaag, de tweede laag van het OSI reference model, en hanteert MAC-adressen om te bepalen op welke poort pakketjes moeten worden doorgegeven.

De techniek die door switches gebruikt wordt heet **frame switching**. De verbinding tussen twee computers duurt net lang genoeg om een frame door te geven. Voor een volgend frame moet een nieuwe verbinding worden gemaakt. Tussen die frames door kunnen echter andere verbindingen tot stand worden gebracht voor het doorgeven van frames tussen andere computers.

Voor het doorgeven van de frames zelf, worden drie mogelijke technieken gebruikt:

♦ Store & forward

Een frame wordt eerst volledig ingelezen en wordt pas daarna doorgegeven. Switches die volgens deze techniek werken controleren de frames ook op fouten. Dat zorgt voor een beetje vertraging van het netwerkverkeer, maar zo worden er wel veel corrupties voorkomen en gaan er minder corrupte frames over het netwerk zwerven. Voor het tijdelijk bewaren van de frames wordt een buffergeheugen gebruikt.

♦ Cut through

Zodra van een binnenkomend frame het MAC-adres van de bestemming gelezen is, wordt het frame al onmiddellijk doorgestuurd naar de bestemming, zelfs al werden alle gegevens van het frame op dat moment nog niet ontvangen. Bit voor bit wordt dan van de ene poort rechtstreeks naar de andere poort doorgegeven. De gegevensoverdracht gaat dan sneller, maar door het ontbreken van een foutcontrole kunnen corrupte frames rondgestuurd worden of zijn botsingen op het netwerk mogelijk. Deze manier van doorgeven van frames wordt ook de **hot potato-strategie** genoemd.

De meeste switches ondersteunen beide technieken (store & forward en cut through). Ze gebruiken dan standaard het principe van cut through, tot een bepaald niveau van fouten werd bereikt. Daarna wordt er overgeschakeld op store & forward. Op die manier wordt zolang mogelijk gebruikt gemaakt van de hoogste doorvoersnelheid.

◆ Fragment free

Hierbij worden de eerste 64 bytes van een frame ingelezen, waarna het frame al doorgestuurd wordt naar de bestemming, zelfs al werd het hele frame nog niet ontvangen. Er kan dan al een foutcontrole worden uitgevoerd op de eerste 64 bytes – de meeste fouten komen immers in de eerste bytes voor. Toch blijft de vertraging beperkt, aangezien niet eerst het volledige frame moet worden ingelezen.



Wanneer een switch de drie technieken aankan, zal die over het algemeen op basis van een eigen analyse van het netwerkverkeer autonoom kunnen beslissen welke techniek gebruikt zal worden. Op sommige switches kan je als netwerkbeheerder zelf de gebruikte techniek instellen. Wanneer de netwerkbeheerder zelf instellingen kan wijzingen in de switch, spreken we van een **managed switch**. Netwerkbeheerders verbinden zo'n switch dan met een computer door middel van een speciale consolekabel en gebruiken UNIX-gebaseerde tekstcommando's om instellingen te wijzigen, maar vaak kan het beheer ook via een webinterface. Via de browser van eender welke computer op het netwerk maakt de beheerder dan contact met het IP-adres van de switch. Nadat correct op de switch werd aangemeld, kan de netwerkbeheerder allerlei instellingen op de switch aanpassen, zoals de naam van de switch, het statische IP-adres enzovoort. Via dezelfde webinterface kan de beheerder bovendien alle informatie bekomen betreffende de werking van de switch. Sommige fabrikanten laten zelfs de configuratie van een switch toe via een meegeleverde inlognaam en wachtwoord op een portaalwebsite op het internet. Dat wordt dan een **cloudportal** genoemd. Switches die door netwerkbeheerders kunnen geconfigureerd worden beschikken over functies uit de netwerklaag van het OSI-model, en worden daarom ook wel **level-3 switches** genoemd. Indien daar ook functies uit de transportlaag bijkomen, spreken we van een **multilayer switch**.

De meeste switches beschikken over 4 of meer gewone poorten. Heb je niet voldoende met het aantal beschikbare poorten op één switch, dan kan je verschillende switches van hetzelfde merk – die dan meestal op elkaar gestapeld zijn – met elkaar koppelen. We spreken dan van een stack. De afzonderlijke switches vormen dan samen één logische switch in het netwerk.

3.3.3 Bridge

Een bridge is een apparaat dat twee netwerksegmenten met elkaar verbindt en gegevens van het ene netwerksegment naar het andere kopieert. Dat gebeurt enkel indien die gegevens ook daadwerkelijk voor het andere netwerksegment bedoeld zijn. Een bridge heeft dus een controlerende functie: ze kijkt elk pakketje dat verstuurd wordt na op haar adressering. Hierdoor hebben de verschillende netwerksegmenten geen last van het gegevensverkeer van de andere segmenten. De totale

beschikbaarheid van het netwerk verhoogt daardoor en de kans op botsingen verkleint. Bovendien zullen corrupte pakketten enkel nog in het lokale netwerksegment kunnen bewegen.

Bridges werken onafhankelijk van het gebruikte netwerkprotocol. Dat is logisch aangezien de adressering werkt op hardware-niveau – op basis van MAC-adressen dus. Daardoor is het mogelijk om subnetwerken die elk een verschillende logische netwerktopologie gebruiken, samen te brengen in één netwerk. Frames worden doorgegeven van het ene netwerksegment naar het andere op basis van de store & forward techniek: een binnenkomend frame wordt gebufferd tot het compleet is en op basis van de meegegeven adressering wordt het daarna naar de juiste poort verstuurd. Dat veroorzaakt wel vaak een kleine vertraging op het netwerk.

Moderne switches worden doorgaans uitgerust met een bridge-functie. Zij combineren de voordelen van een switch met die van een bridge. Met een dergelijke switch kan je het netwerk segmenteren zonder dat daarvoor een aparte bridge nodig is.

Er staat geen limiet op het aantal bridges in een netwerk. In de praktijk worden ze enkel toegepast in uitgebreide netwerken. Ze worden door netwerkbeheerders eerder spaarzaam gebruikt.

Het begrip bridge wordt eveneens gebruikt voor toestellen die verschillende types van netwerken aan elkaar kunnen koppelen. Dat kunnen dan netwerken zijn met een verschillende topologie, een andere bekabeling of een afwijkend toegangsprotocol. Correkter is het om in dat geval te spreken van een **converting bridge**. Niet altijd beschikt zo'n conversie bridge over een echte bridge-functie, waardoor de naamgeving nog verwarrender wordt.

Een conversie bridge die een UTP-netwerk aan glasvezel koppelt.



3.3.4 Router

Routers zijn niet bedoeld om individuele computers maar om netwerken aan elkaar te koppelen. Ze zijn via één poort verbonden met het lokaal netwerk en met één of meer poorten verbonden met andere routers op het internet. De routing gebeurt niet op basis van MAC-adres maar op basis van het IP-adres. Een router is dan ook een apparaat dat actief is op de netwerklaag, de derde laag van het OSI reference model.

De router zal op basis van het IP-adres beoordelen welk pakket naar welke poort gestuurd moet worden. Een router kent immers niet alleen het netwerknummer van het netwerk waaraan hij gekoppeld is maar ook van verderop aangesloten knooppunten op het internet. Daardoor kan de router beslissen welke de kortste of snelste weg is om een pakketje bij zijn bestemming te krijgen. De volgende router zal dit op zijn beurt ook doen. Een router moet dus constant bijhouden welke

netwerken er rond zich heen situeren, want een bepaald netwerksegment kan uitvallen of er kan een betere route bijkomen. Vandaar dat routers complexe en dure apparaten zijn. Hoe IP-routing precies in z'n werk gaat, leer je in hoofdstuk 6.2.1 van deze cursus.



3.3.5 (Wireless) Network Access Point

Basisstations voor draadloze netwerken (WiFi) worden **NAP** (*network access point*) of **WNAP** (*wireless network access point*) genoemd. Soms gebruikt men ook het begrip draadloze router, maar helemaal correct is dat niet. Zelfs al beschikken ze over een bescheiden router-functie, dan werkt die functie niet via het draadloze maar via het bekabelde signaal. Een NAP is eerder het draadloze equivalent van een converting bridge – de benaming draadloze bridge ligt dus dichterbij de waarheid, maar dat begrip neemt men niet in de mond.

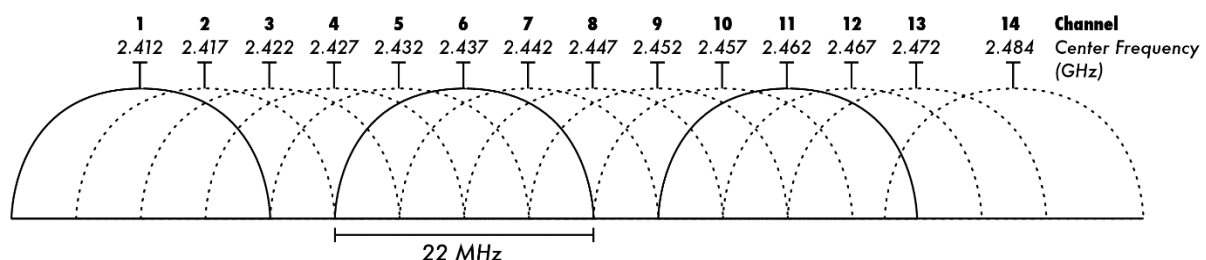


Een NAP is een apparaat dat ingeplugd wordt in een klassiek bekabeld netwerk door middel van een gewone UTP-kabel, of die het signaal van een ander NAP opvangt en weer doorgeeft aan de werkstations. Het verstuurt permanent een signaal, zo dat de draadloze werkstations voortdurend verbonden blijven. Vaak beschikken NAP's ook over enkele bijkomende poorten voor netwerkkabels, zo dat ze tegelijk ook als switch voor een klein bekabeld netwerkje kunnen ingezet worden.

De meeste NAP 's beschikken over één, twee of drie antennes – al zijn die bij sommige modellen niet zichtbaar want ingebouwd in de behuizing van het apparaat. Toestellen met twee of drie antennes zorgen voor een merkkelijk betere ontvangst. Ze gaan immers plaatselijke signaalzwakte door reflectie tegen. Staat een NAP bij een muur, dan kan het signaal dat een antenne uitstuurt teruggekaatst worden. Komen het oorspronkelijke en het gereflecteerde signaal elkaar tegen, dan heffen ze elkaar op en is er geen ontvangst. Met twee of drie antennes, die een beetje uit elkaar staan, wordt het zendpunt verschoven. Het werkstation zal automatisch kiezen om contact te maken met de antenne die het sterkste signaal uitstuurt.

De huidige generatie NAP's maakt gebruik van de **MIMO**-technologie (*multiple input – multiple output*). Daarbij beschikt elk van de antennes over een eigen radiochip die afzonderlijk de signalen van een draadloos apparaat zoals een laptop kunnen opvangen. De radiochips werken op zo 'n manier samen dat de antenne die het sterkste signaal van een mobiel apparaat binnenkrijgt, ook het zwaarst wordt belast bij het verzenden van signalen naar dat apparaat. Op die manier levert zo'n NAP op langere afstand een veel stabielere en snellere verbinding dan oudere NAP's zonder MIMO.

Bij oudere NAP's (802.11b en 802.11g) wordt het frequentiebereik opgesplitst in 14 kanalen, waarvan in Europa alleen het laatste kanaal niet kan gebruikt worden. De kanalen liggen vijf MHz uit elkaar. Voor de 802.11g-specificatie gaat men er van uit dat een NAP met frequentiegolven tot 22MHz uitzendt. Wanneer twee draadloze access points binnen elkaars bereik op eenzelfde of een overlappend kanaal uitzenden, kunnen ze elkaar storen. Daarom worden twee of drie verschillende NAP's die zich binnen elkaars zendbereik bevinden, het best ingesteld op zo ver mogelijk uit elkaar liggende kanalen (gewoonlijk 1, 6 en 11).



Elk NAP zendt met het signaal ook zijn naam uit, die men **SSID** (*service set identifier*) noemt. Bij sommige opstellingen is het mogelijk om met mobiele apparaten doorheen het volledige zendbereik van het draadloze netwerk te bewegen zonder dat de verbinding onderbroken wordt door elke NAP exact hetzelfde SSID te geven en op verschillende kanalen in te stellen. Het mobiele apparaat zal automatisch een verbinding maken met het NAP dat het sterkste signaal uitzendt. Dit principe wordt **roaming** genoemd.

Soms is het signaal van een draadloos netwerk te zwak of is het draadloze netwerk zelfs niet meer te vinden. Dat kan het gevolg zijn van zogenaamde frequentievervuiling of eenvoudiger gezegd: teveel draadloze apparaten in de buurt, die elkaar op dezelfde frequentie in de weg zitten. Enkele tips om de ontvangst van je draadloze netwerk te optimaliseren:

- ◆ Plaats een NAP fysiek zo centraal mogelijk in het netwerk en zo centraal mogelijk in een ruimte, weg van mogelijke fysieke obstakels.
- ◆ Zorg ervoor dat de antennes steeds perfect verticaal gericht zijn. Je kan eventueel ook gebruik maken van een externe antenne.
- ◆ Bij oudere NAP's (IEEE 802.11b/g) kan je eventueel in het instellingenvenster een ander kanaal instellen indien de ontvangst matig is. Bij moderne NAP's (IEEE 802.11n/ac) is dat niet meer nodig, omdat dergelijke toestellen al automatisch van het meest geschikte kanaal zullen gebruik maken.

Wanneer één NAP onvoldoende is om overal op de campus van een bedrijf, school of andere organisatie een behoorlijke ontvangst mogelijk te maken, kan je in plaats van een tweede NAP ook gebruik maken van een **draadloze repeater** (ook: *range extender*). Dat is een toestel dat het draadloze signaal opvangt en versterkt weer doorgeeft. Het voordeel van zo'n opstelling is dat je voor die repeater geen toegang tot het bekabeld netwerk hoeft te voorzien. Er bestaan repeaters die weerbestendig zijn en dus buitenshuis kunnen worden opgesteld.

Aangezien van op eender welke computer met een draadloze netwerkkaart een verbinding kan worden gemaakt met het NAP, bestaat er altijd een reëel gevaar voor indringers. Daarom is de beveiliging van een draadloos netwerk erg belangrijk. Daarover leer je meer in hoofdstuk 5.3 van deze cursus.

4 Servers

Waarin de koningen van een computernetwerk eigenlijk eerder dienaars van hun netwerkvolk blijken te zijn.

In dit hoofdstuk leer je dit:

- ◆ Het concept client/server-verwerking
- ◆ Het doel van een multitier-architectuur
- ◆ Het verschil tussen datadistributie en datacollectie
- ◆ De kenmerken van serverhardware
- ◆ Het doel en de werking van een DHCP-server
- ◆ Het doel en de werking van een domeincontroller
- ◆ Het belang van een doordracht rechtenbeleid
- ◆ Het doel en de werking van een fileserver
- ◆ Het doel en de werking van een mailserver
- ◆ Het doel en de werking van een printserver
- ◆ Het doel en de werking van een application server
- ◆ De kenmerken van thin clients
- ◆ Het doel en de werking van een webserver
- ◆ De kenmerken van een netwerkbesturingssysteem
- ◆ Een server voor een lokaal netwerk configureren

4.1 Client/server-verwerking

Het begrip client/server beschrijft de relatie tussen twee computerprogramma's, waarbij het ene programma (de **client**) een dienst vraagt aan een tweede programma (de **server**). Deze server verleent de gevraagde dienst aan de client.

Het concept van client/server-verwerking wordt toegepast in netwerken. We spreken dan van een **gedistribueerd** computerproces: daarbij zijn de gegevens en programmatuur die nodig zijn voor het proces verspreid over meer dan één computer – dit in tegenstelling tot een **gecentraliseerd** computerproces zoals bij een mainframe.

Aangezien de programma's die diensten verlenen vaak ingewikkelder zijn dan gewone gebruikerstoepassingen en omdat er doorgaans veel clients tegelijk van de diensten van een server gebruik maken, draaien servertoepassingen bij voorkeur op een zeer krachtige computer met een groot inwendig geheugen, een performante processor en een grote opslagcapaciteit. Een computer die serverdiensten verleent in een netwerk wordt server genoemd. Een computer die uitsluitend servertaken vervult, wordt een **dedicated** server genoemd. Een computer die servertaken vervult maar tegelijk ook gebruikt wordt als werkstation, wordt **non-dedicated** server genoemd.

Soms is de grens tussen een non-dedicated server en gewoon werkstation heel dun. In een informaticaklas draait bijvoorbeeld een *classroom management console* – dat is software waarmee een leerkracht de computers van de leerlingen van op afstand kan besturen. Wanneer de leerkracht de computer van een leerling bestuurt van op de leerkrachtencomputer vooraan in de klas, levert de computer van de leerling dus een dienst aan de computer van de leerkracht. In zo'n situatie zijn alle computers van leerlingen in de informaticaklas dus eigenlijk servers. Maar zijn ze dat altijd? Of noemen we ze enkel servers op het ogenblik dat de classroom management console geactiveerd wordt? Het antwoord wordt door verschillende bronnen verschillend geïnterpreteerd.

Vaak worden applicaties speciaal ontworpen voor client/server-verwerking. Zo'n toepassing bestaat dan uit twee verschillende, met elkaar samenwerkende programma's: een serverprogramma dat diensten levert aan het clientprogramma dat bij de gebruiker geïnstalleerd wordt. Het programma op de computer van de gebruiker wordt dan **front-end** genoemd. Het serverprogramma heet dan **back-end**. Wanneer gebruik gemaakt wordt van serverdiensten op het internet, spreken we van **cloudcomputing**.

Complexe servertaken worden vaak gespreid over verschillende servers. Daarvoor bestaan verschillende modellen:

a) 2-tier architectuur

Het gegevensverwerkend proces bestaat uit vier hoofdcomponenten: invoer, verwerking, uitvoer en gegevensbeheer. Bij een gewoon lokaal programma wordt het hele proces uitgevoerd door eenzelfde computer.

In een 2-tier design worden invoer en uitvoer volledig toegeschreven aan de client. Het gegevensbeheer wordt aan de server overgelaten en de eigenlijke verwerking (het uitvoeren van processen op de gegevens) kan worden verdeeld over zowel de client als de server. Meestal bevindt het merendeel van de verwerking bij 2-tier implementaties zich op de client en beperkt de server zich tot het beheer van de gegevens.



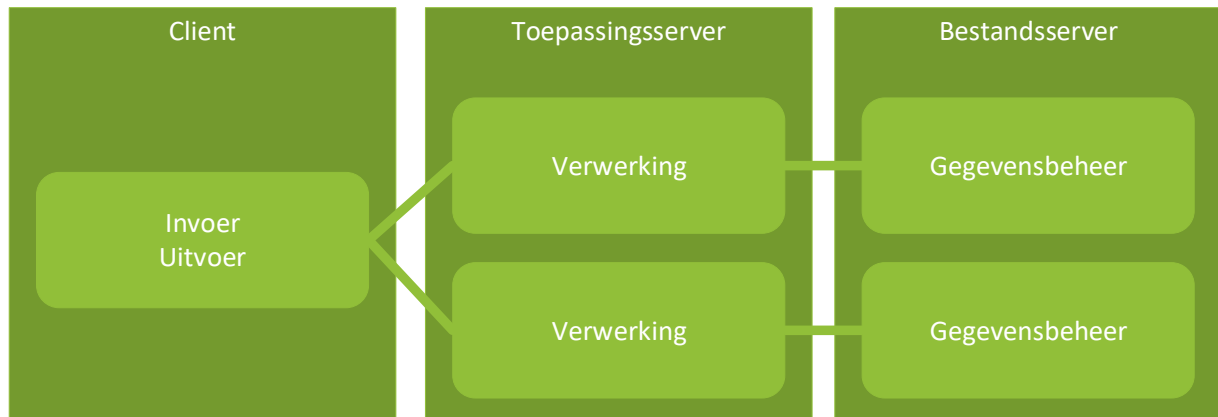
b) 3-tier architectuur

In een 3-tier architectuur wordt een derde computer toegevoegd: een afzonderlijke toepassingsserver. Die neemt het verwerkingsgedeelte van de client over. Daardoor is het verwerkingsproces makkelijker te onderhouden en beter te bewaken en wordt de verwerkingscapaciteit van zowel server als client geoptimaliseerd. Bovendien biedt dit meer garanties op veiligheid, zowel aan de zijde van de client als die van de server.



c) Multitier architectuur

Sommige processen zijn zo gecompliceerd en dienen zo doorgedreven beveiligd te worden, dat verwerking en gegevensbeheer beter worden opgesplitst over verschillende servers. Elke server neemt dan een gespecialiseerd deel van de verwerking of van het beheer van de gegevens op zich. Het totaal aantal toestellen dat in zo'n architectuur ingeschakeld wordt, ligt dan uiteraard niet vast.



De manier waarop servers in zo'n multitier samenwerken is vaak erg verschillend. Vaak wordt gewerkt met een data warehouse of met **clusters**.

Een **data warehouse** is een zeer uitgebreide bestandsserver waarin grote hoeveelheden gegevens worden opgeslagen. De meest opgezochte gegevens worden klaargezet op een tussensysteem, een kleinere fileserver, die de gegevens bevat voor dat bepaalde gedeelte van het netwerk. Daardoor worden de belangrijkste servers voor een groot gedeelte ontlast.

Meerdere servers kunnen samen één cluster of "**server farm**" vormen. De verschillende computers werken dan als één geheel: de gebruiker merkt niet op welke machine in de cluster zijn toepassing verwerkt wordt. Het voordeel van deze manier van werken is de optimalisatie van de gebruikte bronnen – vaak kunnen servers zelfs gebruik maken van elkaars verwerkingscapaciteit – een ver doorgedreven vorm van multitasking en het makkelijker opvangen van hardware fouten. Ook een geheel van redundante servers – dit wil zeggen: servers met dezelfde functie in het netwerk – wordt een cluster genoemd. Redundante servers verhogen de beschikbaarheid van gegevens en diensten.

Het installeren van een cluster van servers is niet eenvoudig en dus specialistenwerk. Hiervoor is een specifiek cluster-netwerkbesturingssysteem vereist en ook de toepassingen die erop draaien moeten geschikt zijn om met clustering overweg te kunnen.

d) Datadistributie en datacollectie

Bij **datadistributie** worden vanuit een server gegevens verstuurd naar een of meer clients in het netwerk. Het gegevensverkeer verloopt enkel in de richting van die clients. Een concrete toepassing van datadistributie is de verspreiding van documenten naar verschillende regionale verkoopkantoren. Ook het installeren van software op clients vanuit een server is een vorm van datadistributie. Dit levert heel wat tijdswinst op voor netwerkbeheerders, zeker wanneer dit volledig geautomatiseerd kan gebeuren.

Datacollectie is het omgekeerde van datadistributie. Daarbij worden gegevens door een server verzameld en verwerkt. Het gegevensverkeer verloopt in de richting van de server. Datacollectie wordt veel gebruikt voor het verzamelen van meetgegevens van bijvoorbeeld luchtvervuiling of weerkundige gegevens vanuit geografisch verspreide meetpunten. Met een datacollectie-systeem

kunnen vele gegevens vanuit de periferie snel centraal beschikbaar komen, wat voor de beleidsvoering van een bedrijf van groot belang kan zijn. Zo leiden reserveringen die door reisbureaus naar een hoofdkantoor worden doorgestuurd tot een efficiënter beheer van de boekingen.

Bij datacollectie kan men naast manuele invoer ook gebruik maken van gegevens die via speciale invoerapparatuur worden ingelezen, zoals een barcodelezer. Meestal zullen bij datacollectie de verschillende bronnen relatief weinig gegevens invoeren, verdeeld over een lange tijdspanne. De verkeersdichtheid is met andere woorden laag. Bij de balie van het reisbureau bijvoorbeeld doet het aanbod van klanten zich gespreid voor over de hele dag. Om het kanaal zo economisch mogelijk te gebruiken vindt de overdracht vaak gebundeld plaats. Een aantal berichten is dan vooraf verzameld en wordt in één keer verzonden. Dat heet **bulkupdating**. Met de doorbraak van breedband internet wordt bulkupdating voornamelijk nog toegepast voor back-ups.

4.2 Serverhardware

Een server is meer dan zomaar een krachtige computer. Hoewel in principe elke computer servertaken kan uitvoeren, onderscheidt een als server geconcipeerde computer zich van een workstation op een aantal punten:

Kwetsbare onderdelen zijn *redundant* aanwezig, waardoor een defect onderdeel de server niet onmiddellijk stillegt. Bovendien zijn servers zo ontworpen dat de meest kwetsbare en aan slijtage onderhevige onderdelen zoals de voeding, ventilatoren of de harde schijf erg snel kunnen worden vervangen, vaak zelfs zonder de behuizing te moeten openen. Daardoor blijft de *downtime* - de tijd dat een server niet beschikbaar is - tot een minimum beperkt. Downtime wordt uitgedrukt in procent. Een server die per jaar slechts 5 minuten onbeschikbaar is, krijgt een score van 99,999 % en dat is behoorlijk goed. Servers die minder dan 99 % beschikbaar zijn en dus meer dan 80 uur per jaar buiten strijd zijn, worden als erg onbetrouwbaar beschouwd.

Servers zijn uitgerust met bijzonder krachtige processoren, soms zelfs meerdere per toestel, die speciaal voor servers ontwikkeld zijn. Dit soort processoren beschikken bovendien over veel grotere cachegeheugens.

Servers hebben vaak nood aan veel opslagcapaciteit en snelle schijftoegang. Daarom wordt vaak gebruik gemaakt van snelle SAS-schijven in plaats van klassieke SATA-schijven. Dankzij de RAID-technologie kunnen meerdere schijven aan elkaar worden gekoppeld, wat niet alleen resulteert in een meer flexibel gebruik van de opslagcapaciteit, maar ook in snellere schijftoegang en een veel hogere betrouwbaarheid.

Het geheugen van servers is doorgaans heel wat uitgebreider dan die van gewone computers. Bovendien zijn de geheugenmodules van servers meestal anders opgebouwd dan doorsnee werkgeheugen. Per rij van 64 bits beschikt zo'n geheugen immers over een extra rijtje van 8 bits voor foutcontrole. Dat soort geheugen wordt **ECC**-geheugen (*error correction code*) genoemd en zorgt ervoor dat processen minder snel vastlopen. Een andere manier om geheugenfouten in servers te beperken, is **mirroring**. Hierbij worden dezelfde gegevens naar twee geheugenbanken geschreven. Loopt er met één geheugenbank iets mis, dan kan de processor nog steeds ongestoord verder werken met de gegevens die zich in de andere geheugenbank bevinden.



Een netwerkserver wordt niet altijd in een klassieke behuizing gemonteerd. Aangezien in serverruimtes netwerkapparatuur zoals routers en switches vaak in speciale rekken – in het Engels “**racks**” – worden ingebouwd, ontstond de behoefte om ook voor servers speciale



behuizingen te ontwerpen die in een rack kunnen worden ingebouwd. Racks hebben altijd dezelfde standaard afmeting. Vaak zijn rack servers zo ontworpen dat ze intensief samenwerken met andere rackservers mogelijk maken. Bovendien kan de bekabeling

naar andere netwerkapparatuur die vaak in hetzelfde rack is ingebouwd, efficiënter worden aangebracht. Niets is immer zo chaotisch als een serverruimte waarin de netwerkkabels kriskras door elkaar lopen.



In meer gespecialiseerde omgevingen kan gebruik gemaakt worden van **blade servers**. Zo'n blade server is in feite een moederbord waarop enkel nog de meeste essentiële onderdelen terug te vinden zijn, zoals een of meer processoren en een uitgebreid werkgeheugen. In een **blade enclosure** of **blade chassis** worden meerdere blad servers ingebouwd. De enclosure zorgt voor de stroomvoorziening, koeling en voor input en output-aansluitingen. Het geheel van een blade enclosure en de ingebouwde blade servers wordt

een **blade system** genoemd. Hoewel elke blade server over een eigen verwerkingseenheid beschikt, zijn blade servers speciaal ontworpen om met elkaar te kunnen samenwerken en elkaars capaciteit te kunnen gebruiken voor complexe rekentaken.

4.3 Serverdiensten in een lokaal netwerk

Wanneer een computer in een netwerk een dienst levert aan een andere computer in dat netwerk, vervult deze de taak van server. We noemen zo'n dienst dan een **serverdienst**. Op basis van het doel worden serverdiensten in verschillende soorten onderverdeeld.

Wanneer een computer servertaken vervult, moet deze beschikken over een besturingssysteem dat het mogelijk maakt dat diensten aan andere computers worden geleverd. Indien het om eenvoudige diensten gaat zoals een printserver, dan volstaan de meeste gewone besturingssystemen en kan de computer in kwestie makkelijk in gebruik blijven als werkstation. Wanneer de serverdiensten complexer of kritischer zijn, dan is een netwerkbesturingssysteem vereist (zie deel 4). Eenzelfde machine kan meerdere serverdiensten aanbieden op een netwerk.

Het is duidelijk dat servers kritische systemen in netwerken zijn. Loopt er iets mis in de server, dan valt minstens een deel van de netwerkfuncties weg. Het is voor netwerkbeheerders uiteraard belangrijk dat zij de oorzaak van het probleem snel kunnen achterhalen. Servers zullen al hun activiteiten registreren en bewaren in speciale databanken, die men dan **server logs** noemt. In die

server logs kan een netwerkbeheerder nagaan wat er precies gebeurt wanneer een probleem zich voordoet. Vaak geeft dat een goede indicatie van de oorzaak van een probleem.

Om te voorkomen dat netwerkfuncties wegvallen kunnen serverdiensten *redundant* worden aangeboden. Dat wil zeggen dat eenzelfde netwerkdienst aangeboden wordt op meer dan één machine. Bij een defect van een machine, zal een andere de netwerkdienst gewoon blijven leveren. De gebruikers van het netwerk merken in dat geval weinig van de storing. Indien meerdere servers eenzelfde netwerkdienst op het netwerk aanbieden, is het wel belangrijk dat de gegevens voor die serverdienst tussen de verschillende servers gesynchroniseerd wordt.

Er bestaan honderden verschillende serverdiensten, waarvan de meeste erg specifiek zijn voor welbepaalde en weinig verspreide toepassingen. We bespreken in dit hoofdstuk enkel universele serverdiensten die vaak voorkomen in lokale netwerken.

4.3.1 DHCP-server

Computers in een netwerk communiceren met elkaar aan de hand van IP-adressen. Het IP-adres kan daarbij vast ingesteld worden in de computer. Op die manier heeft de computer in alle omstandigheden hetzelfde IP-adres. Ook het subnetmasker en het IP-adres van de standaardgateway (de router of server die toegang geeft tot het netwerk) wordt dan handmatig vastgelegd. Het toewijzen van een vast IP-adres wordt statisch adresseren genoemd. We spreken dan van een **statisch IP-adres**.

Tegenover statisch adresseren staat dynamisch adresseren. Daarbij wordt het IP-adres van een computer toegewezen door een server. Die computer hoeft niet noodzakelijk bij elke verbinding hetzelfde IP-adres te krijgen. Zo'n toegewezen IP-adres wordt een **dynamisch IP-adres** genoemd.

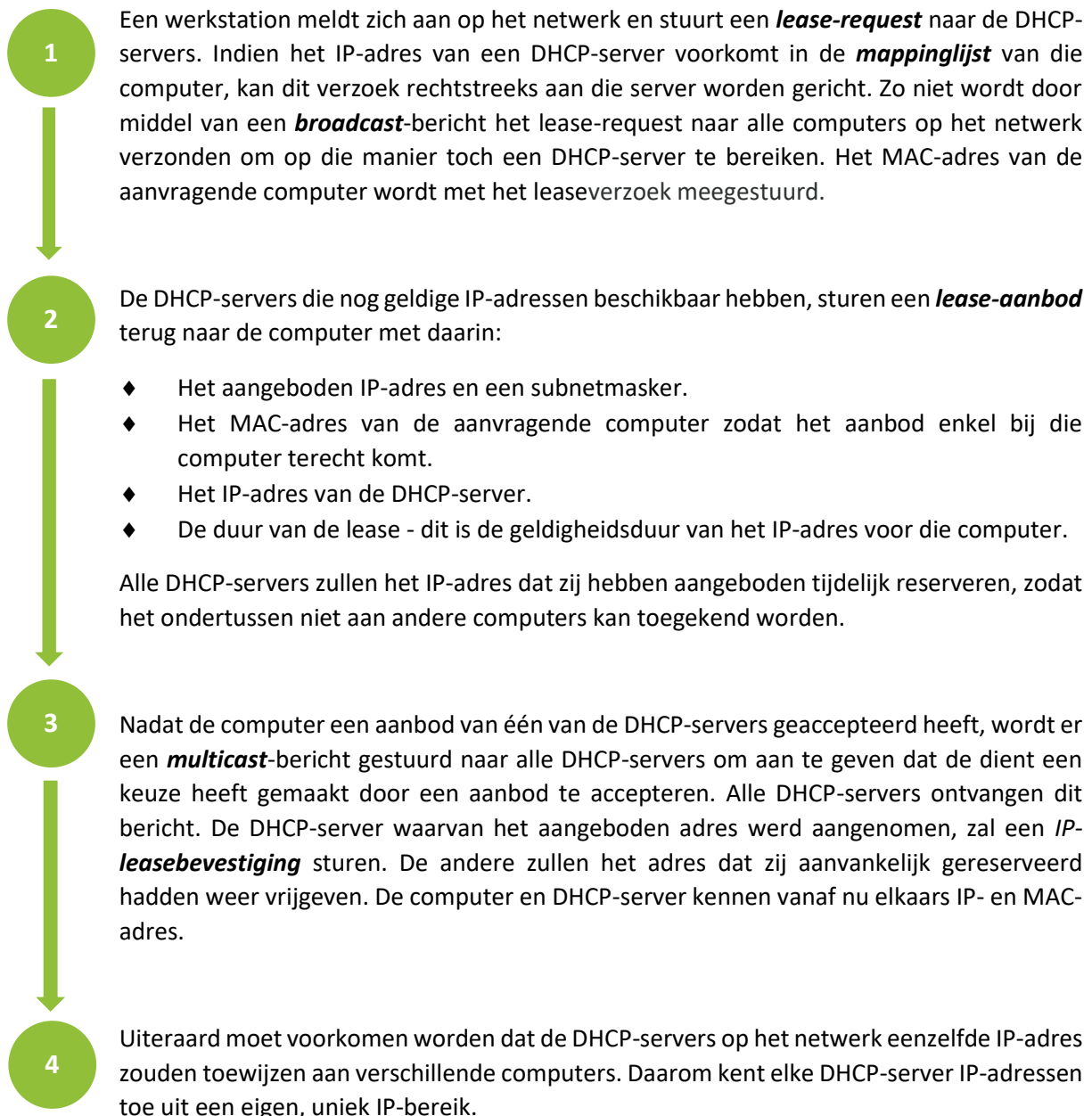
Dynamisch adresseren heeft heel wat voordelen:

1. Het bespaart de netwerkbeheerder behoorlijk wat tijd, aangezien niet elk netwerkcomponent apart hoeft geadresseerd te worden.
2. Een netwerk kan meer aangesloten componenten bevatten dan er IP-adressen binnen die netwerkklassie beschikbaar zijn, aangezien in de meeste computernetwerken niet alle netwerkcomponenten tegelijk actief zijn. Een workstation dat niet ingeschakeld is, hoeft op dat ogenblik niet over een IP-adres te beschikken. Het aantal netwerkcomponenten dat daadwerkelijk actief verbonden is met het netwerk, blijft uiteraard wel beperkt tot het aantal beschikbare IP-adressen binnen het bereik.
3. Netwerkcomponenten zonder een eigen opslagmedium, zoals sommige **thin clients**, kunnen toch van een IP-adres worden voorzien.
4. Het is makkelijker om nieuwe netwerkcomponenten toe te voegen of om oude netwerkcomponenten te vervangen.
5. Mobiele computers zoals laptops, tablets en smartphones kunnen zonder het wijzigen van netwerkinstellingen vlot wisselen tussen verschillende netwerken, zoals het thuis-, school- of bedrijfsnetwerk.
6. De kans op IP-conflicten verkleint. Een IP-conflict ontstaat wanneer binnen hetzelfde netwerk een IP-adres aan twee verschillende netwerkcomponenten wordt toegekend. De kans op het dubbel toewijzen van een IP-adres is veel groter bij statisch dan bij dynamisch adresseren.

a) Werking DHCP

Dynamisch adresseren gebeurt met het **DHCP**-protocol (*dynamic host configuration protocol*) en het programma dat de dynamische IP-adressen toewijst wordt de DHCP-server genoemd. Doorgaans is in eenzelfde netwerk slechts één DHCP-server actief, hoewel meer dan één DHCP-server kan worden voorzien. Wanneer door een defect een DHCP-server niet meer beschikbaar is, kan een andere die taak dan overnemen. Om te voorkomen dat eenzelfde IP-adres door de verschillende DHCP-servers dubbel wordt toegewezen, zal elke DHCP-server gebruik maken van een eigen, uniek IP-bereik.

Zo verloopt dynamisch adresseren bij meerdere DHCP-servers. De werkwijze wanneer slechts één DHCP-server in het netwerk actief is, is gelijkaardig:



De duur van een lease is beperkt in de tijd. Een werkstation vraagt de hernieuwing van de lease aan op het moment dat de helft van de leasduur verstreken is. Hiervoor zendt de client een **DHCP-request** rechtstreeks naar de DHCP-server die het IP-adres verstrekt heeft. Als die DHCP-server online is zal deze de lease vernieuwen, zo niet zal het werkstation gewoon het IP-adres blijven gebruiken

aangezien nog maar de helft van de tijd verstreken is. Deze procedure wordt herhaald wanneer de leasetijd bijna ten einde is en opnieuw bij het volledig verstrijken van de **leasetijd**. Als er dan nog geen bevestiging komt moet het werkstation een nieuw IP-adres aanvragen alsof deze zich voor de eerste keer aanmeldt.

Doorgaans zullen netwerkbeheerders de netwerkcomponenten die voor de andere computers altijd beschikbaar moeten blijven een statisch IP-adres toekennen. Daarbij gaat het haast altijd over toestellen die een **serverfunctie** vervullen of actieve componenten zoals switches en routers. De netwerkbeheerder zal bij het instellen van het bereik voor dynamische adressering rekening houden met het aantal componenten die statisch moeten geadresseerd worden. Wanneer hij in een lokaal klasse C-netwerk het bereik voor dynamisch adresseren bijvoorbeeld instelt voor computernummers tussen 1 en 200, zijn er nog 54 adressen beschikbaar voor statisch adresseren.

b) Gereserveerde dynamische IP-adressen

In een netwerk waarin het dynamische bereik wordt gedeeld door een aantal vaste computers en veel mobiele toestellen kan het probleem ontstaan dat zoveel mobiele toestellen een dynamische IP-adres toegewezen krijgen dat er nog onvoldoende adressen beschikbaar zijn voor de desktopsystemen in het netwerk. Een oplossing is dan om voor elk van die computers een dynamisch IP-adres te reserveren. Dat gebeurt op basis van het MAC-adres. Ook wanneer zo'n computer niet ingeschakeld is, blijft het IP-adres gereserveerd. Dat betekent natuurlijk dat er minder IP-adressen beschikbaar zijn voor de mobiele apparaten. Daarom is het reserveren van dynamische IP-adressen vaak een kwestie van prioriteiten: enkel wanneer een computer steeds toegang moet kunnen krijgen tot het netwerk of wanneer ze voor andere computers steeds bereikbaar moet zijn, wordt er een IP-adres voor gereserveerd.

Er lijkt erg weinig verschil te zijn tussen een statisch IP-adres en een **gereserveerd dynamisch IP-adres**. In beide gevallen identificeert hetzelfde IP-adres altijd dezelfde computer.

Toch zijn er verschillen:

1. Statische IP-adressen moeten in het toestel zelf worden vastgelegd, terwijl gereserveerde dynamische IP-adressen centraal kunnen beheerd worden via de DHCP-server.
2. Gereserveerde dynamische IP-adressen bevinden zich altijd binnen het DHCP-bereik – het bereik dat door de netwerkbeheerder toegewezen is voor dynamische adresseren. Statische IP-adressen bevinden zich buiten dat bereik.
3. Een computer met een gereserveerd dynamisch IP-adres zal bij elke inschakeling een DHCP-request naar een DHCP-server moeten sturen om zijn gereserveerde adres te bekomen. Een computer met een statisch IP-adres stuurt geen DHCP-request.

c) DHCPv6 en stateless address autoconfiguration

Al het bovenstaande geldt voor IPv4-netwerken. In netwerken op basis van IPv6 is het IP-adres van elke netwerkcomponent immers uniek, want gebaseerd op het MAC-adres. Wel bestaat er een mogelijkheid om het netwerknummer voor een lokaal netwerk dynamisch te verkrijgen - dit bestaat uit de eerste vier groepen van een IPv6 -adres. Hiervoor kan DHCPv6, een nieuwere versie van het DHCP-protocol gebruikt worden, maar meestal wordt het netwerknummer toegekend via **SLAAC** (*stateless address autoconfiguration*), een techniek waarmee netwerkcomponenten automatisch geconfigureerd worden voor een IPv6-netwerk. Dat gaat dan zo in z'n werk:

1

Link-local address generation

Een computer die zich op het netwerk aanmeldt, stuurt een verzoek met zijn MAC-adres. Dit adres is sowieso voor elke netwerkcomponent uniek. De SLAAC-host genereert een IPv6-adres dat start met de hexadecimale waarde FE80 in de eerste groep, dan drie groepen met de waarde 0 en vervolgens het unieke computernummer van de aanvragende computer, dat doorgaans gebaseerd is op het meegestuurde MAC-adres. Het IP-adres dat zo ontstaat wordt het **link-local adres** genoemd.

2

Link-local address uniqueness test

De SLAAC-host gaat na of het gegenereerde link-local address werkelijk uniek is. Daarvoor wordt gebruik gemaakt van **NDP** (*neighbour discovery protocol*), dat controleert of het adres al in gebruik is op het netwerk. Dit lijkt overbodig, aangezien het MAC-adres in het computernummer het link-local address al uniek maakt, maar er bestaan ook andere, veel minder vaak gebruikte technieken om IPv6-adressen te genereren waarbij het MAC-adres niet wordt gebruikt.

3

Link-local address assignment

Indien het link-local address slaagt in de uniqueness test, wordt het door de SLAAC-host toegewezen aan de aanvragende computer. Vanaf dan kan de computer communiceren binnen het lokale netwerk, maar nog niet op internet.

4

Router contact

De SLAAC-host probeert contact te maken met de router die het lokale netwerk voorziet van een netwerknummer.

5

Router direction

De SLAAC-host verkrijgt van de router het netwerknummer van het lokale netwerk. Dat kan door te wachten op een aanbod van een router (**router advertisement**) of door zelf op zoek te gaan naar een router (**router solicitation**).

6

Global address configuration

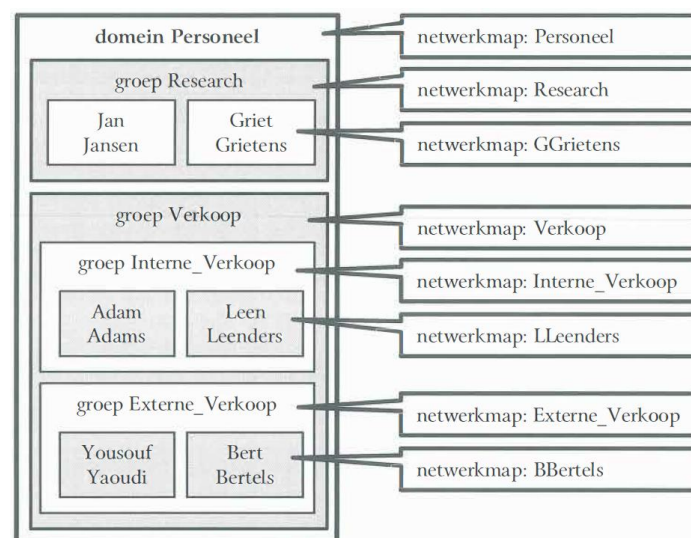
De SLAAC-host vervangt nu de eerste vier groepen uit het link-local address door het netwerknummer van het lokale netwerk. Op die manier ontstaat het **global address**. De SLAAC-host wijst nu dit global address toe aan de aanvragende computer, die vanaf dan kan communiceren met eender welke computer op het internet.

4.3.2 Domeincontroller

In een grote organisatie krijgen niet alle gebruikers dezelfde rechten en toegangen. In een groot bedrijf heeft de research-afdeling geen behoefte aan het inzien van de klantgegevens van het bedrijf, terwijl de verkoopafdeling niets kan aanvangen met informatie over labo-onderzoeken. Toch maken de computers van alle afdelingen deel uit van hetzelfde bedrijfsnetwerk.

Daarom wordt er binnen elk Windows-netwerk een domein aangemaakt. Een domein kan je beschouwen als het **logisch** netwerk binnen een **fysiek** computernetwerk. De server die zo'n domein beheert, wordt de **domeincontroller** of **domeinserver** genoemd. Binnen het domein wordt een lijst met gebruikers aangemaakt, net als een lijst met computers die door het domein vertrouwd worden en er toegang toe geven. Tenslotte worden de toegangsrechten tot netwerkmappen aan gebruikers toegekend.

Om dit overzichtelijk te maken, worden gebruikers in groepen samengenomen. Binnen een groep kunnen weer nieuwe groepen worden gemaakt. Elke gebruiker krijgt toegang tot de netwerkmappen waartoe hij individuele rechten bezit en tot de netwerkwerkmappen die toegankelijk zijn voor alle groepen en subgroepen waartoe hij behoort. Dit wordt duidelijker aan de hand van dit voorbeeld van een deeltje uit een bedrijfsdomein:



Alle gebruikers in dit domein hebben een eigen persoonlijke map en ze krijgen allemaal toegang tot de gezamenlijke map *Personeel*. *Bert Bertels* heeft eveneens toegang tot de map *Externe_Verkoop* omdat hij tot die groep behoort. Bovendien heeft hij toegang tot de map *Verkoop* omdat de groep *Externe_Verkoop* waartoe hij behoort deel uitmaakt van de groep *Verkoop*. De regels die een netwerkbeheerder voor groepen en gebruikers opstelt, worden **policies** genoemd.

Er bestaan verschillende niveaus van gebruikersrechten op netwerkmappen - die worden dan **permissions** genoemd:

- | | |
|------------------------|--|
| ◆ List folder contents | De gebruiker mag de inhoud van de map bekijken. |
| ◆ Read | De gebruiker mag bestanden in de map openen. |
| ◆ Read & execute | De gebruiker mag bestanden in de map openen of uitvoeren. |
| ◆ Modify / change | De gebruiker mag bestanden in de map wijzigen. |
| ◆ Write | De gebruiker mag nieuwe bestanden in de map aanmaken. |
| ◆ Full control | De gebruiker mag alle bewerkingen binnen de map uitvoeren. |

De indeling van gebruikers en computers in domeinen wordt door de **OU** (*organizational unit*) genoemd. De hiërarchische databank op een Windows die alle gegevens van de OU bevat, heet de **Active Directory**. Binnen één OU kunnen verschillende domeinen actief zijn en binnen een domein kunnen andere domeinen actief zijn in een zogenaamde boomstructuur.

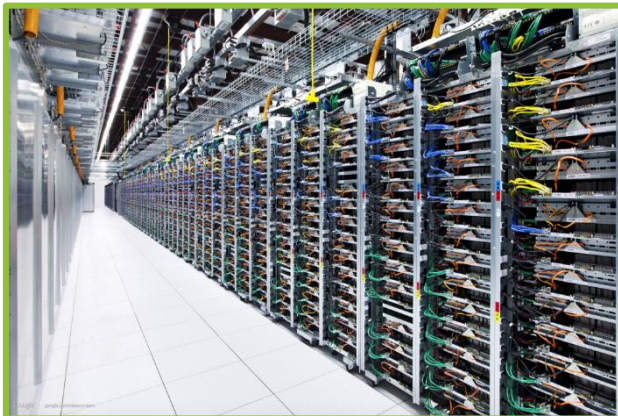
Het werken met domeinen werd bedacht door Microsoft. Omdat de computers in de meeste netwerken voorzien zijn van het Microsoft besturingssysteem Windows, bestaat er tegenwoordig ook software om domeinen te creëren en te beheren in andere netwerkbesturingssystemen zoals Linux servers.

Domeinen krijgen namen. Daarvoor is er samen met een domeincontroller ook een DNS-server actief die zorgt voor de naamgeving van het netwerk. Voor lokale netwerken zijn netwerkbeheerders vrij om zelf een naam én een domeinextensie (.be, .nl, .net...) te gebruiken. Het lokale domein is immers niet rechtstreeks toegankelijk vanuit het internet. Wel gebruikt men best niet dezelfde domeinnaam en -extensie als die reeds bestaat op het wereldwijde web. Een website is onbereikbaar vanuit een lokaal domein met exact dezelfde naam, tenzij de netwerkbeheerder de nodige DNS-omleidingen instelt.

DNS (*domain name system*) is een essentieel onderdeel in de werking van het internet.

4.3.3 Fileserver (bestandsserver)

Deze server is speciaal bedoeld om bestanden te bewaren die door verschillende gebruikers al dan niet gelijktijdig kunnen geopend en bewerkt worden. Elk werkstation op het netwerk kan geconfigureerd worden als fileserver, maar in grotere netwerken doet vaak een speciale computer daarvoor dienst. Zo'n computer moet dan uiteraard beschikken over een zeer grote opslagcapaciteit en is daarom voorzien van meerdere harde schijven, die doorgaans via **RAID** (*redundant array of independent disks*) samenwerken. Ook externe harde schijven met een netwerkaansluiting (**NAS**, *network attached storage*) kunnen vanuit het netwerk benaderd worden als een eenvoudige fileserver. Dit soort netwerkopslag is erg populair in thuisnetwerken.



Veel bedrijven werken niet enkel met eigen fileservers maar huren opslagcapaciteit bij een **datacenter** – dat is een bedrijf dat beschikt over een veilige ruimte waarin een heleboel servers bij elkaar staan. Precies die veiligheid en de zeer hoge beschikbaarheid zijn de voornaamste argumenten om de opslag van gegevens uit te besteden. Datacenters worden zo gebouwd dat ze volledig afgeschermd zijn van mogelijke gevaren van buitenaf. Ze zijn beveiligd tegen brand of overstrooming en kunnen naar eigen zeggen zelfs explosies of

vliegtuigcrashes weerstaan. Datacenters worden voortdurend geklimatiseerd en zoveel mogelijk stofvrij gehouden, zodat de apparatuur in optimale omstandigheden kan werken. Bij stroomuitval worden onmiddellijk noodaggregaten ingeschakeld om toch stroom te blijven leveren. Dankzij een goede back-up politiek en het gebruik van redundante systemen - dat zijn identieke servers die met elkaar verbonden zijn en steeds gesynchroniseerd worden - zijn gegevens ten allen tijde beschikbaar. Zo'n doorgedreven beveiliging is in een gewoon bedrijf moeilijker te realiseren. Via een beveiligde internetverbinding heeft de klant altijd toegang tot zijn gegevens. Bedrijven verzekeren zich er zo van dat belangrijke bedrijfsgegevens nooit verloren gaan.

Sommige fileservers hebben een specifieke functie. Fileservers die enkel gebruikt worden om back-ups op te slaan worden back-up servers genoemd. Het maken van de back-ups naar zo'n server verloopt doorgaans geautomatiseerd. Niet altijd worden **full back-ups** gemaakt. Veel vaker worden enkel gegevens naar de back-up server weggeschreven die gewijzigd werden na de laatste back-up - dat zijn dan **incrementele back-ups**.

Er bestaan drie soorten back-up servers:

Cold server	Warm server	Hot server
Een server waarop eenmalig een back-up wordt geplaatst en die verder blijft uitgeschakeld tot de back-up nodig is.	Een server waarop regelmatig back-ups worden geplaatst maar die na elke back-up weer wordt uitgeschakeld.	Een server die regelmatig back-ups maakt en niet wordt uitgeschakeld. Indien het toestel waarvan de hot server de back-ups bewaart, uitvalt, dan neemt de back-up server het werk onmiddellijk en automatisch over.

Een ander voorbeeld van een specifieke fileserver is een **database-server**. Daarop worden dan één of meer databanken bewaard. Op de server zelf wordt enkel het **back-end** gedeelte van de gegevensbank bewaard. Dat zijn de tabellen met alle gegevens in de databank. Alle interfaces en toepassingen om de gegevens te raadplegen of te manipuleren – formulieren, query's, rapporten, macro's, enz. – vormen samen het **front-end** gedeelte van de gegevensbank. Dat deel bevindt zich op gebruikerscomputers.

4.3.4 Mailserver

Een mailserver verzamelt de elektronische berichten voor alle gebruikers van het netwerk en bewaart ze tot wanneer ze worden afgehaald door de gebruikers. De toepassing op de mailserver die voor het verzenden en ontvangen van elektronische berichten over het netwerk zorgt, wordt **MTA** (*mail transfer agent*) genoemd. De gebruiker merkt van de MTA eigenlijk niets, want hij zal enkel communiceren via de toepassing die lokaal op zijn computer draait om berichten te verzenden en te versturen. Die lokale toepassing wordt dan **MUA** (*mail user agent*) genoemd.

Een MTA is opgebouwd uit twee onderdelen: een **MSA** (*mail submission agent*) die instaat voor het verzenden van berichten naar andere mailservers en een **MDA** (*mail delivery agent*) die de berichten aflevert aan de gebruikers. In de praktijk zitten ze samen vervat in eenzelfde servertoepassing. Wanneer je een e-mail verstuurt zal de MTA van je provider nagaan of dit bericht bedoeld is voor een van de eigen agents. Indien dat niet het geval is, wordt het bericht doorgestuurd naar een volgende MTA. Elke MTA die het bericht ontvangt en weer doorgeeft voegt een stukje informatie toe aan de headers van het e-mail bericht. Op die manier kan de route die een e-mail heeft afgelegd van de zender tot aan de ontvanger worden gereconstrueerd.


```

From: janedoe@acme.com Tue Jan 27 23:06:24 2000
Return-Path: <janedoe@acme.com>
Received: from mailhost.widget.com (mailhost.widget.com [12.9.120.1.1])
    by workstation1.widget.com (8.8.7/8.8.7) with ESMTP id XAA25079
    for <qpublic@workstation1.widget.com>; Tue, 27 Jan 2000 23:06:23 -0600 (CST)
Received: from acme.com (janedoe@fohnix.acme.com [192.245.137.2])
    by mailhost.widget.com (8.8.8/8.8.8) with SMTP id XAA09696
    for <qpublic@widget.com>; Tue, 27 Jan 2000 23:10:53 -0600 (CST)
Received: by acme.com id AA27837
    (5.67a/IDA1.5hp for qpublic@widget.com); Tue, 27 Jan 2000 23:10:49 -0600
From: janedoe <janedoe@acme.com>
Message-Id: <200001280510.AA27837@acme.com>
Subject: Re: 1/26/00 Meeting Notes
To: qpublic@widget.com
Date: Tue, 27 Jan 2000 23:10:48 -0600 (CST)
In-Reply-To: <200001271545.JAA24165@workstation1.widget.com> from "J.Q. Public" at Jan 27,
    98 09:45:11 am
Reply-To: janedoe@acme.com
Return-Receipt-To: janedoe@acme.com
X-Mailer: ELM [version2.4 PL24]
Mime-Version: 1.0
Content-Type: text/plain; charset=US-ASCII

```

Internetproviders voorzien vaak een basisbescherming voor hun klanten door middel van spamfilters en antivirusscanners op de mailserver. Op die manier kunnen spamberichten en virussen onschadelijk worden gemaakt vooraleer ze de bestemming kunnen bereiken. Waterdicht is die bescherming echter nooit.

4.3.5 Printserver

Een printserver verzamelt alle afdrukopdrachten voor een printer, plaatst ze in de gewenste afdrukvolgorde en stuurt ze door naar de printer om afgedrukt te worden. Indien een printer voorzien is van een netwerkaansluiting, beschikt ze over een eigen printserver. Er hoeft dan geen computer als printserver te worden ingesteld. Bij sommige printers beschikken zelfs over een draadloze netwerkmodule, zodat de printer rechtstreeks beschikbaar kan worden gemaakt via een draadloos netwerk. Je kan van een printer zonder netwerkfuncties een onafhankelijke netwerkprinter maken via een externe printserver die voorzien is van een ingang voor een netwerkkabel, een antenne voor draadloos netwerk of beide (zie afbeelding).



In een netwerk kan je eender welke computer inschakelen als printserver voor een lokaal aangesloten computer. De mogelijkheid daarvoor zit ingebouwd in elk besturingssysteem. Je hebt er dus zeker geen aparte servermachine voor nodig. Een printer die lokaal geïnstalleerd wordt en via het werkstation beschikbaar wordt gemaakt voor het netwerk, wordt een **gedeelde printer** genoemd. Een printer met een ingebouwde printserver wordt een **netwerkprinter** genoemd.

4.3.6 Application server (toepassingsserver)

Op een application server bevinden zich computerprogramma's (toepassingen) die door de gebruikers via een workstation worden uitgevoerd. Een workstation vraagt een bepaalde functie uit te voeren op de application server, die na de verwerking het gevraagde resultaat zal terugsturen. De verwerkingscapaciteit van dat workstation wordt minimaal belast, terwijl de server maximaal wordt belast. Als je dit consequent toepast in een netwerk - alle software wordt op de application server samengebracht en het workstation doet enkel dienst als doorgeefluik naar die application server, spreekt men van het **thin client-model**. Application servers die hun diensten aanbieden op het wereldwijde web worden **web application servers** genoemd.

Voordelen van het werken met een application server:

1. Je kan de beschikbare software makkelijker up-to-date houden.
2. Werkstations hoeven niet aan erg hoge eisen te voldoen.
3. Je bespaart kosten aangezien werkstations minder snel moeten vervangen worden.
4. Het is eenvoudiger om het netwerk vrij te houden van malware.
5. Je bespaart energie indien je werk met thin clients.
6. Thin clients zijn nutteloos buiten het netwerk dus minder diefstalgevoelig.

Aan de machine waarop de application server draait, worden wel hoge eisen gesteld. Hoe meer clients die moet bedienen, hoe performanter het systeem moet zijn.

De meeste misverstanden betreffen het probleem van de **softwarelicenties**. Sommigen denken dat, aangezien de toepassing enkel draait op de server, er enkel voor die server een licentie nodig is, maar dat klopt doorgaans niet. In de meeste gevallen zal je eveneens licenties moeten aankopen voor alle werkstations of alle gebruikers.

Thin clients zijn werkstations met een zeer beperkte verwerkingscapaciteit. Dat kunnen oudere, afgeschreven computers zijn, maar er worden ook thin clients verkocht die speciaal voor dit doel vervaardigd worden. Dat soort thin clients beschikt over een beperkte of zelfs helemaal geen opslagcapaciteit en is meestal voorzien van een specifiek besturingssysteem, zoals Windows Embedded of het Linux gebaseerd Thin OS. Verder vind je op een thin client geen optisch station terug en heel wat minder aansluitingen voor randapparaten. Een thin client is veel stiller en minder onderhevig aan slijtage dan een gewone computer. De grafische prestaties zijn erg beperkt; een thin client is immers geen multimediamachine. Doorgaans zitten thin clients in een behuizing die wat lijkt op een grote externe harde schijf, maar er bestaan ook thin clients die ingebouwd worden in de behuizing van een beeldscherm.



4.3.7 Webserver (informatieserver)

Op een webserver bevinden zich webpagina's die door internetgebruikers in de hele wereld of intranetgebruikers van een bedrijfsnetwerk via een browser kunnen worden geraadpleegd. Webservers bestaan in twee soorten:

In-kernel webserver	User mode webserver
Een webserver die geïntegreerd is in het besturingssysteem. Dit soort webserver zijn dedicated servers: ze worden enkel voor deze servertoepassing gebruikt. Dergelijke webserver zijn erg performant omdat ze kunnen beschikken over alle hardware bronnen, van het computersysteem waarop ze draaien. Voorbeelden van in-kernel webserver zijn het op Linux gebaseerde TUX en Apache HTTP Server.	Een webserver die als een computertoepassing op een computer wordt geïnstalleerd. Het computersysteem waarop de webserver draait kan nog andere taken vervullen. De serverdienst werkt trager dan een in-kernel webserver, maar deze oplossing is wel veel goedkoper. De bekendste user mode webserver is Microsoft IIS (<i>Internet Information Services</i>).

Webserver accepteren informatieaanvragen via het **HTTP**-protocol (*hypertext transfer protocol*) en beantwoorden die door de gevraagde documenten ter beschikking te stellen. Typisch daarvoor zijn de informatiepagina's die in de **HTML**-code (*hypertext markup language*) werden opgemaakt, maar het kunnen ook gewone tekstdocumenten, afbeeldingen of multimediabestanden zijn.

De webmaster, de beheerder van een website, moet uiteraard in de mogelijkheid worden gesteld om de nodige bestanden te uploaden naar de webserver. Hiervoor wordt meestal een **FTP**-toepassing (*file transfer protocol*) gebruikt. Op het computersysteem waar de webserver draait, is daarom ook een FTP-servertoepassing actief die ervoor zorgt dat de bestanden die een webmaster uploadt, in de juiste map terechtkomen zodat ze kunnen geraadpleegd. Die toepassing zorgt er eveneens voor dat de webmaster enkel toegang heeft tot de bestanden van zijn eigen website en niet die van andere websites die eventueel ook nog op dezelfde webserver geplaatst werden.

Het uploaden van informatie naar een webserver gebeurt dus op een totaal andere manier dan het raadplegen van die informatie door de internetgebruikers. Dat moet beheerders van webserver systemen in de mogelijkheid stellen om hun webserver voldoende te beveiligen. Sommige crackers maken er immers een sport van om in te breken in webserver en informatiepagina's te wijzigen. Dat is een vorm van **defacing** waar vele grote bedrijven in de IT-wereld al mee te maken hebben gehad.

Sommige netwerkapparaten zoals switches of netwerkprinters beschikken over een ingebouwde webserver. Die dient niet om informatiepagina's weer te geven, maar wordt gebruikt om de instellingen van het apparaat te raadplegen of te wijzigen. Op die manier hoeft er op de computer van de beheerder geen speciale beheerderssoftware te worden geplaatst en kunnen de apparaten beheerd worden van op eender welke computer op het netwerk.

Web hosting bedrijven verhuren opslagruimte aan een webserver waarbij elke klant een afgeschermd map ter beschikking krijgt. Een erg populaire website kan flink wat capaciteit wegkapen van andere websites die op dezelfde server gehost worden. De andere websites worden daardoor moeilijker of trager bereikbaar.

Tegenwoordig kan je bij een web hosting bedrijf ook een **VPS** (*virtual private server*) huren. Dat is een virtuele webserver die op een krachtig computersysteem draait. Vaak draaien op zo'n toestel tientallen virtuele webserver, die elk een gereserveerd stukje van de hardware bronnen (processor- en geheugencapaciteit) gebruiken. Websites die op een VPS gehost worden, ondervinden geen invloed van de drukte op een website die op een andere VPS op dezelfde machine gehost wordt. Bovendien biedt een VPS meer mogelijkheden aan de klant. Die kan de VPS als een volledige onafhankelijke webserver beheren en heeft geen last van beperkingen die een webhost om veiligheidsredenen op een klassieke web hosting server legt. Dat kan vooral belangrijk zijn wanneer men actieve inhoud wil hosten, zoals online applicaties, content management systemen, gameservers of gegevensbanken.

Hoewel het voornamelijk voor webserver wordt toegepast, kan VPS gebruikt worden voor eender welke andere serverdienst.

4.4 Netwerkbesturingssystemen

Sommige serverdiensten kunnen geconfigureerd worden binnen een klassiek besturingssysteem: van eender welke netwerkcomputer kan je een fileserver of een printserver maken. Voor andere serverdiensten zoals een DHCP-server of een domeincontroller heb je een specifiek netwerkbesturingssysteem (**NOS** of *network operating system*) nodig. Belangrijke serverdiensten maken integraal deel uit van het netwerkbesturingssysteem. Serverdiensten kunnen eveneens als applicatie bovenop een netwerkbesturingssysteem worden geïnstalleerd.

Er bestaan twee soorten netwerkbesturingssystemen:

Algemeen NOS	Embedded NOS
Een netwerkbesturingssysteem dat geïnstalleerd kan worden op een computersysteem wordt een algemeen NOS genoemd. Ze beschikken over een eigen grafische interface die doorgaans erg lijkt op die van een gebruikerscomputer. Niet verwonderlijk, aangezien die interface meestal van een standaard besturingssysteem werden afgeleid. Een algemeen NOS kan je los van het computersysteem waarop het geïnstalleerd wordt, aanschaffen. Bekende voorbeelden zijn Windows Server, MacOS X Server en diverse op Linux en Unix gebaseerde netwerkbesturingssystemen.	De software die een netwerkkapparaat zoals een netwerkprinter, een switch of een router doet werken, wordt een embedded NOS genoemd. Die wordt ontwikkeld door of in opdracht van de fabrikant van het apparaat en wordt er niet afzonderlijk van verkocht. Aangezien dit soort van apparaten niet van een eigen beeldscherm voorzien is hebben ze geen geïntegreerde grafische interface. Doorgaans kan je ze beheren met een web interface die je opent binnen een browser van eender welke computer op het netwerk.

Netwerkbesturingssystemen zijn op enkele punten verschillend van besturingssystemen voor gebruikerscomputers:

- ◆ Netwerkbesturingssystemen zijn speciaal ontworpen voor serverdiensten.
- ◆ Netwerkbesturingssystemen kennen meer doorgedreven beveiligingsmogelijkheden.
- ◆ Netwerkbesturingssystemen hebben niet noodzakelijk een grafische interface.
- ◆ Netwerkbesturingssystemen zijn doorgaans stabiel.
- ◆ Netwerkbesturingssystemen zijn ontworpen om op complexere hardware te draaien.
- ◆ Netwerkbesturingssystemen volgen vaak een andere licentiepolitiek.

Vooraf bij commerciële netwerkbesturingssystemen worden vreemde regels gehanteerd voor het toekennen van een geldige licentie. Zo was de kostprijs van een Windows Server licentie vaak afhankelijk van het aantal aangesloten werkstations of het aantal gebruikers, maar er zijn ook Windows-producten waarbij het aantal processoren in een server als criterium geldt.