Pctuts.be
Computer Help forum

Versie

2009 - 2010

CURSUS NETWERKEN

Gemaakt voor PCTUTS.be door Yveske

Inhoudstabel

Hoofdstuk 1: Inleiding

Een computernetwerk ontstaat door verschillende computers en randapparaten onderling met elkaar te verbinden. Er wordt gesteld dat twee computers onderling met elkaar verbonden zijn als ze in staat zijn informatie uit te wisselen.

Om een netwerk samen te stellen, moet je hardwarecomponenten met elkaar verbinden, rekening houdend met de vereisten en specificaties van een gekozen netwerkarchitectuur en netwerk voorzien van een netwerkbesturingssysteem om het zaakje te beheren.

Hoofdstuk 2: Bouwstenen voor een thuisnetwerk - Hardware

2.1 Netwerkkaart voor een computer

Voordat je een computernetwerk gaat aanleggen moet elke computer uitgerust zijn met een netwerkkaart. Vaak hebben computers een ingebouwde netwerkkaart op het moederbord. Zo niet, wordt er gebruik gemaakt van een PCI netwerkkaart die in een PCI slot op het moederbord gezet wordt. (zie afbeelding)

De gangbare snelheid voor een netwerkkaart was 10/100 Mbits. Tegenwoordig is 1 Gigabit de gangbare snelheid. 1 Gigibit maakt een doorvoersnelheid van zo'n 1000 mb per seconde mogelijk, mits er aan de andere kant ook een 1 Gigabitskaart aanwezig is natuurlijk.

2.2 Netwerkkaart voor een draagbare computer

Deze kaart heeft de vorm van een dikke netwerkkaart en wordt gebruikt (althans vroeger) om draagbare computers (waar geen netwerkkaart ingebouwd zit) aan te sluiten op het netwerk. De huidige generatie van draagbare computers heeft een netwerkkaart ingebouwd. De PC-kaart wordt meestal gebruikt om draagbare computers op een draadloos netwerk aan te sluiten.

2.3 Draadloze netwerk-interface voor een computer of draagbare computer

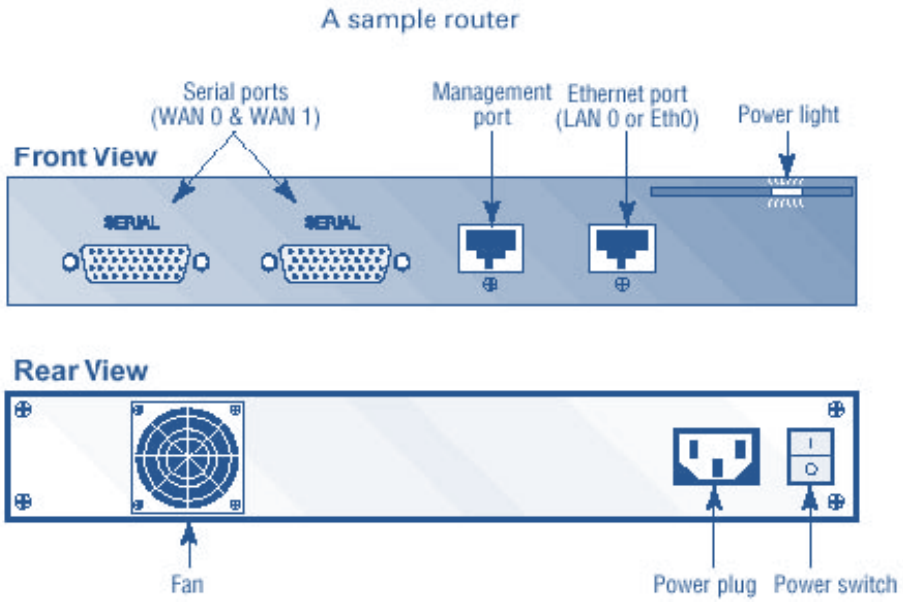
Een "wireless"-netwerkinterface is een zender die aan de client wordt gekoppeld zodanig dat de gebruiker verbinding kan maken met een "wireless"-station. Deze interface kunnen in de vorm van een netwerkkaart, PC-kaart of USB-zendstation gekocht worden. Ze hebben telkens de zelfde functie. Signalen die draadloos verzonden worden door het station op te vangen en door te geven aan de client die op zijn beurt signalen terug zendt naar het station.

2.4 Router

Om pakketten uit te wisselen tussen computers op totaal verschillende netwerken, moet er een mechanisme gebruikt worden waarbij de pakketten van het ene netwerk naar het andere doorgegeven worden via een aantal tussenstations.

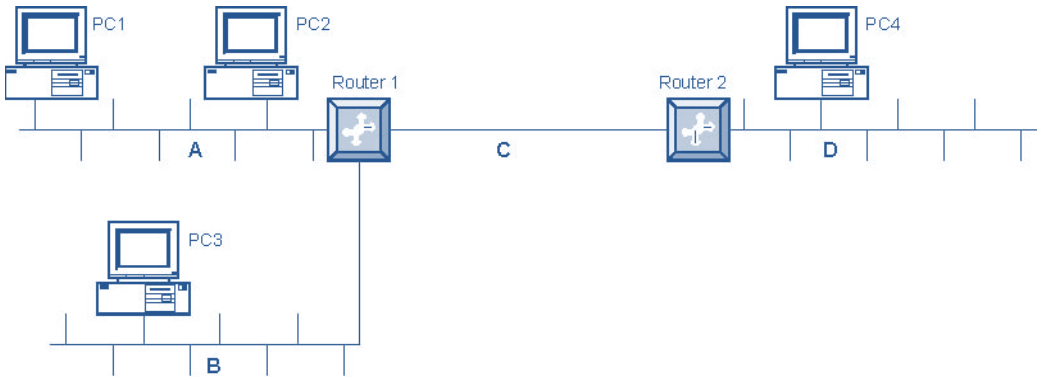
Een dergelijk tussenstation dat bepaalt welke route een pakket zal nemen wordt een **router** genoemd. Een router is een toestel dat instaat voor het doorgeven van pakketten van het ene netwerk naar het andere, net zoals een bridge, maar deze keer op basis van het logische adres.

Een router is gesofisticeerder dan een bridge. Routers openen datapakketten, zetten de inhoud om in een ander type pakket en versturen dat pakket. De ontvangende router zal de data opnieuw omzetten en verder versturen. Hierbij gebruikt hij packetswitching: in elk tussenstation wordt op basis van het netwerkadres van de bestemming beslist wat het volgende tussenstation is waar het pakket naar toe moet. Dit wordt de next hop genoemd.



Net zoals bij een bridge worden voor de routing tabellen gebruikt. Een belangrijk verschil met de equivalente werking van een bridge is dat wanneer een bestemmingsnetwerk niet voorkomt in de routertabellen, het pakket niet zal doorgegeven worden naar alle poorten, maar naar één welbepaalde default router. Hierdoor kan de lengte van de routertabellen sterk beperkt worden, en wordt ook het inter-netwerk verkeer beperkt.

2.4.1 Voorbeelden



Eerste situatie: een pakket moet van pc1 naar pc2

Pc1 detecteert op basis van het IP-adres van pc2 dat beiden op hetzelfde netwerk aangesloten zijn. Pc1 bepaalt het MAC-adres van pc2, en verstuurt het pakket rechtstreeks naar pc2.

Tweede situatie: een pakket moet van pc1 naar pc3

pc1 detecteert dat pc3 niet op hetzelfde netwerk aangesloten is, en geeft het pakket door naar de default router. Voor pc1 is dit router 1. Router 1 ziet dat het pakket bedoeld is voor een computer op een aanliggend netwerk (B). Router1 bepaalt het MAC-adres van pc3 en geeft het pakket dan rechtsreeks door naar pc3 via netwerk B.

Derde situatie: een pakket moet van pc1 naar pc4

pc1 detecteert dat pc4 niet op hetzelfde netwerk aangesloten is, en geeft het pakket door naar router 1. Na raadpleging van zijn interne routertabellen geeft router 1 het pakket door naar router 2. Router 2 ziet dat het pakket bedoeld is voor een computer op een aanliggend netwerk (D), bepaalt het MAC-adres van pc4 en geeft het pakket dan door naar pc3 via netwerk D.

2.4.2 Kenmerken van routers

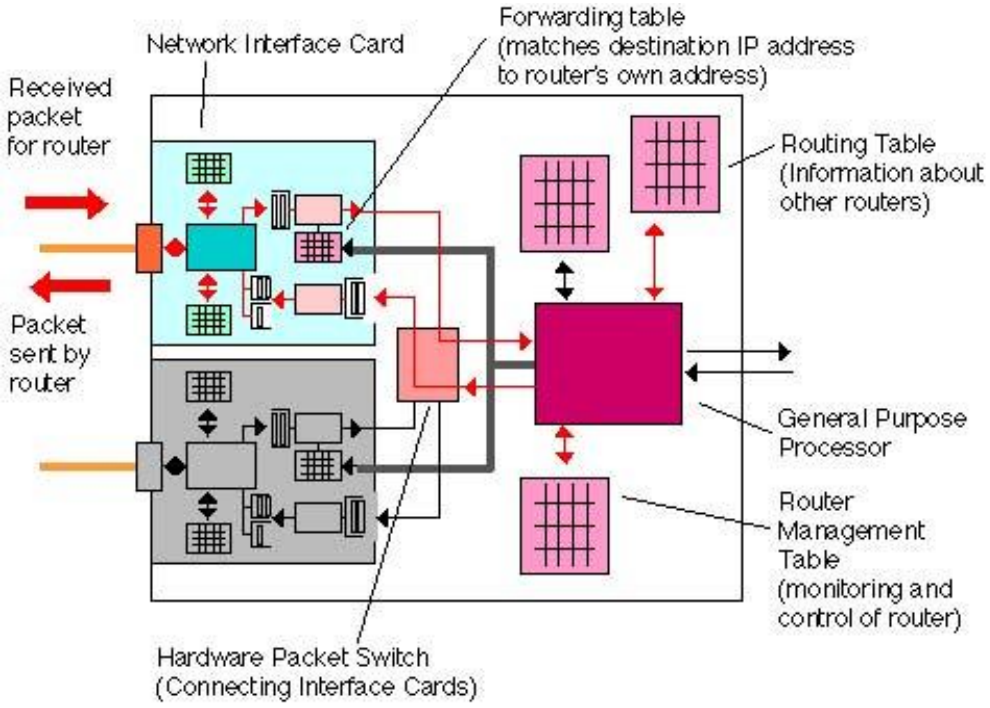
- Vermits de adressering specifiek is voor een bepaald **netwerk-protocol**, zal een router slechts pakketten kunnen verwerken voor de protocols die hijzelf 'kent'. In de praktijk zijn de meeste routers tegenwoordig 'multi-protocol-routers'. Dit betekent dat ze meerdere protocollen aankunnen (typisch IP, IPX, Appletalk, XNS).
- Routers **communiceren** onder elkaar, onder meer om de goede route te bepalen voor bestemmelingen, om alternatieve routes te melden, enz…
- Bij het doorgeven van pakketten kunnen in een router verschillende **strategieën** gevolgd worden: 'minimal delay', 'lowest cost', 'maximum capacity',…
- **Static** routers zullen de data altijd langs dezelfde weg versturen, terwijl **dynamic** routers de weg zullen kiezen (zoals vastgelegd in hun specificaties).
- In tegenstelling tot de bridges kennen de routers de exacte plaats van bestemming niet. Zij werken met subadressen en versturen de pakketten naar een bepaald netwerk dat er dan zijn plan mee trekt.

- Om te verhinderen dat pakketten door configuratiefouten blijven circuleren tussen routers, krijgt elk IP-pakket bij de creatie een **Time To live** mee: een teller die in elke router die gepasseerd wordt verlaagd wordt. Krijgt die teller in een router de waarde nul, dan wordt het pakket niet meer verder doorgegeven, en wordt een foutbericht naar de afzender verstuurd.

- De verbinding tussen netwerken gebeurt vaak met behulp van WAN-verbindingen over modems en dergelijke. Het kan dan ook gebeuren dat in de router een **modem** ingebouwd zit of dat er poorten beschikbaar zijn onder de vorm van seriële verbindingen (synchroon, asynchroon, V35).

- Vrij recent is de technologie van **switches** ook beschikbaar voor routers. Het doorschakelen van pakketten gebeurt dan volledig in hardware (snelheid), maar wel op basis van het logisch netwerkadres (i.p.v. het MAC-adres). Er wordt dan gesproken over **switching routers** (of **layer-3 switches**). Deze toestellen zijn overigens nog relatief duur.

- Routers zullen individuele pakketten doorsturen maar hebben geen enkel zicht op de verbinding of sessie waar die pakketten deel van uitmaken. Het is dan ook perfect mogelijk dat verschillende pakketten uit één verbinding verschillende routes zullen volgen om uiteindelijk bij de bestemming te geraken. Hierbij kan ook de volgorde waarin pakketten toekomen op de bestemming niet op voorhand gegarandeerd worden.



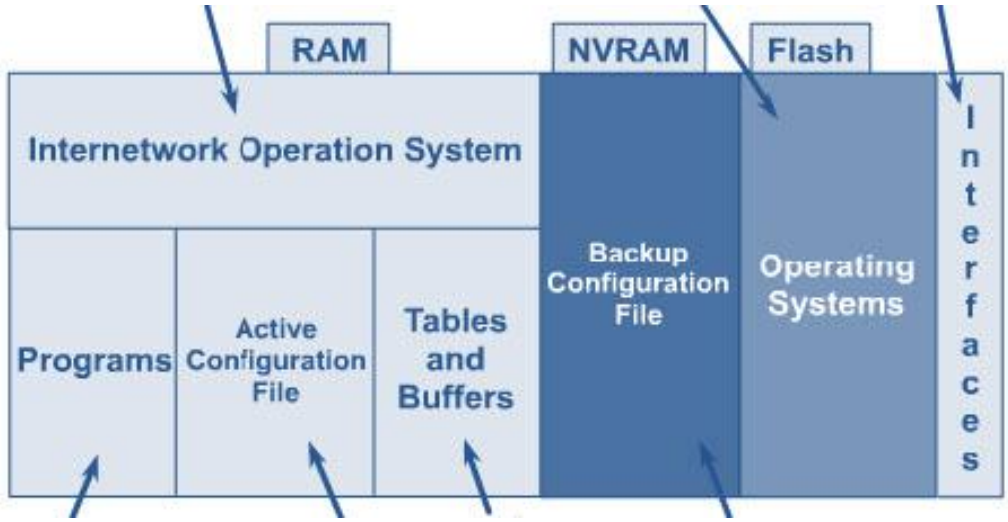
Behalve voor het onderling verbinden van netwerken, kunnen routers ook gebruikt worden om een netwerk intern te structureren. Er wordt in dat geval gesproken over **subnetten** en **subnetting**. Nochtans wordt deze techniek steeds minder toegepast, onder andere vanwege de complexiteit voor het beheer en het aantrekkelijke alternatief van de switches.

2.4.3 Besturingssysteem van een router

Een router heeft dezelfde bouw als een computer, deze bezit ook een geheugen, een vorm van een harde schijf die meestal uitgevoerd wordt in Flashgeheugen en een besturingssysteem.

Het is niet zo alle fabrikanten hetzelfde besturingssysteem gebruiken. Per fabrikant is meestal een andere versie van het besturingssysteem ter beschikking.

Als je gebruik maakt van Cisco-routers, dan noemt het besturingssysteem IOS (Internetwork Operation System). Je hebt het voordeel dat alle routers van deze fabrikant hetzelfde IOS gebruiken en dat nieuwe versies van IOS gemakkelijk implementeerbaar zijn op een oudere router.



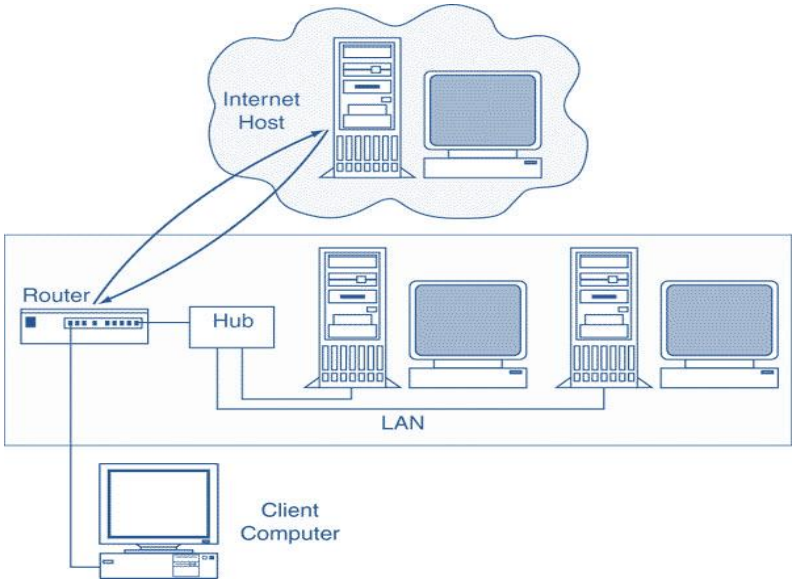
2.4.4 Soorten routers

Er zijn verschillende soorten routers, maar in de praktische netwerken worden ze vooral in twee verschillende functies gebruikt.

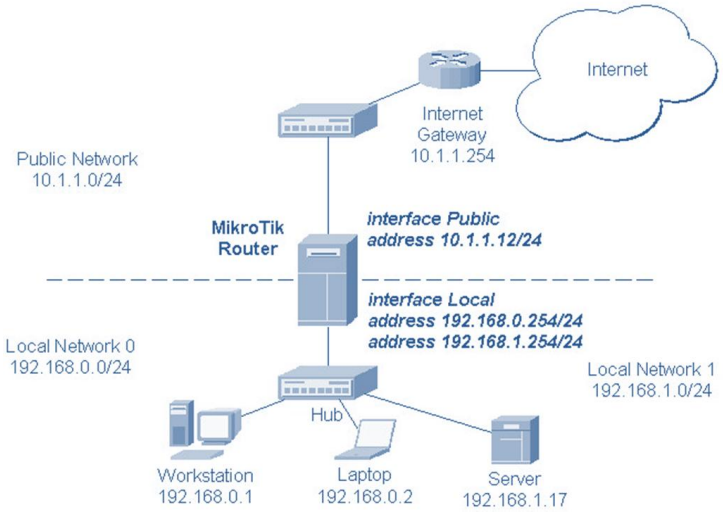
- **LAN tot Internet-routers**

Dit zijn routers die gebruikt worden om een verbinding te maken tussen een lokaal netwerk en het Internet.

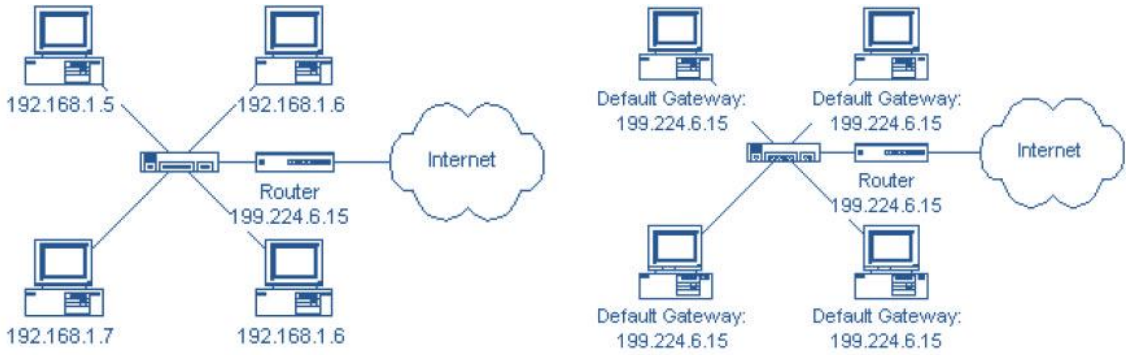
Er zijn verschillende manieren om een verbinding te realiseren met het Internet. Dit bepaalt ook het type router dat je nodig hebt. Je hebt routers die een ASDL-verbinding ondersteunen, ADSL over een ISDN-lijn, routers waar je nog een modem kunt achter plaatsen, …



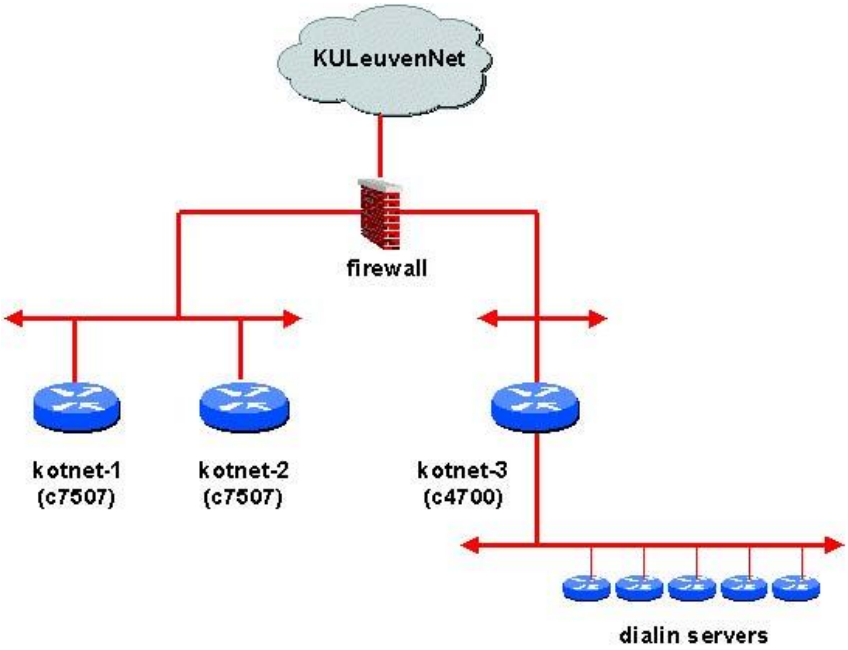
Deze soort routers hebben ook bijna altijd een NAT-functie in zich. **NAT** staat voor **Network Adress Translation** en betekent dat een computer binnen een lokaal netwerk allemaal een eigen lokaal privaat IP-nummer hebben. De router vertaalt dit inwendig IP-nummer in een IP-nummer dat kan gebruikt worden op het Internet. De router verzorgt de communicatie met de buitenkant, zowel voor binnenkomend als voor uitgaand verkeer.



De computers in het lokale netwerk hebben allemaal de router als **default gateway** in hun configuratie staan.



• **LAN to LAN-routers**



• **Internetrouters**

Op het Internet zijn het routers die de weg bepalen die een pakket dient te volgen om zijn bestemming te bereiken.

2.5 Hub en Switches

Een hub of switch is een netwerkkruispunt. Hubs en switches zijn voorzien van poorten om UTP kabels in te steken. Je kunt zo netwerkcomputers met elkaar verbinden.

Een hub en een switch voeren dezelfde taak uit op een verschillende manier. Een switch stuurt data direct naar de juiste computer door, terwijl een hub data stuurt naar alle computers in een netwerk. De computers beslissen dan zelf of de data voor hen bestemd is of niet.

Het snelheidsverschil is voor thuisnetwerken echter niet merkbaar bij het surfen op internet, maar wel bij het versturen van bestanden tussen netwerkcomputers. Een switch is aan te raden, zeker gezien het geringe prijsverschil met een hub.

Het uitzicht van beide is gelijk. Op het zicht is het dus niet mogelijk een onderscheid te maken tussen een hub en een switch. In het gebruik daarentegen voel je duidelijk een snelheidsverschil.

2.6 Gateway

Om grote structuurverschillen tussen verschillende systemen op te lossen, gebruikt men **gateways**. Een gateway leest een datapakket volledig en vormt het om naar een bruikbaar dataformaat voor de ontvanger. Een mainframe heeft meestal een ander frame-formaat dan een gewone pc. Wanneer de pc gekoppeld wordt aan de mainframe is een gateway onvermijdelijk omdat het werkstation anders de gegevens van de mainframe niet kan lezen.

2.7 Bekabeling

De bekabeling is de ruggegraat van het netwerk. Ze dient om de signalen en hiermee de gegevens van de ene pc naar de andere pc over te brengen. Er zijn verschillende types die kunnen gebruikt worden. Elk heeft zijn specifieke eigenschappen. Binnen elke type zijn er meerdere kwaliteiten.

Er zijn 3 groepen van bekabeling:

- Coax kabel
- Twisted pair
- Fiber optic

2.7.1 Coax

Coax bestaat uit een vaste koperen geleider die omgeven is door de isolatie, een metalen vlechtwerk en daarrond een plastic buitenrand. Langs de koperen geleider verplaatst het elektrische signaal zich. De isolatie houdt de geleider tegen om contact te hebben met andere geleiders. Het metalen vlechtwerk houdt elektrische signalen die van buitenaf kommen tegen, zodat ze het signaal op de

geleider niet storen. De coax kabel heeft een heel sterke weerstand tegen storende signalen van buitenaf.

2.7.1.1 Soorten

- **Thin coax**

Een buigzame kabel met een dikte van 0.25 inch. De kabel wordt rechtstreeks op de netwerkkaart aangesloten. De kabel is goedkoop en eenvoudig te installeren. Hierdoor wordt hij vaakst gebruikt in kantoren

- **Thick coax**

Een onbuigzame kabel van 0.5 inch doorsnede. De kabel wordt op een apart apparaatje los van de computer aangesloten. Dit apparaatje is op zijn beurt aan de computer gekoppeld. Thick coax heeft als voordeel dat het signaal erover verder kan gestuurd worden dan bij Thin. De weerstand tegen signalen van buitenaf is nog sterker. In industrieën en voor grotere afstanden is dit de aangewezen kabel.

Coax lijkt op de normale kabel die we kennen van de kabel-TV. Toch zijn ze niet onderling uitwisselbaar. Het verschil zit hem in de weerstandsfactor.

Crosstalk: is een storing van het signaal dat optreedt door dat meerdere kabels te dicht bij elkaar liggen. Hierdoor beïnvloedt de ene de andere kabel.

Attenuation: is het verlies van de signaalsterkte over een lange afstand.

2.7.2 Twisted Pair

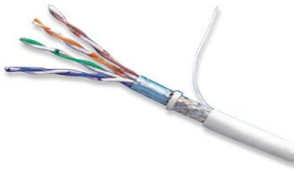
Twisted-pair bestaat uit twee geïsoleerde koperen draden die rond elkaar zijn gedraaid. De kabels voor normale telefonie zijn ook twisted-pair kabel. Doordat in vele kantoren reeds (ongebruikte) telefoonkabels liggen kunnen deze gebruikt worden.

2.7.2.1 Soorten

- **UTP (Unshielded Twisted-Pair)**

Deze is flexibeler, maar heeft geen metaalfolie, enkel een plastiek omhulsel (net als STP).

- **FTP (Foiled Twisted-Pair)**



Deze heeft enkel een metaalfolie om alle draden heen, niet per paar draden.

- **STP (Shielded Twisted-Pair)**

Dit houdt in dat iedere paar van draden omhuld is met een metaalfolie en dat het geheel van deze paren ook nog eens omhuld is met zo'n folie.

2.7.2.2 Categorieën

Onthoud de volgende 3 categorieën van dit soort bekabeling. Een hogere categorie betekent een betere kwaliteit.

5	Hoge snelheid tot 100 Mbps – UTP cat5
5e	Snelheid tot 1 Gbps – FTP cat5e
6	Snelheid tot 1 Gbps – STP cat6

2.7.3 Fiber Optic

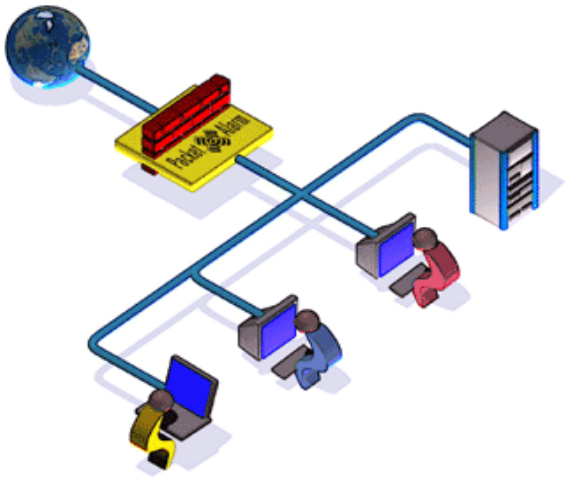
Dit is glasvezel bekabeling. Hier is geen elektrische signaal maar er zijn lichtpulsen. Vanzelfsprekend is dit een heel snel medium. Het heeft totaal geen last van elektrische storingen.

Belangrijk bij dit soort kabels is, dat het signaal niet opgevangen worden van buitenaf. Hierdoor is het een veilige bekabeling, de data kan niet gestolen worden.

De kabel bestaat uit 2 heel dunne cilinders van glas. Deze zijn nogmaals door glas of plastic omgeven. Dit alles is nogmaals omgeven door een buitenrand in Kevlar. In de cilinder passeert de lichtpuls. Elke cilinder wordt in één richting gebruikt. Snelheden kunnen tot 1 Gbps gaan.

Het nadeel van fiber optic kabels is dat ze heel erg duur zijn en dat het specialistenwerk is om ze te installeren.

2.8 Bridge



Een bridge kan zoals een repeater het netwerk groter maken, maar doet meer. Terwijl een repeater elk signaal dat binnenkomt verder zendt zal een bridge slechts een deel van de signalen verder sturen. Door een bridge te plaatsen krijgt men dus 2 netwerken. Een links en een rechts. De bridge oordeelt of een binnenkomend signaal voor het linkse of het rechtse deel bestemd is. Op basis hiervan zal het signaal doorgezonden worden of niet. Dit gebeurd door het controleren van het bestemmings-adres. Ligt het bestemmings-adres aan dezelfde kant als de verzender dan wordt het niet verder gezonden, zoniet wordt het verder gezonden op elke andere poort.

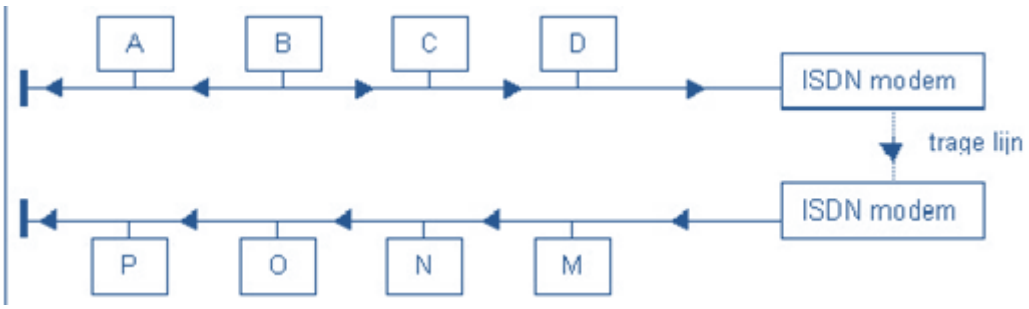
Een bridge wordt vooral gebruikt om een netwerk onder te verdelen in meerdere subnetwerken. Hierdoor wordt de traagheid van grote netwerken omzeild.

Door een signaal dat een computer over de kabel stuurt dat elke andere computer moet bereiken kan dit bij een groot aantal computers een traag netwerk opleveren. Wanneer een deel van de computers gescheiden zijn van de rest door een trage verbinding (modem of ISDN) zal dit zeker een probleem opleveren. Door net voor en net na de trage verbinding een bridge te plaatsen, wordt vermeden dat een signaal dat voor hetzelfde deel van het netwerk bestemd is als de zender, over deze trage lijn gaat.

Voorbeeld: Een netwerk bestaande uit 2 delen, elk met een 20-tal computers, gescheiden door een ISDN modem. Het netwerk werkt op 10 Mbs, de ISDN-lijn slechts op 64 Kbps. Het netwerk werkt dus 160 x sneller dan de trage verbinding ertussen.

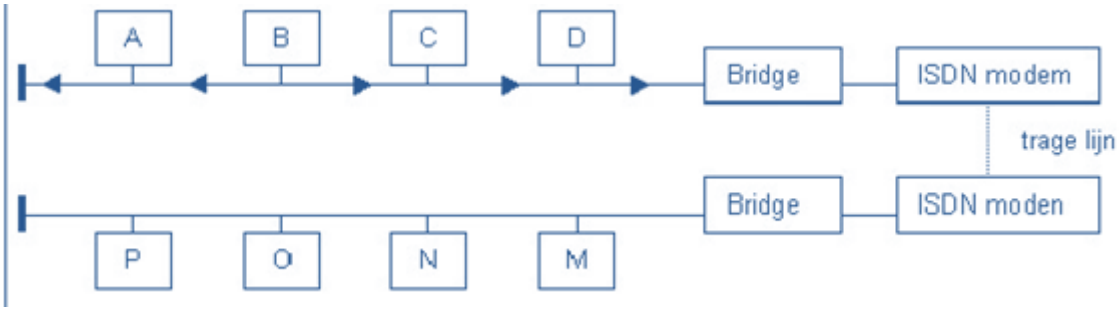
- **Situatie zonder bridge**

Computer B zendt een signaal dat voor computer A bestemd is. In bepaalde gevallen komt het signaal over de trage lijn toch in het tweede netwerk terecht. De rest van het netwerk kan niet verder werken zolang het signaal niet geabsorbeerd is door de terminator.



- **Situatie met bridge**

Computer B zendt een signaal dat voor computer A bestemd is. Wanneer het signaal op de bridge komt zal het niet verder gezonden worden aangezien de bridge weet dat de bestemmings-computers toch niet aan de ander kant kunnen liggen. De bridge absorbeert het signaal en het netwerk kan onmiddellijk verder werken.

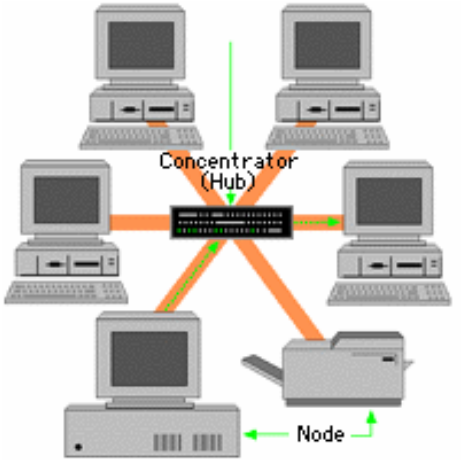


Hoofdstuk 3: Basistopologieën

De topologie van een netwerk valt uiteen in twee aspecten: de fysische en de logische (ook elektrische) topologie genoemd.

- De fysische topologie van een netwerk omschrijft de fysieke opstelling van de netwerkcomponenten t.o.v. de andere componenten en de netwerkbekabeling. Een component van de topologie wordt node of knooppunt genoemd. Een knooppunt in een netwerk kan bijvoorbeeld een computer of een hub zijn.
- De logische of elektrische topologie van een netwerk beschrijft de manier waarop een gegevenspakket doorgegeven en ontvangen wordt.

3.1 Ster netwerk



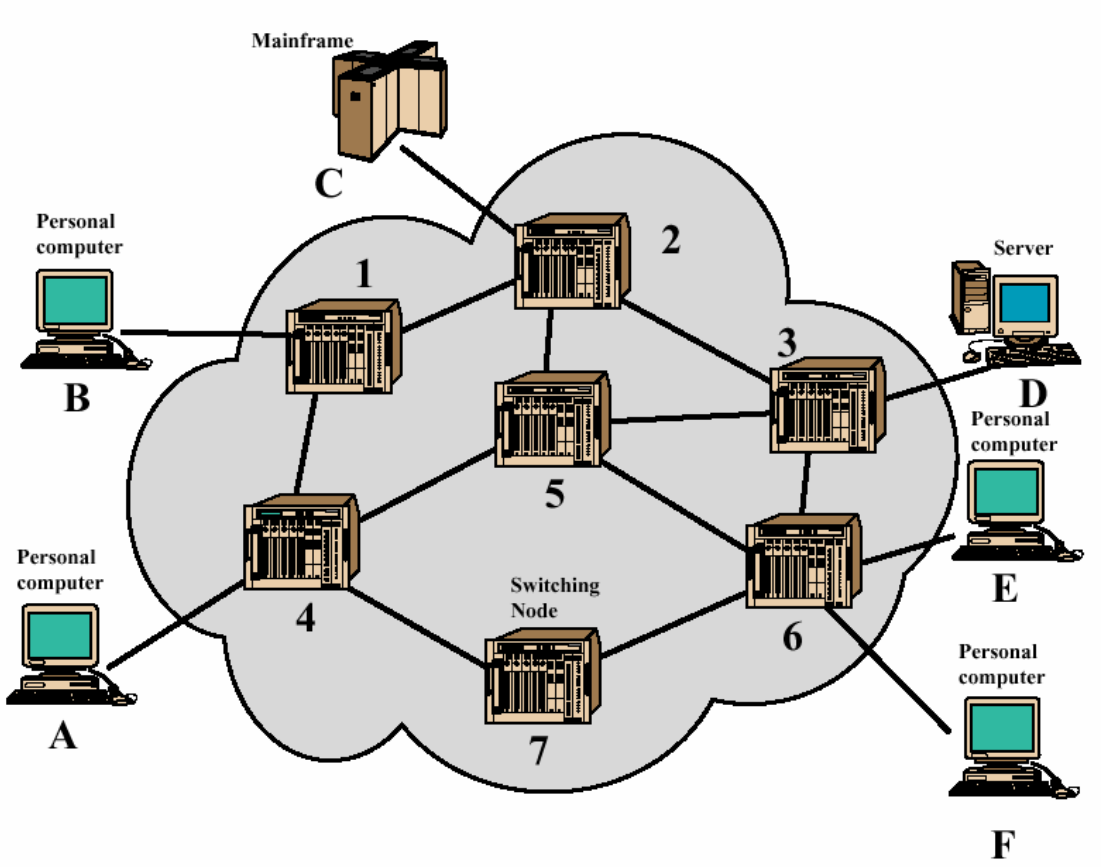
Elk werkstation is via een eigen kabel (meestal UTP) op een centraal apparaat, een hub of concentrator, aangesloten. Alle berichten lopen via dit centrale knooppunt. Dit centrale apparaat kan ook een switch of router zijn, maar dan zijn de andere apparaten zeker niet steeds gewone werkstations. Er kan bijvoorbeeld ook een ster van routers gemaakt worden.

Deze topologie vereist veel kabel, maar maakt het eenvoudig om de oorzaak van een storing te identificeren.

Een hardwarestoring zal zelden het functioneren van het hele netwerk beïnvloeden. Valt een werkstation uit, dan wordt de verbinding in het centrale knooppunt overbrugd. Daardoor kan je gemakkelijk een werkstation toevoegen, verwijderen of verplaatsen.

3.2 Gemaasd netwerk

In een maasnetwerk heeft elke node een willekeurig aantal verbindingen met andere nodes: er is dus geen duidelijke structuur. Er moet tenminste één route zijn tussen twee nodes, maar er kunnen er ook vele zijn. Het Internet is een voorbeeld van een maasnetwerk. Je kunt echter ook kleinschaliger maasnetwerken be denken.

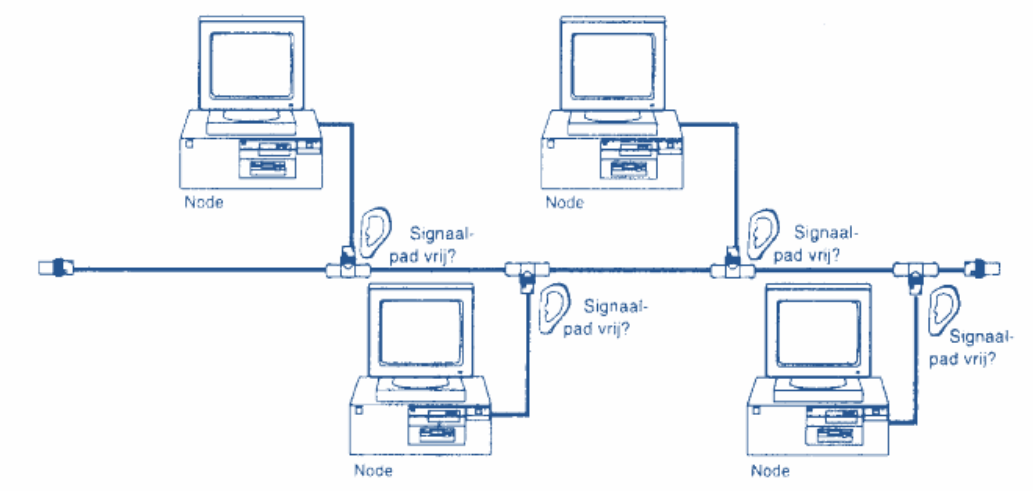


Hoofdstuk 4: Basisprotocollen

4.1 CSMA/CD-protocol

Het **CSMA/CD-protocol (Carrier Sense Multiple Access/Collision Detection)** bestaat uit verschillende bouwstenen.

- Het protocol steunt op de techniek van lijnaftasting. Wanneer een werkstation een pakketje informatie wil versturen, luistert het station eerst of de weg vrij is. Indien de weg vrij is, wordt het pakketje verstuurd.
- Doordat alle systemen gelijktijdig toegang hebben tot dezelfde gegevensdrager (Multiple Access) kunnen twee stations tegelijkertijd vaststellen dat het netwerk vrij is voor het versturen van informatie.
- Ze zenden dan tegelijk, waardoor een botsing ontstaat. Het zendende werkstation zal daarom blijven luisteren of er een botsing plaatsgrijpt **(Collision Detection)**. Vindt er gedurende een bepaald tijdsinterval geen botsing plaats, dan is de overdracht geslaagd. Grijpt er wel een botsing plaats, dan zal de zender na een lukraak vastgesteld tijdsinterval opnieuw trachten het pakketje te versturen.

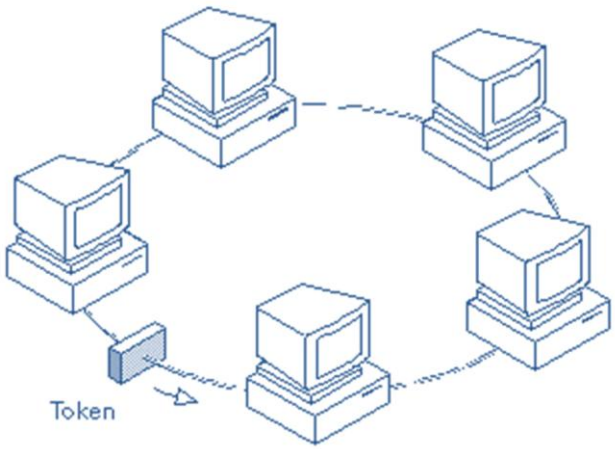


De andere werkstations op de gegevensdrager gaan na of het bericht voor hen bestemd is en kopiëren het desgevallend. Het is dus een passief netwerk.

Netwerken die het CSMA/CD-protocol gebruiken, noemt met ook dikwijls broadcasting: iedere node kan op een willekeurig ogenblik een bericht versturen. Alle andere nodes kunnen dit bericht 'horen'. Als meerdere stations gelijktijdig berichten verzenden is er kans op botsingen (collisions) en moeten de berichten opnieuw verzonden worden.

Deze toegangsregeling levert een hoge efficiëntie op in omgevingen waar de gegevensstroom op het netwerk meestal pieksgewijs verloopt. Bij intensief netwerkverkeer zullen er veel botsingen plaatsgrijpen, waardoor de performantie van het netwerk terugloopt.

4.2 Token passing ring



Dit is het toegangssprotocol, ontwikkeld door IBM, dat gebruikt wordt voor de meeste ringnetwerken, maar kan ook in andere netwerktopologieën gebruikt worden. Daarin zijn computers met elkaar verbonden door middel van een simplex-verbinding.

Een speciaal bitpatroon (het token) wordt verstuurd door de eerste computer die wordt aangezet. Een computer die informatie wil versturen, moet wachten op dat token. Wanneer die computer geen informatie te verzenden heeft, moet deze het token doorgeven aan de volgende computer. Wanneer die computer wel informatie wil versturen, dan bevestigt deze die informatie aan het token, zet er het netwerkadres van bestemming achter, en stuurt alles door over het netwerk.

De computers voor wie de informatie niet is bestemd, geven deze gewoon verder door over het netwerk. Wanneer de informatie de bestemmeling bereikt, kopieert die de gegevens, en stuurt ze ongewijzigd verder, tot ze weer bij de zender aankomen. De zender weet daardoor dat de informatie is aangekomen, en geeft weer 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 het niet is. Om dat probleem op te lossen, wordt het principe van bitstuffing toegepast : er wordt aan de verstuurde informatie een bit toegevoegd, met als waarde een 0 of een 1, zo gekozen dat het nieuwe bitpatroon altijd verschillend is van het token. De ontvanger herkent de toegevoegde bit, en zal die bij de verwerking ervan weer verwijderen. Op dat ogenblik is de informatie echter al weg van het netwerk, en worden de andere computers er niet door beïnvloed.

4.3 Token passing bus

Dit is een alternatief toegangsprotocol voor ring- en busnetwerken, en wordt ook MAP (*Manifacturers Automatic Protocol*) genoemd. Het protocol is vergelijkbaar met token passing ring.

Hoofdstuk 5: Soorten netwerken

5.1 Point-to-point netwerk

Een LAN dat bestaat uit twee computers. Deze computers kunnen dan elkaars gegevens en randapparaten gebruiken.

5.2 Peer to peer netwerk

Een peer-to-peer netwerk is te omschrijvien als een netwerk waarbij de verschillende clients aan elkaar gekoppeld zijn en waarbij elke client evenwaardig in de hiërachie van het netwerk. Geen van de deelnemende clients neemt het beheer van het netwerk waar. Elke gebruiker kan zelf bepalen of andere gebruikers van het netwerk gegevens op zijn harde schijf mogen lezen/bewaren/schrijven. Of iemand een document op zijn printer mag afdrukken, ... Het is de gebruiker van de pc die het beheer van zijn eigen pc in handen heeft.

Daardoor wordt het soms moeilijk werkbaar. In een netwerk van 5 pc's bewaart elkeen meestal zijn documenten op zijn eigen pc. Wil iemand anders deze tekst gebruiken moet de "beheerder" (meestal iemand die iets meer van computers kent dan zijn collega's) de toegang tot deze pc configureren. De beheerder loopt van pc tot pc om dit alles in orde en werkbaar te houden.

Alle documenten in het netwerk staan verspreid over alle pc's. Zoek je een bepaald document dan kan dit nogal eens duren voor je dit gevonden hebt. Je weet niet precies waar het document zich bevindt. De eigenaar van het document of een andere netwerkgebruiker kan het verplaatst hebben. Dit kan toch wel wat ergenis opwekken.

Een veiligheidskopie niemen van deze docoumenten is ook al een heikele opdracht. Wil je bijvoorbeeld 's nachts (wanneer niemand werkt) een veiligheidskopie (backup) nemen dan moeten alle pc's aanstaan. Van de pc's die uitgezet zijn bij het verlaten van het kantoor kan geen backup genomen worden. Doordat de gebruiker zelf kan beslissen waar hij zijn gegevens bewaart is het mogelijk dat de folder waar deze zijn documenten bewaart niet in de procedure van de veiligheidskopie is opgenomen.

Dit zijn een aantal nadelen van een peer-to-peer netwerk. Het heeft een uiteraard ook een aantal voordelen. Het grootste voordeel is dat men voor een minimale investering aan hardware (Windows ondersteunt peer-to-peer netwerken) communicatie tussen verschillende pc's mogelijk wordt. Verschillende bronnen kunnen dus op een goedkope manier ter beschikking gesteld worden van alle gebruikers. Door tijds- en financiële besparingen (bvb. geen twee printers moeten kopen voor twee gebruikers – één is voldoende) is de investering voor een peer-to-peer netwerken snel terug verdiend.

Gezien de minimale beheerstaken is het een netwerk dat snel kan gelegd worden en waarvoor geen specifieke kennis nodig is. Weten hoe je een netwerk leggen moet en hoe je werkstations te configureren is moet voldoende zijn.