Hoofdstuk 5

Computernetwerken

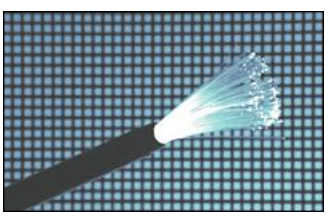
Betrouwbare en snelle toegang tot informatie is tegenwoordig essentieel voor het dagelijkse leven. Zowel voor het werk als voor het privéleven wordt de computer ingezet om allerlei informatie te verwerven en te verwerken. Net als warmte en licht is nu ook een verbinding met het internet een basisvoorziening in elk huis.
Voor organisaties en bedrijven is het ondenkbaar niet op een netwerk te zijn aangesloten voor de wereldwijde communicatie met mobiele medewerkers, klanten, leveranciers en andere betrokkenen. Eenvoudige en snelle uitwisseling van grote hoeveelheden gegevens uit archieven en databases naar een grote diversiteit aan werkstations is een voorwaarde voor het succes van organisaties, bedrijven en maatschappelijke ontwikkeling. Voor samenwerking tussen collega's die wereldwijd verspreid hun werkplek hebben ingericht zijn mondiale verbindingen in een toegankelijk netwerk essentieel. De handel via internet is nu zo ingeburgerd, dat vele bedrijven zoals e-veilingen en webwinkels duizenden euro's van hun omzet per uur verliezen als hun verbinding met internet niet functioneert.

De permanente snelle toegang naar alle vertier, vermaak en communicatie via internet wordt zo langzamerhand een voorwaarde voor het persoonlijke welzijn.
Het beeld van de eenzame computerfreak die met allerlei moeilijke commando's de computer bedient maakt plaats voor een laptop in de huiskamer waarmee via een draadloos netwerk contact onderhouden wordt met vrienden in de vorm van communicatie en samen spelen.

In dit hoofdstuk bekijken we de basisconcepten, onderdelen en werking van computernetwerken die de informatie uitwisseling ondersteunen.

5.1 Onderdelen van netwerken

Een *computernetwerk* bestaat uit een groep computers die aan elkaar gekoppeld zijn via verbindingen (Engels: connection) om informatieberichten uit te wisselen. Een kleine netwerk in een bedrijf heet een *Local Area Network* (*LAN*). Een groot netwerk heet een *Wide Area Network* (*WAN*).
Door LAN's en WAN's aan elkaar te koppelen ontstaat er op den duur een erg groot netwerk. In het geval van het Internet is dat wereldwijd.
De *verbindingen* kunnen bestaan uit draden of uit elektromagnetische golven. Er zijn twee soorten bekabeling voor een elektrisch signaal: *Coaxiale kabel* (zoals de TV kabel) en *UTP*, *Unshielded Twisted Pair* (zoals de telefoonkabel). Optisch signaal wordt door een *glasvezel* geleid.

		
Coaxiaal	*UTP*	*Glasvezel*

Figuur 1 Soorten kabels

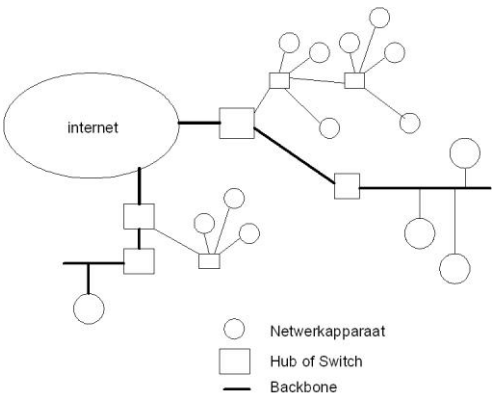
Wanneer er elektromagnetische golven gebruikt worden spreken we over draadloze verbindingen. *WIFI* is daar een voorbeeld van.

Figuur 2 Wireless werken -- NB VERVANGEN! --

De computers en andere apparatuur in het netwerk (bijvoorbeeld printers en externe geheugens) vormen elk een *aansluitpunt* (Engels: *node*) met een uniek adres. Door dat unieke adres is het apparaat in het netwerk herkenbaar. Het lijkt op de combinatie van je postcode en huisnummer waardoor bekend is waar je woont.
De verbindingen waarop de netwerkapparaten zijn aangesloten kunnen onderling aan elkaar worden gekoppeld via *schakelpunten* (Engels: hub, switch).

Figuur 3 Hub met UTP aansluitingen

Een *segment* van een netwerk is een schakelpunt met de daaraan gekoppelde netwerkapparaten. Segmenten kunnen weer onderling verbonden zijn door schakelpunten. De verbindingen tussen die schakelpunten vormen samen de *hoofdverbinding* (Engels: *backbone*) van het netwerk.

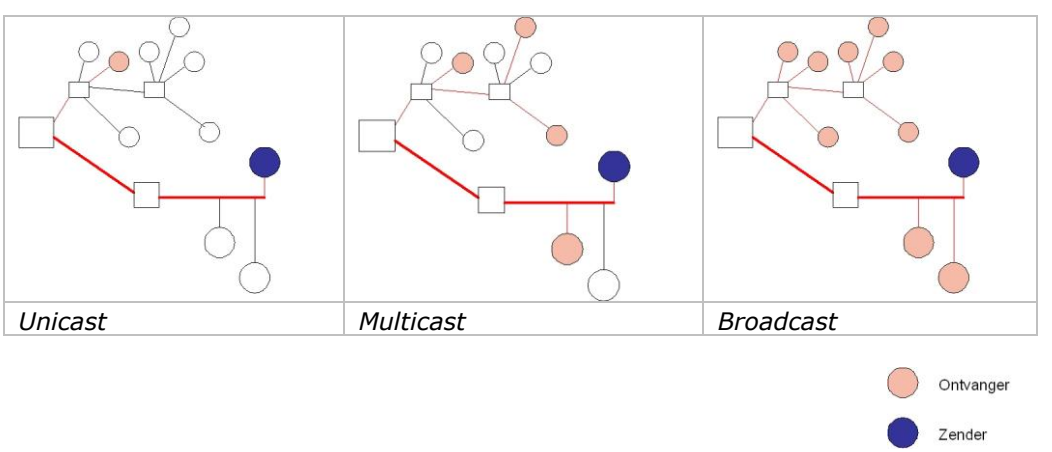


Figuur 4 Netwerk onderdelen

Elk apparaat is in een netwerk aangesloten via een *netwerkkaart* met een uniek adres: het *MAC-adres*. MAC staat voor *Media Access Control* (vertaald: medium toegangscontroleadres). Dat is het unieke fysieke adres waardoor het apparaat toegang heeft tot het netwerk(medium). Het MAC-adres is 6 bytes (48 bits) lang en daarmee kunnen ruim 280 biljard (2^{48}) verschillende adressen worden gecodeerd.

Berichten in een netwerk kunnen op verschillende manieren verstuurd worden.
Elk aansluitpunt kan drie typen berichten sturen.

1 Een enkelvoudig bericht (Engels: *unicast*) bevat één adres en is dus bestemd voor één aansluitpunt.
2 Een meervoudig bericht (Engels: *multicast*) bevat een groep adressen en is bestemd voor alle aansluitpunten in de groep.
3 Een omroepbericht (Engels: *broadcast*) is bestemd voor alle aansluitpunten in het netwerk.



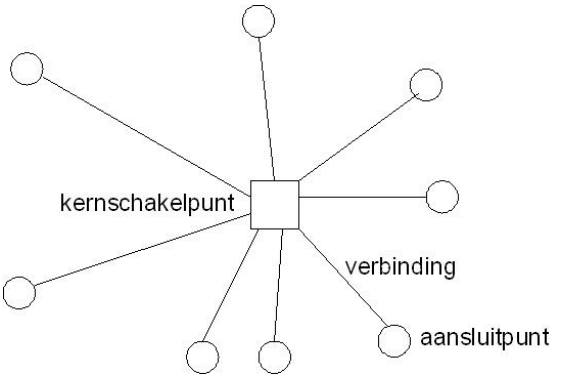
Figuur 5 Drie typen berichten

5.2 Netwerk topologie

De netwerk topologie bepaalt de structuur van de verbindingen tussen de aansluitpunten. De meest voorkomende netwerkstructuren zijn:

Sternetwerk

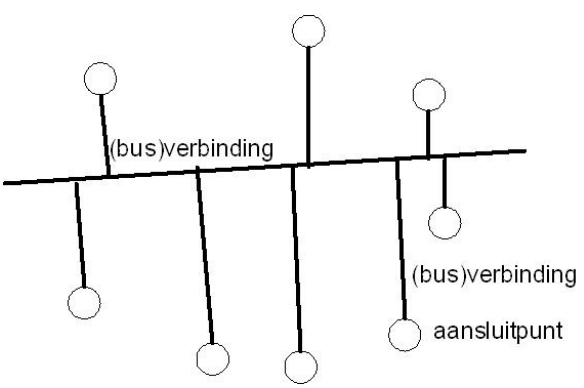
In een *sternetwerk* is elk aansluitpunt verbonden met een centraal schakelpunt. Dat *kernschakelpunt* (Engels: *hub*) geeft elk bericht door naar alle andere aansluitpunten in de ster. Het kernschakelpunt geeft in feite de elektronische signalen direct door en doet niets met de inhoud van het bericht.



Figuur 6 Sternetwerk

Busnetwerk

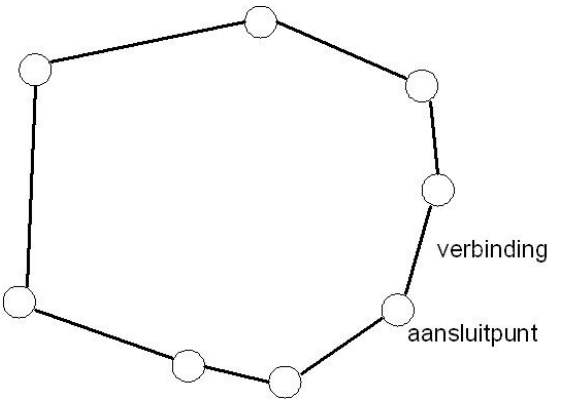
De kern van een *busnetwerk* is de busverbinding. Daarmee wordt elk aansluitpunt op de bus verbonden met elk ander aansluitpunt. Via een busstructuur kan elk aansluitpunt direct berichten uitwisselen met elk ander aansluitpunt (op dezelfde busverbinding). Het zendende aansluitpunt zet een bericht op de busverbinding en bereikt direct alle andere aansluitpunten. Het bericht bevat het adres van het bestemde aansluitpunt. Alle ontvangende aansluitpunten bepalen of het adres overeenkomt met hun eigen adres. Het juiste aansluitpunt leest de boodschap en kan erop reageren. Als een boodschap wordt gestuurd naar een adres dat niet voorkomt in het netwerk zal na een korte tijd de zender merken, dat er niet gereageerd wordt: (knooppunt onbekend, boodschap onbestelbaar).



Figuur 7 Busnetwerk

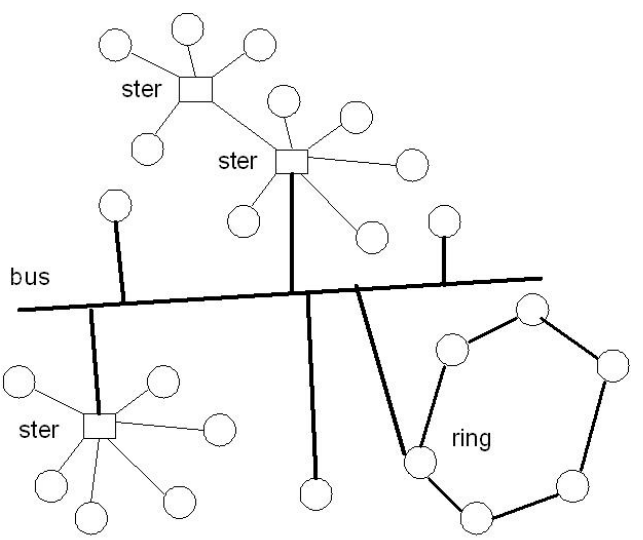
Ringnetwerk

In een *ringnetwerk* zijn de aansluitpunten verbonden in een ring. De berichten worden verstuurd van aansluitpunt naar aansluitpunt als een enveloppe (Engels: token) met inhoud. Elk opvolgend aansluitpunt in de ring ontvangt de enveloppe en bepaalt of het adres overeenstemt met het eigen adres. Als dat niet zo is, dan wordt de enveloppe naar het volgende aansluitpunt gestuurd. Als dat wel het geval is wordt de boodschap gelezen en de enveloppe wordt opnieuw gebruikt voor een volgende boodschap. Als een 'lege' enveloppe wordt doorgegeven kan een ontvangend aansluitpunt een nieuwe boodschap verzenden. We kunnen het token ook zien als een postbode die (heel snel) met een enveloppe rondgestuurd wordt. Elk aansluitpunt wordt bediend als de postbode langskomt.



Figuur 8 Ringnetwerk

Als de drie basisstructuren in een groot netwerk gecombineerd voorkomen is er sprake van een combinatie van deze structuren.



Figuur 9 Combinatienetwerk

5.3 Schakelpunten

Er zijn vier typen schakelpunten om de verbindingen in een netwerk aan elkaar te koppelen.

Kernschakelpunt

Een *kernschakelpunt* (Engels: *hub*) geeft elk binnenkomend bericht via een verbinding door aan alle andere verbindingen. Dat gebeurt in volgorde van binnenkomst een voor een, dus na elkaar. De aansluitpunten verdelen de transportcapaciteit van het kernschakelpunt.

Kruisschakelpunt

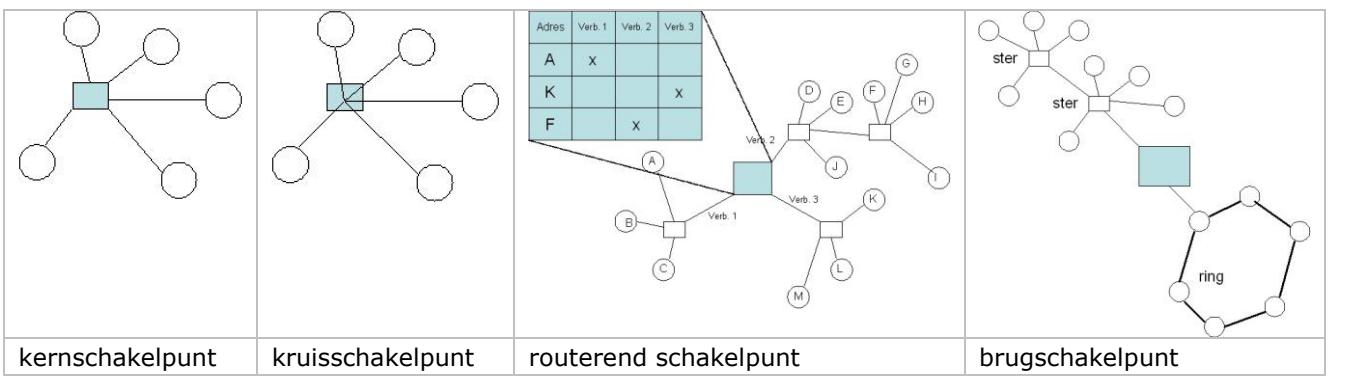
Een *kruisschakelpunt* (Engels: *switch*) kan elke binnenkomende verbinding afzonderlijk koppelen op elke andere verbinding. Verschillende verbindingen kunnen nu tegelijkertijd (parallel) gekoppeld worden om berichten uit te wisselen. Het kruisschakelpunt kan elke verbinding voorzien van de maximale transportsnelheid.

Routerend schakelpunt

Een *routerend schakelpunt* (Engels: *router*) koppelt niet zozeer de fysieke verbindingen maar bekijkt de adressering van de berichten en stuurt die dan via de meest optimale logische verbinding door het netwerk. De route bepalen voor de verbinding kost verwerking, maar die weegt ruimschoots op tegen de mogelijkheid verschillende verbindingen in het netwerk voor de logische verbinding te benutten.

Brugschakelpunt

Een *brugschakelpunt* (Engels: *bridge*) koppelt verbindingen van verschillend type. Bijvoorbeeld een ringnetwerk dat anders functioneert dan een busnetwerk moet via een brugschakelpunt worden gekoppeld.



kernschakelpunt	kruisschakelpunt	routerend schakelpunt	brugschakelpunt

Figuur 10 Schakelpunten: hub, switch, router en bridge

Een kernschakelpunt of hub is het meest simpele schakelpunt. Alle netwerkapparaten kunnen via een hub communiceren op basis van volgorde van aanvraag. Een kernschakelpunt met tien verbindingen is dus een potentiële bron van wachttijden. Er kan van alle tien verbindingen op elk moment een bericht komen dat via het schakelpunt moet worden doorgegeven naar alle betrokkenen.
Een kruisschakelpunt of switch heeft al enige intelligentie in het leggen van verbindingen. In een switch kunnen netwerkapparaat 1 en 3 op het zelfde moment communiceren als netwerkapparaat 4 en 8.
Een ander essentieel verschil tussen een kernschakelpunt (hub) en een kruisschakelpunt (switch) is dat alle aansluitpunten van een hub de transportcapaciteit (bandbreedte) moeten verdelen, terwijl een apparaat in een switch de volledige transportcapaciteit per verbinding kan handhaven. Als bijvoorbeeld 10 aansluitpunten een hub in een 10Mbps netwerk gebruiken dan krijgt elk aansluitpunt slechts 1Mbps, omdat de andere aansluitpunten ook hun berichten verzenden. Een kruisschakelpunt kan elk aansluitpunt op een verbinding met 10 Mbps schakelen.

Een kernschakelpunt of kruisschakelpunt stuurt elke omroepmelding door naar alle andere verbindingen met segmenten, maar een routerend schakelpunt doet dat niet zonder meer. De router kijkt naar het bestemmingsadres van het bericht en bepaalt of dat adres binnen een netwerksegment voorkomt. In die richting wordt het dan doorgestuurd.

Brugschakelpunten oftewel bridges zijn de meest intelligente schakelpunten. Zij kunnen schakelen tussen netwerksegmenten met verschillende verbindingstypen. Wanneer een bestemming van een pakket in een ringnetwerk ligt kan een bridge een token aan het pakket meegeven zodat het door een ringnetwerk begrepen wordt.

Pakketschakelen

Schakelpunten hanteren vaak de methode van *pakket schakelen* (Engels: *packet switching*). In deze wijze van schakelen wordt een bericht opgeknipt in kleine pakketjes die gegevens bevatten van de geadresseerde en de zender en de plek waarin zij in het totale bericht geplaatst dienen te worden. In een netwerk kan elk pakketje een eigen route volgen om uiteindelijk bij de ontvanger weer keurig in een bericht geplaatst te worden.
Een kruisschakelpunt realiseert een koppeling tussen twee verbindingen net lang genoeg om een berichtpakket te kunnen doorsturen. Ontvangen pakketten worden opgeslagen in een buffer tot het bericht compleet is om doorgestuurd te worden.

5.4 Kenmerken van netwerken

De werking van een netwerk wordt bepaald door een aantal kenmerken.
De vijf belangrijkste zijn:

Vertragingstijd

Vertragingstijd (Engels: *latency*) is de tijd die een boodschap nodig heeft om na het verzenden, via het netwerk, bij het ontvangende adres aan te komen. Dit duurt langer als de boodschap via een groot aantal verbindingen en schakelpunten in het netwerk moet worden verzonden. Die tijd kan variëren van enige milliseconden tot enkele seconden.
Een andere soort vertraging treedt op als het bericht erg groot is en uit veel (miljoenen) pakketjes bestaat. Die pakketjes moeten door elk schakelpunt worden doorgegeven, maar tegelijkertijd worden ook miljoenen andere pakketjes van andere berichten in het netwerk getransporteerd. Het zal dus wel even duren, totdat alle pakketjes bij de geadresseerde aangekomen zijn.

Netwerkfouten

In een netwerk komen vele potentiële foutenbronnen of storingsbronnen voor die *netwerkfouten* kunnen veroorzaken. Elk apparaat, elke verbinding en elk schakelpunt kan transportproblemen in het netwerk veroorzaken. Bijvoorbeeld door ongecontroleerd en ongelimiteerd omroepberichten te sturen. Kruisschakelaars kunnen de maximale transportsnelheid van een verbinding controleren en daarmee de verstoringen tot een deel van het netwerk beperken.

Botsingen

Een bussysteem maakt gebruik van een set van afspraken (protocol) waarin *botsingen* tussen berichten kunnen voorkomen. Een aansluitpunt stuurt bijvoorbeeld uitsluitend een bericht als de busverbinding vrij is. Als twee aansluitpunten op de bus toevallig op hetzelfde moment een bericht sturen, ontstaat een ‘botsing’ en gaan de berichten verloren. Op dat moment wachten beide aansluitpunten elk een verschillende tijd en sturen hetzelfde bericht nog een keer.
Een netwerk met veel aansluitpunten loopt meer risico op botsingen waardoor tijd en transportcapaciteit verloren gaat. Door het netwerk in onafhankelijke segmenten te verdelen wordt de kans op botsingen per segment beperkt. Daar heeft wel een nadeel, want er zijn dan extra schakelpunten nodig.

Schaalbaarheid

Wat gebeurt er als een netwerk groeit van 100 naar 1000 aansluitpunten? Als dan het netwerk goed blijft functioneren, noemen we het voldoende schaalbaar. Vaak echter kun je een netwerk niet zomaar ongelimiteerd uitbreiden.
Door nieuwe toepassingen neemt het aantal netwerkberichten sterk toe. Ook daar spreken we over een goede *schaalbaarheid* als het netwerk goed blijft functioneren. Zo vereist de communicatie van videobeelden naar vele gebruikers in omvangrijke netwerken een hoge transportcapaciteit om een redelijke videokwaliteit te bieden.

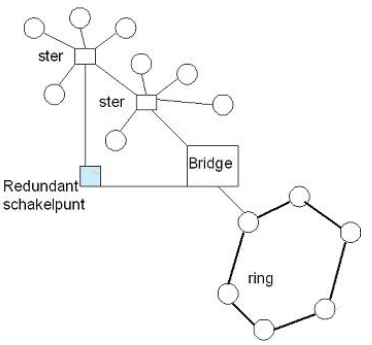
In een sternetwerk worden de knooppunten verbonden via een hub die de boodschappen doorgeeft. De doorvoersnelheid van een hub neemt af als het aantal aansluitpunten op de hub toeneemt. In een busstructuur neemt bij een toenemend aantal aansluitpunten ook het

aantal berichten op de bus toe. Dat verhoogt de kans op botsingen. In een ringstructuur neemt bij een toenemend aantal aansluitpunten de 'wachttijd' op de postbode (token) toe. Voor elke netwerkstructuur moeten maatregelen genomen worden om minimaal dezelfde transportsnelheid te behouden bij groei (opschaling) van het netwerk.

Zoals al besproken, is naast de toename van het aantal aansluitpunten een tweede bron van groei de toename van het aantal boodschappen in het netwerk. De beschikbare transportcapaciteit wordt normaal over alle berichten verdeeld en dat leidt tot verhoging van de vertragingstijd. Om voldoende transportcapaciteit te handhaven zullen netwerkonderdelen moeten worden toegevoegd of netwerkonderdelen vervangen door nieuwe onderdelen die hogere transportsnelheden kunnen realiseren.

Redundantie

Als er een fout in een computernetwerk optreedt, kan de schade snel oplopen en de kosten daarvan duizenden euro's bedragen. Daarom wordt van te voren getracht door extra maatregelen het risico van uitval te beperken. Zo'n extra maatregel is het opnemen van extra netwerkcomponenten. De extra componenten nemen de taak van een andere falende component over. Die extra componenten worden ook wel *redundant* genoemd. Het gaat dus om de afweging van de kosten van de fouten en de kosten van de redundante componenten. In netwerkstructuren vormen de kritische verbindingen met veel aansluitpunten en de schakelpunten de belangrijkste risicofactoren. Als een kritische verbinding, een kernschakelpunt of kruisschakelpunt uitvalt zijn alle betrokken aansluitingen onbereikbaar. Als door een enkelvoudige fout de werking van het netwerk uitvalt, kan voor het betreffende onderdeel een extra (redundant) exemplaar worden toegevoegd. Ook een verbinding kan dubbel opgenomen worden. Door schakelpunten met een extra verbinding parallel op te nemen kan een deel van het netwerk blijven functioneren als een van de schakelpunten faalt.



Figuur 11 Redundantie

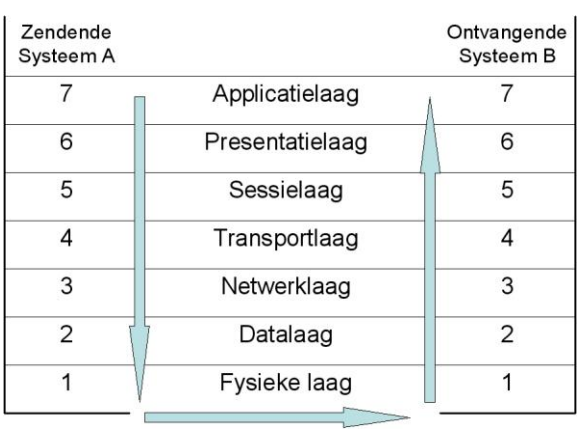
5.5 Communicatie in een netwerk

Om het transport van berichten in een netwerk te standaardiseren is het *OSI-model* opgesteld. OSI staat voor *Open Systems Interface* en is de standaard voor het communiceren in netwerken geworden. Het model geeft een overzicht wat er allemaal gebeurt om een bericht tussen twee aansluitpunten in een netwerk uit te wisselen. De lagen van het OSI-model zie je in tabel 1.

Laag nr.	Laag naam	Uitleg	Schakelpunt
7	Applicatie	Communicatie tussen verschillende applicaties	Subroutine
6	Presentatie	Management van de inhoud. Compressie en decompressie.	Programma
5	Sessie	Datatransport regelen m.b.v. dialoogcontrole tekens. Synchronisatie van de datastroom en resynchronisatie bij verstoring van de datastroom.	Besturingssysteem
4	Transport	Betrouwbaar datatransport regelen doormiddel van het opdelen van het bericht in datapakketjes bij de zender en het her(samen)stellen van het bericht bij de ontvanger.	Werkstation
3	Netwerk	Routering van datapakketjes regelen.	Routerend schakelpunt Router
2	Dataverbinding	Herkennen van fouten tijdens de communicatie en het herstellen daarvan.	Kruisschakelpunt Switch
1	Fysieke verbinding	Op correcte wijze de transmissie over het medium regelen.	Kernschakelpunt Hub

Tabel 1 OSI-lagen voor netwerkcommunicatie.

Een bericht doorloopt de lagen twee keer. Van de zendende applicatie (in het zendende systeem) via de lagen 7,6,5,4,3,2,1 naar de ontvangende applicatie via de lagen 1,2,3,4,5,6,7 (in het ontvangende systeem)

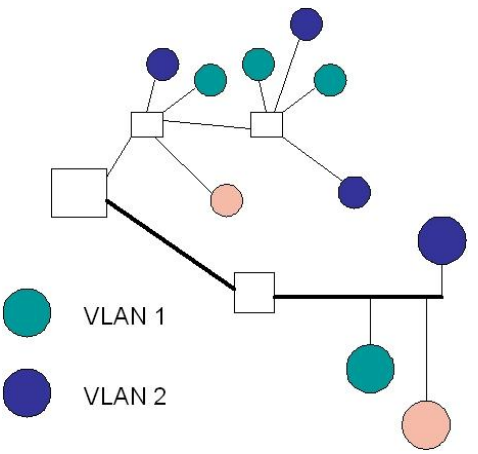


Figuur 12 Twee communicerende systemen via OSI-lagen

De verschillende typen netwerkschakelpunten schakelen op verschillende niveaus. Figuur 12 laat zien dat de kernschakelpunten de fysieke verbindingen schakelen. De kruisschakelpunten kunnen dynamisch twee aansluitpunten onafhankelijk van het netwerk met elkaar verbinden. Kruisschakelpunten functioneren op laag 2 (de dataverbinding) van het OSI-model.
Routerende schakelpunten functioneren op laag 3 van het OSI-model. Zij werken met IP-adressen die statisch of dynamisch bij de opzet van een netwerkverbinding worden toegekend. Op de hogere niveaus ‘schakelt’ het werkstation de berichten door de binnenkomende berichten op de i/o-poorten (laag 4) via het besturingssysteem aan het juiste programma door te geven. Het programma stuurt het bericht naar de juiste invoer/uitvoerapparatuur en de subroutine in het programma bepaalt hoe en waar de mededeling op het scherm van de monitor wordt geplaatst.

5.6 Virtuele Netwerken

Omdat netwerken in omvang en complexiteit groeien is het begrip *virtuele locale netwerken* (*VLAN*) ontstaan. Een VLAN is een groep aansluitpunten die samen een eigen netwerkdomein vormen. Dat netwerkdomein is niet gebaseerd op fysieke locaties, maar op het feit dat deze aansluitpunten logisch bij elkaar horen.



Figuur 13 Virtueel LAN

Virtuele netwerken bieden een aantal voordelen. Beveiliging wordt versterkt door de scheiding van systemen met vertrouwelijke informatie van de rest van het netwerk. Hierdoor neemt de kans af dat personen toegang krijgen tot informatie die niet voor hen bestemd is. Bijvoorbeeld in een school kunnen de computers voor personeel en voor studenten in twee verschillende VLAN's staan. Hierdoor kan het domein van het personeel goed afgeschermd worden en kunnen bijvoorbeeld op het VLAN voor leerlingen meer mogelijkheden om te communiceren gecreëerd worden.

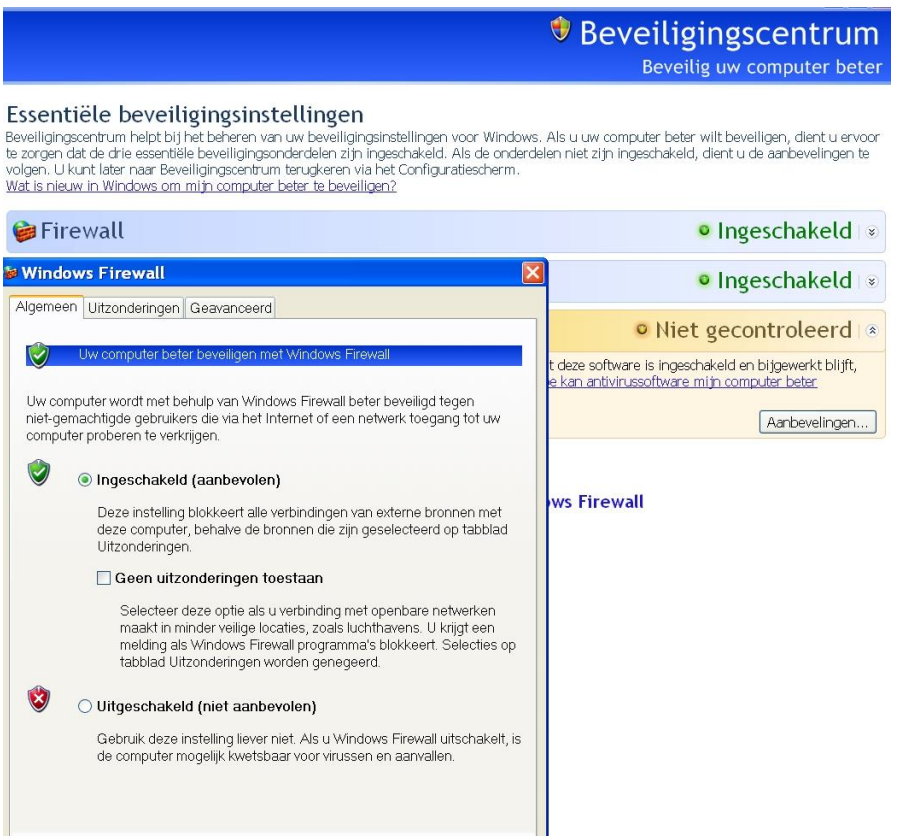
Bij de uitvoering van projecten of voor de installatie van specifieke applicaties is het vaak zinvol de groep die toegang moet krijgen tot specifieke ict-voorzieningen ook als groep in een eigen 'afgeschermd' deel van het totale netwerk te plaatsen.

Door een VLAN te creëren voor het gebruik van specifieke applicaties kan er voor gezorgd worden, dat de gebruikers van deze applicatie altijd de beschikking hebben over een bepaalde vereiste bandbreedte. Hierdoor heeft drukte op het netwerk geen invloed op de beschikbaarheid van de applicatie. Andersom kunnen omroepberichten en verkeersstromen binnen een VLAN worden gehouden. Daardoor is het mogelijk andere delen van het netwerk te ontlasten van onnodig netwerkverkeer.

De netwerkbeheerder kan via toegangslijsten het netwerkverkeer controleren en veranderingen in de netwerkbelasting registreren. Daardoor wordt het mogelijk proactief maatregelen te treffen en bepaalde netwerkonderdelen meer of minder bandbreedte toe te wijzen.
Een VLAN creëren kan eenvoudig door via toegang op afstand de parameters (naam, domein en betrokken netwerkdelen) op het VLAN-schakelpunt in te stellen. Communicatie tussen VLAN's kan door gebruik van een routerend schakelpunt bewaakt en dan waar nodig gecontroleerd toegestaan worden.

5.7 De firewall

Netwerken geven veel mogelijkheden. Dat betekent ook dat, wanneer er boze opzet in het spel is, er ook heel wat problemen kunnen ontstaat. De *firewall* is een programma of een apparaat dat netwerken beschermt.
Bij het gebruik van Internet speelt de term Firewall een belangrijke rol. Soms zijn op school bepaalde sites geblokkeerd. Ook kan een computer thuis zo worden ingesteld dat niet alle sites zondermeer zijn te bereiken.



Figuur 14 Windows beveiligingscentrum met firewall

De firewall is niet alleen een belemmering voor het bezoeken van sites maar zorgt er ook voor dat hackers moeilijker binnen kunnen komen in een computer. De firewall checkt het verkeer over de verbinding en in navolging van de ingestelde beveiligingsregels zal de firewall blokkeren of doorlaten.
Een hacker zal bijvoorbeeld om in te breken een *FTP* verbinding (File Transfer Protocol) willen leggen met een computer. Met een FTP verbinding kunnen er programma's op de computer geïnstalleerd worden. Die programma's kunnen data vernietigen of, erger, naar passwords zoeken.
Een firewall is zo in te stellen dat een FTP verbinding niet gemaakt kan worden.

Een firewall kan de computer beschermen tegen:

Login van afstand

Hackers proberen via het IP-nummer van de computer verbinding te leggen en in te loggen. Daarna kan er meegekeken worden of programma's opgestart worden.

Email bommen

Een emailbericht dat, in korte tijd, duizenden keren naar je verzonden wordt blokkeert je eigen communicatie (volle postbus).

Spam en het ongewild verzenden van spam

Ongewild reclame ontvangen kan heel vervelend zijn. Nog erger is het, als via een binnen gedrongen macro via jouw postbus ongewild reclame wordt verstuurd. Het wordt dan heel moeilijk om de echte afzender te traceren en jij wordt beschuldigd van iets wat je niet gedaan hebt.

Macros

Veel applicaties kennen een soort script om veel voorkomende taken te automatiseren. Hackers maken daarvan gebruik om de applicaties van de doelcomputer bepaalde taken te laten doen.

Virussen

Een virus en een klein programma dat zich zelf snel en regelmatig kopieert en daarmee andere programma's ongeschikt maakt, intern geheugen vol laat lopen en/of het schijfgeheugen wist.

Het moeilijkste van een firewall is het afstemmen van de bescherming en de mogelijkheden die de gebruikers van de computersystemen aan de binnenkant willen hebben.
Het komt regelmatig voor dat de bescherming zo streng is dat gebruikers niet meer kunnen werken. In grote bedrijven is het inregelen van een firewall daarom een continu proces waarbij de risico's steeds afgewogen worden tegen de beperkingen.