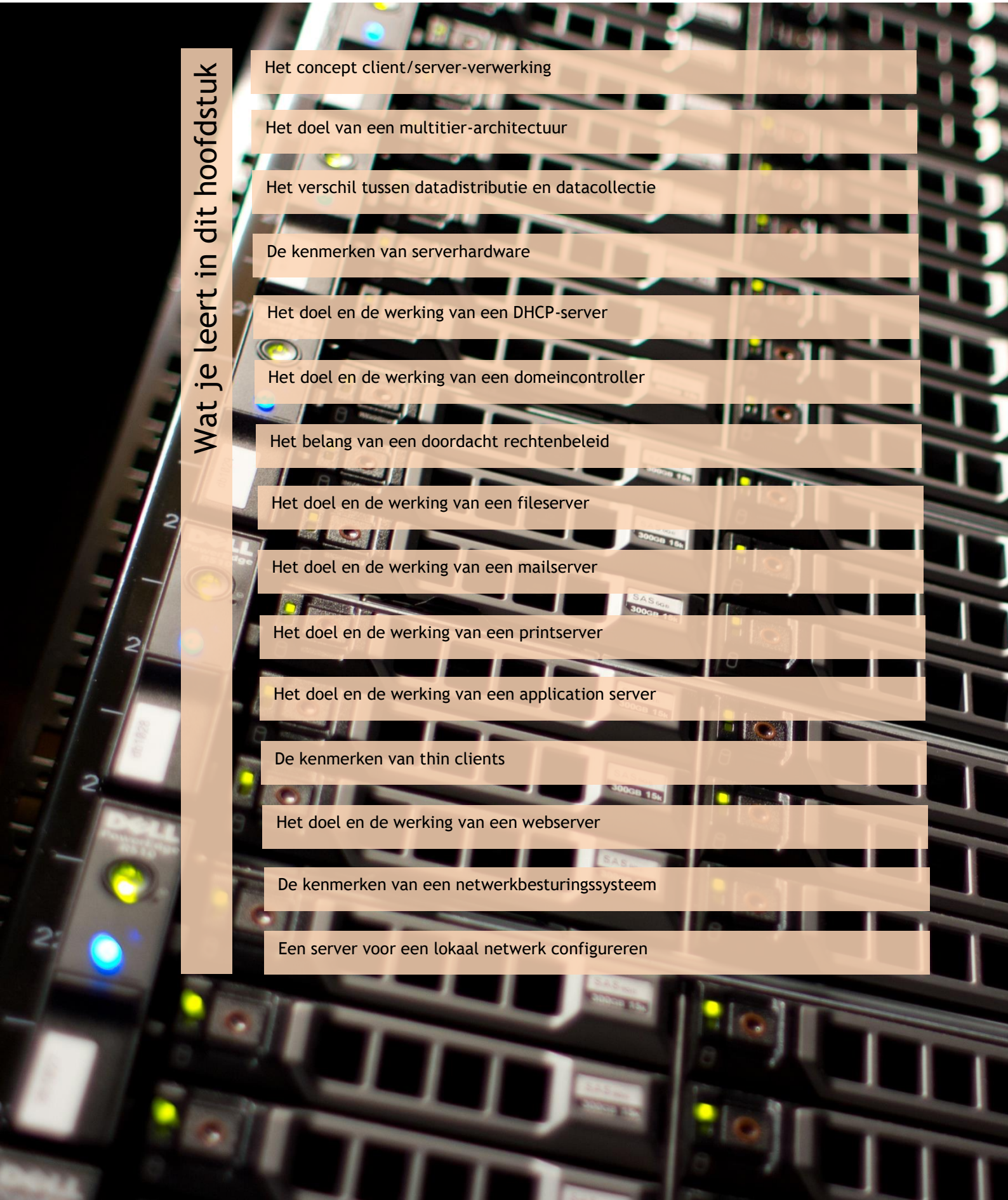
4. Servers

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



Wat je leert in dit hoofdstuk

- 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 doordacht 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.

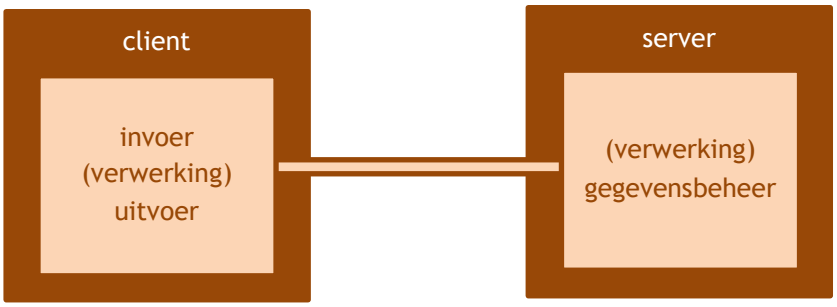
Het concept van client/server verwerking wordt toegepast in netwerken. We spreken dan van een gedistribueerd computerproces: daarbij zijn de gegevens en programmatuur die nodig zijn voor het proces verspreid over meer dan één computer – dit in tegenstelling tot een gecentraliseerd computerproces zoals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

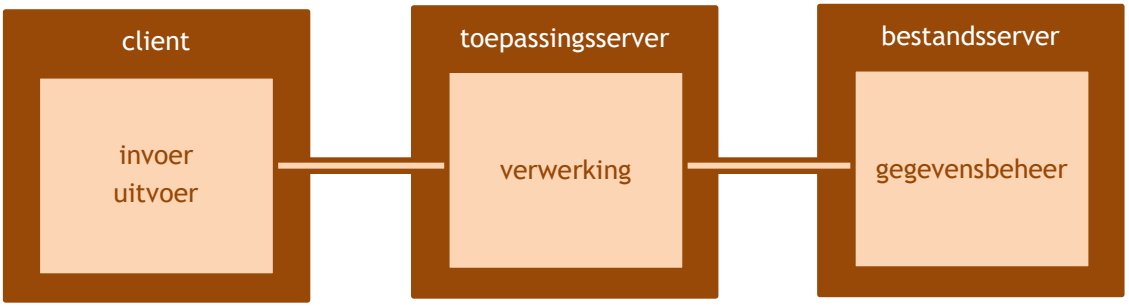
Vaak worden applicaties speciaal ontworpen voor client/server-verwerking. Zo'n toepassing bestaat dan uit twee verschillende, met elkaar samenwerkende programma's: een serverprogramma dat diensten levert aan het clientprogramma dat bij de gebruiker geïnstalleerd wordt. Het programma op de computer van de gebruiker wordt front-end genoemd. Het serverprogramma heet back-end. Wanneer gebruik gemaakt wordt van serverdiensten op het internet, spreken we van cloud computing. Daarover leer je meer in hoofdstuk 6.5.

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. Complexe servertaken worden vaak gespreid over verschillende machines. 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.



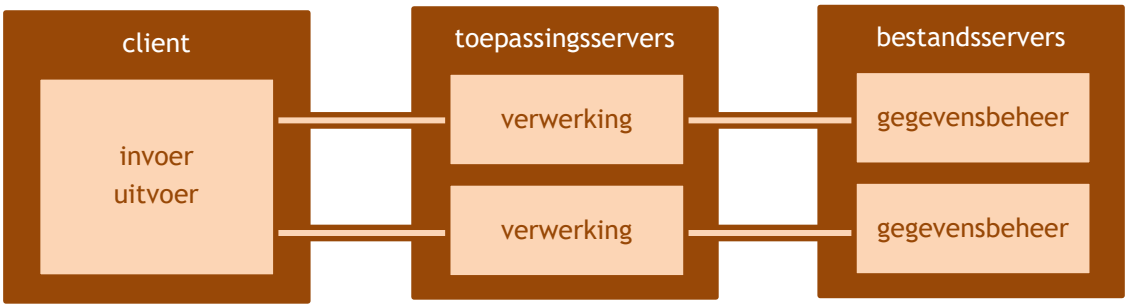
2-tier architectuur

In een 3-tier architectuur wordt een derde computer toegevoegd: een afzonderlijke toepassingsserver. Die neemt het verwerkingsgedeelte volledig voor zijn rekening. 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 aan die van de server.



3-tier 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 niet vast.

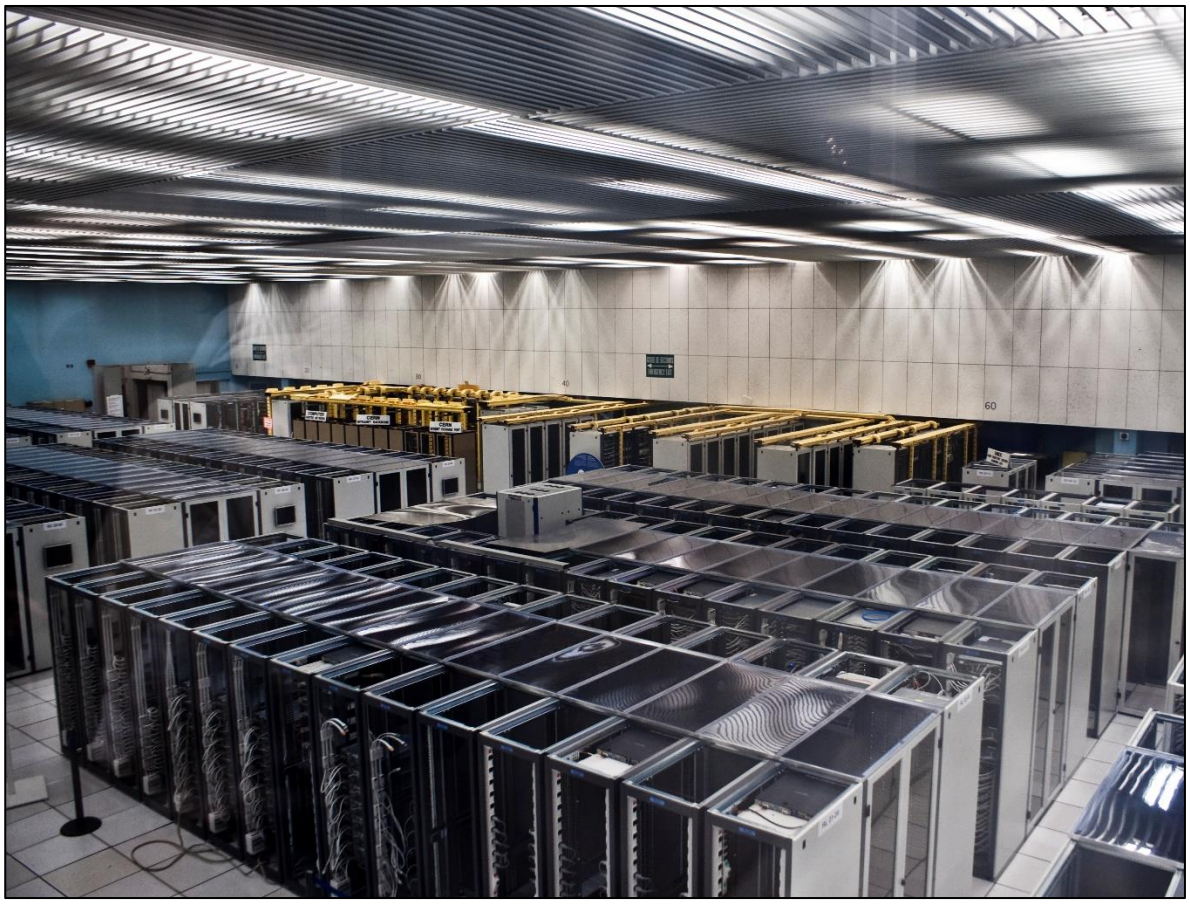


multitier architectuur

De manier waarop servers in zo'n multitier samenwerken is vaak erg verschillend. Soms 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 hardwarefouten. 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.



Het gegevensverkeer tussen servers en clients kan geautomatiseerd worden. Daarbij kunnen twee modellen gehanteerd worden: 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 tijdwinst 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 geconcipieerde computer zich van een werkstation op een aantal punten.

Zo zijn kwetsbare onderdelen 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 of de server stil te leggen. 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 met een lagere beschikbaarheid dan 99 % zijn meer dan 80 uur per jaar buiten strijd en 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 eveneens vaak nood aan een grote 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 verschillende geheugenbanken geschreven. Loopt er met één geheugenbank iets mis, dan kan de processor nog steeds ongestoord verder werken met de gegevens zich in de andere geheugenbank bevinden.

Hardware servers bestaan in heel wat verschillende gedaanten:

Voor kleinere computernetwerken bestaan er tower server cases. Die lijken erg op tower cases voor gewone desktopcomputers, maar hebben iets grotere afmetingen om een groter moederbord en/of meerdere schijven te herbergen.

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 afmetingen. Vaak zijn rack servers zo ontworpen dat ze intensief samenwerken met andere rack servers mogelijk maken. Bovendien kan de bekabeling naar andere netwerk-apparatuur die vaak in hetzelfde rack is ingebouwd, efficiënter worden aangebracht. Niets is immers zo chaotisch als een serverruimte waarin de netwerkbekabeling kriskras door elkaar loopt.

In meer gespecialiseerde omgevingen kan gebruik gemaakt worden van blade servers. Zo’n blade server is in feite een moederbord waarop enkel nog de meest essentiële onderdelen terug te vinden zijn, zoals een of meer processoren en een uitgebreid werkgeheugen. In een blade enclosure of blade chassis worden meerdere blade 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

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 blijft de computer in kwestie meestal in gebruik als werkstation. Wanneer de serverdiensten complexer of kritischer zijn, dan is een netwerkbesturingssysteem vereist (zie hoofdstuk 4.4). 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.

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:

- Het bespaart de netwerkbeheerder behoorlijk wat tijd, aangezien niet elke netwerkcomponent apart hoeft geadresseerd te worden.
- Het is makkelijker om nieuwe netwerkcomponenten toe te voegen of om oude netwerkcomponenten te vervangen.
- Mobiele computers zoals laptops, tablets en smartphones kunnen zonder het wijzigen van netwerkinstellingen vlot wisselen tussen verschillende netwerken, zoals het thuis-, school- of bedrijfsnetwerk.

Een netwerk kan meer aangesloten componenten bevatten dan er IP-adressen binnen die netwerkklasse beschikbaar zijn, aangezien in de meeste computernetwerken niet alle netwerkcomponenten tegelijk actief zijn. Een werkstation dat niet ingeschakeld is, hoeft op dat ogenblik niet over een IP-adres te beschikken. Het aantal netwerk-componenten dat daadwerkelijk actief verbonden is met het netwerk, blijft uiteraard wel beperkt tot het aantal beschikbare IP-adressen binnen het bereik.

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.

Netwerkcomponenten zonder een eigen opslagmedium, zoals sommige thin clients, kunnen toch van een IP-adres worden voor-zien.

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 in uitgebreide netwerken 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.

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

1. Een werkstation meldt zich aan op het netwerk en stuurt een lease-request naar de DHCP-servers. Indien het IP-adres van een DHCP-server voorkomt in de mappinglijst van die computer, kan dit verzoek rechtstreeks aan die server worden gericht. Zo niet wordt door middel van een broadcast-bericht het lease-request naar alle computers op het netwerk verzonden om op die manier toch een DHCP-server te bereiken. Het MAC-adres van de aanvragende computer wordt met het leaseverzoek meegestuurd.

2. De DHCP-servers die nog geldige IP-adressen beschikbaar hebben, sturen een lease-aanbod terug naar de computer met daarin:

   - Het aangeboden IP-adres en een subnetmasker.
   - Het MAC-adres van de aanvragende computer zodat het aanbod enkel bij die computer terecht komt.
   - Het IP-adres van de DHCP-server.
   - De duur van de lease – dit is de geldigheidsduur van het IP-adres voor die computer.

   Alle DHCP-servers zullen het IP-adres dat zij hebben aangeboden tijdelijk reserveren, zodat het ondertussen niet aan andere computers kan toegekend worden.

3. Nadat de computer een aanbod van één van de DHCP-servers geaccepteerd heeft, zendt deze een broadcast-bericht uit om aan te geven dat hij een keuze heeft gemaakt door een aanbod te accepteren. Alle DHCP-servers ontvangen dit bericht. De DHCP-server waarvan het aangeboden adres werd aangenomen, zal een IP-leasebevestiging sturen. De andere zullen het adres dat zij aanvankelijk gereserveerd hadden weer vrijgeven. De computer en DHCP-server kennen vanaf nu elkaars IP- en MAC-adres.

4. Uiteraard moet voorkomen worden dat de DHCP-servers op het netwerk eenzelfde IP-adres zouden toewijzen aan verschillende computers. Daarom kent elke DHCP-server IP-adressen toe uit een eigen, uniek IP-bereik.

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 leaseduur 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. Niet alleen worden ze zo sneller gevonden door de andere computers op het netwerk, het maakt ze voor de beheerder van het netwerk ook eenvoudiger bereikbaar wanneer instellingen moeten worden aangepast.

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. Van die statische adressen houdt de beheerder best een lijst bij. Zo kan vermeden worden dat eenzelfde IP-adres aan twee verschillende toestellen wordt toegewezen. Als dat gebeurt ontstaat er een IP-conflict en kan het laatst ingeschakelde toestel van de twee geen verbinding maken met het netwerk.

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 dynamisch 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:

- Statische IP-adressen moeten in het toestel zelf worden vastgelegd, terwijl gereserveerde dynamische IP-adressen centraal kunnen beheerd worden via de DHCP-server.

- Gereserveerde dynamische IP-adressen bevinden zich altijd binnen het DHCP-bereik – het bereik dat door de netwerkbeheerder toegewezen is voor dynamisch adresseren. Statische IP-adressen bevinden zich buiten dat bereik.

- 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.

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 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). Dat gaat dan zo in z'n werk:

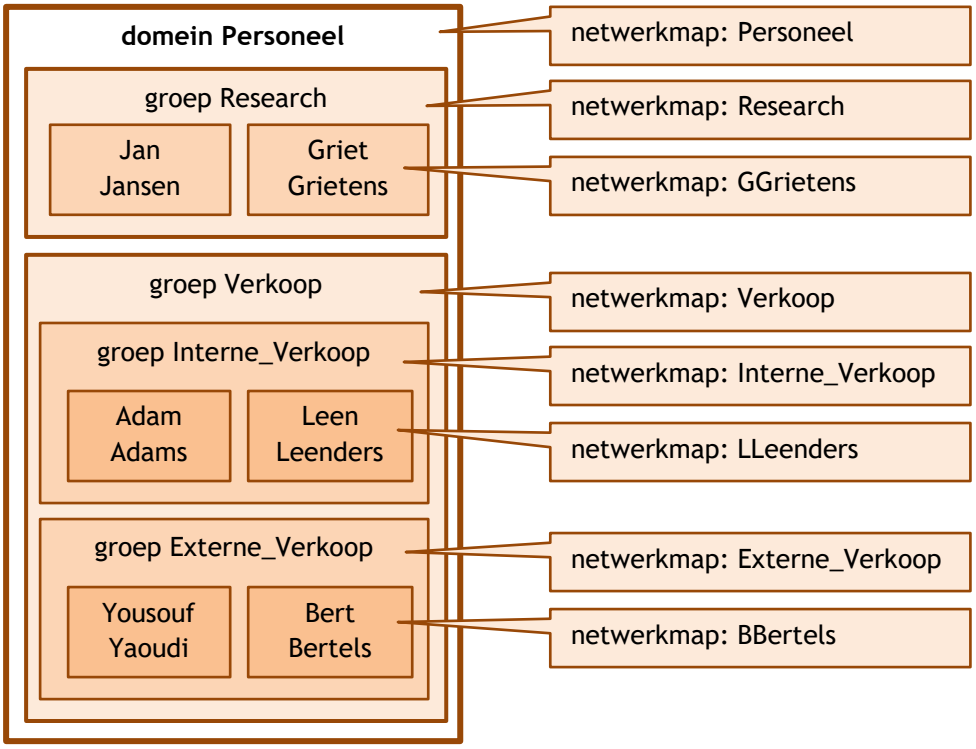
1	**link-local address generation**
	Een computer die zich op het netwerk aanmeldt, stuurt een verzoek met zijn MAC-adres. Dit adres is sowieso voor elke netwerkcomponent uniek. De SLAAC-host genereert een IPv6-adres dat start met de hexadecimale waarde FE80 in de eerste groep, dan drie groepen met de 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. Daarmee kan de computer communiceren met andere computers op hetzelfde lokale netwerk, maar niet met computers op het internet.
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 die niet gebaseerd zijn op het MAC-adres.
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 het 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 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 organisaties krijgen niet alle gebruikers dezelfde rechten en toegangen. In een groot bedrijf heeft de researchafdeling geen behoefte aan het inzien van de klantengegevens 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 en uitvoerbare bestanden uitvoeren.
modify / change	De gebruiker mag bestanden en submappen in de map wijzigen en verwijderen.
write	De gebruiker mag nieuwe bestanden en submappen in de map aanmaken.
full control	De gebruiker mag alle bewerkingen binnen de map uitvoeren, zoals de mapnaam of de beveiligingsinstellingen van de map wijzigen, de map delen en de map verwijdren.

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 en 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. De werking van DNS wordt meer gedetailleerd verklaard in hoofdstuk 6.2.2 van dit boek.

De indeling van gebruikers en computers in domeinen wordt de OU (organizational unit) genoemd. De hiërarchische databank op een Windows-computer 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 meeste clients in 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.

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 samenwerken. Wat RAID is, leer je in hoofdstuk 5.1.5 van het Sleutelboek Computerhardware.

Ook externe harde schijven met een netwerkaansluiting (NAS, netwok 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 overstroming 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. Meer over back-ups leer je in hoofdstuk 10.2 van het Sleutelboek Computerhardware.

Er bestaan drie soorten back-up servers:

cold server	Een server waarop eenmalig een back-up wordt geplaatst en die verder blijft uitgeschakeld tot de back-up nodig is.
warm server	Een server waarop regelmatig back-ups worden geplaatst maar die na elke back-up weer wordt uitgeschakeld.
hot server	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 een 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.

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 bestemmeling 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 om via het netwerk te kunnen afdrukken. Sommige printers beschikken 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 werkstation worden uitgevoerd. Een werkstation vraagt een bepaalde functie uit te voeren op de application server, die na de verwerking het gevraagde resultaat zal terugsturen. De verwerkingscapaciteit van dat werkstation 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 werkstation 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:

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

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 op 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	Een webserver die geïntegreerd is in het besturingssysteem. Dit soort webservers zijn dedicated servers: ze worden enkel voor deze servertoepassing gebruikt. Dergelijke webservers zijn erg performant omdat ze kunnen beschikken over alle hardware-bronnen van het computersysteem waarop ze draaien. Voorbeelden van in-kernel webservers zijn het op Linux gebaseerde TUX en Apache HTTP Server.
user mode webserver	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 (Internet Information Services).

Webservers 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 webservers voldoende te beveiligen. Sommige crackers maken er immers een sport van om in te breken in webservers en informatiepagina's te wijzigen. Met deze vorm van defacing hebben al vele grote bedrijven in de IT-wereld te maken 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 afgeschermde 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 die op dezelfde machine gehost worden, dreigen daardoor moeilijker of trager bereikbaar te worden.

Tegenwoordig kan je bij een web hosting bedrijf daarom 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 webservers, 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 webservers 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 dan integraal deel uit van het netwerkbesturingssysteem. Serverdiensten kunnen eveneens als applicatie bovenop een netwerkbesturingssysteem worden geïnstalleerd.

Er bestaan twee soorten netwerkbesturingssystemen:

Algemeen 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 gebruikerscompter. 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.
Embedded NOS	De software die een netwerkapparaat 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 webinterface die je opent in een browser van eender welke computer op het netwerk.

Netwerkbesturingssystemen zijn op enkele punten verschillend van gewone besturingssystemen:

- Netwerkbesturingssystemen zijn speciaal ontworpen voor serverdiensten.
- Netwerkbesturingssystemen zijn doorgaans stabieler.
- Netwerkbesturingssystemen kennen meer doorgedreven beveiligingsmogelijkheden.
- Netwerkbesturingssystemen zijn ontworpen om op complexere hardware te draaien.
- Netwerkbesturingssystemen hebben niet noodzakelijk een grafische interface.
- Netwerkbesturingssystemen volgen vaak een andere licentiepolitiek. Vooral bij commerciele netwerkbesturingssystemen worden vreemde regels gehanteerd voor het toekennen van een geldige licentie. Zo was de kostprijs van een Windows Server licentie vroeger afhankelijk van het aantal aangesloten werkstations of het aantal gebruikers, maar tegenwoordig geldt vaak het aantal processoren in een server als criterium.