Doorreizen

Als je de praktijkopdracht in paragraaf 3 van dit hoofdstuk naar tevredenheid hebt gemaakt, kun je na overleg met je docent doorgaan naar het volgende hoofdstuk.

Informatiebeleid en informatieplanning

1.1 Inleiding

Informatiesystemen hebben in relatief korte tijd een belangrijke plaats in organisaties ingenomen. Van hulpmiddel om enige taken makkelijker te verrichten zijn ze uitgegroeid tot een essentieel onderdeel van de bedrijfsvoering. Het belang van een adequate, goed georganiseerde, efficiënte en bij het bedrijf passende informatievoorziening wordt door iedereen onderkend. Computers, netwerken en andere apparatuur maken deel uit van deze informatiesystemen.

In dit hoofdstuk staan we stil bij de manier waarop een organisatie een informatiebeleid kan opzetten.

1.2 Aanwijzingen voor de leerling

We bespreken de manier waarop een bedrijf zijn informatiebeleid kan opzetten en inrichten. Informatie is voor een bedrijf natuurlijk nooit een doel. Om tot een weloverwogen informatiebeleid te komen doorloopt een bedrijf of organisatie meestal een aantal stappen.

Begrippen die in dit hoofdstuk aan de orde komen zijn:
- informatiebeleid
- informatieplan
- communicatieplan
- implementatieplan

Na bestudering van dit hoofdstuk heb je inzicht gekregen in de wijze waarop een bedrijf een informatiebeleid kan opzetten en ten uitvoer kan brengen.

1.3 Praktijkopdracht

Zoek een bedrijf (of afdeling van een bedrijf of organisatie) dat niet al te lang geleden een ingrijpende wijziging heeft doorgevoerd op één van de volgende terreinen (of een onderdeel daarvan):
- het informatiebeleid;
- de communicatiestrategie;
- het beleid.

Interview daar enige mensen. Bereid vervolgens een presentatie voor over de manier waarop het bedrijf dit heeft aangepakt en ga in op de effectiviteit van deze aanpak.

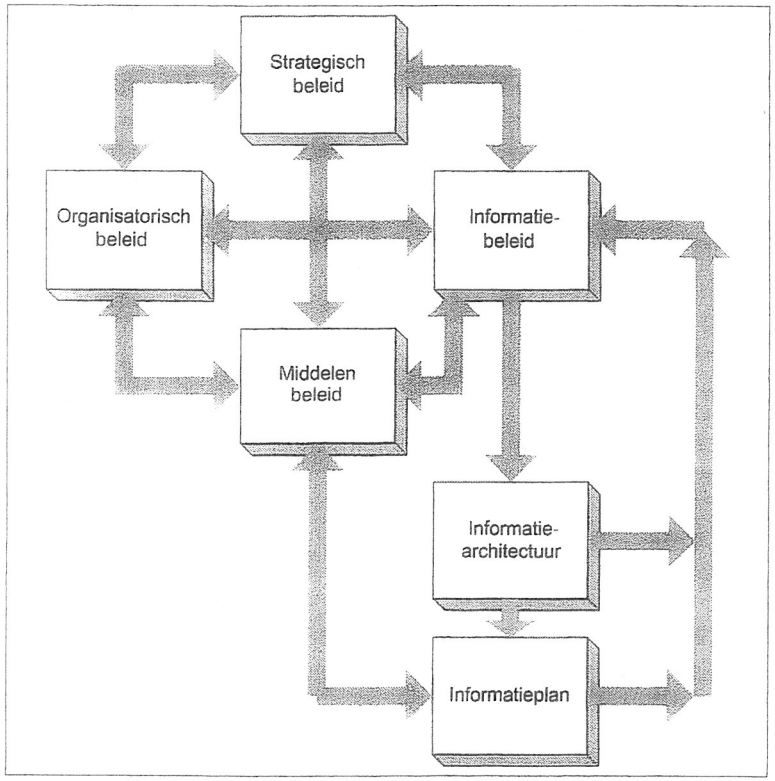
1.4 Het informatiebeleid

Computersystemen vormen tegenwoordig een cruciale schakel in de informatie- en communicatie-infrastructuur van organisaties. ICT maakt het mogelijk bedrijfsprocessen efficiënter te organiseren. Door de mogelijkheden van ICT optimaal te benutten kunnen bedrijven hun positie in de markt versterken, en mensen en middelen optimaal inzetten.

Dit vereist natuurlijk wel een zorgvuldig uitgewerkt **informatiebeleid**, waarin duidelijke keuzes gemaakt worden, die in lijn zijn met het strategisch beleid van de organisatie. Dit informatiebeleid wordt met behulp

ICT
informat
informat

De afkor
Informat
Technolo
IT (zond
wordt, u
Technolo



Figuur 1.1 Informatieplan en informatiebeleid.

Het informatiebeleid moet dus zo mogelijk vertaald worden naar een concrete 'kalender' (informatieplan), dit met aandacht voor de bedrijfsprocessen en de technologische mogelijkheden. Bijna altijd is dit maatwerk, waarbij diepgang en reikwijdte bepaald worden in samenspraak (interviews, enquêtes, workshops) met een aantal medewerkers van het bedrijf. Welke medewerkers dat zijn, wordt op basis van de organisatiestructuur bepaald. In ieder geval komen doorgaans het management en de direct belanghebbenden in aanmerking. Meestal worden via een projectstructuur enkele fundamentele veranderingen in de organisatie voorbereid, die later worden ingevoerd.

1.5 Het informatieplan

Het **informatiebeleid** beschrijft op een heldere en bondige wijze de doelstellingen, organisatie en randvoorwaarden van de informatievoorziening. Het geeft in grote lijnen de gewenste ontwikkeling weer van de informatievoorziening in de komende jaren. Het is tevens een raamwerk voor een op te stellen **informatieplan**.

Figuur 1.1 laat zien hoe het informatiebeleid is verankerd binnen de overige beleidsterreinen. Het beleid bepaalt waarin de ICT-investeringen worden gedaan. Het informatiebeleid heeft betrekking op:

- de doelstellingen;
- de benodigde ondersteuning in termen van toepassingen en gegevens;
- de relevante randvoorwaarden op het terrein van de technische infrastructuur;
- de organisatorische inrichting van de informatiefunctie.

Het **informatieplan** is de vertaling van het informatiebeleid in een realistisch **actieplan** voor een periode van drie tot vijf jaar. In dit plan wordt de bestaande situatie van de informatievoorziening afgezet tegen de gewenste ontwikkelingen. Dit wordt beschreven aan de hand van de **informatiearchitectuur**: het geheel van informatiesystemen ter ondersteuning van de bedrijfsprocessen, de bedrijfsvoering en de besturing door het management.

Vervolgens worden er projectbeschrijvingen gegeven voor de hoofdsystemen die deel uitmaken van de informatiearchitectuur. Deze **projecten** worden in onderling verband gebracht en van een realistische planning en een kostenraming voorzien. Dit onderlinge verband heeft betrekking op de vraag: wat, wanneer en wat eerst voordat aan de volgende fase kan worden begonnen. Vaak worden vervolgens in een **projectplan** de **mijlpalen** vastgelegd. Als niet alle onderdelen evenveel tijd in beslag nemen maar deel uitmaken van één eindproduct, hoeft ook niet aan alle delen tegelijk begonnen te worden. In de praktijk kán ook vaak niet alles tegelijk, en dus moeten er prioriteiten gesteld worden.

1.6 Voorbeeld van een informatiebeleid

Een ziekenhuis wordt door een verouderd ziekenhuisinformatiesysteem gehinderd in zijn ambitieuze plannen om procesgeoriënteerd en klantgericht te werken. Door een reeks van mislukte innovaties is de gebruikersorganisatie passief geworden en heeft men het vertrouwen in de afdeling

Met dank
Gemini En

Index

ziekenhuisinformatiesysteem
communicatie
communicatieplan
implementatieplan

Met hulp van enkele consultants wordt met een brede projectorganisatie een nieuw informatiebeleid ontwikkeld, dat toegesneden is op de organisatie. Vervolgens wordt dit beleid binnen enkele maanden omgezet in een gedetailleerd informatieplan, waarin onder andere een migratiepad wordt beschreven naar een nieuw (leverancieronafhankelijk) **ziekenhuisinformatiesysteem**. Onderdeel daarvan zijn een aantal concrete projecten die gefaseerd zijn beschreven en die met behulp van een realistische planning en reële kostenindicatie zijn neergezet. Het ziekenhuis is weer klaar voor de toekomst!

1.7 Communicatie en implementatie

Als er een nieuw informatiesysteem moet worden ontwikkeld en ingevoerd, is het van groot belang dat er vanaf het allereerste begin aandacht is voor **communicatie**. Vooral huidige en toekomstige gebruikers van het systeem moeten vanaf het eerste moment van de plannen op de hoogte worden gehouden. Een systeem dat eerst wordt ontwikkeld en pas daarna aan de toekomstige gebruikers ter beschikking wordt gesteld, heeft een grote kans op mislukken. Het risico dat het gewoon niet, of totaal verkeerd, gebruikt zal worden is groot. Een dergelijk systeem (we spreken dan wel van een 'over de muur gegooid systeem') brengt zijn geld zeker niet op.

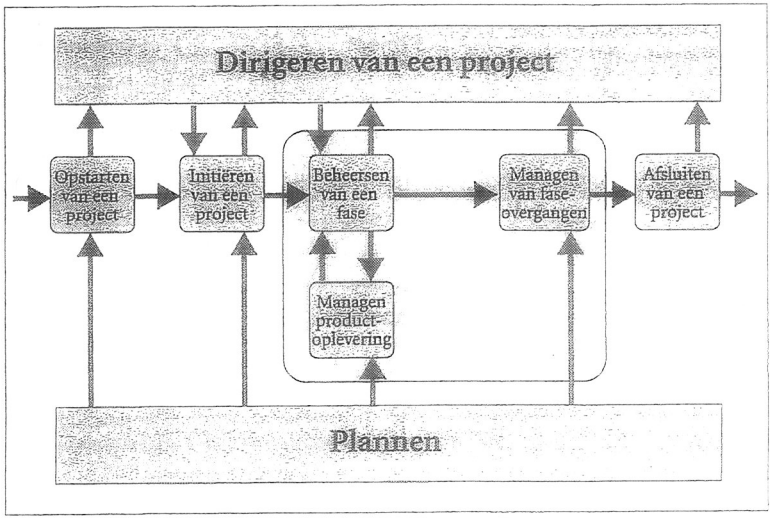
In de praktijk blijkt dat veel ontwikkelde informatiesystemen niet gebruikt worden. Daar is een hoog percentage 'over de muur gegooide' systemen bij. Het is essentieel dat vanaf het eerste begin duidelijk wordt verteld welk systeem in aantocht is, voor welke doelgroep en waarom. Hiermee wordt de kans vergroot dat het om een levensvatbaar product gaat, dat in de praktijk duidelijk mogelijkheden en kansen biedt.

Om een systeem geaccepteerd te krijgen worden een communicatieplan en een implementatieplan opgesteld:

- Het **communicatieplan** dient om in een vroeg stadium duidelijk te kunnen maken welk systeem voor welke groep welke meerwaarde gaat leveren.
- Het **implementatieplan** maakt duidelijk wat de consequenties zijn als het systeem aan de rest van de organisatie ter beschikking wordt gesteld.

1.8 Prince2

Een ontwerp voor een nieuw netwerk wordt meestal in de vorm van een **project** aangepakt; in de ICT is een projectmatige aanpak bijna altijd standaard. Een veelgebruikte methodiek om projecten in de hand te houden is **Prince2.** Deze, van oorsprong Engelse, **projectmanagementsystematiek** beschrijft onder meer het traject en de diverse fasen die doorlopen moeten worden.



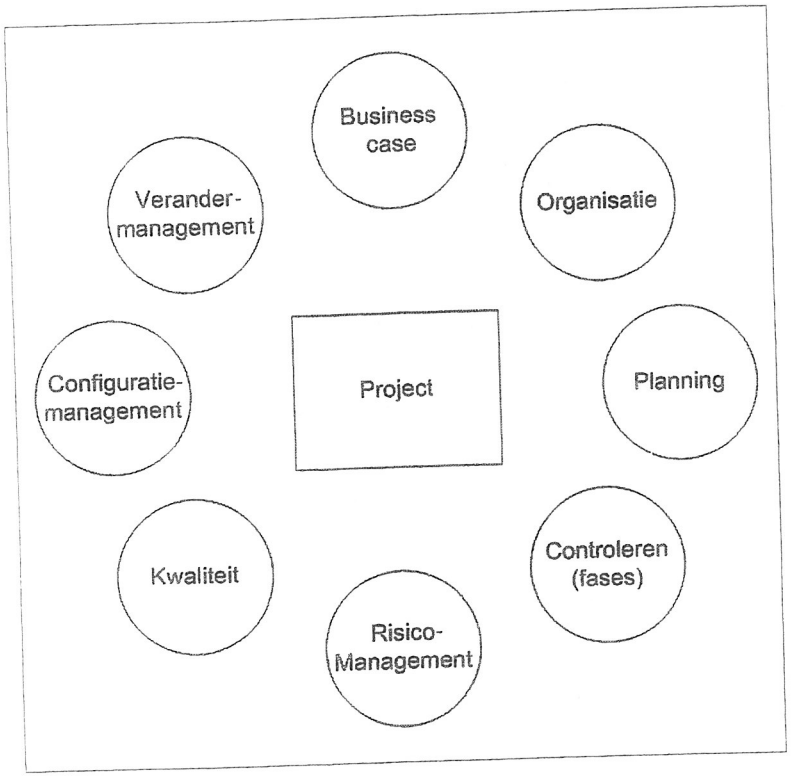
Figuur 1.2 Prince2 in schema.

Een project wordt gestart, na een zogenaamde **pre-projectfase** geïnitieerd en daarna doorloopt het project de van tevoren gedefinieerde fasen. Uiteindelijk wordt het afgesloten (zie figuur 1.2). Prince2 is op acht componenten gebaseerd:

1. business case
2. organisatie
3. planning
4. controleren
5. risicomanagement
6. kwaliteit
7. configuratiemanagement
8. verandermanagement

project
Prince2
projectr
pre-pro

De initi
een doc
Initiatie
genoem



Figuur1.3 De componenten van Prince2.

Met behulp van deze methode kunnen complexe, maar ook eenvoudige projecten gestructureerd worden uitgevoerd op een wijze waar alle belanghebbenden achteraf tevreden over kunnen zijn. Een veelgehoord punt van kritiek op Prince2 is dat het erg veel papier oplevert. Zonder dat we dit willen tegenspreken is het echter ook een werkwijze die vaak het gewenste product oplevert. Veel ontwerpprocessen worden met behulp van Prince2 uitgevoerd.

1.9 Vragen en opdrachten

1.9.1 Open vragen

1. Waarom is het van groot belang dat bedrijven en organisaties een informatiebeleid ontwikkelen?
2. Beschrijf kort de samenhang tussen een informatieplan en informatiebeleid.
3. Welke terreinen moeten door een informatiebeleid minimaal bestreken worden?
4. Wat is het nut van een communicatieplan?
5. Zet in de juiste volgorde: informatieplan, informatiebeleid, implementatieplan, communicatieplan.

1.9.2 Opdrachten

1. Zoek op hoe een informatieplanning eruit ziet.
2. Vraag het ICT Informatiebeleid van je school op (of van je laatste stagebedrijf), bestudeer het en doe verbetervoorstellen.
3. Zoek op het internet een informatiebeleidsplan op en benoem in maximaal één A4'tje de hoofdonderwerpen.
4. In de BVE-sector wordt informatiebeleid onder andere ondersteund door een gegevenswoordenboek. Zoek dit op de site van de BVE Raad (www.bveraad.nl) op en probeer aan te geven voor welke systemen op school dit consequenties heeft.

Het ontwerpproces, een praktische inleiding

Doorreizen

Als je de praktijkopdracht in paragraaf 3 van dit hoofdstuk naar tevredenheid hebt gemaakt, kun je na overleg met je docent doorgaan naar het volgende hoofdstuk.

Het ontwerpproces, een praktische inleiding

2.1 Inleiding

In dit boek staat de manier waarop een netwerk ontworpen kan worden centraal. Daartoe zal veelal een ontwerpstrategie worden gebruikt.
In dit hoofdstuk ontwerpen we bij wijze van inleiding een netwerkje voor thuisgebruik: een zogenoemd SOHO-netwerk (Small Office Home Office). Later zal blijken dat we daar een methode voor kunnen gebruiken die in wezen niet veel afwijkt van wat we voor grotere netwerken gebruiken.

2.2 Aanwijzingen voor de leerling

In dit hoofdstuk behandelen we het ontwerp en de inrichting van een 'huisnetwerkje'. Er is veel aandacht voor de wijze van fasering. We werken aan de hand van onderstaand schema, dat in het hele boek als leidraad geldt.

Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER-PROCES
De benodigde en gewenste architectuur van het netwerk.	
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

2.3 Praktijkopdracht

In paragraaf 2.4 wordt een methode beschreven om een SOHO-netwerk te ontwerpen. Daar wordt onder andere een fasering gebruikt die moet leiden tot het netwerk met de gewenste specificaties.

Gebruik deze methode om voor je eigen thuissituatie een netwerk te ontwerpen. Ga uit van een netwerk dat bestemd is voor alle bewoners/gebruikers. Geef duidelijk aan wat de conclusies per fase zijn en hoe je deze in de volgende fase gebruikt.

2.4 Ontwerpen (van netwerken)

In dit boek komt het ontwerpen van netwerken uitgebreid aan de orde. In dit proces zijn een aantal essentiële fasen te onderscheiden:

1. Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk dat nodig is voor dit informatiesysteem.

Index

huisnetwerk
functioneel ontwerp
informatiesysteem
architectuur van het netwerk
wifi
wireless LAN
draadloos netwerk
switch
hub
gateway
firewall

3. De hardware die nodig is om de gewenste functionaliteit te garanderen.
4. De benodigde (systeem)software voor het netwerk; dit kan zowel om servers als om werkplekken gaan.
5. Het realiseren van de gewenste functionaliteit; dit heeft betrekking op het plannen van de installatie, het organiseren en de uitvoering.
6. Het praktische gebruik. Deze laatste fase is niet alleen de ingebruikname, maar ook de planning van beheer en onderhoud. Hoe wordt het netwerk up-to-date gehouden, enzovoort?

Dit proces laat zich op meerdere niveaus beschrijven. Als we een eenvoudig **huisnetwerk** ontwerpen zien we deze fasen ook terug:

1. Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk
Vaak wil men op diverse plekken in huis een computer kunnen gebruiken met standaardsoftware (tekstverwerkings- en spreadsheetpakket, en eventueel een presentatiepakket of een database). Daarnaast wil men graag de beschikking over een grafisch pakket om eenvoudige afbeeldingen te kunnen maken of ontwerpen. Ook een internetverbinding behoort tot de standaardwensen, evenals e-mailfaciliteiten.
Het ontwerpen van een eigen **informatiesysteem** is hier natuurlijk niet aan de orde. Wel zullen er bijvoorbeeld eisen worden gesteld aan het type software dat gebruikt moet kunnen worden. Dat is dan bijvoorbeeld een grafisch pakket voor iemand met als hobby fotografie, of een tekenpakket voor iemand die graag ontwerpt.

2. De benodigde en gewenste architectuur van het netwerk
Voor de architectuur moet een keuze worden gemaakt uit de ter beschikking staande technologieën. Sinds kort behoort ook een draadloze (**wifi**) oplossing tot de realiseerbare mogelijkheden. Tot voor kort was dat een bijna onbetaalbare oplossing, maar de 802.11b (11 Mb wireless LAN) en 802.11g (54 Mb **wireless** LAN) netwerken zijn nu betaalbaar. Anders moet een keuze worden gemaakt waar het huisnetwerk aan het netwerk van de ISP wordt verbonden. Afhankelijk van de benodigde snelheid moeten keuzes gemaakt worden of intern een **switch** of een **hub** gebruikt wordt. Een keuze voor een UTP-netwerk (cat 5) ligt voor de hand, maar er zijn ook andere opties.
De toegang kan gerealiseerd worden door een aparte computer als **gateway** neer te zetten. Dat kan een grote Linux machine met meerdere netwerkkaarten zijn die een eigen **firewall** draait (ipchains, ipfwadm of nog iets anders) en een internet-cache als squid, maar ook een Windows machine met soortgelijke software. Een andere optie kan een 'één flops FreeSCO of LRP. Er zijn tegenwoordig tegen een aantrekkelijke prijs ook gecombineerde switch kabel/ADSL-modems leverbaar die deze functionaliteit combineren. Dit gaat echter wel ten koste van functionaliteit in configuratie.

3. De hardware die nodig is om de gewenste functionaliteit te garanderen
Het selecteren van de **netwerkhardware** is een proces dat deels al in de vorige fase is gedaan. De specifiek voor het netwerk benodigde hardware is meestal al bekend. De benodigde hardware voor een nieuw informatiesysteem (of in het geval van een thuisnetwerk: de benodigde hardware om de gewenste software te kunnen gebruiken) volgt hier uit het functioneel ontwerp.

4. De benodigde (systeem)software
De volgende fase, die van softwareselectie, wordt in een huisnetwerk meestal overgeslagen, of beter gezegd: men denkt vaak geen keuze te hebben. Meestal kiest men voor een Windows versie met een Microsoft Office-suite. Ook een Linux distributie met X en een Window-manager kan echter een perfecte combinatie opleveren, bijvoorbeeld OpenOffice en Gimp als grafisch pakket.
Veel grafische gebruikers zweren nog steeds bij een Apple configuratie. Dit is voor deze gebruikers een veel bekendere en eigenlijk ook betrouwbaardere omgeving dan Windows. Photoshop is oorspronkelijk voor de Apple Macintosh ontwikkeld. Ook bestaat er een Mac-versie van Microsoft Office (trouwens ook een OpenOffice). De huidige generatie Powerbooks bestaat uit sterke, stabiele systemen.

5. Het realiseren van de gewenste functionaliteit
Dit komt hier overeen met het bouwen van het netwerk, het realiseren van de verbindingen en het installeren en configureren van de machines. In een groter netwerk wordt daarvoor altijd eerst een **implementatieplan** gemaakt.

6. Het praktische gebruik
Als laatste fase wordt meestal beschouwd het in gebruik nemen, of houden, van een netwerk. Dit lijkt een eindpunt van het ontwerpproces, maar feitelijk is dit het begin van de onderhoudscyclus. Het netwerk moet regelmatig onderhouden worden. De laatste patches moeten worden geïnstalleerd en onderdelen moeten worden vervangen door nieuwere, betere of snellere.

In het schema hieronder is het **ontwerpproces** weergegeven:

Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER-PROCES
De benodigde en gewenste architectuur van het netwerk.	
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

Een aparte fase in dit proces is in feite het **documenteren**. Eigenlijk moet het documenteren niet als apart proces worden bekeken, maar als een continu proces dat bij alle fasen hoort. Bij elke fase moet vastgelegd worden wat de eisen zijn, welke gevolgtrekkingen daaruit mogelijk zijn en tot welke conclusies dit leidt. Ook moet hier vastgelegd worden welke gevolgen bepaalde stappen hebben. Bijna elk besluit heeft namelijk ook ongewenste gevolgen. Een aantal dingen wordt onmogelijk. Dit betekent dat dit bij alle belanghebbenden ook duidelijk moet zijn.

2.5 Opdrachten

1. Ontwerp een netwerkje 'voor thuis'. Ma gebruikt een computer voor haar werk en neemt regelmatig haar laptop mee naar huis. Pa gebruikt de computer voornamelijk voor de administratie van de zwemvereniging. Je zus gebruikt hem voor school en msn. Je broer gebruikt hem voor gaming en voor school. Let bij het ontwerp op:
   a. infrastructuur;
   b. functionaliteit;
   c. hardware;
   d. software;
   e. beheer;
   f. veiligheid.

2. Je werkt in een computerwinkel. Een klant komt binnen en wil een klein netwerk thuis installeren.Welke vragen stel je en in welke situatie kom je met welk advies?

3. Enkele leden van de basketbalvereniging willen een eigen website opzetten. Ze weten niet goed hoe ze dit aan moeten pakken. Ze vragen jou advies, want jij hebt verstand van informatica. Hoe pak je het aan en welk advies geef je aan de vereniging?

4. Op school wil men een experiment met notebooks en wireless access opzettten. Er wordt een projectteam samengesteld met daarin ook enkele leerlingen (als toekomstige gebruikers). Jij bent een van hen. Licht toe welke stappen het team moet zetten om volgens de principes van Prince2 dit project uit te voeren.

Het functioneel netwerkontwerp

Doorreizen

Als je de praktijkopdracht in paragraaf 3 van dit hoofdstuk naar tevredenheid hebt gemaakt, kun je na overleg met je docent doorgaan naar het volgende hoofdstuk.

Het functioneel netwerkontwerp

3.1 Inleiding

Netwerken zijn in organisaties niet meer weg te denken. Bijna elk bedrijf waar op administratief gebied ook maar iets gebeurt, heeft een netwerk. Voor bedrijven die van dergelijke activiteiten hun belangrijkste bezigheid hebben gemaakt, is het netwerk zelfs cruciaal.

Vroeger ontstond het netwerk meestal tegelijk met de technologie. Vandaag de dag neemt een klant daar geen genoegen meer mee. Hij wil de garantie dat het netwerk kan wat het moet kunnen (niet minder, maar ook niet meer) en dat hij dat tegen een concurrerende prijs koopt.

In dit hoofdstuk gaan we in op de uitgangspunten en de wijze waarop een netwerkontwerp gemaakt kan worden voor een klein tot middelgroot bedrijf. We bespreken het deel van het ontwerpproces dat wel het functioneel ontwerp wordt genoemd.

3.2 Aanwijzingen voor de leerling

In dit hoofdstuk maken we een functioneel netwerkontwerp voor een bedrijf dat qua omvang in het midden- en kleinbedrijf (MKB) thuishoort. We doen dit door eerst de vereiste functionaliteit vast te leggen en vervolgens te onderzoeken welke techniek er nodig is om een netwerk te maken dat aan die vereisten voldoet.

Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER-PROCES
De benodigde en gewenste architectuur van het netwerk.	
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

Vervolgens presenteren we de resultaten van dat onderzoek aan onze klant. Het functioneel netwerkontwerp is de basis voor het later te maken inrichtingsplan. Begrippen die in dit hoofdstuk aan de orde komen zijn:

- netwerk als business tool
- functioneel netwerkontwerp (FNO)
- ontwerpmethodieken
- outsourcen of zelf doen
- BE-matrix

We beginnen dit hoofdstuk echter met een korte inleiding over de watervalontwerpmethode.

3.3 Praktijkopdracht

Voor een bedrijf dat via internet vitaminepillen verkoopt en dat verhuist naar een nieuwe locatie in Almere moet een functioneel netwerkontwerp gemaakt worden. De markt is 'booming' en er is besloten dat er in Almere een nieuw netwerk moet komen. Op deze plaats wil men ook de web-

functioneel netwerkontwerp
functioneel ontwerp
technisch ontwerp

Maak voor dat bedrijf een functioneel netwerkontwerp en maak een PowerPoint-presentatie om de resultaten van je onderzoek aan de klant te presenteren. Je kunt het materiaal in dit hoofdstuk gebruiken om tot je ontwerp te komen.

3.4 Het functioneel netwerkontwerp

Tegenwoordig is het bijna onvermijdelijk in automatiseringstrajecten dat op een gegeven moment het netwerk om de hoek komt kijken. Bij een groot bedrijf, dat al zwaar in netwerken heeft geïnvesteerd, moet worden beoordeeld of het huidige netwerk voldoende capaciteit en functionaliteit biedt. Bij een klein bedrijf kan het voorkomen dat een netwerk gerealiseerd moet worden, hoewel deze situatie de laatste tijd natuurlijk steeds minder vaak aan de orde is.

Wat nog wel steeds voorkomt, is dat het netwerk ontwerptechnisch als sluitpost wordt gezien. Het hele automatiseringstraject wordt met zorg doorlopen en aan het eind wordt er opeens nog bedacht dat er een netwerk nodig is om de applicatie o.i.d. te gebruiken. Op het laatste moment moet er dan nog een netwerk komen.

Vaak betekent dit dat het ontwerp van het netwerk niet goed doordacht is en dat er met bijvoorbeeld beheer nauwelijks rekening is gehouden. Niet alleen ontstaan hierdoor functionele problemen, maar bovendien worden bedrijven in dat geval ook voor veel hogere kosten gesteld dan oorspronkelijk is voorgespiegeld. Er zouden veel minder automatiseringstrajecten mislukken als eerder en beter aandacht geschonken zou worden aan het ontwerp van het netwerk.

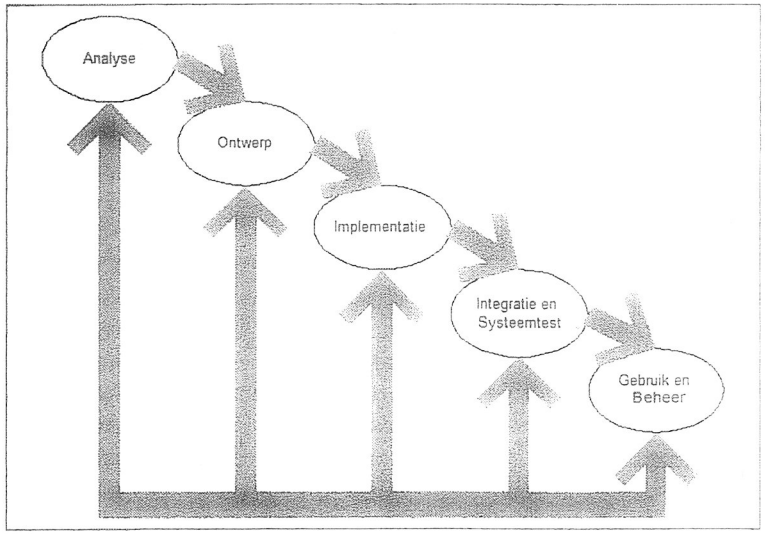
Een vast discussiepunt is waar het **functioneel ontwerp** (FO) eindigt en het **technisch ontwerp** (TO) begint. In de praktijk is hier vaak geen scherpe lijn te trekken. In het algemeen hoort alles wat rechtstreeks uit functionele eisen volgt, thuis in het functioneel ontwerp. Dit kan soms al heel technisch zijn. Om een voorbeeld te geven: als er 'full internet access' moet zijn (functionele eis), dan ligt al vast dat het een TCP/IP-netwerk moet worden. Daarmee is bijvoorbeeld het nummerplan een onderdeel van het functioneel ontwerp geworden.

In dit hoofdstuk gaan we zoals gezegd in op het FNO. Met dit document wordt vastgelegd welke functionaliteit het netwerk moet krijgen om aan de toekomstige gebruikersvraag tegemoet te komen. Daarmee is ook de vaak nog redelijk eenvoudig te doen; de toekomstige vraag zal echter voor een deel gebaseerd zijn op aannamen.

3.4.1 De projectdocumentatie

Een netwerk wordt bijna altijd ontworpen in het kader van een groter geheel. Een bedrijf ontwerpt en implementeert bijvoorbeeld een nieuw informatiesysteem en in het kader daarvan wordt ook een nieuw netwerk ontworpen. Bij een (groot) project wordt normaal gesproken een **projectmanagementmethode** gebruikt om onder andere grenzen af te bakenen, de voortgang vast te leggen en meetpunten te hebben om een project voortgang te laten hebben (of niet). Een veelgebruikte methode is **Prince2**. Met deze methode wordt tegelijkertijd een deel van de documentatie gewaarborgd.

3.5 Ontwerpmethodiek en valkuilen



Figuur 3.1 Watervalmethode.

In deze paragraaf kijken we wat de gevolgen zijn van de keuze voor een bepaald systeemontwikkeltraject. Afhankelijk hiervan wordt het vervolgtraject bepaald. We gaan hier uit van de zogeheten **watervalmethode**,

mogelijk geweest. Hierdoor zou het vervolgtraject er overigens wel anders uit hebben zien. Veel grote bedrijven hanteren een eigen ontwikkelmethode. Zo maakt IBM voor (software)ontwikkeling gebruik van RUP (Rational Unified Process) en heeft Cisco het CCDA certificaat (Cisco Certified Design Associate).

In de **systeemontwikkeling** wordt vaak gewerkt met de watervalmethode. Deze is schematisch afgebeeld in figuur 3.1. Bij deze methodiek worden enkele fasen onderscheiden die in principe na elkaar worden doorlopen. We kunnen dit zien als een **levenscyclus** ('life cycle') van een product.

3.5.1 Analyse

De **fase Analyse** is het startpunt van elk ontwerptraject. Welke functionaliteit is nodig? Wat kan elk network operating system/mailsysteem of applicatie bieden om een bijdrage te leveren aan de eindoplossing? Ook een analyse van benodigde hardware hoort hierbij.

3.5.2 Ontwerp

In de **fase Ontwerp** wordt bepaald hoe de benodigdheden worden geïmplementeerd die uit de analysefase zijn voortgekomen. Bij een groot ontwerp wordt het wel in stukken verdeeld, om dan elk deel apart uit te werken en het geheel later weer samen te voegen.

Het is van groot belang om bij een netwerkontwerp zo vroeg mogelijk met documenteren te beginnen. Dan kan later worden nagegaan welke besluiten op welk moment zijn genomen. In deze fase moet ook al een overzicht worden gemaakt van de applicaties die nodig zijn. Bovendien moet beschreven worden welke voorzieningen ten aanzien van hardware en ruimte er getroffen moeten worden. De **netwerkinfrastructuur** moet hier dus ook al globaal vastgelegd en gedocumenteerd zijn. Alle netwerkcomponenten moeten zijn gespecificeerd, zowel qua type als qua configuratie. (Denk ook aan beveiliging etc.)

3.5.3 Implementatie

In de **fase Implementatie** wordt het netwerk volgens het ontwerp gereali- [illegible] gebouwd en geplaatst. De software wordt geïn-

aangelegd, getest en in gebruik genomen, enzovoort. Iets wat hier niet vergeten moet worden, is dat ook gebruikers moeten worden opgeleid en met het netwerk bekend worden gemaakt.

Een aspect dat wel eens in de verdrukking komt en waar soms onvoldoende rekening mee gehouden wordt, is dat het in gebruik nemen van een netwerk (of informatiesysteem) voor een groot aantal werknemers een ingrijpende verandering in hun werkzaamheden betekent. Vaak zijn er groepen mensen van wie het werk enigszins tot ingrijpend gewijzigd gaat worden. Het kan bijvoorbeeld betekenen dat iemand een veel groter deel van zijn of haar tijd zittend achter een toetsenbord moet doorbrengen en/of dat bepaalde taken (bijvoorbeeld archiveren) in zijn geheel verdwijnen. Niet iedereen zit daarop te wachten. Integendeel, velen krijgen het idee dat hun werk minder leuk en afwisselend gaat worden. Dit kan betekenen dat er binnen de organisatie weerstand is bij het invoeren van een nieuw systeem. Een systeem waartegen weerstand bestaat, wordt doorgaans niet gebruikt!

Het belang van het zorgvuldig omgaan met de invoering kan niet voldoende benadrukt worden. Zorg ervoor dat gebruikers het systeem positief zien en dat ze erachter staan. Betrek toekomstige gebruikers bij de ontwikkeling en benadruk de positieve kanten van de invoering. Niet alleen verlaagt dit de eventuele weerstand, maar het komt ook de functionaliteit van het systeem ten goede. Toekomstige gebruikers weten immers het beste wat voor werk ze doen en welke functionaliteit ze het meest gebruiken. Ook zijn zij beter in staat de volgorde van sommige stappen te bepalen. De **user interface** kan beter door een gebruiker worden bedacht dan door een ontwikkelaar.

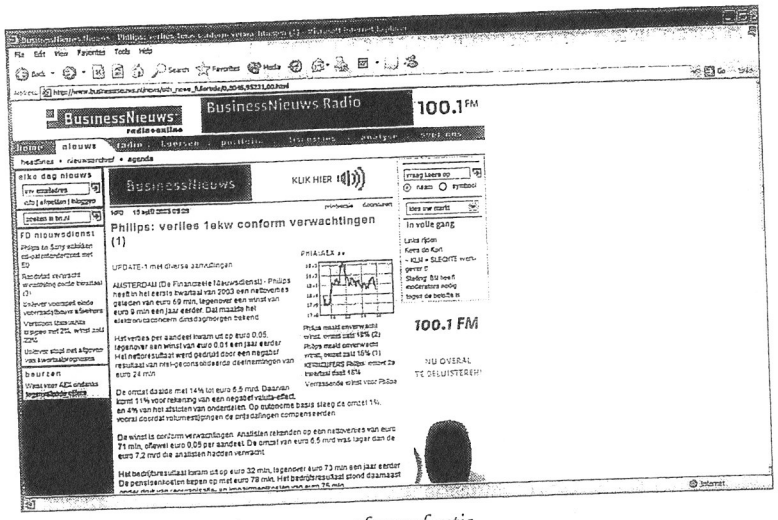
3.5.4 Integratie en systeemtest

In de **testfase** wordt het netwerk in gebruik genomen en wordt gekeken of de procedures die zijn beschreven voldoende zijn om voor een probleemloze werking te zorgen. Is het systeem stabiel genoeg? Is de functionaliteit conform het geformuleerde?

Systeemtests moeten voortdurend uitgevoerd worden. In de praktijk blijkt vaak dat er na lange tijd nog fouten aan het licht komen die de werking van het systeem negatief kunnen beïnvloeden.

user inte
systeemt
testfase

Een gebr
gebruikt
zetten, e
knoppen
hebben
meest tr
voorbeel
gebruike
voor de
tie vier k
voor de
één mak



Figuur 3.2 Ten gevolge van een softwarefoutje...

Een netwerk bevat bijvoorbeeld vaak data die niet algemeen beschikbaar mag zijn. Een foutje op dit gebied betekent in eerste instantie niet dat de functionaliteit van het netwerk bedreigd wordt, maar wel dat de beschikbaarheid van data voor derden op termijn een ramp kan veroorzaken. Denk maar eens aan het zichtbaar zijn (voor ongeautoriseerde derden) van de creditcard-gegevens van een e-commercesite.

3.5.5 Gebruik en beheer

Gebruik en beheer is de fase waarin een goed en uitgebreid getest systeem gedurende langere tijd functioneel is. Er is dan natuurlijk nog wel sprake van (noodzakelijk) onderhoud. Deze onderhoudstaken kunnen onderscheiden worden in:

- **Dagelijks beheer:**
  - backups;
  - controleren kritische system software updates;
  - viruscontrole;
  - nalopen van security items, zoals firmware upgrades (security en exploits).

- **Periodiek onderhoud:**
  - Eenmalige (onderhouds)acties:
    - vervangen van defecte onderdelen.

Ook het installeren van andere dan security softwarematige upgrades op OS'en, NOS'en en applicaties maakt deel uit van het onderhoud, net zoals het (in beperkte mate) upgraden van andere onderdelen. In de levenscyclus van een netwerk kan na verloop van tijd op een enkele plek behoefte aan meer bandbreedte zijn. Het vervangen van een enkele hub door bijvoorbeeld een switch kan hier een oplossing zijn die we nog tot onderhoud kunnen rekenen. Een over de gehele linie veel grotere behoefte aan bandbreedte vereist een herontwerp van het netwerk.

In de praktijk komt het nogal eens voor dat het netwerkontwerp ergens in fase 3 (de implementatiefase) wordt opgepakt. Het netwerk is dan gebouwd zonder dat er duidelijke keuzes zijn gemaakt. Dit betekent vaak dat onbekend en onduidelijk is welke eisen aan het netwerk gesteld kunnen worden. Veel gebruikers zijn dan ontevreden over het netwerk, en het risico bestaat dat het niet wordt gebruikt voor het doel waarvoor het gemaakt is. Een dergelijke vorm van kapitaalvernietiging kan natuurlijk nooit de bedoeling zijn. Aan de andere kant van de balans staat een netwerk dat wel aan de verwachtingen voldoet, maar zodanig overgedimensioneerd is dat het ook voor veel minder dan het nu bestede bedrag gerealiseerd had kunnen worden. Ook dit is natuurlijk onwenselijk.

3.6 Zelf doen of outsourcen?

3.6.1 Installatie van het netwerk

Er zijn twee (of eigenlijk drie) manieren om een netwerk te installeren:

1. **Doe het zelf:**
   - Kies en koop hardware en software.
   - Installeer hardware, software, kabels, netwerkkaarten, servers, printers; configureer gebruikers, mail en dergelijke.

Hiervoor heeft een bedrijf natuurlijk nogal wat kennis en kunde nodig. Hoe groter en/of ingewikkelder het netwerk is, hoe meer deskundigheid vereist is.

2. **Het alternatief** voor een bedrijf dat zijn netwerk alleen als tool nodig heeft: vertrouw de klus toe aan een (ander) bedrijf. Met ander

Index

Service Level Agreement
SLA
onderhoud
onderhoudscontract

Assist

In een SLA wordt afgesproken welke functionaliteit en services geleverd worden tegen welke prijs. Als Nederlandse term kom je wel SNO tegen, wat staat voor Service Niveau Overeenkomst. Ook DNO (Diensten Niveau Overeenkomst) is niet ongebruikelijk. Het begrip SLA komt uit ITIL, in deze beheermethodiek speelt de SLA een centrale rol.

prijs. Laat een gespecialiseerd bedrijf het netwerk aanleggen en onderhouden.

De optie om te 'oursourcen' wordt steeds vaker gekozen. Steeds meer bedrijven willen zich alleen met hun 'core business' bezighouden en wensen zelf niet de deskundigheid op te bouwen om een netwerk te exploiteren. Met behulp van een **Service Level Agreement** (SLA) wordt vervolgens een deal gesloten en is er een gegarandeerd aanbod van netwerkservices.

3. **Een tussenvorm** is ook mogelijk: daarbij is de aanleg van de infrastructuur uitbesteed en levert een (ander?) bedrijf de hardware. Installatie en ingebruikname worden in eigen hand gehouden. Hoe dit wordt gerealiseerd, is afhankelijk van de know-how en menskracht van de eigen organisatie.

3.6.2 Onderhoud van het netwerk

Voor wat betreft **onderhoud** is er dezelfde keuze: zelf doen of uitbesteden? In dit verband moet wel onderscheid gemaakt worden tussen twee soorten onderhoud: iets wat we voor het gemak maar even 'reparatiewerk' noemen, en preventief onderhoud. Het bijwerken van versies, installeren van patches etc. kan als preventief onderhoud worden gezien. Bij reparatiewerk moet zowel met hardware- als softwarematige herstelwerkzaamheden rekening gehouden worden.

Eigenlijk zijn er drie opties:

1. Alle reparaties zelf uitvoeren.

2. Bij een defect het product isoleren en naar de fabrikant terugsturen. Het probleem is dan vaak dat men geen of weinig controle heeft wanneer het weer (al of niet gerepareerd) terugkomt. Afhankelijk van hoe cruciaal het onderdeel voor het functioneren van het netwerk is, is dit een groter of minder groot probleem.

3. **Onderhoudscontracten** (SLA's) afsluiten die volledig voorzien in het beheer. In een dergelijk contract kan ook opgenomen worden welke service men tegen welke prijs verwacht en wat de maximale storingen zijn (in hevigheid en 'duur') waar men rekening mee moet houden.

[illegible] van het informatiesystem [illegible] ontwerp van het netwerk	
De benodigde en gewenste architectuur van het netwerk.	HET DOCUMENTEER-PROCES
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

3.7 Onderdelen van het functioneel ontwerp

Een FNO is het startpunt voor het ontwerpen van een netwerk; het is een ontwerp van het netwerk vanuit functionele eisen. Een **functioneel netwerkontwerp** legt aan een niet-technisch onderlegd persoon uit welke functionele eisen aan het netwerk gesteld worden en welke gevolgen dat heeft voor het ontwerp.

Dit betekent niet dat het FNO in principe geen technische taal mag bevatten. Als er uit de benodigde functionaliteit technische eisen en/of randvoorwaarden naar voren komen, horen deze zeker in het FNO thuis. In een FNO moet zonodig de conclusie getrokken kunnen worden dat een netwerk (nog) niet te realiseren is, bijvoorbeeld omdat de bandbreedte niet voldoet. Als het FNO geen techniek zou mogen bevatten, kan deze conclusie niet getrokken worden. Op papier is een 200 Tb-netwerk gemakkelijk genoeg op te schrijven. Het daadwerkelijk realiseren hiervan is een ander verhaal.

Het is lastig om een standaard format voor een FNO te geven. Veel hangt af van de situatie en de wensen van de klant. Er zijn eigenlijk geen twee identieke netwerken en dus ook geen twee gelijke functionele ontwerpen. Het vertrekpunt met betrekking tot de business case is vrijwel altijd verschillend en als gevolg daarvan ook de grenzen van het functioneel ontwerp. De basis is een programma van eisen dat een ruwe schets geeft van de vereisten die aan het netwerk worden gesteld.

Uit de literatuur zijn er diverse definities van een FNO bekend. Zonder deze fout te willen [illegible]

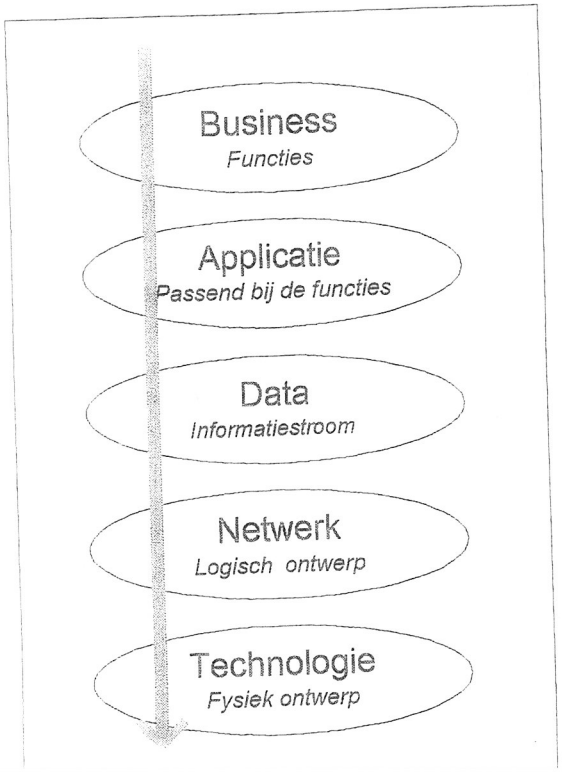
Index

top–down
business requirements

Functioneel netwerkontwerp
Het FNO is een duidelijke, 'talige' omschrijving van het toekomstige netwerk. Er wordt (met een grote mate van detail) een beschrijving gegeven van de inrichting van het toekomstige netwerk.

Voor een opdrachtgever is het van belang om te weten in hoeverre het netwerkontwerp tegemoet komt aan de ICT-wensen en welke (fysieke) veranderingen met de invoering van het netwerk gepaard gaan. Het FNO kan dan ook als overeenkomst met de opdrachtgever worden gezien.

Essentieel voor het ontwerpproces is dat er **top–down** wordt gewerkt. Het startpunt is niet wat er technisch mogelijk is of wat er voor leuks op de markt is. Nee, het startpunt vormen de vereisten vanuit de werkzaamheden van de opdrachtgever. In het Engels worden dit de **business requirements** genoemd.



Het functioneel ontwerp heeft een tweeledig doel:
1. Het moet een gedetailleerde basis zijn voor de volgende fase van het netwerkontwerp.
2. Het moet leesbaar zijn voor de opdrachtgever.

Deze aspecten kunnen in de praktijk wel eens strijdig zijn. Als te veel rekening gehouden wordt met het gegeven dat een niet-technisch onderlegd persoon het FNO moet kunnen lezen, kan het te weinig technische details bevatten om later een bruikbaar uitgangspunt voor de realisatie van het netwerk te zijn. Het gaat voor de opdrachtgever over functies en niet over de techniek. Daarom is er een verschil tussen het functioneel en technisch ontwerp. In het FNO kan bijvoorbeeld wel het volgende staan: er moet een verbinding over een TCP/IP-connectie met een minimale bandbreedte van 2 Megabit per seconde beschikbaar zijn, omdat er maximaal n transacties tegelijkertijd op de database moeten kunnen worden uitgevoerd, die elk m bandbreedte vragen. Er hoort niet in te staan dat daarvoor de Cisco router PX123ABC geschikt is.

3.7.1 BE-matrix

Om een top-down benadering te waarborgen wordt vaak van een BE-matrix gebruik gemaakt. Daarmee wordt – bij goed gebruik – gegarandeerd dat de eisen die vanuit de opdrachtgever worden gesteld, centraal staan.

	Informatie in het primaire bedrijfs-proces	Geld besparen	Toename productivi-teit	Toename beschik-baarheid informatie	Grotere desktop band-breedte	Betrouw-baarheid	Gemakke-lijk te installeren	Gema lijk te gebru
Kleurenlaserprinters								
Cd-rom server								
Internet-verbinding								
Customapplicatie								
Modems								
2 Mbps connectie								
Bestandsdeling								
Corporate (customer) database								
Mainframeverbinding								

Index

functionee
doel
BE-matrix

plattegrond
conceptdiagram

Elke technische voorziening die niet bijdraagt aan een van de doelstellingen op de bovenste rij is blijkbaar niet belangrijk genoeg om te worden gerealiseerd.

3.7.2 Conceptdiagram

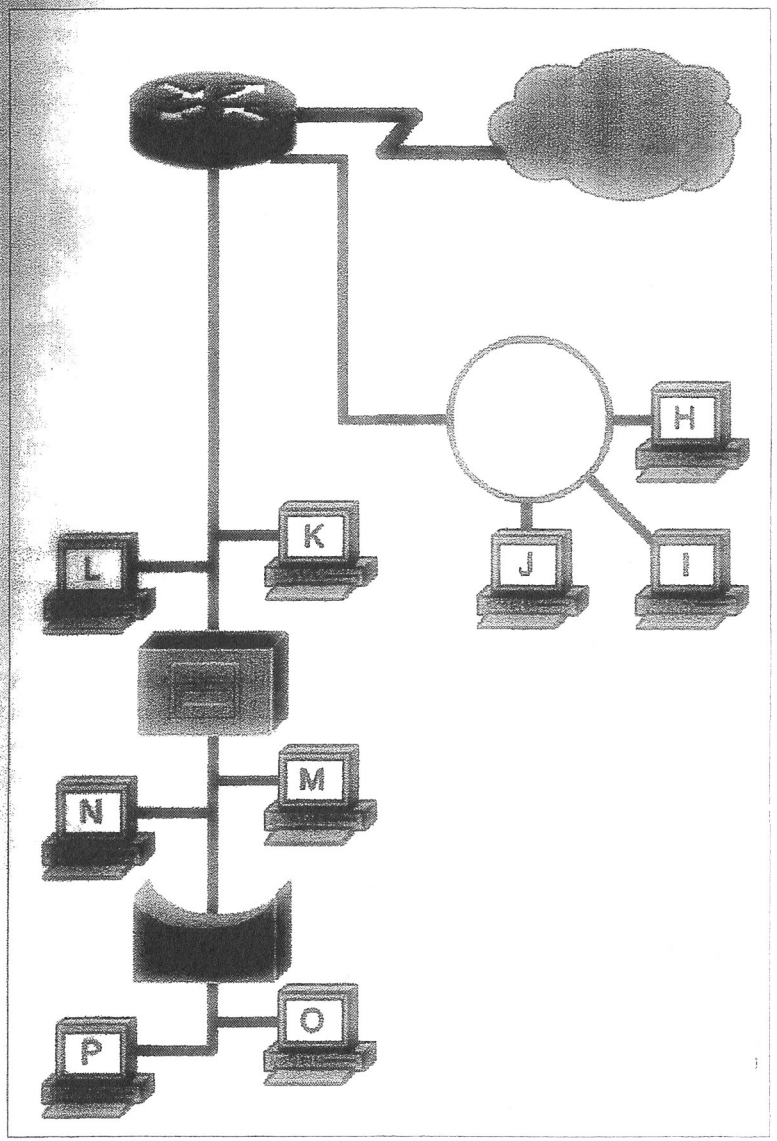
Centraal in het ontwerp staat zoals gezegd de functionaliteit, wat zijn weerslag vindt in de benodigde applicaties. Uit de eisen van de opdrachtgever en de interviews die met toekomstige gebruikers worden gehouden, én uit de professionaliteit van de ontwerper, volgt een voorstel voor de software die later op het netwerk wordt aangeboden.

Het is gebruikelijk om deze zaken in een tabel te verwerken. Met zo'n tabel kan namelijk eenvoudig (ook later) worden gecontroleerd of het netwerk aan de vereisten voldoet. Het aanbieden van de functionaliteit heeft datastromen tot gevolg. Deze moeten in kaart gebracht worden. Daarbij moet niet alleen naar het gemiddelde dataverkeer worden gekeken, maar ook naar de piekbelasting. Vrijwel elk netwerk is in staat de gemiddelde datastroom van een dag te verwerken. Cruciaal is echter de vraag of dit ook lukt als iedereen om acht uur binnenkomt en zijn of haar computer aanzet, of dat er voldoende tijd is om die voorgenomen backup van de server te maken in de tijd die daarvoor gereserveerd is.

De kopjes boven de kolommen in onderstaande tabel dienen als voorbeeld. Per programma zal waarschijnlijk een aantal (andere) eisen aan het toekomstige netwerk worden gesteld en het netwerk moet niet aan het gemiddelde voldoen, maar aan het maximum.

Applicatie	Benodigde bandbreedte	System resources server	System resources werkstation	Eisen database-server
Programma 1				
Programma 2				
Programma 3				

Bij een FNO moet ook rekening gehouden worden met de al aanwezige infrastructuur en de aanwezige apparatuur. Verder is van belang welke mogelijkheden het gebouw heeft. Een **plattegrond** van de toekomstige infrastructuur is noodzakelijk, evenals een inschatting van eventueel extra ruimtebeslag (server en de rest van de infrastructuur). Soms wordt geen **conceptdiagram**. In het latere ontwerp komt dan pas de plattegrond. In een conceptdiagram wordt het netwerk als logische structuur getekend; zie figuur 3.4.



Figuur 3.4 Conceptdiagram.

Voor het tekenen van dit soort diagrammen worden over het algemeen de symbolen gekozen die fabrikant van netwerkapparatuur Cisco gebruikt.

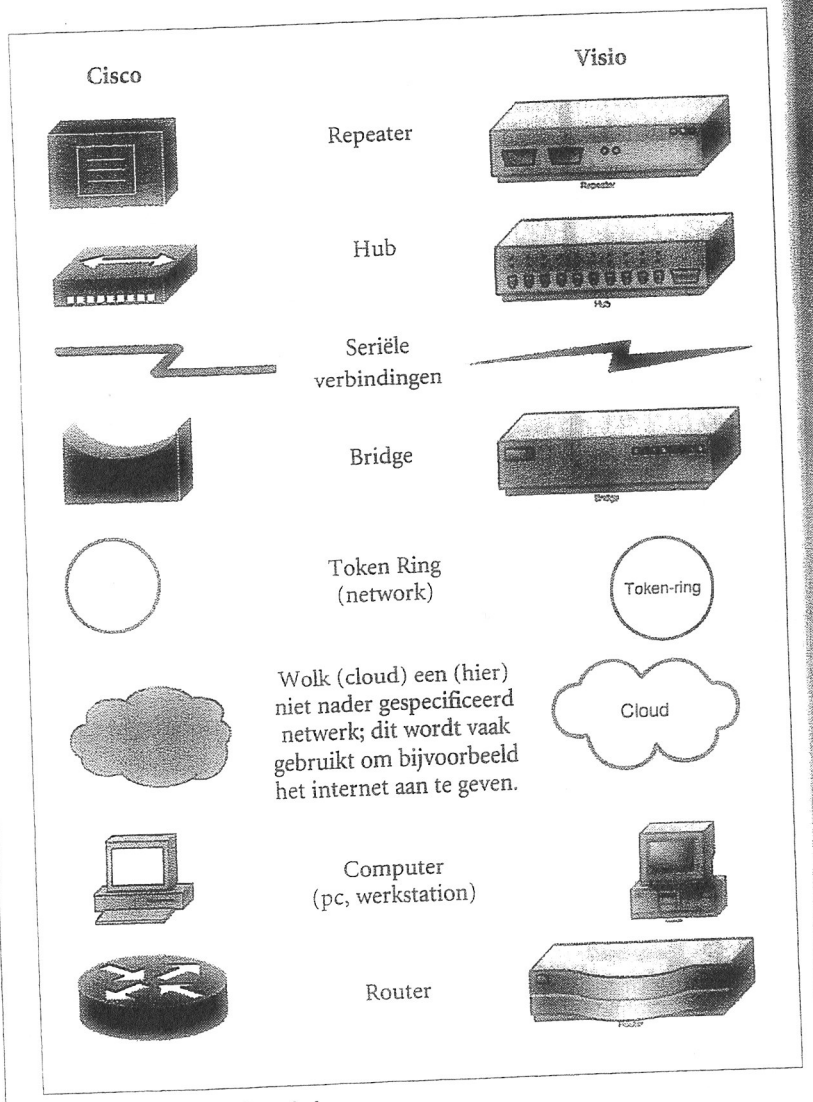
Index

Cisco-symbolen
Visio
netwerksymbolen
DIA

Knipsel

Buiten het pakket Visio is ook het tekenpakket **DIA** heel bruikbaar. Bijkomend voordeel is dat het freeware (of eigenlijk GPL) is.

Dit is echter geen bindend voorschrift. In onderstaande figuur zijn zowel de meest gebruikte **Cisco-symbolen** gegeven als die van het populaire tekenpakket **Visio** van Microsoft, dat vaak wordt gebruikt om netwerken te tekenen.



Figuur 3.5 Netwerksymbolen.

Let bij dit deel van het ontwerp ook op de haalbaarheid. Je kunt niet overal zomaar kabels gaan leggen. Je moet steeds voor ogen houden dat het conceptdiagram later wel in het pand (of de panden) gerealiseerd moet kunnen worden. Ook zou je niet de eerste zijn die een internetverbinding in een plan opneemt die op de locatie van je opdrachtgever niet leverbaar is.

Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER-PROCES
[illegible] gewenste [illegible] van het netwerk.	
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

Een FNO is een blauwdruk van het toekomstige netwerk, waarbij met een beperkte groei (10%?) rekening gehouden moet worden. Een FNO van een netwerk dat exact de huidige bedrijfsprocessen qua omvang en grootte afdekt, kan nooit goed zijn. Mogelijk kost het wel € 200.000 om één station bij te plaatsen omdat de infrastructuur precies 'vol' is. Deze zaken zijn natuurlijk sterk afhankelijk van de situatie. Als je bij een snelgroeiend bedrijf een netwerk ontwerpt, houd je misschien wel rekening met meer dan 10% groei. Vaak zijn percentages van 20 tot 40% geen uitzondering.

Aparte aandacht voor het **beheer** is om eenzelfde reden van belang. Een spotgoedkoop netwerk dat vervolgens niet te beheren is, is niet echt in het belang van je opdrachtgever.

Kort samengevat kun je stellen dat een FNO 'goed' is als:

- de opdrachtgever zich op basis van het rapport een voorstelling kan maken van de toekomstige ICT-omgeving en zijn 'plan van eisen' daarin herkent. Hij moet daar een blauwdruk van zijn toekomstige netwerk in kunnen lezen.
- een technisch ontwerper een netwerk kan ontwerpen dat (exact) voldoet aan de specificaties van het FNO.

in die fase doet.

3. Noem drie activiteiten die bij de laatste fase van de watervalmethode horen.

4. Omschrijf in maximaal drie zinnen wat een functioneel netwerkontwerp is.

5. Wat is outsourcen?

6. Wat is hosten?

7. Waarom staan er in een FNO geen technische details?

3.8.2 Meerkeuzevragen

1. Lees onderstaande stelling goed door en beantwoord dan de vraag:
   Implementeren van het netwerk hoort niet bij het ontwerpen.
   a. De stelling is juist.
   b. De stelling is onjuist.
   c. Hier is geen uitspraak over te doen.

2. Lees onderstaande stelling goed door en beantwoord dan de vraag:
   Communicatie volgt na implementatie.
   a. De stelling is juist.
   b. De stelling is onjuist.
   c. Hier is geen uitspraak over te doen.

3. Lees onderstaande stelling goed door en beantwoord dan de vraag:
   Systeemtests worden altijd pas na implementatie uitgevoerd.
   a. De stelling is juist.
   b. De stelling is onjuist.
   c. Hier is geen uitspraak over te doen.

a. De stelling is juist.
b. De stelling is onjuist.
c. Hier is geen uitspraak over te doen.

6. Lees onderstaande stelling goed door en beantwoord dan de vraag:
   Netwerkontwerp kan het best in fase 3 van de watervalmethode gestart worden.
   a. De stelling is juist.
   b. De stelling is onjuist.
   c. Hier is geen uitspraak over te doen.

7. Lees onderstaande stelling goed door en beantwoord dan de vraag:
   In een functioneel netwerkontwerp worden de technische specificaties van de gebruikte apparatuur en het typenummer nog niet benoemd.
   a. De stelling is juist.
   b. De stelling is onjuist.
   c. Hier is geen uitspraak over te doen.

8. Lees onderstaande stelling goed door en beantwoord dan de vraag:
   Een functioneel ontwerp volgt op een technisch ontwerp waarin de gebruikte technieken zijn vastgelegd.
   a. De stelling is juist.
   b. De stelling is onjuist.
   c. Hier is geen uitspraak over te doen.

9. Lees onderstaande stelling goed door en beantwoord dan de vraag:
   In een FNO mag geen techniek worden genoemd. De opdrachtgever moet het immers kunnen lezen.
   a. De stelling is juist.
   b. De stelling is onjuist.
   c. Hier is geen uitspraak over te doen.

10. Lees onderstaande stelling goed door en beantwoord dan de vraag:
    Een conceptdiagram is handig om in een FNO op te nemen.
    a. De stelling is juist.
    b. De stelling is onjuist.
    c. Hier is geen uitspraak over te doen.

3.8.3 Opdrachten

1. Vul voor het netwerk van je eigen opleiding een BE-matrix in. Licht je keuzes toe.

2. Neem als voorbeeld je laatste stagebedrijf en pas de eerste twee fasen van de watervalmethode toe om een netwerk te ontwerpen.

3. Je bent benaderd door een bedrijf in oprichting dat zich bezig wil gaan houden met kennismanagementsystemen. Het idee is dat dit bedrijf een inventarisatie maakt van alle (vele) op de markt verkrijgbare systemen en dat andere bedrijven op basis hiervan een goed advies krijgen wat ze zouden kunnen aanschaffen. Formuleer de 'business requirements' voor dit bedrijf.

4. Teken figuur 3.4 nogmaals, maar nu met gebruik van Visio-symbolen.

Inleiding technisch ontwerp

Doorreizen

Als je de praktijkopdracht in paragraaf 3 van dit hoofdstuk naar tevredenheid hebt gemaakt, kun je na overleg met je docent doorgaan naar het volgende hoofdstuk.

Inleiding technisch ontwerp

4.1 Inleiding

In het vorige hoofdstuk hebben we gekeken naar de functionele eisen die aan netwerken worden gesteld en de consequenties die deze kunnen hebben voor het ontwerp. Vanuit business requirements wordt een ontwerp gemaakt dat voor de klant bruikbaar is. In dit stadium gaan we nader in op de keuze van de apparatuur en enkele bijkomende aspecten, die zeker niet minder belangrijk zijn. Deze fase kun je zien als de start van het technisch ontwerp van het netwerk.

4.2 Aanwijzingen voor de leerling

Een ontwerp is in vele stappen onder te verdelen. We noemen een indeling in verschillende (opeenvolgende) stappen of fasen een fasering. Jammer genoeg is ook de fasering zelf vaak onderwerp van discussie. Er zijn verschillende wijzen waarop een ontwikkeltraject gefaseerd kan worden. In paragraaf 3.5 is de watervalmethode besproken. Bij de hier gebruikte fasering komen de volgende aspecten aan de orde:

- infrastructuur:
  - bekabeling etc.
  - netwerk en computerkenmerken
  - actieve netwerkcomponenten
- hardware:
  - printerkeuze
  - computer(kenmerken)
  - randapparatuur
  - overige apparatuur
- software:
  - standaardsoftware
  - maatwerksoftware
- overige:
  - beveiliging
  - performance en reliability
  - overige
- financiën:
  - TCO, ROI en afschrijven
  - de 10% regel
- logistiek:
- het inrichtingsplan

4.3 Praktijkopdracht

Je werkt bij een bedrijf dat complete netwerken ontwerpt en installeert. De laatste tijd gaan er regelmatig orders aan jullie neus voorbij. Daarom krijgt een extern bureau het verzoek om afgehaakte klanten te inter-

viewen. Veel van deze klanten melden dat ze ontevreden zijn over de kwaliteit van het ontwerp. Ze hebben niet het idee dat het ontwerp speciaal voor hen is gemaakt. De indruk bestaat dat er een soort 'generiek ontwerp' uit de kast is gehaald waar de naam van het bedrijf voor de vorm boven is getikt.

Jou is gevraagd een checklist te ontwerpen die gebruikt kan worden om een netwerkontwerp te screenen en te beoordelen. De bedoeling is dat op deze wijze de ontwerpen weer van een niveau worden dat er geen klanten meer vertrekken.

4.4 Keuzes in het technisch ontwerp

Bij het opzetten van een **functioneel ontwerp** moeten enkele technische keuzes gemaakt worden, die – omdat ze rechtstreeks uit de gewenste functionaliteit volgen – in het FNO uitgewerkt moeten worden.

Een voorbeeld is de keuze van de **bekabeling**: daarvan moeten aspecten als kabeltype en topologie vastgelegd worden. Dit in relatie tot het gebouw waar het netwerk gerealiseerd moet worden. Vanwege fysieke beperkingen kan niet in elk gebouw een wireless LAN gerealiseerd worden. Het lijkt misschien alsof tegenwoordig elk netwerk een cat 5 UTP-bekabeling heeft en als protocol TCP/IP gebruikt. Bij een ontwerp hoort een zorgvuldige afweging of dit wel de verstandigste en juiste keuze is. Veel problemen met bijvoorbeeld de prestaties van een netwerk worden veroorzaakt doordat vaak maar 'voor een UTP Ethernet-netwerk met TCP/IP' wordt gekozen zonder dat een goede afweging is gemaakt. In sommige gevallen kan het ontbreken van een gegarandeerde Quality of Service er de oorzaak van zijn dat de prestaties van zo'n netwerk onvoldoende zijn. Een Token Ring netwerk (dat wel een maximale responstijd kan garanderen) kan dan een betere keuze zijn.

Met betrekking tot de **bandbreedte** wordt vaak een even snelle en ondoordachte keuze gemaakt. "Laten we maar 100 Mb doen." Dit kan grote problemen veroorzaken, omdat als gevolg van het CSMA/CD-principe, één verbinding de bandbreedte kan monopoliseren. De gevolgen hiervan kunnen op de langere duur funest zijn.

Gekoppeld aan deze keuze van protocollen, topologie en bandbreedte is die van de bekabeling, die we hierboven al even genoemd hebben. Deze betreft zowel het type bekabeling als een onderzoek naar de fysieke moge-

type? Kunnen we beter glasvezel gebruiken? Of misschien nog iets anders? Kunnen er kabelgoten gebruikt worden? Is er een handig systeemplafond waarachter kabels weggewerkt kunnen worden? Vaak zijn er allerlei beperkingen waarmee rekening gehouden moet worden. In een pand dat op de monumentenlijst staat, kunnen niet zomaar overal doorgangen gemaakt worden. Ook bij niet al te grote netwerken is het vaak verstandig om een centrale plaats te kiezen als centrum voor het netwerk, daar een 19 inch kast neer te zetten en daar ook alle kabels te concentreren.

Ook worden netwerken soms aangelegd op plaatsen met een verhoogde kans op storingen. Dan moet er voor een ander bekabelingstype of voor extra afgeschermde kabels worden gekozen. Netwerken worden nu eenmaal ook aangelegd op plaatsen waar extreme omstandigheden heersen: in een chemische fabriek worden bijvoorbeeld ook computers gebruikt. Er is apparatuur op de markt die daarop speciaal is voorbereid. Daarmee moet in een ontwerp rekening gehouden worden.

De keuze voor een bekabelingstype kan tegenwoordig ook een keuze voor een draadloos netwerk zijn (wifi). Bedenk wel dat zich daarmee dan weer dezelfde problemen kunnen voordoen. Ook draadloos verkeer kan onder bepaalde omstandigheden verstoord worden. In sommige kantoorpanden zijn bijvoorbeeld de systeemwanden van metaal. Voor het toepassen van een draadloos netwerk moet in dat geval gerekend worden op één Service Access Point (SAP) per ruimte. Dat maakt het netwerk duur, maar erger is dat daar weer veel kabels voor nodig zijn, en dat was juist het probleem! Ook kan de ontvangst sterk verstoord worden door elektromagnetische straling uit een andere bron. Bepaalde elektrische apparaten produceren een grote hoeveelheid straling.

Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER-PROCES
De benodigde en gewenste architectuur van het netwerk.	
[illegible] die nodig is om de [illegible] functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

Index

server
RAID
beschikbaarheid
fault recovery
opslagcapaciteit
werkstation
apparatuur

Assist

Bij RAID (Redundant Array of Inexpensive Disks) wordt de data over meerdere schijven verdeeld. Dit gaat op een manier waarbij het meestal mogelijk is om, als een van de schijven het begeeft, de data 'on the fly' te herstellen.

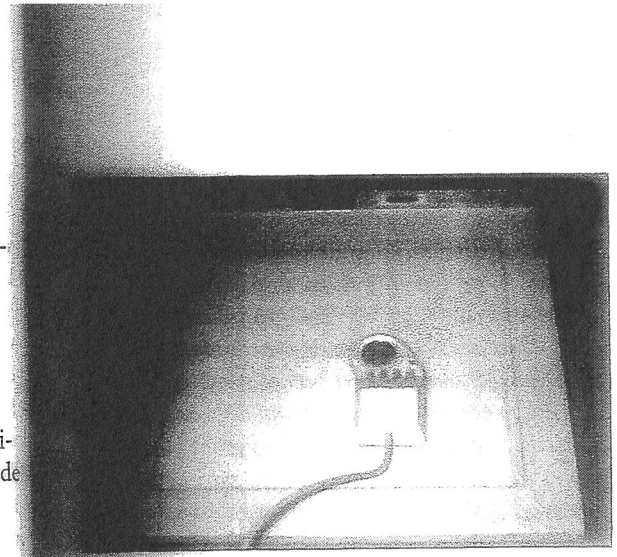
4.4.1 Servers

Voor een netwerk van pc-achtige machines moeten meerdere typen computers geselecteerd worden. Voor elke **server** moet zorgvuldig worden afgewogen aan welke kenmerken deze moet voldoen. Specificaties van high-end servers zijn fors en het zijn dure systemen. Systemen met 265 GB intern geheugen, schijfeenheden in de Terabytes en twee of vier processors zijn niet ongebruikelijk. Deze schijfsystemen zijn dan bijna altijd van het type **RAID**. De juiste keuzes qua benodigde snelheid, functionaliteit en betrouwbaarheid dragen bij tot een netwerk dat een voordeel op de concurrentie oplevert. Een beter toegesneden netwerk zal voor een efficiëntere uitvoering van de primaire processen van de klant zorgen.

Bij dergelijke systemen is aan elk onderdeel aandacht besteed om de **beschikbaarheid** ('availability') te maximaliseren. Het geheugen is van een error correction type, de voeding is zowel overgedimensioneerd als dubbel uitgevoerd. In de keuze van dit systeem is meegenomen welke operationele eisen er worden gesteld. Ongetwijfeld zal in een netwerk van een beetje afmeting een vorm van netwerkmanagement worden geïmplementeerd (SNMP-1, 2, 3 of nog een ander protocol). Ook dient aandacht aan **fault recovery** (op serverniveau) besteed te worden. Kiest men voor duplexing, mirroring, een RAID-oplossing of zelfs een combinatie met file server duplexing? Ook over de **opslagcapaciteit** (nu en in de toekomst) van het serverpark moet nagedacht worden. Hoe lang kan de aanbevolen configuratie nog mee en wanneer is er naar verwachting een (hardwarematige) upgrade nodig? Als dat binnen twee maanden is, dan lijkt er sprake van een ontwerpfout. Een serieuze analyse van de databehoefte is een absolute noodzaak.

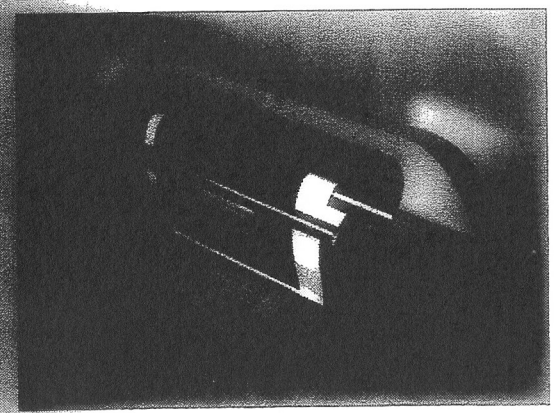
4.4.2 Werkstations

Naast een of meer servers heeft een netwerk ook gebruikersstations. In de meeste netwerken kan niet met één keuze voor een **werkstation** volstaan worden; dit is sterk afhankelijk van de situatie. Een call centre met 300 werkstations zal een hoge mate van standaardisatie wensen. Daar is misschien alleen een apart station voor de beheerder en een aparte configuratie voor de administratieve stations nodig. Bij een ingenieursbureau zal veel minder standaardisatie in hardware, software en configuratie noodzakelijk of gewenst zijn. In een studie naar benodigde **apparatuur** hoort een onderzoek naar extra eisen en wensen ten aanzien van die apparatuur.



Figuur 4.1 Digitizer.

CAD-ontwerpers gebruiken bijvoorbeeld vaak zeer specialistische apparatuur (zoals high tech scanners, A0-plotters en digitizers). Ondersteuning voor dit soort apparatuur is een vereiste in een netwerk dat voor dergelijke klanten wordt ontworpen. Vaak vindt een klant het heel vanzelfsprekend dat bekend is dat men bepaalde apparatuur heeft en wil blijven gebruiken, terwijl de netwerkleverancier daar pas later achter komt. Als daar in het ontwerp geen rekening mee gehouden is, kan dit ertoe leiden dat deze apparatuur niet gebruikt kan worden (omdat bijvoorbeeld de hardware-ondersteuning niet te realiseren is, of de drivers incompatible zijn met het gekozen operating system op de desktop). Een zorgvuldige inventarisatie en analyse van de benodigde apparatuur, zowel de al aanwezige als de nieuw aan te schaffen, is dus een vereiste voordat keuzes gemaakt kunnen worden.



Figuur 4.2 A0-plotter.

Index

topologie
functioneel netwerkontwerp
structuur van het netwerk

4.5 Topologie en structuur

Het netwerk omvat behalve bekabeling en computers ook andere apparatuur. Daarin onderscheiden we zowel passieve als actieve apparatuur. Voor de hand liggen routers, switches en hubs. In het **functioneel netwerkontwerp** worden de specificaties daarvan vastgelegd. De **structuur van het netwerk** is essentieel voor de prestaties van het geheel. Het netwerk moet een logische structuur hebben en er moet nagedacht zijn over de datastromen. Een juiste dimensionering van de apparatuur is van groot belang.

Vaak kan een netwerk met een uitgekiend logisch ontwerp tot veel grotere prestaties worden gebracht dan oorspronkelijk verwacht. We moeten dan denken aan zaken als beschikbare bandbreedte, de verdeling ervan en het opdelen in segmenten. De netwerkleveranciers die denken dat je een netwerk alleen sneller kunt maken door van 100 Mb naar 1000 Mb over te stappen, leveren niet altijd 'value for money'.

In deze fase van het ontwerp is het ook goed om nogmaals naar de eventuele inherente (on)betrouwbaarheid van het ontwerp te kijken. Dit moet eigenlijk al in het functioneel netwerkontwerp aan de orde zijn geweest, maar in dit stadium zijn er regelmatig nog makkelijk te vermijden 'single points of failures' in het netwerk aan te wijzen. Vaak is met een eenvoudige ingreep een stabieler netwerk te creëren, bijvoorbeeld door een verbinding redundant uit te voeren of een centraal knooppunt twee keer te realiseren en op deze wijze voor een fall-back te zorgen (qua verbinding).

Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER-PROCES
De benodigde en gewenste architectuur van het netwerk.	
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

4.6 Printers

In ieder netwerkontwerp vormen één of meer **printers** uiteraard een verplicht onderdeel. Er bestaan netwerken die alleen zijn aangelegd om printers te delen! De aanschaf en installatie van allemaal stand-alone printers op even zovele computers is meestal veel duurder en inefficiënter dan enkele grote bulkprinters en eventueel nog een handvol special purpose printers.

Met printers kan echter ook veel misgaan; vaak wordt er een verkeerde inschatting van de situatie gemaakt. Vraag aan een manager van een bedrijf waar een netwerk geïmplementeerd gaat worden, om aan te geven hoeveel afdrukken hij denkt te gaan maken. De kans is dan groot dat hij zijn antwoord baseert op de bestaande situatie. Dat lijkt vrij logisch, maar de praktijk wijst uit dat een netwerk ook zijn eigen printbehoefte schept. Het is een lastige zaak om in te schatten:

- Hoeveel afdrukken worden er nu gemaakt?
- Hoeveel afdrukken worden er straks (direct na implementatie) gemaakt?
- Hoeveel afdrukken worden er over drie jaar gemaakt?
- Hoeveel printers zijn er nodig en hoe moeten die verdeeld worden over het netwerk?
- Is er een inschatting gemaakt van minimale, maximale en gemiddelde wachttijd op een afdruk?
- Is de hoeveelheid (extra) dataverkeer die printen oplevert in de dimensionering, qua hoeveelheid en qua tijdigheid, meegenomen? (Printen genereert erg veel data; veelal wordt alles grafisch, als bitmap, naar de netwerkprinter gestuurd.)
- Welke eisen moeten er aan de printer(s) worden gesteld?
  - afdruksnelheid;
  - kleur of zwart/wit (inkjet of laser);
  - resolutie;
  - kosten per pagina;
  - etc.

Tegenwoordig kan vaak voor een combinatie van een fotokopieermachine en een printer worden gekozen. Deze apparaten fungeren dan als (snelle) printer en met deze keuze wordt één apparaat uitgespaard. Alle grote kopieermachineleveranciers voorzien in de optie hun kopieermachine als netwerkprinter aan te sluiten.

In

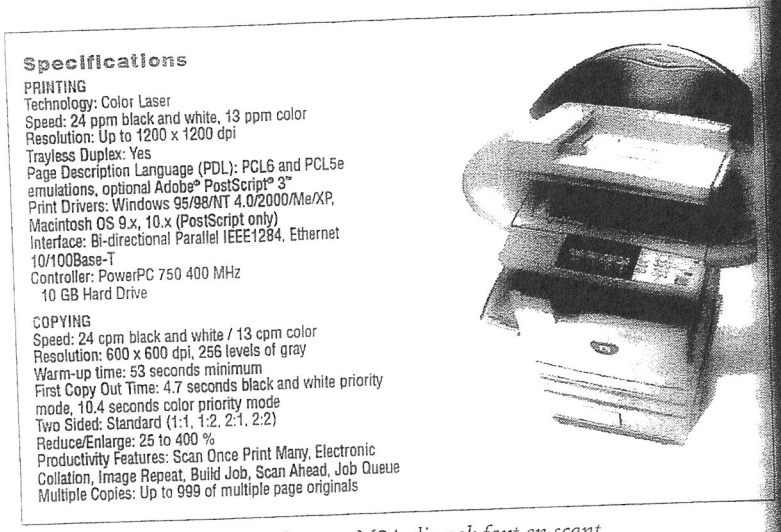
printers

As

Denk bij sp
ters aan bij
(bulk)kleur
bepaalde n
ciënt te kur
een enkele
printer. Ook
Printing On
vanuit een
kopieerapp
werk wordt

Index

beveiliging
externe beveiliging
interne beveiliging
hackers
crackers
firewall



Figuur 4.3 De Xerox workcentre M24, die ook faxt en scant.

Op basis van onderzoek kan uiteindelijk een keuze voor een of meer typen printers worden gemaakt en deze kan in het netwerkontwerp verder uitgewerkt worden.

4.7 Beveiliging

Het begrip **beveiliging** van een netwerk kent verschillende invalshoeken:

- **Externe beveiliging:** wie of wat zal het netwerk van buitenaf bedreigen?
- **Interne beveiliging:** welke gebruikers mogen wat (niet)? Maar ook: hoe ga je om met onbetrouwbaar of vertrekkend personeel?

4.7.1 Externe beveiliging

Netwerken worden bedreigd door **hackers** en **crackers**. Vaak geldt als onderscheid tussen deze twee groepen dat hackers als doel hebben de onveiligheid van een netwerk aan te tonen, terwijl crackers kwade bedoelingen hebben. Beide categorieën zijn echter vanuit het oogpunt van netwerkbeheer ongewenst. Als er een continue internetverbinding is, loopt een bedrijf veel risico.

...buitenaf een **firewall** in het net-

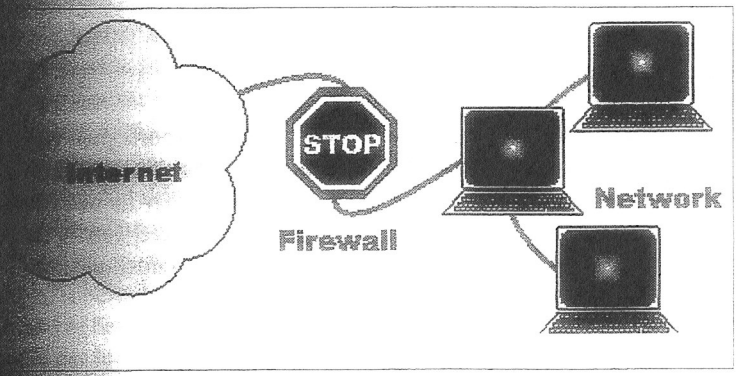
...seerde systemen die veel configuratie-opties hebben. Er zijn drie basic ...all-systemen:

...**filtering** – Pakketten (IP en TCP) worden op basis van een set ...('rules') gefilterd.

...*walls op applicatieniveau* – Deze kunnen bijvoorbeeld FTP of HTTP ...ren of filteren.

...service – Informatie wordt door de firewall van het internet ...d en dan door de proxy naar de client gezonden. Voor de buiten- ...lijkt het alsof alle verkeer van en naar de proxy komt/gaat. De ...-systemen lijken voor de buitenwereld niet te bestaan.

...ruikt zijn **iptables** en **ipchains**. Beide zijn open source software en ...ect geschikt om op een Linux machine te draaien.



...4.4 *Firewall.*

...lijkheden van firewalls

...kunnen gemaakt worden op basis van:

...-adressen

...meinnamen

...otocollen

...rts

...cifieke tekst

...rotocollen, ports en specifieke tekst geven we hieronder nadere ...atie.

...ollen

...gende **protocollen** zijn de meest gebruikte (en meest gefilterde): ...nternet Protocol): het belangrijkste onderliggende protocol;

In

packet filte
proxy serv
iptables
ipchains
filter
protocolle
IP
TCP

K

Een proxy
rechtssyst
iemand ar
van...) op

- UDP (User Datagram Protocol);
- HTTP (Hyper Text Transfer Protocol);
- FTP (File Transfer Protocol);
- ICMP (Internet Control Message Protocol): onder andere gebruikt om informatie tussen routers uit te wisselen;
- SMTP (Simple Mail Transport Protocol): gebruikt om e-mail tussen hosts uit te wisselen;
- SNMP (Simple Network Management Protocol): gebruikt om systeem-informatie van gebruikte apparatuur te verzamelen;
- **Telnet**: om in te kunnen loggen op (remote) systemen.

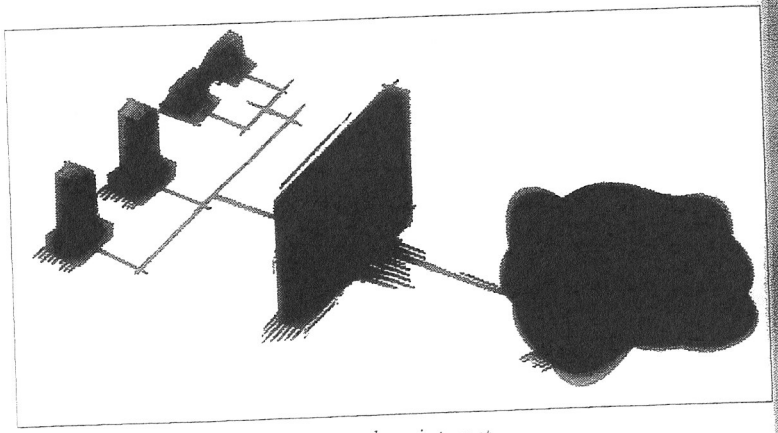
Ports

Elke machine stelt via genummerde **poorten** zijn services beschikbaar op het internet, één voor elke service:

- De **webserver** (HTTP) zit meestal op poort 80.
- De **FTP-server** zit op poort 21.

Specifieke tekst

De firewall zal door elk pakket heen zoeken naar het voorkomen van bepaalde tekst. Je kunt een firewall 'vertellen' dat elk pakket met de term "X-rated" geblokkeerd moet worden. Het "X-rated"-filter zal niet reageren op "X rated" (zonder koppelteken). Maar je kunt dan weer een "X rated"-filter toevoegen. Virusscanners gebruiken meestal deze methode om 'virushandtekeningen' te 'zoeken'.



Figuur 4.5 Scheiding tussen netwerk en internet.

Er zijn ook firewalls die je op een enkele pc kunt gebruiken. In een net-

...ling op werkstations kan door gebruikers vaak gewoon uitgezet ...n (en dat doen veel mensen ook omdat het als 'lastig' of vertragend ...ervaren).

...eigingen

...irewall beschermt dus tegen bedreigingen van buitenaf. Wat zijn nu ...terne bedreigingen waartegen beveiligd moet worden? Hackers en ...kers maken gebruik van een aantal methoden om de integriteit van ...netwerk of systeem te ondermijnen. Niet tegen alle methoden kan een ...wall bescherming bieden, maar tegen een aantal wel:

- **Remote login:** een poging om vanaf een ander station in te loggen en het beheer van een server over te nemen.
- **Application backdoors:** sommige programma's hebben een functionaliteit die remote access mogelijk maakt.
- **SMTP session hijacking:** SMTP is een bron van mogelijke bedreigingen. Buiten wat foutjes in oudere versies, die toegang tot het root account mogelijk maakten, is er ook bij slecht geconfigureerde mail-servers een risico dat deze gebruikt kunnen worden om junkmail (spam) naar duizenden gebruikers te sturen.
- **Operating system bugs:** net als applicaties hebben sommige operating systems zogenoemde 'backdoors' met onvoldoende security, of zijn er bugs. De beruchte **ping of death** is hiervan een voorbeeld.
- **Denial of Service (DoS):** een dergelijke aanval belast een server zo met 'werk' dat hij aan zijn eigen werk niet meer toekomt. Een veelgebruikte methode is om een verbinding maar half te openen. (De three way handshake wordt niet afgemaakt.) Door dit vele malen te doen 'loopt de server uit zijn resources' en is deze praktisch onbenaderbaar.
- **Distributed Denial of Service (DDoS):** deze variant op de voorgaande zorgt er eerst voor dat er op veel plaatsen agents zijn die meedoen aan Denial of Service. Op deze wijze kan via relatief trage verbindingen toch een succesvolle aanval worden opgezet.
- **E-mailbommen:** een **e-mailbom** is meestal een aanval op een persoon, maar deze kan ook tegen een organisatie worden ingezet. (E-mail)virus-golven beginnen het karakter van een e-mailbom te krijgen. Bij recente uitbraken verspreidde een virus zich soms zo snel dat SMTP-servers onder het verkeer bezweken.
- **Macro's:** gezien de vele **macrovirussen** die de Office-suite van Microsoft de afgelopen jaren heeft 'gegenereerd' is het niet nodig hier nader op in te gaan. Een firewall kan hiertegen soms iets ondernemen.
- **Virussen:** een aantal firewall-producten is in staat om dataverkeer op

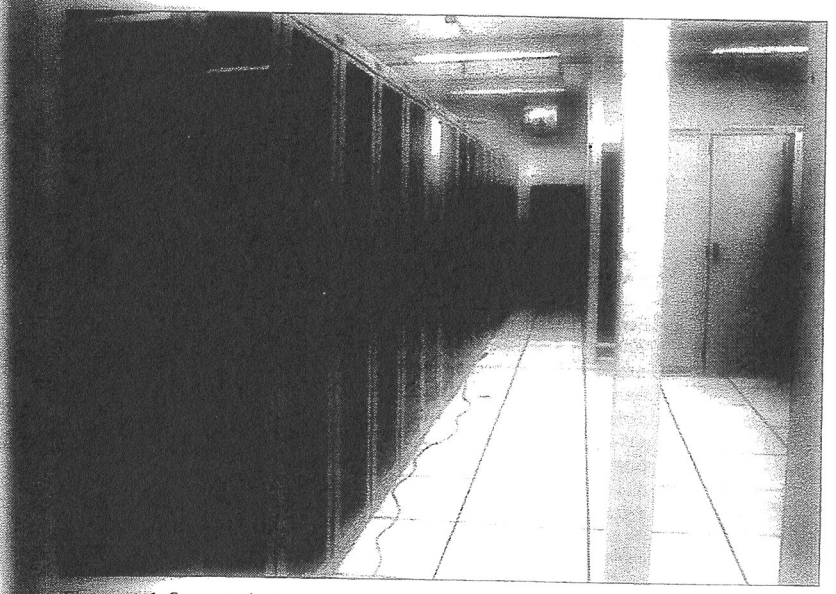
- **Spam**: op basis van verzendadres of andere specifieke eigenschappen kan een firewall e-mailverkeer filteren. Op deze manier is **spam** tegen te gaan.
- **Redirect bombs**: ICMP kan gebruikt worden om informatie over de te volgen route te wijzigen ('redirect'). Dit is een van de manieren waarop een DoS-attack is te arrangeren.
- **Source routing**: in de meeste gevallen wordt de route van TCP/IP-verkeer bepaald door de ontvangende host. De makkelijkste en/of snelste weg om die te bereiken, wordt gekozen. Bij **source routing** wordt de route echter door het verzendende station bepaald. Op deze wijze kan voor een bepaald type verkeer een route worden afgedwongen. Uit veiligheidsoverwegingen kan dit soms de voorkeur hebben. Op deze wijze kan bijvoorbeeld ook een hacker zijn verkeer zo maskeren dat het lijkt alsof het ergens anders vandaan komt. Firewalls zetten source routing meestal standaard uit.

Sommige van de genoemde bedreigingen zijn door een firewall niet of nauwelijks te onderscheppen. Bepaalde firewalls zijn in staat een aantal virussen tegen te houden, maar het blijft verstandig om ook virusscanners te gebruiken. Spam is vervelend, maar de enige manier om er echt van af te komen is geen e-mail meer toe te staan. Maar dat wil vrijwel niemand. Overigens wordt met **heuristic scanning** de laatste tijd een redelijk resultaat bereikt. De graad van beveiliging die je kunt bereiken, is altijd een afweging tussen de functionaliteit en de veiligheid. Een perfect veilig netwerk laat geen enkel verkeer door.

De meest gebruikte strategie bij het bouwen van een firewall is om in eerste instantie alles te blokkeren, en vervolgens stapje voor stapje open te zetten wat je wel wilt.

4.7.2 Interne beveiliging

Ook aan de interne veiligheid moet aandacht worden geschonken: aan het onderscheid in verschillende gebruikersgroepen en daaraan gekoppelde rechten. Wie kan en mag wat op welke plaats? In een Windows omgeving kan met 'policies' worden gewerkt. Ook met Novell NetWare als serverplatform kan een standaard policy worden ingesteld en kan desgewenst met een 'roaming profile' worden gewerkt. Dit geheel wordt in een **netwerkautorisatieplan** gedocumenteerd en vastgelegd. Dit maakt deel uit van de systeemdocumentatie.



Figuur 4.6 Serverruimte.

Vaak gaan organisaties ervan uit dat bedreigingen van buitenaf komen, maar lang niet altijd is dat het geval. In de praktijk blijken veel netwerkaanvallen een oorzaak en oorsprong binnen de organisatie te hebben. Het gebruik van een firewall om intern verkeer te regelen is vaak geen overbodige luxe. Ook een fysieke beveiliging tegen interne bedreigingen is een goed idee. Denk hierbij aan de volgende maatregelen:

- Serverruimten moeten alleen voor bevoegd personeel toegankelijk zijn.
- Kabels moeten weggewerkt zijn.
- Het dataverkeer moet ook binnen het netwerk versleuteld worden; geen onversleutelde (draadloze) verbinding die afgeluisterd kan worden.
- Niemand moet meer rechten krijgen dan nodig of functioneel is.
- Er moet sprake zijn van een goed **wachtwoordbeleid**. Bij vertrek van een werknemer moeten zeker de cruciale wachtwoorden worden gewijzigd. Dit geldt ook (juist) als iemand zonder ruzie of meningsverschillen weggaat.


BusinessWeek online

DAILY BRIEFING

DECEMBER 13, 2000

NEWS ANALYSIS

When the Hacker Is on the Inside

Thousands of attacks each year come from current or former employees -- and companies are only now beginning to step up their defenses

For Elite Web Hosting in Orlando, Fla., September, 2000, was a nightmare. A disgruntled former employee allegedly hacked into the company's computer system without authorization. He then allegedly sent e-mails that contained vulgar language and implying that Elite was moving into the Web porn business to every Elite customer. The missives further claimed that the company's majority owner, Augustino Mireles, had been raiding Elite's coffers for personal use.

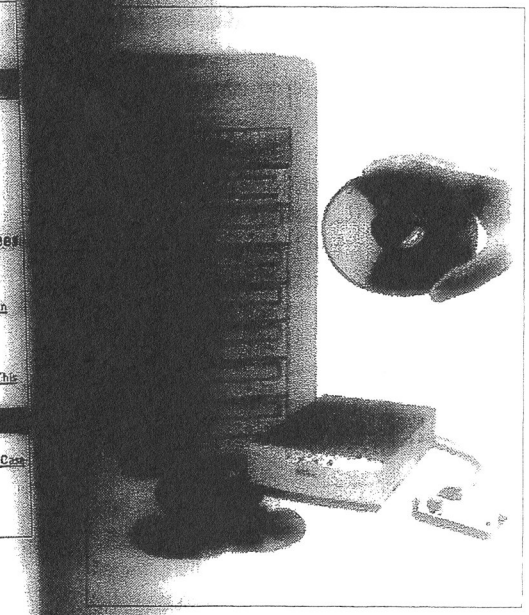
Printer-Friendly Version
E-Mail This Story
Find More Stories Like This

TODAY'S HEADLINES

Bush in Iraq: A B-School Case Study
The Many Shapes of Tomorrow's PC

Sectors
Economy & Bonds
Investing Glossary
Newsletter Sign-Up

Figuur 4.7 Een artikel uit BusinessWeek.



Figuur 4.8 Cd-romserver.

4.8 Overige randapparatuur

Allerlei andere apparatuur kan nog nodig zijn. Een paar voorbeelden:

- *Modems.* Sommige leveranciers hebben nog steeds voor supportdoeleinden een **bulletin board system**. Om dit te bereiken is een **modem** nodig. Modems kunnen centraal via een modem- of communicatieserver aan de gebruikers ter beschikking gesteld worden.
- *Fax-apparaten* zijn vaak op het netwerk aan te sluiten. Dan kan er gefaxt worden en kunnen binnenkomende faxberichten via het netwerk verspreid worden.
- *Fotokopieermachines* zijn vaak als printer in een (groot) netwerk opgenomen.
- *Specialistische apparatuur.* Bij bepaalde bedrijven is specialistische apparatuur in gebruik. Dat kan gaan om speciale afdrukapparatuur bij grafische bedrijven, maar ook om bijvoorbeeld apparatuur waarop vanuit een printontwerpprogramma gelijk de printplaat wordt gemaakt. Ook kan er bijvoorbeeld een draai- of freesbank zijn gekoppeld om in één keer een prototype te kunnen vervaardigen.
- **Cd-romservers** kunnen meerdere (tientallen) cd's (en dvd's) ter beschikking stellen. Vaak vereisen ze een aparte configuratie.

Zo kan het zijn dat er nog allerlei apparatuur in het netwerk opgenomen moet worden, die apart aandacht behoeft.

4.9 Performance en reliability

Netwerkperformance kan naar drie deelgebieden onderscheiden worden:

1. Performance van de applicaties.
2. Performance op netwerkniveau (lagenmodel, netwerklaag, routers, protocollen, efficiëntie).
3. Performance van de infrastructuur (bekabeling, datalinklaag).

Eigenlijk zou het niet nodig moeten zijn om **performance** als apart item te behandelen. In een weldoordacht netwerkontwerp is uiteraard rekening gehouden met een optimale performance. Het is echter aan te bevelen om wel apart aandacht aan performance te schenken. Onder een kopje als dit kun je aangeven waarom server(s), clients en overige apparatuur in een netwerk optimaal presteren en welke maatregelen zijn genomen om dit te bereiken. Wat kan er eventueel gedaan worden om dat te verbeteren? En – heel belangrijk – wat heeft dit te maken met de oorspronkelijke wensen en

Index

betrouwbaarheid
beschikbaarheid
netwerk, kosten
Total Cost of Ownership
TCO

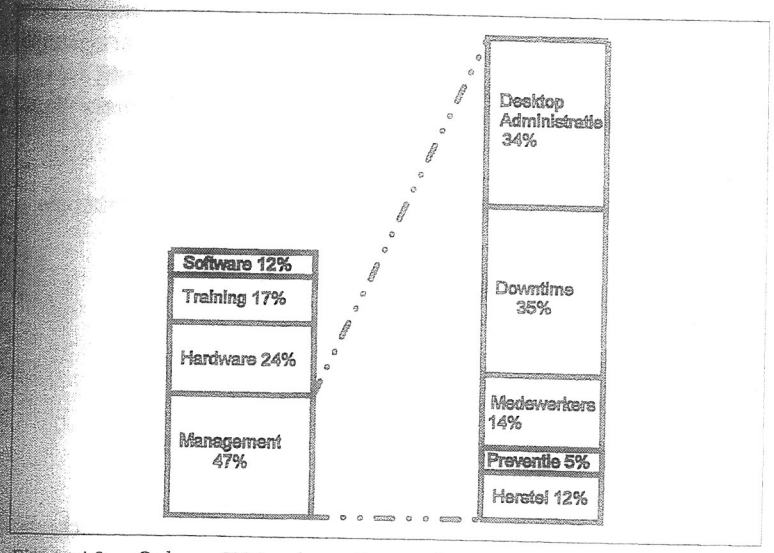
Hier komt ook om de hoek kijken hoe de **betrouwbaarheid** en **beschikbaarheid** van het netwerk is. Is 99 procent uptime voldoende of is 100 procent echt het streven? Een klant zal desgevraagd altijd 100 procent uptime wensen, maar dat betekent niet dat hij ook de consequenties daarvan, met name op financieel gebied, doorziet. Het is de taak van een netwerkleverancier om in samenspraak met de klant tot de juiste afweging te komen. De regel 'de klant is koning' gaat in de ICT-wereld niet op. De klant wil namelijk alles en het mag niets kosten. Het belang van de leverancier lijkt daar soms lijnrecht mee in tegenspraak. Niet elke klant heeft evenveel te besteden en daarmee zijn klanten dus ook niet 'evenveel' koning. De uitdaging is om de juiste middenweg te vinden.

4.10 TCO, ROI en afschrijvingstermijn

Een netwerk vormt voor bijna alle bedrijven een forse investering, en het is tot de bedrijfskritische systemen gaan behoren. Als het netwerk niet operationeel is, kan het bedrijf niet functioneren. De periode die het bedrijf kan overleven zonder netwerk neemt af. Er zijn bedrijven waar het bedrijfsnetwerk zo onmisbaar is bij het uitvoeren van de primaire bedrijfsprocessen dat een storing van enkele uren het bedrijf al in zijn voortbestaan kan bedreigen.

Dit betekent natuurlijk niet dat het niet uitmaakt wat de kosten zijn. Elk bedrijf zal op een efficiënte wijze een netwerk willen aanschaffen, beheren en uiteindelijk, als het afgeschreven is, willen vervangen. In die zin geldt voor een netwerk hetzelfde als voor een bureaustoel of de vloerbedekking. Zeker uit de beginperiode van de automatisering zijn voorbeelden bekend van uit de hand gelopen kosten, die uiteindelijk een project of bedrijf de das om gedaan hebben.

De **kosten** van een netwerk zijn zeer divers; er moet geprobeerd worden zowel de delen als het geheel in de hand te houden. Om een duidelijke afweging te kunnen maken tussen kosten en baten, en om ook te bepalen welke apparatuur gekozen kan worden, wordt vaak gewerkt met het begrip **Total Cost of Ownership** (TCO) van een pc.



Figuur 4.9 Opbouw TCO volgens Gartner Group.

Een veelgebruikte en eenvoudige definitie van TCO is:

Total Cost of Ownership
De totale kosten van aanschaf, onderhoud en gebruik van ICT assets (hardware) binnen een organisatie.

Het lijkt in tegenspraak met de lage prijzen van de diverse 'dozenschuivers', maar men is het er over het algemeen wel over eens dat een TCO van € 10.000 tot € 15.000 een redelijke schatting is. Dit heeft dan meestal betrekking op een periode van drie jaar. De kosten voor onderhoud, serverpark en ICT-infrastructuur drukken veel zwaarder op dit bedrag dan de relatief lage aanschafprijs van een pc.

De eenvoudigste benaderingswijze bij een investering is de terugverdienmethode:

$$\frac{\textit{Oorspronkelijke investering}}{\textit{Jaarlijkse netto inkomsten}} = \textit{Aantal jaren}$$

Index

Return On Investment
ROI

Een andere benadering voor een bedrijf dat een netwerk implementeert, is de **Return On Investment (ROI)**. Hoeveel levert het netwerk nu eigenlijk aan besparingen op en is dat bedrag hoger dan de investering zelf? Daartoe bepaal je eerst de inkomsten die de investering genereert:

$$\frac{(\textit{Totale inkomsten} - \textit{Totale kosten} - \textit{Afschrijving})}{\textit{Economische levensduur}} = \textit{Netto inkomsten}$$

om vervolgens aan het percentage van de ROI te komen:

$$\frac{\textit{Netto inkomsten}}{\textit{Totale oorspronkelijke investering}} \times 100\% = \textit{ROI}$$

De vraag is wat dit betekent voor de termijn waarop het netwerk zichzelf heeft terugverdiend. Is dat een termijn die gezien de technische en economische levensduur van het netwerk reëel is? Bedenk wel dat, hoewel de technische levensduur van een pc op dit moment vele jaren bedraagt, een pc in economisch opzicht in drie jaar zijn waarde geheel verliest. Een vervangingstermijn van drie jaar wordt voor desktops als normaal gezien. Voor servers wordt met een iets langere periode rekening gehouden, en voor andere apparatuur is het wisselend. Vaak gaan apparaten als routers wel veel langer mee, maar moeten deze toch vervangen worden omdat bijvoorbeeld de bandbreedte niet meer voldoet.

4.11 10% regel

Het functioneel netwerkontwerp is leidend voor de latere ontwerpfasen en de bouw van het netwerk. Het is de bedoeling om het netwerk exact volgens deze specificatie te maken. In de praktijk lukt dat echter soms niet. Apparatuur die beschikbaar is op het moment dat het FNO wordt gemaakt, kan niet meer leverbaar zijn, of de specificaties zijn gewijzigd. Ook kan het gebeuren dat de minimale specificaties zo laag zijn dat het goedkoper is een snellere oplossing te kiezen. Dat laatste klinkt misschien gek, maar een netwerk dat trager is dan 10 Mbps is momenteel duurder dan een 10 Mbps oplossing. (Het verschil tussen 100 Mbps en 10 Mbps is erg klein.)

...richtingsplan, dat op het functioneel ...kent wel dat steeds het functioneel ontwerp moet worden geraadpleegd om na te gaan of dit geen onvoorziene consequenties heeft. In de praktijk gaan we meestal van de '10% regel' uit. Dit is het percentage dat het inrichtingsplan mag afwijken van het functioneel ontwerp.

In

10% rege

4.12 Vragen en opdrachten

4.12.1 Open vragen

1. Voor welk type bedrijf zijn digitizers en A0-plotters interessant?
2. Welke actieve componenten zijn in een netwerk van belang?
3. Hoe bepaal je de afschrijving van netwerkapparatuur?
4. Bepaal de Return On Investment van je pc thuis.
5. Wat is de in dit hoofdstuk genoemde 'ping of death'? Van welke eigenschap werd gebruik gemaakt?

4.12.2 Opdrachten

1. Ontwerp voor het bedrijf in paragraaf 3.3 het netwerk op serverniveau. Presenteer dit ontwerp aan de eigenaren van het bedrijf. Besteed zowel aandacht aan de servers als aan de werkstations. Zeker voor het serverplatform wil het bedrijf een high-end systeem inzetten. De markt is 'booming' en er wordt nogal wat groei verwacht vanwege de vergrijzing.

2. a. Maak een overzicht van de op dit moment leverbare high-end pc's.
   b. Geef aan welke nieuwe technologieën erin zijn verwerkt.
   c. Geef tevens aan welke pc je voor welk soort klant zou kiezen. Let daarbij goed op de gewenste prijs/kwaliteit/functionaliteitverhouding.

3. Maak voor je school een plan om de printfaciliteiten te verbeteren en presenteer het aan de schoolleiding.
   Een van de eisen die worden gesteld, is dat de kosten voor de school niet hoger mogen zijn dan nu het geval is. Je kunt eerst een aantal leerlingen uit een ander (lager) jaar interviewen.

4. Onderzoek wat je school heeft gedaan om de diverse aspecten van de beveiliging van het netwerk te regelen. Let daarbij ook op de performance en de betrouwbaarheid. Schrijf een rapport voor de afdeling [illegible] voorstellen ter verbetering.

Servers, Netwerk Operating Systems en Directory Services

Aspecten van het inrichtingsplan

Doorreizen

Als je de praktijkopdracht in paragraaf 3 van dit hoofdstuk naar tevredenheid hebt gemaakt, kun je na overleg met je docent doorgaan naar het volgende hoofdstuk.

Aspecten van het inrichtingsplan

6.1 Inleiding

Een niet al te omvangrijk netwerk is in feite met een functioneel ontwerp als ontwerpdocument voor een groot deel beschreven. In een dergelijk ontwerp is echter nog niet noodzakelijkerwijs vastgelegd wat er aan techniek nodig is om het netwerk te kunnen implementeren. Ook is nog niet zichtbaar hoe een en ander er in het pand (of de panden) van de klant daadwerkelijk uit komt te zien.

- Waar komt bekabeling?
- Welke kast komt waar te staan?
- Welke servers draaien exact welke service?
- Wordt het netwerk gesegmenteerd?
- Komt er een een structuur met VLAN's?

Antwoorden op al die vragen komen in het inrichtingsplan.

6.2 Aanwijzingen voor de leerling

Het inrichtingsplan is het document dat op basis van het functioneel netwerkontwerp wordt gemaakt en dat wordt gebruikt door het bedrijf dat het netwerk uiteindelijk gaat installeren. Dit laatste betekent dat het inrichtingsplan het netwerk tot in detail moet vastleggen. Denk daarbij onder meer aan de volgende aspecten:

- het verloop van de bekabeling;
- de plaats waar de kabelgoten moeten komen, en het type ervan;
- de locatie en functie van de patchkast en hoe de apparatuur erin wordt geplaatst;
- welke software op welke machine moet staan;
- hoe het netwerk geconfigureerd moet worden;
- welke backup-apparatuur op welke manier geconfigureerd wordt.

Zelfs wat er als achtergrond op de desktop van de gebruikers komt, moet bij wijze van spreken vastgelegd zijn.

Het is overigens niet zo dat functioneel ontwerp en inrichtingsplan bij elkaar horen. Ze volgen wel op elkaar, maar een inrichtingsplan bevat noodzakelijkerwijs herhalingen ten opzichte van het functioneel ontwerp. Een netwerkinstallateur heeft in de praktijk vaak alleen de beschikking over het inrichtingsplan. Dat moet op alle vragen dus een antwoord geven.

Onderwerpen die aan de orde komen zijn:

- de infrastructuur:
  - segmenteren
  - nummerplan/adresseringsplan
  - VLAN
- serverpark met typen servers en selectie
- keuze van operating system (Novell of Microsoft)
- werkplekken:
  - OS
  - applicaties

Index

inrichtingsplan
technisch netwerkontwerp
infrastructuur
bekabeling
apparatuur

Attentie

Een inrichtingsplan wordt ook wel technisch (netwerk)ontwerp genoemd.

6.3 Praktijkopdracht

In een van de vorige hoofdstukken heb je een functioneel ontwerp gemaakt. Dat ontwerp is, mits goedgekeurd door je opdrachtgever, een van de uitgangspunten van dit hoofdstuk. Het is, samen met de kennis die je van netwerken hebt, nodig om tot een inrichtingsplan te komen voor het te realiseren netwerk.

Maak voor je functioneel ontwerp een inrichtingsplan op basis van de extra informatie die je ter beschikking wordt gesteld. Gebruik ook dit hoofdstuk voor verdere informatie.

6.4 Het inrichtingsplan

Nadat er een 'go' op het functioneel ontwerp is ontvangen, en daarmee is gegarandeerd dat de gewenste en de afgesproken functionaliteit op elkaar zijn afgestemd, moet het netwerk technisch nog uitgewerkt worden voordat het geïmplementeerd kan worden.

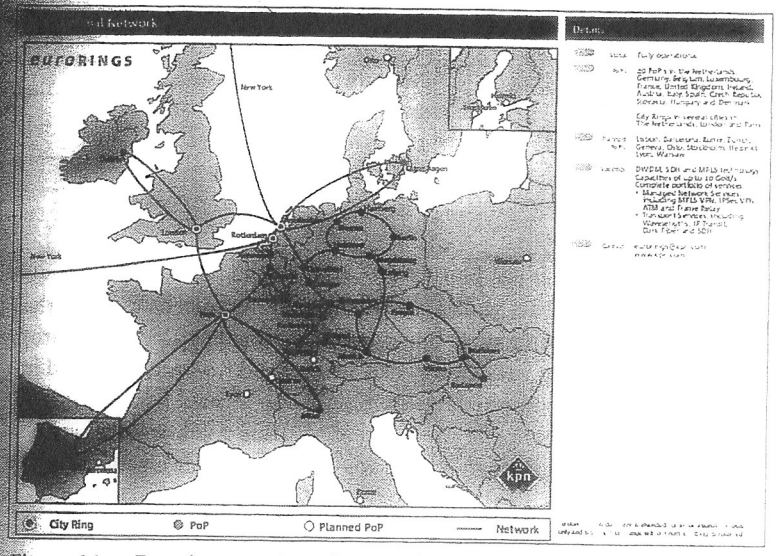
Het functioneel ontwerp moet dan uitgewerkt worden in een ontwerp dat op de afgesproken plaats gerealiseerd moet en kan worden. Daartoe wordt een **inrichtingsplan** gemaakt. Je komt voor dit plan ook wel de naam '**technisch netwerkontwerp**' tegen. In dit hoofdstuk nemen we een aantal aspecten van dit ontwerp door.

6.5 De infrastructuur

In het inrichtingsplan komt een volledige beschrijving van de interne en externe **infrastructuur**. Dat betekent: alle verbindingen met snelheid, configuratie en gebruikte apparatuur. Natuurlijk worden van alle gebruikte apparatuur typenummers, configuratie en extra opties vermeld. Alle **kabels** in het netwerk dienen gedocumenteerd te worden. Vaak gebruiken bedrijven een kleurcode en een code op de kabel om deze uit elkaar te houden. Met behulp van de kleur worden dan de soorten kabels onderscheiden (bijvoorbeeld grijs is data naar de werkplek, groen is telefoon, rood is de 1000 Mb backbone). Daarnaast is op de kabel steeds af te lezen van welk netwerksegment deze deel uitmaakt en waar hij heen gaat (waar hij is gepatcht).

weergezet? Wordt er gebruik gemaakt van switches om het netwerk op te delen en broadcastverkeer te minimaliseren? Ook wordt van elk segment de snelheid vastgelegd; op deze snelheden worden vervolgens backbones en andere verbindingen gebaseerd.

Bij elke fase van een netwerkontwerp is het verstandig steeds naar de **business case** te kijken. Klopt dit met de functionele eisen en is het prijstechnisch de beste oplossing? Apart aandachtspunt vormen de verbindingen tussen de LAN's. Deze kunnen qua prijs snel uit de hand lopen, want hogesnelheidsverbindingen zijn erg duur.



Figuur 6.1 Euroring, een nieuw Europees hogesnelheidsnetwerk (2003).

6.5.1 Segmenteren

Het is in een netwerk van groot belang dat de hoeveelheid verkeer over het netwerk wordt beperkt. Dat is natuurlijk niet bedoeld als een oproep om het netwerk niet te gebruiken, maar meer om de hoeveelheid verkeer in de hand te houden.

Was tot voor enkele jaren het gebruik van **hubs** in een netwerk gangbaar, tegenwoordig worden bijna altijd **switches** gebruikt. Dat beperkt het ver-

Index

business c
segmenter
hub
switch

goed gebruik van **bridges** en door een goed IP-plan kan nog een groot deel van dit verkeer worden beperkt. Het terugdringen van onnodig verkeer laat meer bandbreedte over voor het gewenste verkeer. Samen met een **IP-plan** legt dit een basis voor de verdeling van het fysieke verkeer over het netwerk.

6.5.2 Nummerplan en adresseringsplan

In de praktijk functioneren veel netwerken tegenwoordig op basis van het protocol **IP**. In dat geval wordt er intern vaak gewerkt met een van de zogeheten '**public address spaces**'. Deze zijn vastgelegd in RFC 1918. Het betreft:

IP Address Range	Network mask	Aantal adressen
10.0.0.0 – 10.255.255.255	10.0.0.0/8	16.777.216 (2^{24})
172.16.0.0 – 172.31.255.255	172.16.0.0/12	1.048.576 (2^{20})
192.168.0.0 – 192.168.255.255	192.168.0.0/16	65.536 (2^{16})

Het kan ook zijn dat er een blok **IP-adressen** beschikbaar is. Bij het gebruik van private space wordt het hele netwerk vervolgens vaak weer via één of twee IP-adressen met de buitenwereld verbonden. De wijze waarop de interne IP-adressen worden ingedeeld en gebruikt, wordt vastgelegd in een IP-**nummerplan**. In een dergelijk plan wordt bepaald hoeveel IP-adressen nodig zijn en hoe ze worden verdeeld, dus ook hoeveel er voor elk doel beschikbaar zijn. Een organisatie legt daar ook de algemene regels vast, bijvoorbeeld:

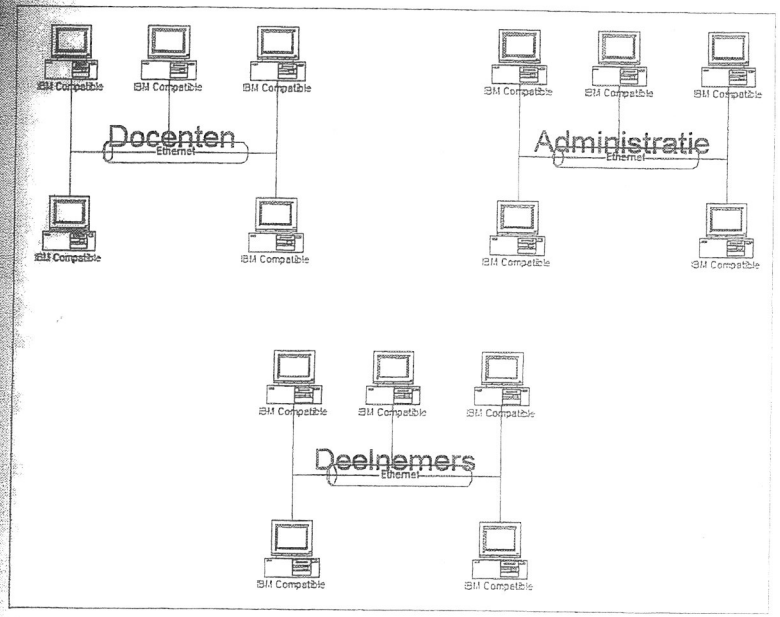
- servers altijd onder de x.x.x.16;
- printers altijd vast IP-adres van x.x.x.16 tot x.x.x.25;
- DHCP range loopt altijd van x.x.x.26 tot x.x.x.250;
- default router is altijd op x.x.x.254.

Daarnaast wordt elke computer of groep computers van een IP-adres of adresreeks voorzien. Ook wordt hier vastgelegd hoe de IP-adressen verspreid gaan worden (Static, DHCP).

Bij het ontwerpen kan ervoor worden gekozen om het netwerk alvast op **IPv6** voor te bereiden. De meeste netwerktechnologieën kunnen dat op dit moment verzorgen. Als het er dan ooit van komt dat IPv6 wordt ingevoerd, kan probleemloos overgestapt worden.

6.6 Splitsen van netwerken

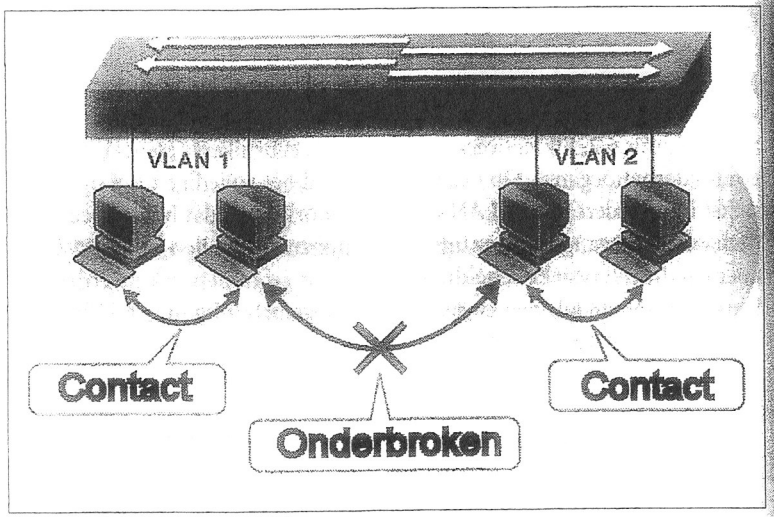
Netwerken in bedrijven en organisaties worden vaak in delen gesplitst. Op veel scholen was tot voor kort een verdeling gebruikelijk zoals deze is te zien in figuur 6.2. Elk netwerk had zijn eigen gebruikers (en vaak ook zijn eigen internettoegang). Op deze manier werd het volledige LAN opgesplitst in meerdere aparte LAN's en werd voorkomen dat bijvoorbeeld deelnemers toegang tot de resultatenadministratie konden krijgen. We noemen dit een **fysieke scheiding**. Om in een groot netwerk meerdere logische LAN's te kunnen creëren worden tegenwoordig meestal **Virtual LAN's**, zogenoemde VLAN's, gebruikt.



Figuur 6.2 Fysiek verdelen van een netwerk.

6.7 VLAN

VLAN staat voor Virtual Local Area Network. Door gebruik van VLAN's ontstaan er logische LAN's binnen een bestaand groot fysiek LAN. Op deze wijze worden beheer en onderhoud eenvoudiger. Een VLAN is onafhankelijk van de fysieke status van de gebruiker. Een gebruiker kan zich binnen een VLAN op een willekeurige locatie van het netwerk bevinden zonder dat dit invloed heeft op het VLAN waarin de gebruiker wordt



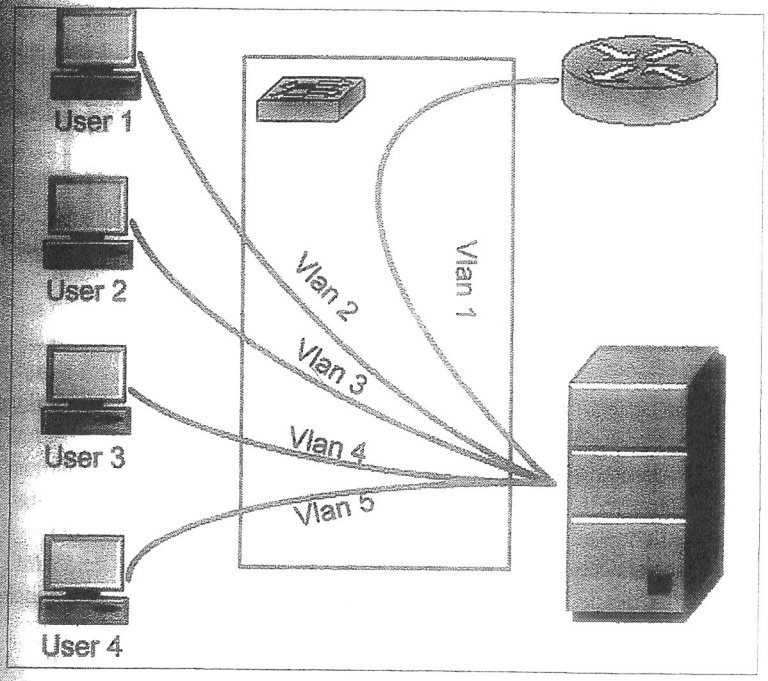
Figuur 6.3 VLAN's scheiden netwerken binnen één netwerk.

6.7.1 Wat is VLAN?

VLAN (Virtual LAN) is dus een techniek waarbij een groter netwerk wordt opgedeeld in segmenten. Deze opdeling kan bijvoorbeeld plaatsvinden op basis van gebruikersgroep of domein. Normaal gesproken is een netwerk van verschillende afdelingen één groot geheel. De behoefte kan echter ontstaan om de diverse afdelingen weer als een klein LAN te zien. Dit kan gerealiseerd worden met behulp van een VLAN. Het opdelen kan zowel op basis van gegevens van OSI-laag 2 als van OSI-laag 3 worden gedaan. Dit houdt in dat een VLAN op IP-niveau, poortniveau en MAC-niveau gedefinieerd kan worden (zie ook paragraaf 6.7.4).

Een dergelijk netwerk is veel beter beheerbaar dan een 'gewoon' LAN. Je kunt een persoon van de ene naar de andere fysieke locatie verhuizen zonder dat je een nieuw IP-adres en/of groep aan de persoon hoeft toe te kennen. De user blijft gewoon gebruiker van hetzelfde VLAN.

Een VLAN heeft ook voordelen als het gaat om het beperken van de **broadcasts**. Door het creëren van een VLAN worden de broadcasts binnen een fysiek netwerk niet door het hele netwerk, maar alleen binnen het VLAN doorgegeven. Je kunt de belasting van het netwerk op deze wijze reduceren en dus met minder bandbreedte toe om dezelfde functionaliteit en performance te bieden.



Figuur 6.4 VLAN's kunnen plaatsonafhankelijk zijn.

6.7.2 Specificaties van een VLAN

De specificaties van VLAN's zijn (sinds 1999) gestandaardiseerd door de IEEE. Deze instantie heeft de manier van indelen en de andere technische aspecten van VLAN's beschreven.

6.7.3 IEEE 802.1x

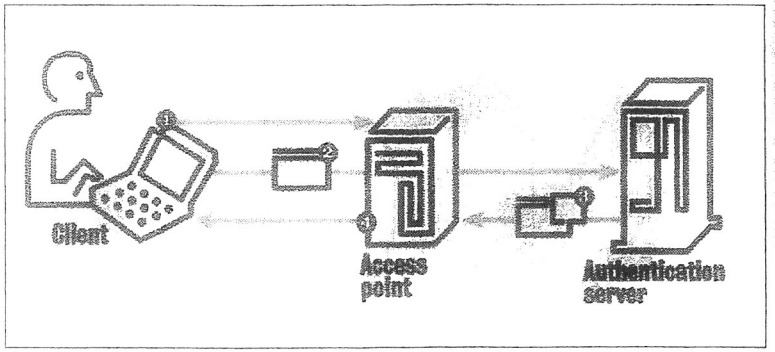
Het is mogelijk om (onder andere in een VLAN) een extra stuk beveiliging te bereiken door middel van het protocol IEEE 802.1x. Dit protocol zorgt voor een deel van de **authenticatie**. Een gebruiker komt – waar hij zich fysiek ook op het LAN bevindt – altijd in hetzelfde VLAN. Alle verdere gegevens zijn aan de gebruiker gekoppeld. Het **IP-adres** is dus niet meer gekoppeld aan het MAC-adres, maar aan de gebruiker. Een gebruiker die onbekend is op het netwerk, zal dus ook geen IP-adres meer krijgen en hem wordt alle toegang het netwerk ontzegd. Veel ISP's eisen tegenwoordig dat van aangesloten netwerken altijd alle verkeer tot een

Index

beveiliging
VLAN, indeling
Port-based VLAN
MAC-based VLAN
Layer 3-based VLAN

Attentie

In dit voorbeeld is uitgegaan van een wifi-client, maar dat maakt voor het principe niet uit.



Een constructie als deze wordt steeds meer gebruikt. De **beveiliging** werkt als volgt:

1. Een client stuurt een 'start'-boodschap naar een access point. Dit vraagt om de identiteit van de gebruiker.
2. De client stuurt vervolgens een respons (met identiteitsgegevens) naar het access point, dat deze informatie doorstuurt naar een authenticatieserver (Radius).
3. De authenticatieserver stuurt een 'accept' naar het access point.
4. Het access point zet de poort via welke de client contact heeft, op 'geautoriseerd' en het verkeer is toegestaan.

6.7.4 VLAN-indeling

Een VLAN kan op meerdere niveaus in het OSI-model worden gemaakt. We onderscheiden: port-based VLAN, MAC-based VLAN, Layer 3-based VLAN en policy-based VLAN. Op deze typen gaan we nader in.

Port-based VLAN

Op de switch wordt elke port aan een VLAN toegekend. Deze methode kent als belangrijkste nadeel dat de hele configuratie aangepast moet worden als de gebruiker verhuist. Ook kan een port maar aan één VLAN worden toegekend.

MAC-based VLAN

Op basis van het MAC-adres wordt een computer in een VLAN geplaatst.

Layer 3-based VLAN

Op basis van Layer 3-gegevens – dat kan bijvoorbeeld zijn op basis van het IPX-adres (Novell) of het IP-adres – wordt een computer in een dit niet noodzakelijk op een individuele gebruiker is terug te voeren (behalve als deze alleen dáár mag inloggen).

Policy-based VLAN

Deze (latere) methode van indelen kan op basis van criteria als:
- iedereen die TCP/IP gebruikt;
- al het verkeer met een bepaald type veld in het Ethernet-pakket;
- alle computers met 3COM netwerkkaarten.

Een computer kan hier in meer VLAN's tegelijk zijn opgenomen.

Deze laatste optie is het krachtigst en wordt het meest gebruikt. Hiermee kunnen gebruikers of groepen gebruikers (via de Directory Service) worden gekoppeld aan bijvoorbeeld een bepaalde groep applicaties. Deze methode kan ook een bepaalde functionaliteit weigeren op basis van deze indeling.

Om VLAN's met elkaar te verbinden moeten er tussen de VLAN's weer routers opgenomen worden.

6.8 Selectie van servers en operating systems

Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER-PROCES
De benodigde en gewenste architectuur van het netwerk.	
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

In een netwerk komen bijna altijd een aantal van de in paragraaf 5.4 genoemde servers voor. Het is echter niet altijd even eenvoudig om de juiste keuze voor een operating system en/of applicatie te maken. Alle

Om e-mailfaciliteit te bieden kun je een Windows XP-server met Exchange neerzetten, maar ook een UNIX of Linux machine met een SMTP-daemon. Als geen van de genoemde de voorkeur heeft, kun je ook een Novell NetWare-server met Groupwise inzetten.

Bij het kiezen van een NOS (server) en applicatie wordt met een aantal aspecten rekening gehouden, onder andere:

- *Integratie met bestaande infrastructuur.* In principe ligt de tijd van volstrekt incompatible systemen en fabrikanten die alleen hun eigen protocollen ondersteunen nu wel achter ons. Om er echter van uit te gaan dat integratie van systemen altijd vlekkeloos verloopt, is ook wat te optimistisch.
- *Afstemming op applicaties.* Het is niet erg zinvol om in een LAN waar enkel Microsoft producten worden gebruikt opeens UNIX als mailserver in te zetten.
- *Ervaring en kennis van ICT-medewerkers.* Het ondersteunen van een extra platform kost veel tijd en geld. Er wordt vaak voor gekozen om het aantal ondersteunde producten laag te houden; ook als bekend is dat dit ten koste gaat van mogelijkheden, functionaliteit en/of betrouwbaarheid.
- *Kennis en deskundigheid van in te zetten platform.* Het is logisch dat men geen service op een totaal onbekend platform inzet.
- *Beheerbaarheid.*
- *Stabiliteit.* Dit is een punt waar (soms) nogal wat emotie bij komt kijken. Iedereen wenst een zo stabiel mogelijk netwerk met een minimale hoeveelheid onderhoud. Niet alle OS'en zijn echter even stabiel. Een echte UNIX aanhanger zal geen enkel bedrijfskritisch systeem op een Microsoft product willen zien draaien, maar er zijn ook wel degelijk fans van Microsoft.
- *Servicevoorwaarden.*
- *Wel of niet open source.* Voor veel serverproducten zijn tegenwoordig 'gratis' GPL-oplossingen, maar het is de vraag of dat een pre is. Sommige bedrijven weigeren consequent GPL-producten omdat er niemand aanspreekbaar is als het product faalt of niet de beloofde functionaliteit biedt. De servicevoorwaarden kunnen een argument zijn om een product wel of niet te kiezen.
- *Het functioneel netwerkontwerp.* De in het FNO afgesproken functionaliteit is natuurlijk hoofdzaak. Als daar al een keuze voor een bepaald product of OS is gemaakt, dan kan daar niet zomaar op teruggekomen worden.

6.9 Het inrichten van de werkplekken

6.9.1 Typen werkplekken

In een netwerkontwerp worden vrijwel altijd meerdere mogelijke **werkplekken** beschreven. Er zijn wel organisaties waar een 'one size fits all'-benadering mogelijk is en er maar één soort werkplek is gedefinieerd, maar die zijn zeldzaam. In de praktijk bestaan er meestal meerdere typen gebruikers die elk een eigen soort werkstation hebben met eigen configuraties en software.

Om de ondersteuning door helpdesk en systeembeheer zo efficiënt mogelijk te maken wordt meestal gestreefd naar een minimaal aantal configuraties. Zo zal er bijvoorbeeld een standaard administratief station zijn beschreven (inclusief operating system, applicaties, enzovoort), en zo min mogelijk overige stations voor andere typen gebruikers. Een gulden regel is hier niet te geven. In een kantooromgeving kan soms worden volstaan met één type standaardstation voor een grote groep medewerkers. Bij een ingenieursbureau moeten waarschijnlijk meerdere typen ontwerpstations worden vastgelegd. Een ontwerper zal nu eenmaal vaker met een CAD-pakket als AutoCAD of Arkey werken dan met een Office-applicatie.

Uit oogpunt van beheer moet het aantal typen standaardstations zoveel mogelijk beperkt worden. Verder heeft elk specialisme vaak zijn eigen voorkeur voor software/hardware.

6.9.2 (Desktop) besturingssystemen

Voor het **operating system** op de desktop lijken er niet zoveel mogelijkheden te zijn. De ondersteuning voor oudere **Windows**-versies laat sterk te wensen over. Windows 2000 of hoger lijkt een minimale vereiste. Voor Microsoft Office is 2000 ook het minimum. Oudere versies worden niet meer ondersteund.

Afhankelijk van de gewenste mogelijkheden is het echter ook mogelijk om in zijn geheel naar een van de **Linux** distributies over te stappen. Als de specifieke applicaties die de klant nodig heeft ook in een Linux variant leverbaar zijn, kan OpenOffice of StarOffice boven op een betrouwbare Linux distributie met een moderne Xwindow manager (Gnome of KDE) een betrouwbaar platform opleveren. Er is zelfs een Outlook-implementatie onder Linux (weliswaar niet door Microsoft ondersteund).

Index

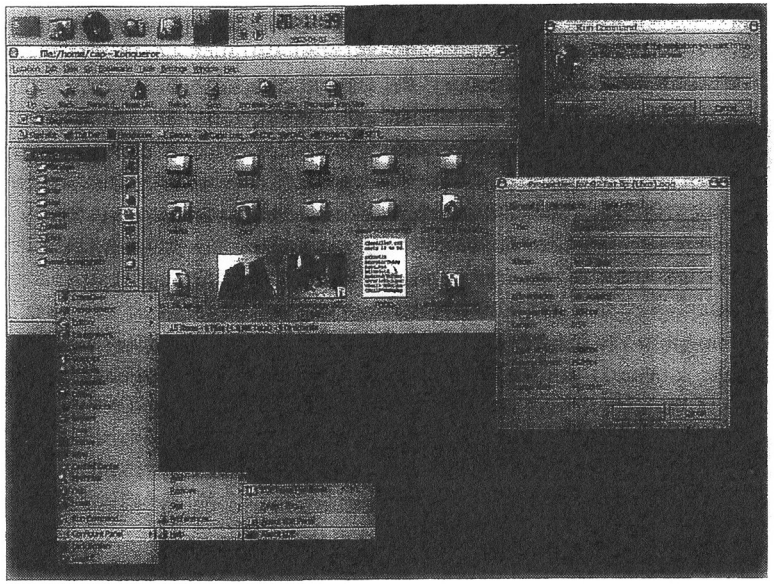
UNIX

Knipsel

Een stad als München is bezig deze conversie te maken, voornamelijk vanwege de als exorbitant ervaren licentiekosten van Windows en Office. In Nederland overwegen diverse gemeenten en organisaties hetzelfde.

Een compleet netwerk op basis van Linux op de desktop lijkt wat vreemd, maar als een groot deel van de software die gebruikt wordt webbased is en het personeel toch moet worden opgeleid, kan een keuze voor Linux-KDE meer dan voldoende functionaliteit leveren. Men krijgt dan de beschikking over Konqueror als browser, Koffice als Office suite en over de KDE PIM (personal information manager). Verder omvat dit Gnome met OpenOffice en Outlook for UNIX.

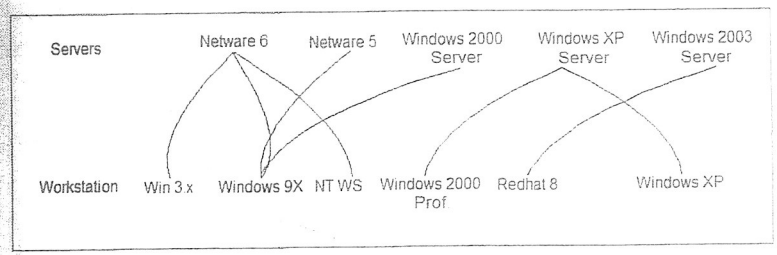
Voor een technisch bedrijf kan het gewenst zijn een UNIX netwerk te installeren. Veel gespecialiseerde software voor specifieke ontwerptaken is er alleen in een Xwindow-versie.



Figuur 6.5 KDE 3.0.

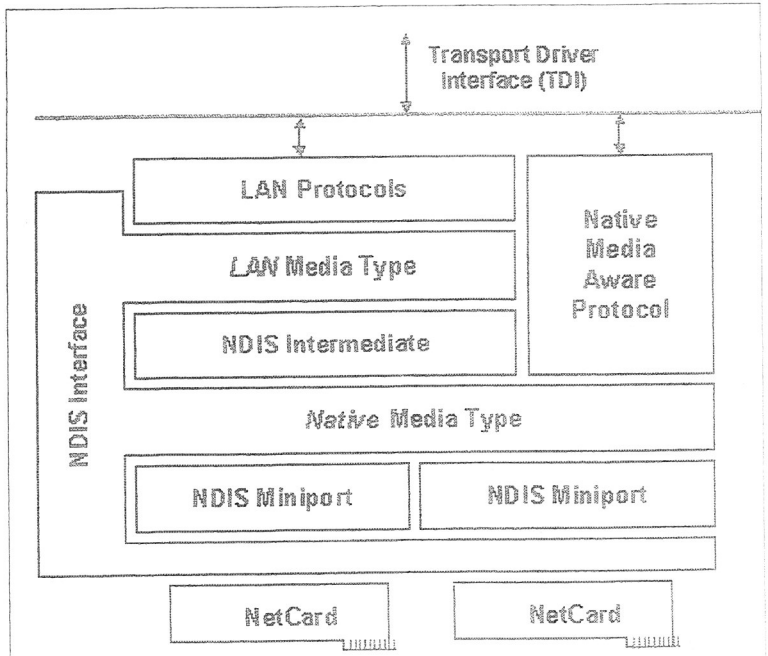
6.9.3 Heterogene netwerken

Of alle operating systems op server en client met elkaar overweg kunnen, is altijd maar de vraag. Er wordt op het gebied van connecties nog steeds vaak meer beloofd dan gerealiseerd. Een schema als dat van figuur 6.6 kan je helpen duidelijk te krijgen welke operating systems onderling geen contact kunnen leggen. Dit schema is slechts een voorbeeld, voor elk netwerk zul je apart moeten kijken of voor de essentiële diensten de noodzakelijke uitwisseling van gegevens mogelijk is.



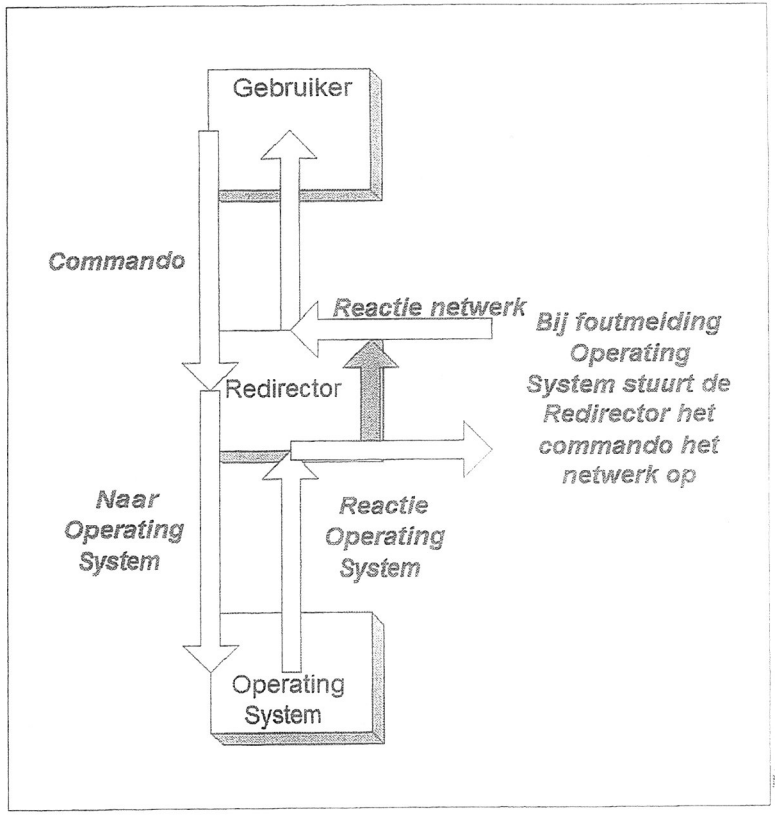
Figuur 6.6 OS'en van clients en servers (niet compleet).

Contact leggen tussen een werkstation en een serverpark vindt plaats door middel van een **protocolstack**. Er worden enkele drivers en protocollen geladen en deze verzorgen de contacten met het netwerk. Voor wat betreft een Windows werkstation en een Windows server(park) gebeurt dit op basis van NDIS. In figuur 6.7 zie je de drivers en layers van deze stack. NDIS heeft in de loop der jaren nogal wat (versie)wijzigingen ondergaan.



Operating System	Supported NDIS Version	CoNDIS Driver	Deserialized Driver	Intermediate
Windows 95 Windows NT 4.0 DDK Windows 95 DDK	3.1			
	Added support for miniport drivers and Plug and Play.			
Windows 95 OSR2 Windows NT 4.0 DDK Windows 95 DDK	4.0			
	Protocol driver is a vxd-type driver.			
Windows 98 Windows NT 4.0 DDK Windows 98 DDK	4.1	X	X	X
	Protocol driver is a vxd-type driver.			
Windows 98 SE Windows NT 4.0 DDK Windows 98 DDK	5.0	X	X	X
	Added support for Power Management and WMI.			
Windows Me Windows 2000 DDK Windows 98 DDK for Vxds	5.0	X	X	X
Windows NT 3.5 Windows NT 3.5 DDK	3.0			
Windows NT 4.0 Windows NT 4.0 DDK	4.0			
	Added these features: *MiniportSendPackets* *ProtocolReceivePacket* *MiniportAllocateComplete*			
Windows NT 4.0 SP3 Windows NT DDK with updated NDIS header and library	4.1	X	X	X
Windows 2000 Windows 2000 DDK	5.0	X	X	X
	Added support for: *New INF file format compatible with Windows 95/98/Me* *Plug and Play and Power Management* *WMI* *LBFO* *Scatter/gather DMA support for deserialized miniport drivers*			
Windows XP Windows XP DDK	5.1	X	X	X
	Added support for: *MiniportCancelSendPackets* *MiniportPnPEventNotify* *MiniportShutdown* *Scatter/gather support for both serialized and deserialized miniport drivers Packet stacking for intermediate drivers* *VLAN tagging* **Dropped support for:** *Full Mac drivers* *NDIS 3.0 protocols*			

De meeste protocolstacks nemen de gedaante van een **redirector** aan. Dat betekent dat ze tussen operating system en gebruiker in zitten en de ontvangen commando's rechtstreeks doorgeven aan het operating system. Mocht het OS een commando niet kunnen interpreteren, dan stuurt de redirector het door naar de netwerkprotocolstack om uit te zoeken of het een netwerkcommando betreft. Is dit het geval, dan wordt dit verwerkt. Anders wordt de melding van het operating system aan de gebruiker doorgegeven.



Figuur 6.8 Redirector

Het meest gebruikte protocol is TCP/IP. Elke leverancier ondersteunt TCP/IP: het is op dit moment de 'de facto' standaard. Standaard kende Novell het IPX/SPX-protocol en Microsoft NetBEUI. Deze twee zijn ech-

6.10 Vragen en opdrachten

6.10.1 Open vragen

1. Waarom zou je netwerken segmenteren? Geef drie redenen.

2. Wat is een VLAN? Beschrijf de werking.

3. Wie beheert de standaarden van VLAN?

4. a. Noem de verschillende wijzen waarop een VLAN kan zijn ingedeeld.
   b. In welke laag van het OSI-model vindt elke indeling plaats?

5. a. Welke IP-reeksen zijn voor 'public address space' vrijgegeven?
   b. Hoe groot zijn ze?

6. Waarom worden netwerken vaak logisch gesplitst?

7. a. Wat is het protocol 802.1x?
   b. Waar wordt het (voor) gebruikt?

6.10.2 Opdrachten

1. Maak een IP-plan voor de afdeling waar je les hebt. Op welke regels baseer je dat?

2. a. Ontwerp het standaardwerkstation voor het lokaal of de plaats waar je op school het meest zit. Houd rekening met:
      - standaard software (al of niet lokaal geïnstalleerd);
      - onderhoudbaarheid;
      - operating system;
      - alle andere onderwerpen die van belang zijn.
   b. Bereid een presentatie voor om je keuze aan de schoolleiding te presenteren en het huidige standaardstation door jouw voorbeeld te vervangen.

lementatie, uik en beheer

Doorreizen

Als je de praktijkopdracht in paragraaf 3 van dit hoofdstuk naar tevredenheid hebt gemaakt, kun je na overleg met je docent doorgaan naar het volgende hoofdstuk.

Implementatie, gebruik en beheer

7.1 Inleiding

In het vorige hoofdstuk is een groot deel van de structuur van het toekomstige netwerk vastgesteld. De logische structuur ligt vast; de operating systems zijn bepaald. Wat zou er in een inrichtingsplan verder aan bod moeten komen? Waar nog geen aandacht aan besteed is, is de manier waarop het netwerk geëxploiteerd gaat worden en hoe de ingebruikname in zijn werk zal gaan.
In dit hoofdstuk behandelen we een aantal zaken die daarmee te maken hebben.

7.2 Aanwijzingen voor de leerling

De aspecten van de voorbereiding van de ingebruikstelling, de daadwerkelijke ingebruikname en de voorbereidingen voor de periode erna komen in dit hoofdstuk aan de orde. De centrale onderwerpen zijn:
- implementeren en de afdeling ICT
- opleiden
- testen
- de roll-out
- de eventuele conversie

7.3 Praktijkopdracht

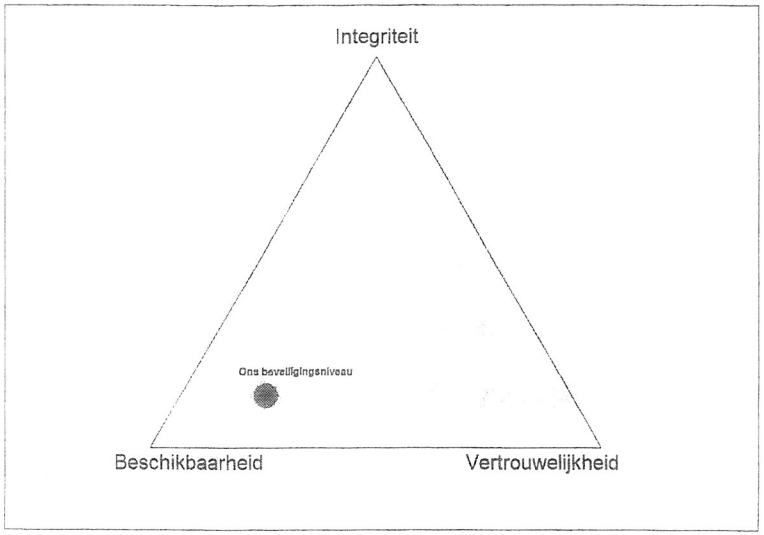
Breid je document van het vorige hoofdstuk uit met de aspecten die in dit hoofdstuk aan de orde komen. Maak voor je functioneel ontwerp een inrichtingsplan op basis van de extra informatie die je ter beschikking wordt gesteld. Gebruik ook dit hoofdstuk voor verdere informatie.

7.4 Security

Een belangrijk aandachtspunt bij netwerken, dat vanaf het eerste moment in de overwegingen moet worden meegenomen, is **security**. In eerste instantie wil iedereen natuurlijk een veilig netwerk. Vaak echter wordt daarbij vergeten dat niet ieder netwerk in het Amerikaanse ministerie van Defensie hoeft te gaan opereren. Het is verstandig om eerst na te gaan hoe vertrouwelijk de informatie is en wat er nu exact beveiligd moet worden. Veiligheid is goed, maar te veel veiligheid gaat vaak ten koste van gebruikersgemak en functionaliteit.

Een aardig hulpmiddel is de zogenaamde 'security triangle'. Er zijn drie aspecten die met veiligheid te maken hebben:
1. integriteit van het netwerk
2. beschikbaarheid
3. vertrouwelijkheid

Eigenlijk willen we bij alle drie aspecten een 100% score, maar dat is in de praktijk niet haalbaar. Ergens in de onderstaande driehoek zal ons netwerk zich bevinden.



Figuur 7.1 De 'security triangle'.

7.5 Implementeren

Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER-PROCES
De benodigde en gewenste architectuur van het netwerk.	
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

Als een van de laatste fasen van het ontwerpen van netwerken kan het implementeren van het netwerk en de infrastructuur worden genoemd. Daarvoor wordt een **implementatieplan** gemaakt.

Het komt vaak voor dat een goed ontworpen systeem niet of niet goed

is 'neergezet'. Het is de organisatie niet duidelijk wat het vervangt. Het is geen verbetering ten opzichte van de voorgaande situatie, of het wordt tenminste niet als zodanig ervaren. Het kan ook zijn dat over de introductie onvoldoende is nagedacht: het systeem is 'over de muur gegooid'.

Een goed implementatieproces voorkomt deze problemen en daarom is zorgvuldige implementatie van levensbelang. In deze paragraaf gaan we in op implementeren en de plaats van de implementatie in het ontwerpproces.

7.6 ICT als facilitaire dienst

De meeste bedrijven beschouwen ICT als een **facilitaire dienst**. Daarmee staat het netwerk op hetzelfde niveau als andere hulpmiddelen die bedrijven hanteren om prettig en efficiënt te werken. Denk aan:

- schoonmaak
- catering
- beveiliging
- vervoer
- onderhoud
- inkoop
- voorraadbeheer

Dit betekent niet dat het netwerk een onderschatte positie inneemt, maar wel dat iedereen zich realiseert dat het netwerk een hulpmiddel is om de primaire processen uit te voeren. Met andere woorden: met een netwerk wordt geen geld verdiend, maar wel *met behulp van* het netwerk.

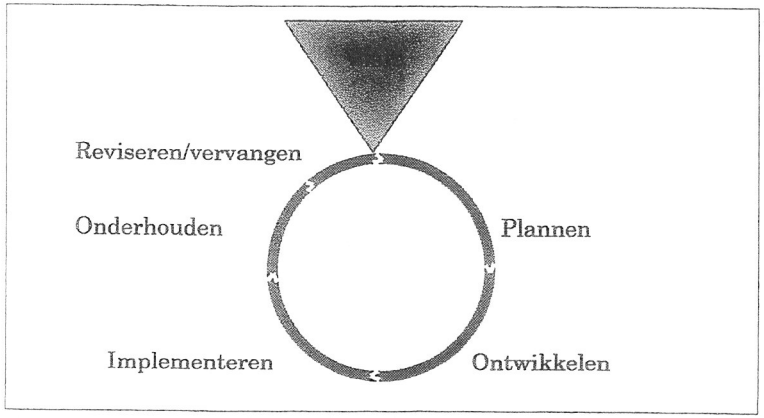
In de praktijk is ICT om twee redenen belangrijk voor een facilitaire afdeling:

1. als hulpmiddel voor het eigen functioneren;
2. als hulpmiddel voor het optimaliseren van secundaire processen.

Vaak wordt met een **Service Level Agreement** (SLA) een contract binnen het bedrijf gesloten tussen de ICT-beheerders en ICT-gebruikers. In een SLA wordt afgesproken welke functionaliteit en services geleverd worden tegen welke prijs. Dit gaat dan ook om zaken als beschikbaarheid en hersteltijd. SLA's zijn binnen ITIL (een standaardbeheermethodiek) belangrijke hulpmiddelen om de kwaliteit van beheer vast te leggen. We gaan er hier verder niet op in, maar elders – zowel in dit boek als in de opleiding – wordt er meer aandacht aan besteed.

Index

implementatie
roll-out
conversie
opleidingsplan



Figuur 7.2 Implementatie in de levenscyclus van een product.

Implementeren is niet alleen het neerzetten en aansluiten van de apparatuur. Tot het domein van de **implementatie** worden over het algemeen de volgende aspecten gerekend:

- acceptatie van het product en het voorbereiden daarvan;
- voorbereiden van de benodigde technische infrastructuur;
- opleiden van de gebruikers en beheerders;
- testen van het product in een testopstelling en bij normaal gebruik;
- **roll-out**: het daadwerkelijk plaatsen en installeren;
- **conversie** van de data, procedures en wat verder noodzakelijk is in de nieuwe situatie;
- voorbereiden van het beheer van het nieuwe systeem;
- evaluatie en nazorg.

7.7 Opleiden

Medewerkers moeten leren om in de nieuwe situatie te functioneren en dus moeten ze leren om met de nieuwe software en/of het netwerk om te gaan. Daartoe moeten ze de systemen, handleidingen, help-functies en helpdesk leren gebruiken. Voor dit doel kunnen cursussen zinvol zijn, maar ook ondersteuning door collega's kan hier een rol spelen. Opleiden kan overigens (mede) een draagvlak voor acceptatie vormen.

In het **opleidingsplan**, dat onderdeel van de implementatie is, worden de kaders voor de te volgen (of op te zetten) opleidingen geschetst. Ook wie (qua functie) voor welke opleiding in aanmerking komt, moet daarin tot

- Doel en doelgroep
- Wie, wat, waar, wanneer en hoe?
- Taken
- Benodigdheden
- Afhankelijkheden
- Risico's

7.8 Testen

In het ideale geval stuurt het **testen** de bouw van het product. De ontwikkelaar test voortdurend om het gewenste product op te kunnen leveren. Vaak is dit niet mogelijk, of is het niet gewenst (ontwikkelaars zijn nu eenmaal geen testers). In dat geval is testen na oplevering de enige optie. Daarbij moet niet worden vergeten om ook te onderzoeken hoe een product zich in een productie-omgeving houdt. Vaak wordt een applicatie of (netwerk)configuratie alleen getest in een situatie die niet representatief is voor het daadwerkelijke gebruik. Als de 'normale' gebruikers een systeem in gebruik nemen, ondernemen zij vaak heel andere acties dan een ontwikkelaar heeft bedacht. Deze laatste is echter wel vaak de tester geweest. Een uitgebreide veldtest kan vaak veel vertraging na de initiële oplevering voorkomen.

Aan elk ontwikkeltraject is een **testfase** gekoppeld. Elk product – of dat nu een softwaresysteem, een netwerk of een auto is – moet uitvoerig worden getest voordat het in gebruik kan worden genomen. Testen is noodzakelijk, zowel om te onderzoeken of de beloofde functionaliteit er is als om na te gaan of er bugs en/of andere ongerechtigheden in de software zijn achtergebleven.

Vaak vindt het testen plaats aan de hand van een **testplan**. De bedoeling van zo'n plan is dat er duidelijk in staat wie, waarom, wat, wanneer moet testen. Ook moet vastgelegd worden hóe elk product moet worden getest. Het is gebruikelijk om per product een testprotocol op te stellen dat deze zaken vermeldt. Vaak begint het testen al in de bouwfase en is het gedurende het hele proces een continue activiteit. Duidelijk moet ook zijn wiens verantwoordelijkheid het is en wat de gevolgen zijn van een niet-geslaagde test. In detail-testplannen wordt een en ander verder uitgewerkt.

testen
testfase
testplan

7.8.1 De tien geboden van het testen

Testen heeft een slecht imago, terwijl het een heel belangrijke activiteit is om de kwaliteit van software en/of hardware vast – en veilig – te stellen. Houd bij testen daarom rekening met de de onderstaande tien geboden:

1. **Noem een tester een tester.** De afgelopen jaren hebben testers allerlei namen gekregen. Wat te denken van toetser, kwaliteitsmeter, 'requirement checker' of zelfs 'advanced quality advisor'? Noem een tester een tester en laat daar geen misverstand over bestaan.

2. **Laat testen een aparte activiteit zijn.** Testen is geen onderdeel van bijvoorbeeld programmeren. Een onafhankelijke partij kan beter en grondiger risico's inschatten en voorkomen.

3. **Beschrijf wat een tester mag doen, moet doen en hoort te doen.** Bij veel organisaties zijn voor de rollen en functies uitgebreide competentieprofielen geschreven. Voor testers ontbreekt zo'n beschrijving vaak, met excuses als "testen is een eenmalige activiteit" (althans, dat dachten ze).

4. **Bied de tester de gelegenheid te leren wat hij test.** Testen is onder andere een risicobeperkende maatregel. Een tester vormt daardoor een risico op zich. Als hij onjuist of onvoldoende test, kunnen bepaalde risico's niet ondervangen worden. Daarom is het belangrijk dat een tester niet alleen weet wat goed gestructureerd testen is, maar ook wat hij test.

5. **Zet testers fysiek midden in de organisatie.** Omdat testen zich begeeft op het kruispunt van vele beroepen, moeten testers, naast kennis van de verschillende vakgebieden, veel contact hebben met de professionals op deze terreinen. Door de testers niet af te zonderen sla je twee vliegen in één klap: de testers lijken belangrijk en ze hebben veel contact.

6. **Sta achter de testers.** Een tester ligt altijd onder vuur; hij is vaak de brenger van slecht nieuws. Wanneer een defect is gevonden, kan de betreffende programmeur dit opvatten als een slechte beoordeling van zijn werk. Het is heel belangrijk dat het management achter de testers staat. (Al mag ook van de tester verwacht worden dat hij/zij op een beschaafde manier communiceert).

7. **Geef testers de ruimte.** Laat niet pas op het allerlaatste moment onder grote (tijds)druk testen.

8. **Laat testers door testers beoordelen.** Alleen een andere tester kan het werk van een tester beoordelen.

9. **Beloon testers gepast.** Een hedendaagse trend is om testers, naast een vast salaris, een variabel salaris in de vorm van een bonus te geven. De hoogte van dit variabele deel wordt afhankelijk gesteld van het behalen van bepaalde doelen. Als het halen van de deadline van een project een voorwaarde is, dan is dit voor de tester (die natuurlijk vaak zijn werk pas aan het einde van het project doet) geen reëel criterium. Testers moeten op een andere manier beloond worden.

10. **Zet testen op de agenda van het management.** Veel mensen vergeten dat testen een belangrijk instrument kan zijn voor het management. Met deze activiteit kan de kwaliteit bewaakt worden, maar kan ook de kwaliteit van het organisatieonderdeel gemeten worden.

Deze tien geboden respecteren kost tijd en het zal niet van de ene op de andere dag lukken. Maar al lukt het alleen maar om één, misschien zelfs twee of drie geboden te volgen... Dit zal meteen effect hebben op de testers in de organisatie en de manier waarop zij bekeken worden.

Alleen leven volgens de geboden is niet voldoende; ze moeten ook verkondigd worden. Daar ligt een taak voor de testers zelf. Er moet dus nog veel werk verzet worden om het testvak een beter imago te geven. Ooit komt echter de dag dat de waardering die de testers toekomt, hun ook werkelijk ten deel zal vallen.

7.9 Roll-out

Een onderwerp dat volgens sommigen meer bij implementatie hoort, is de wijze van invoering. In dit boek behandelen we het bij het onderdeel inrichtingsplan, maar er is zeker discussie mogelijk. Waar geen discussie over mogelijk is, is dat de invoering van het systeem een zaak is waarover een weloverwogen besluit moet worden genomen.

Index

big bang
gefaseerde invoering
sterfhuisinvoering
parallelle invoering

In het algemeen worden vier methoden onderscheiden om een nieuw systeem in te voeren:

1. **Big bang** of **flits.** Bij een zogenoemde **big bang** of flits wordt in één keer omgeschakeld. Deze methode vereist natuurlijk wel de absolute garantie dat alles naar behoren werkt. Er is geen tijd of gelegenheid om de kinderziekten er langzaam uit te halen. Deze methode is in principe niet duur; er hoeft geen dubbel werk gedaan te worden, maar 'de flits' zelf kan kostbaar (en hectisch) zijn. De vraag is wel gerechtvaardigd of het bij een netwerk mogelijk is om – vanuit het oogpunt van de klant – op vrijdag het kantoor te verlaten en er maandag weer binnen te komen met een geheel nieuw netwerk operationeel. Bij een softwarematige omschakeling kan dit vaak wel.

2. **Gefaseerde invoering.** Bij een dergelijke invoeringsmethode wordt geleidelijk overgeschakeld. Bij een netwerk betekent dit dat bijvoorbeeld afdeling voor afdeling naar het nieuwe systeem wordt overgegaan. Dat moet natuurlijk wel mogelijk zijn. Als het om een nieuw informatiesysteem gaat, is het wat lastig als de ene helft met het oude systeem (inclusief database etc.) werkt en de ander met een nieuw.

3. **Sterfhuis.** Bij een **sterfhuisinvoering** wordt het oude netwerk of informatiesysteem niet afgedankt. Alle nieuwe gegevens komen echter op het nieuwe systeem. Dit betekent dat het lang kan duren voordat het nieuwe volledig is ingevoerd. Een optie als deze wordt bij een informatiesysteem, netwerk of ander ICT-product eigenlijk zelden gebruikt; daarbuiten wel.

4. **Parallel.** De duurste maar ook de veiligste oplossing is **parallel invoeren.** In dat geval blijft het oude systeem in gebruik en wordt het nieuwe 'ernaast' gezet. Bij een informatiesysteem betekent dit dat gedurende deze periode alle data tweemaal beschikbaar is, maar ook dubbel moet worden bijgehouden. Bij iets als een netwerk zal een dergelijke invoering zelden plaatsvinden, al was het alleen maar omdat niet op elke werkplek plaats is voor twee computers, niet in elk pand twee serverruimten beschikbaar zijn, en het leggen van kabels naast kabels over het algemeen als minder zinvol wordt beschouwd.

7.10 Conversie

Een onderwerp dat in het implementatieplan zeker aandacht verdient is de **conversie** van de 'oude' situatie naar de nieuwe. Deze conversie heeft niet alleen betrekking op data, maar kan op allerlei zaken slaan. Zo moeten ook bijvoorbeeld onderhoudsprocedures tegen het licht gehouden worden. In andere situaties kan het nodig zijn dat programma's of scripts geconverteerd worden. In een UNIX omgeving is het na een upgrade een goed idee om alle scripts na te lopen, omdat er ten gevolge van kleine versieverschillen problemen kunnen ontstaan.

Het **conversieplan** maakt dus deel uit van het implementatietraject. In dit plan staat alles beschreven wat geconverteerd moet worden. Tevens wordt aangegeven waarom dat moet, hoe dat moet, welke tijd ervoor nodig is, wanneer het moet en wie het doet.

7.11 Beheer

Het eigenlijke **beheer** behoort feitelijk niet tot het implementatiedomein, maar wel het opzetten van een **beheerstructuur.** Als zo'n structuur tijdig is opgezet, kan gelijk na de implementatie het beheer volgens die structuur plaatsvinden. De beheerprocedures volgen voor een deel uit de conversie en zullen voor een deel nieuw zijn. Essentieel is natuurlijk wel dat beheer het gebruik dient. Het beheerhoofdstuk in het implementatieplan schetst de contouren van het toekomstige beheer.

Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER-PROCES
De benodigde en gewenste architectuur van het netwerk.	
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

conversie
conversie
beheer
beheerstr

Een wijd
lijkt te zij
gegevens
Voor con
zoals op
ICT: Garb
(GIGO).

Index

implementatieplan
primaire processen
secundaire processen

Het **implementatieplan** kunnen we dus zien als een generiek plan waarin de implementatiefase op hoofdlijnen wordt beschreven. In de inhoud komen we tegen:
- doel en doelgroep;
- op te leveren producten;
- taakomschrijving;
- verantwoordelijkheden;
- activiteiten: wie doet wat?;
- risico's en afhankelijkheden;
- planning, inclusief mijlpalen.

In de praktijk blijken succesvolle implementaties vaak afhankelijk van de volgende factoren:
- of de toekomstige gebruiker een rol in het implementatieproces heeft;
- of er een heldere scheidslijn is vastgelegd tussen het punt waar de verantwoordelijkheid van de projectorganisatie eindigt en die van de bestaande organisatie begint;
- of het management voldoende ondersteuning biedt;
- of één project niet te complex is (desnoods moet een project in deelprojecten worden gesplitst);
- hoe de kwaliteit van het management van het implementatieproces is.

Onder een complex project verstaan we hier niet alleen een moeilijk project. Ook de volgende zaken beïnvloeden de complexiteit van een project:
- omvang van het project;
- structuur van het project en/of de omgeving waarbinnen het gerealiseerd moet worden;
- aantal betrokkenen;
- ervaring met de te gebruiken technologie;
- complexiteit of omvang van de primaire of ondersteunende processen.

Primaire en secundaire processen

Het draait in bedrijven natuurlijk altijd om de **primaire processen**. Deze primaire processen worden door **secundaire processen** ondersteund. Een netwerk zal altijd een secundair proces zijn. Geen enkel bedrijf verdient met alleen zijn netwerk geld. Het netwerk moet dus de primaire processen (mede) ondersteunen. Wat zijn voor de meeste bedrijven nu eigenlijk primaire en secundaire processen?

Kenmerken van primaire processen zijn:
- van levensbelang voor de organisatie;
- aandacht van het management op het allerhoogste niveau;
- carrières staan op het spel;
- de gehele organisatie is betrokken.

Kenmerken van secundaire processen zijn:
- beperkte reikwijdte;
- aandacht verantwoordelijke manager(s);
- soms van levensbelang voor organisatie (bijvoorbeeld factureersysteem).

De secundaire processen ondersteunen het primaire proces. Ze scheppen voorwaarden waaronder het primaire proces optimaal kan functioneren. Het zijn de secundaire processen die eventueel voor outsourcing in aanmerking komen.

Valkuilen voor een succesvolle implementatie zijn dat:
- de uiteindelijke kosten vaak een pijnlijke verrassing zijn (zowel de ontwikkelkosten als de beheerkosten vormen hierbij een potentieel probleem);
- de planning vaak te optimistisch is.

Deze twee kwesties bepalen of het ontwikkel- en implementatietraject zinvol is geweest.

Kort sa
het prir
verdien
busines

2. Waarom is implementeren vaak een taak van de facilitaire dienst of een facilitair bedrijf?

3. Het opleiden van werknemers wordt vaak gezien als een onderdeel van het creëren van draagvlak voor acceptatie. Licht dat toe.

4. Welke vier vormen van roll-out ken je en wat zijn van elke vorm de belangrijkste eigenschappen?

5. Licht met enkele voorbeelden toe waarom ook procedures geconverteerd moeten worden bij het vervangen van een netwerk.

7.12.2 Opdrachten

1. Zoek een voorbeeld van een implementatie van een netwerk (uit je stage, je school, je bijbaan o.i.d.) en schets de projectorganisatie die daar is gehanteerd.

2. Je bent projectleider bij de inrichting van een nieuwe server in een klein bedrijf met twaalf werknemers. Schrijf een implementatieplan.

3. Je bent projectleider bij de inrichting van een extra applicatieserver (naast de twee andere) in een grote onderneming (500 werknemers). Op deze server gaat het CRM-systeem draaien dat nu op een van andere twee staat en voor veel belasting zorgt. Alle afdelingen gebruiken dit pakket. Het gaat om:
   - Verkoop
   - Research and development
   - Productie
   - Personeelszaken
   - Facilitaire dienst

   Beschrijf de gewenste projectorganisatie alsmede de rollen, taken en verantwoordelijkheden van de deelnemers aan de projectorganisatie

Architectuurontwerp

9.1 Inleiding

In de laatste paragrafen van het vorige hoofdstuk hebben we gegevens verzameld en geanalyseerd die gebruikt worden om de architectuur van een omvangrijk netwerk te ontwerpen. Daarna moeten de stappen doorlopen worden om de functionaliteit te realiseren en de (systeem)software te kiezen.

In dit hoofdstuk gaan we in op de architectuur.

9.2 Aanwijzingen voor de leerling

Bij het ontwerp van een groot netwerk kunnen kleine beslissingen in het beginstadium van het ontwerp grote gevolgen hebben voor het uiteindelijke netwerk. Dit betekent dat je bij het ontwerpproces niet zorgvuldig genoeg te werk kan gaan.

In dit hoofdstuk gaan we in op het fysieke en logische ontwerp van grote en kleine LAN's en WAN's. Verder behandelen we kort de redenen van het bestaan van legacy systemen en de wijze waarop ze in een (later) LAN gehandhaafd kunnen worden.

9.3 Praktijkopdracht

Het ontwerp van de architectuur is de structuur waarop het latere netwerk zal gaan draaien. Het gebouw waar jij je opleiding volgt, maakt deel uit van een groter geheel.

Binnen de organisatie bestaat al een tijdje het idee dat de dienstverlening wel goed is, maar dat deze wat minder zou moeten kosten. Het College van Bestuur heeft daarom een adviesbureau in de arm genomen. Jij werkt daar toevallig.

Onderzoek hoe op dit moment de (netwerk)structuur er uit ziet. Daartoe interview je bij voorkeur iemand van de afdeling infrastructuur van je ROC. Gebruik dit hoofdstuk om een lijst met te stellen vragen te ontwikkelen, die je bij dit interview als leidraad gebruikt. Formuleer vervolgens een advies om dezelfde dienstverlening op een even goede manier, maar goedkoper, te realiseren.

9.4 Ontwerpen

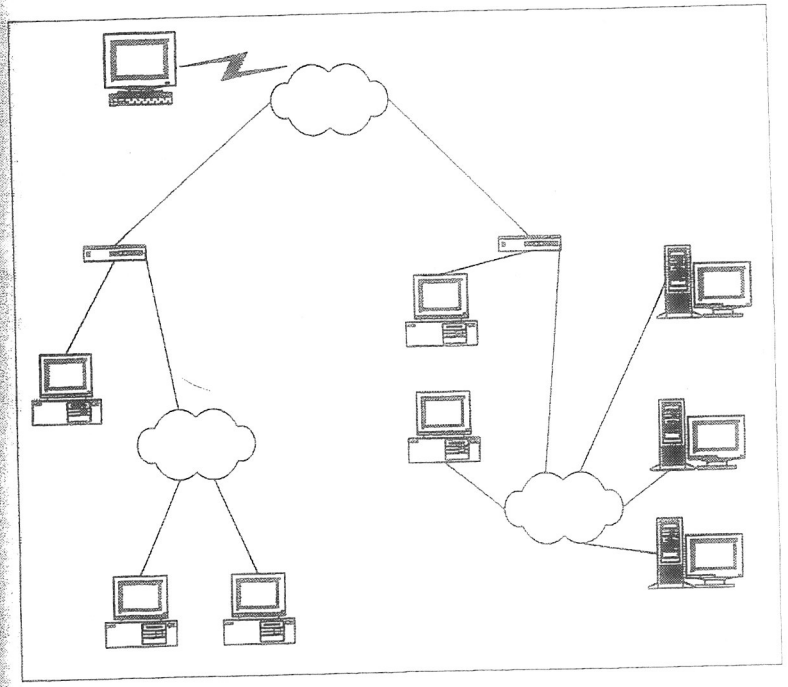
Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER-PROCES
De benodigde en gewenste architectuur van het netwerk.	
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

Als de requirements-analyse is afgerond, zal de ontwerper een globaal plan voor het netwerk maken. We noemen dit ook wel de (onderliggende) **architectuur** van het netwerk. Dit ontwerp heeft dan betrekking op de verbindingen tussen de knooppunten van het nieuwe netwerk. Details als servers en inrichting van locaties zullen hier nog buiten beschouwing worden gelaten. In het gekozen voorbeeld wordt nu het WAN tussen de locaties ontworpen.

De vragen waar de ontwerper zich voor gesteld ziet zijn:
- Hoe realiseer ik een ontwerp voor de architectuur op dit niveau van het netwerk?
- Hoe laat ik zien dat dit ontwerp recht doet aan de vereisten?
- Hoe bepaal ik met een redelijke mate van nauwkeurigheid de kosten van het ontwerp?
- Hoe geef ik aan waar nog eventuele bottlenecks zitten? Wat moet nog opgelost worden?

Vier belangrijke aspecten in dit stadium zijn:
1. de kosten van de diverse mogelijke technologieën;
2. performance (network delay en doorvoer);
3. betrouwbaarheid;
4. potentiële risico's (bijvoorbeeld door gebruik van nog onvoldoende in de praktijk geteste technologie).

De fysieke layout van het netwerk komt nu aan de orde. In het geval van ons WAN zijn dat de **verbindingen** tussen de locaties



Figuur 9.1 Netwerkontwerp op WAN-niveau.

Ook in het geval dat het niet om een WAN maar om een LAN gaat, zal de ontwerper zich eerst buigen over de vraag welke topologieën en technologieën hem ter beschikking staan. Het voornaamste verschil zijn de beschikbare technologieën: voor connecties binnen een WAN zijn andere technologieën voorhanden dan voor een LAN.

De kosten van WAN-verbindingen moeten niet onderschat worden. Een dienst als KPN Eurorings hanteerde in augustus 2003 de volgende tarieven:
- Een 64 kbps internationale verbinding tussen Amsterdam en Frankfurt kost per maand circa € 900 en een 2 Mbps verbinding rond de € 3000.
- Vergelijkbare verbindingen vanaf Amsterdam naar New York zijn respectievelijk circa € 1800 en € 5000 per maand.

De verbindingen in ons WAN zijn van zo'n type dat waarschijnlijk voor externe leveranciers van dataverbindingen zal worden gekozen. Als we als voorbeeld een campusnetwerk zouden hebben genomen, was het goed mogelijk dat de verbindingen tussen de diverse locaties op de campus in eigen beheer gerealiseerd konden worden.

Index

LAN
Ethernet
backbone
10BaseT-netwerk
100BaseT-netwerk
busnetwerk
Token Ring
MAU
sternetwerk

Knipsel

Een MAU is een Multi Access Unit.

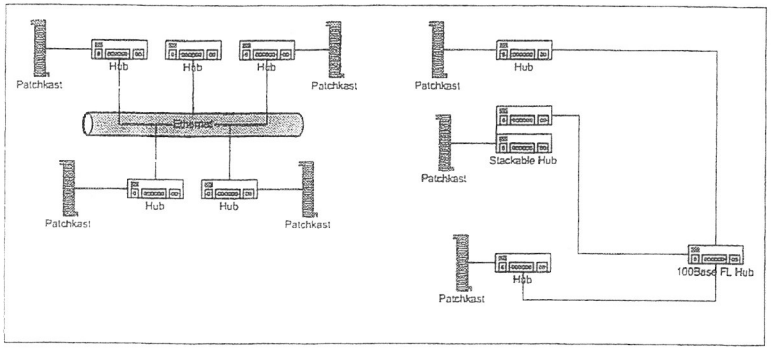
9.5 Fysiek ontwerp

9.5.1 Kleine LAN's

In kleine LAN's zijn er in theorie vele manieren om de structuur te implementeren. In de praktijk worden er eigenlijk maar twee gebruikt: Ethernet en Token Ring.

Ethernet

In het geval van een Ethernetwerk kan voor twee typen **backbone** gekozen worden; zie figuur 9.2.

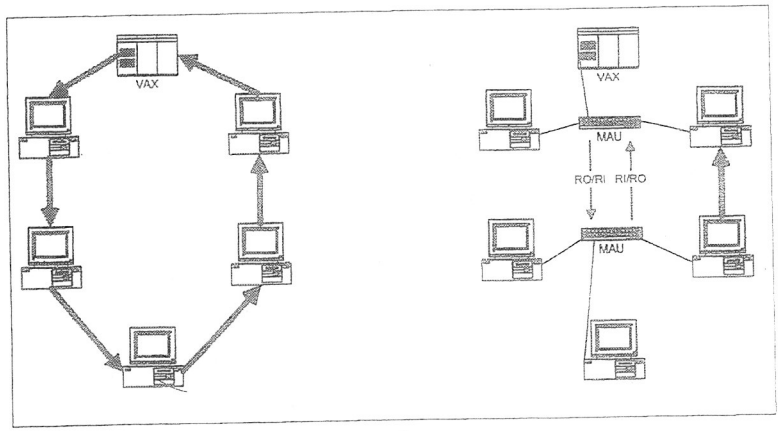


Figuur 9.2 Ethernet-backbones.

Het **10BaseT**- en **100BaseT-netwerk** hebben beide fysiek een stervorm. Logisch gezien zijn het echter **busnetwerken**. Er kan voor een busstructuur op backbone-niveau gekozen worden, of voor een ster. Er zijn hier verder hubs en twee stackable hubs gebruikt, maar switches zijn natuurlijk ook mogelijk (afhankelijk van de situatie). We gaan er wel van uit dat deze netwerken de performance bieden die in de user requirements zijn vastgelegd. Eventueel kan voor de backbone natuurlijk ook voor glasvezel worden gekozen.

Token Ring

Een Token Ring netwerk wordt fysiek gerealiseerd met behulp van **MAU's**. Deze worden via de Ring In- en Ring Out-connectors met elkaar doorverbonden en vormen dan verder elk op zich een fysiek **sternetwerk**. Logisch gezien gaat het om een sternetwerk.



Figuur 9.3 Token Ring, logisch en fysiek ontwerp.

9.5.2 Core-ontwerp van WAN's

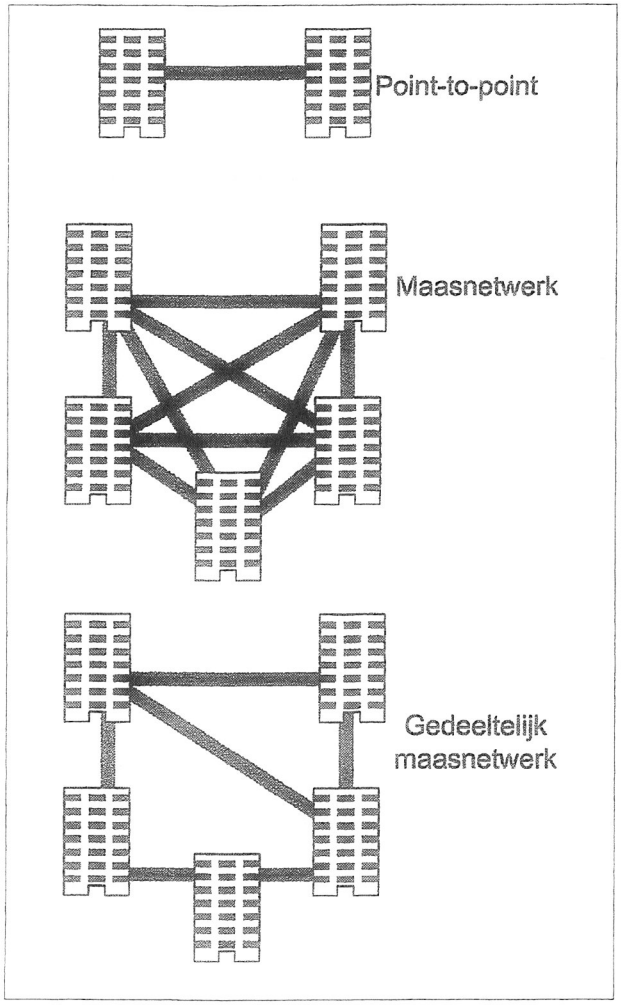
Het ontwikkelen van het informatiesysteem en het functionele ontwerp van het netwerk.	HET DOCUMENTEER-PROCES
De benodigde en gewenste architectuur van het netwerk.	
De hardware die nodig is om de gewenste functionaliteit te garanderen.	
De benodigde (systeem)software.	
Het realiseren van de gewenste functionaliteit.	
Het praktische gebruik.	
Het beheer en de beheerorganisatie.	

Voor WAN's is de keuze wat gevarieerder dan voor LAN's. Een WAN is vaak aangewezen op relatief trage verbindingen tussen de LAN's. Het zodanig ontwerpen dat er een minimale hoeveelheid data tussen de locaties vervoerd hoeft te worden, is kostentechnisch een must. Dat criterium is bij een LAN-ontwerp nauwelijks van belang. Daar kan vaak tegen relatief geringe kosten een vertienvoudiging van de bandbreedte worden geregeld. Bij een WAN is dit ondenkbaar (lees: onbetaalbaar).

Om de koppelingen te realiseren zijn meerdere technologieën beschikbaar:

- bridges
- switches
- routers

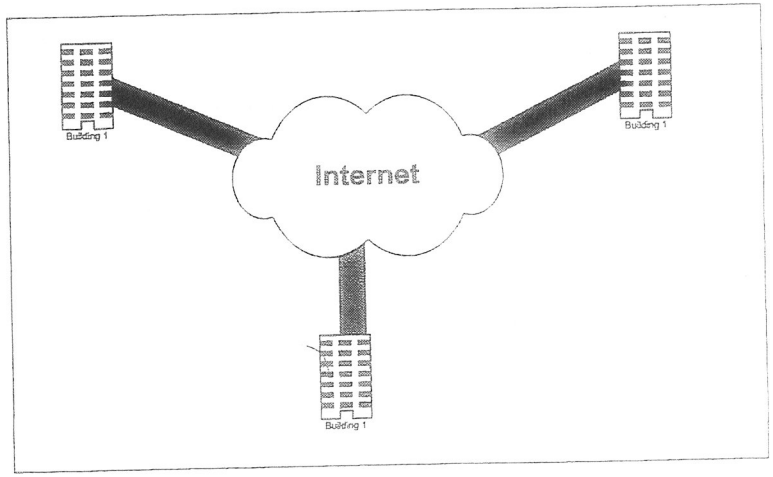
Deze apparatuur is in andere delen van je opleiding aan de orde geweest. VLAN's, worden de laatste jaren vaak gebruikt om binnen het LAN (maar ook op hogere niveaus) structuur aan te brengen. Je hebt er in paragraaf 6.7 over kunnen lezen. Alle genoemde technologieën zijn zowel voor Token Ring als Ethernet te gebruiken.



Figuur 9.4 WAN.

Binnen een WAN zijn diverse vormen van interconnectie tussen de locaties mogelijk; in figuur 9.4 zijn er een aantal getekend. In het geval van twee locaties volstaat een eenvoudige **point-to-point verbinding**. Bij een groter netwerk (meer locaties) kan elke locatie met elke andere worden verbonden. We krijgen dan een **maasnetwerk**. Dit is bij grote netwerken een dure, maar wel heel betrouwbare, oplossing. In de praktijk zie je dat netwerken vaak gedeeltelijk maasvormig worden uitgevoerd. Alle belangrijke locaties worden met elkaar verbonden. Dat betekent dat er tussen belangrijke locaties altijd (tenminste: bij maximaal één storing) een verbinding opgebouwd kan worden.

Een optie die ook wel wordt gekozen is weergegeven in figuur 9.5.



Figuur 9.5 Internet als connectie.

Als elke vestiging een internetverbinding heeft, kan daarover een VPN (**Virtual Private Network**) worden gelegd. Het verdient dan natuurlijk aanbeveling om met de ISP een goede SLA af te sluiten. In al deze gevallen moet vervolgens natuurlijk nog een fysieke connectie worden gekozen. Ontwikkelingen gaan nog steeds erg snel en de hier gegeven informatie zal waarschijnlijk snel verouderd zijn, maar de volgende services en snelheden zijn op dit moment (begin 2004) beschikbaar:

Index

verbinding, keuze
MTU
CBR
Constant Bit Rate
Quality of Service
QoS
Committed Information Rate
CIR

Knipsel

MTU staat voor: Maximum Transfer Unit, oftewel maximale pakketgrootte.

Technologie	Snelheid	Opmerkingen
PSTN Dial up	300 bps - 56 kbps	Normale telefoonmodem. Snelheid afhankelijk van verbinding. Bij hogere snelheden downstream kanaal groter dan upstream (asynchroon).
ISDN Dial up	64 kbps - 2 Mbps	2*64 kbps of 30*64 (24 in de USA).
X.21	64 kbps of 56 kbps	
Digital point-to-point	9.6kbps - Gbps	In de praktijk vanaf 64 kpbs tot 2 Mbps (E1) (1,5 Mbps in de USA T1). Bij hogere snelheden vaak glasvezel met SDH- of SONET-technologie.
X.25	2.4 kbps - 2Mbps	Niet veel in gebruik als LAN-interconnectie.
Frame Relay	64 kpbs – 2 Mbps	Vaak als gateway naar ATM. Ontwerper moet zelf per PVC (Permanent Virtual Circuit) parameters vastleggen.
ATM	2 Mbps – 2,4 Gbps	
IP VPN	64 kpbs - Gbps	Relatief nieuwe (veelbelovende) service.

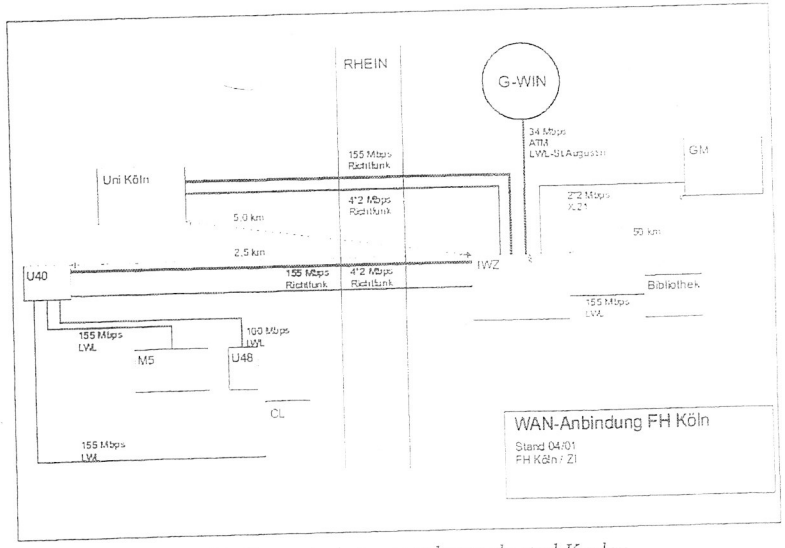
Belangrijke vragen bij de keuze van het type **verbinding** zijn:

- Welke bandbreedte is nodig?

- Hoe groot zijn de datapakketten die verzonden moeten worden?
  Als de **MTU** kleiner is dan de te verzenden pakketgrootte, heeft dit (in verband met overhead door fragmentatie etc.) consequenties voor de bandbreedte. Vaak kan dit door 'tuning' optimaal ingesteld worden.

- Is deze bandbreedte constant nodig of alleen op piekmomenten?
  Dat kan in kosten nogal uitmaken. Als van ATM een constante bandbreedte wordt vereist, kan een **CBR**-verbinding (**Constant Bit Rate**) worden afgesproken; overigens wel tegen een forse (meer)prijs. Als de verbinding niet constant dezelfde snelheid hoeft te hebben – of delen van de dag zelfs helemaal niet nodig is – kan een ander verbindingstype worden gekozen. Het centrale begrip is hier '**Quality of Service**' (**QoS**). De meeste verbindingen garanderen een **Committed Information Rate** (**CIR**), die altijd beschikbaar is, met daarbij de belofte (niet de garantie) dat de verbinding een (groot) deel van de tijd sneller is. Door een protocol te gebruiken dat in staat is pakketten weg te gooien als de bandbreedte even tot de CIR zakt, kan dit opgevangen worden. Om informatieverlies tegen te gaan moet daarboven dan wel een protocol gebruikt worden dat een betrouwbare end-to-end communicatie garandeert (bij-

- Hoe vaak en hoe lang is de verbinding in gebruik?
  Vaak worden verbindingen voor 24 uur per dag gedurende zeven dagen per week gehuurd. Het is goed mogelijk dat een verbinding alleen overdag nodig is. Als de gewenste bandbreedte laag is, kan een gewone inbelverbinding soms volstaan (tegen een fractie van de kosten). Een verbinding die alleen 's nachts nodig is, kan misschien worden gedeeld met een bedrijf of organisatie met een tegenovergestelde wens.



Figuur 9.6 De verbindingen in het netwerk van de stad Keulen.

9.5.3 Legacy-systemen

Met legacy-systemen worden bedoeld: systemen die al een functie binnen de organisatie hebben en die moeten blijven draaien, maar waar het netwerk eigenlijk niet voor ontworpen is. Vaak gaat het om systemen die zo'n cruciale rol in de bedrijfsvoering spelen dat ze niet afgeschaft kunnen worden. Je ziet bijvoorbeeld wel eens dat er ooit een applicatie op een minicomputer is ontwikkeld die de complete personeelsadministratie omvat. Je kunt dan niet eenvoudig zeggen dat daar even een nieuwe applicatie voor moet komen. Je wilt een dergelijke applicatie toch ook op het nieuwe netwerk aan de gebruikers aanbieden.

Het kan ook gaan om een veel groter systeem, waarmee het bedrijf een verbinding heeft. Als je een nieuw netwerk voor KLM/Air France zou

Index

Scrap
Trap
Wrap
logisch ontwerp
uid
MAC-adres
SRB

Assist

Een uid is een Unit Identifier.

Knipsel

Dit is volgens sommigen de reden dat Ethernet-kaarten tegenwoordig vaak een 'instelbaar' MAC-adres hebben. Dit betekent dat in een SNA-omgeving, als er een netwerkkaart vervangen moet worden, alleen het MAC-adres hoeft te worden ingesteld zonder dat de configuratie gewijzigd hoeft te worden.

teem dat alle luchtvaartmaatschappijen onderling gebruiken tegelijkertijd mee wordt vernieuwd volgens jouw normen.

Er zijn diverse manieren om legacy-systemen over een LAN te ondersteunen:

- **Scrap.** Als een legacy-systeem aan het eind van zijn levenscyclus komt, kan er gekeken worden of in de ontwikkeling van het LAN/WAN tegelijkertijd een mogelijkheid is voor het vervangen van deze applicatie. Vervangen kan inhouden: het aanschaffen van een nieuwe applicatie, of het implementeren van de functionaliteit van de legacy-applicatie in één of meer van de nieuw te ontwikkelen applicaties.

- **Trap.** Laat de applicatie gewoon draaien, reserveer tijd en geld voor het onderhoud en laat voldoende van het oude netwerk (software en hardware) in stand om de applicatie te ondersteunen.

- **Wrap.** Een optie kan zijn om de legacy-systemen te handhaven, maar te kijken of het mogelijk is een connectie met het nieuwe netwerk te maken en ze via dat netwerk te benaderen. Misschien kan hun protocol 'ingepakt' ('gewrapped') over het netwerk en is het implementeren/ontwikkelen van enige protocolconverters voldoende.

9.6 Logisch ontwerp

In de vorige paragraaf is het netwerk fysiek ontworpen. In deze paragraaf gaan we verder met het **logische ontwerp.** Alle items (computers, routers, enzovoort) moeten op de een of andere wijze een unieke identificatie krijgen. Deze **uid**'s worden later onder meer bij het beheer gebruikt

Er zijn diverse wijzen om dit te aan te pakken:

1. Op basis van het MAC-adres. In het oude IBM mainframe-tijdperk kon netwerkapparatuur op basis van het **MAC-adres** worden ingedeeld. Aan de hand van dit adres kan in een modern netwerk de DHCP-server ingesteld worden en deze kan dan IP-adressen uitdelen op basis waarvan stations geïdentificeerd zijn.

2. Token Ring netwerken maken vaak gebruik van 'source routing bridge technology' (SRB) om pakketten rechtstreeks door meerdere LAN-segmenten heen te vervoeren. Bij deze technologie kennen netwerkbeheerders aan elke ring een (uniek) ringnummer toe. Bridges zijn ook genummerd, maar een bridge heeft alleen een ander nummer dan 1 als meer dan één bridge twee ringen verbindt. Dit laatste kan bijvoorbeeld voorkomen als er redundante verbindingen zijn. Op deze wijze wordt het verkeer van bridge tot bridge gezonden tot de bestemmingsring bereikt is. Het algoritme is dus eigenlijk:
   - Als deze ring mijn nummer heeft, dan ga ik op zoek naar mijn bestemmingstation;
   - zo nee, dan ga ik naar 1;
   - als dat niet werkt dan zijn er redundante verbindingen en wordt teruggevallen op standaard routeringsprotocollen die bij de technologie horen.

3. IP is natuurlijk een voor de hand liggende optie. Welke IP-adresreeks kan gebruikt worden? Is er een A-, B- of C-adres? Of toch CIDR? Is er sprake van NAT? Zal er een proxy worden ingezet? Is er een eigen namespace? Is er een eigen nameserver nodig? Hoe wordt deze geconfigureerd? Waar is dan de secundaire nameserver? In dit geval moet er, zoals al eerder is betoogd, natuurlijk ook een nummerplan gemaakt worden. Aangegeven moet worden welke **IP-adressen** en -adresreeksen waarvoor zijn gereserveerd. Bovendien is van belang hoe deze zo verdeeld worden dat een logisch netwerk ontstaat, dat ook nog onderhoudbaar en uitbreidbaar is. (Let op een logische, haalbare en vooral efficiënte routering!)

4. Is er sprake van een VLAN? Op basis waarvan worden stations in een VLAN geplaatst en hoe wordt dit verder verwerkt?

5. Tegenwoordig worden in een netwerk steeds vaker **draadloze stations** ondersteund. Volgens de standaard **IEEE 802.11b** (11 Mbps) of **IEEE 802.11a** of g (54 Mbps) worden **wifi**-stations aangesloten. Ook deze moeten ergens in het LAN opgenomen worden. Vaak wordt uit beveiligingsoogpunt een extra authenticatie vereist (bijvoorbeeld **IEEE 802.1X**) en plaatsing in een VLAN (**IEEE 802.1Q**). Dit dient om te voorkomen dat elke willekeurige gebruiker met een laptop en een wifi-kaartje zomaar internettoegang heeft. Meestal eist de ISP dat elke actie op het internet aan een individuele gebruiker te koppelen is. Dan kun je niet 'zomaar' een open DHCP-server neerzetten die aan 'iedereen' een IP-adres geeft.

6. TCP/IP is tegenwoordig ook bij Novell de default en te prefereren instelling. Daarom kan er tegenwoordig ook als het NOS van **Novell NetWare** gebruikt gaat worden, voor het protocol TCP/IP worden gekozen. Dan kunnen de adressering en naming daarvan gebruikt

Index

IPX/SPX
routering
nummerplan

Attentie

Op de verschillen tussen de beide belangrijkste routeringsprotocollen (distance vector en link state) gaan we hier niet nader in, noch op OSPF-achtige structuren. Deze zijn al in een andere context aan de orde geweest.

worden. Wordt toch voor **IPX/SPX** gekozen, dan wordt het MAC-adres gebruikt door IPX en moet elk netwerksegment een eigen (uniek) netwerknummer krijgen. Dit vereist zorgvuldig configureren, zeker omdat de default-instellingen van NetWare eigenlijk niet correct zijn voor een groot, complex netwerk.

7. **Routering.** In dit stadium moet de basisroutering worden vastgelegd. Wordt alles dynamisch gedaan? Welke statische routes worden vastgelegd? Wordt er in (een deel van) het netwerk source routering toegepast?

Op basis van deze en andere argumenten kan vervolgens een logisch ontwerp van het netwerk gemaakt worden. Daarmee komt alle apparatuur op zijn logische plaats in het netwerk terecht. Hoewel je kunt verdedigen dat het logisch ontwerp losstaat van het latere fysieke ontwerp, is dat natuurlijk niet zo. Als je bijvoorbeeld een **nummerplan** maakt omdat het netwerk op TCP/IP gaat draaien, dan doe je dat natuurlijk met de huidige fysieke structuur in gedachten, zodat je keuzes ook later te implementeren zijn. Ook een VLAN-indeling moet niet alleen logisch zijn maar ook en vooral implementeerbaar.

9.7 Vragen en opdrachten

9.7.1 Open vragen

1. Op welke twee manieren kunnen Ethernet-backbones gerealiseerd worden?

2. a. Wat is een VPN?
   b. Wat kan het belang van een VPN zijn voor een groot corporate netwerk?

3. Is het altijd verstandig om een service provider in te zetten om een connectie tussen vestigingen te realiseren?

4. a. Leg uit wat CIR is en wat CBR is.
   b. Wat is het belang van beide voor een netwerkontwerp?
   c. Beschijf twee situaties waarin je voor een verbinding met een grote CIR zou kiezen, en wanneer je een verbinding met een grote CBR zou prefereren.

5. a. Wat zijn legacy-systemen?
   b. Waarom kunnen deze systemen bij het ontwerpen van een netwerk voor problemen zorgen?

6. Beschrijf de drie manieren om legacy-systemen in een (nieuw) netwerk op te nemen.

7. Volgens welke methode is het logisch ontwerp gemaakt van het netwerk waar jij op school het meest zit?

9.7.2 Opdrachten

1. Ontwerp een fysieke en logische structuur van een netwerk voor een (internationaal) reisbureau.
   a. Het bureau heeft vestigingen in de meeste Europese hoofdsteden alsmede in Sydney, Buenos Aires, New York, Los Angeles en Houston.
   b. Het systeem is verbonden met de belangrijke boekingssystemen van luchtvaart- en hotelmaatschappijen.

Netwerkdocumentatie

Doorreizen

Als je de praktijkopdracht in paragraaf 3 van dit hoofdstuk naar tevredenheid hebt gemaakt, kun je na overleg met je docent doorgaan naar het volgende hoofdstuk.

Netwerkdocumentatie

11.1 Inleiding

Documenteren is om de een of andere reden niet het meest populaire onderwerp binnen de ICT. Toch is het noodzakelijk om het ontwikkelen, de onderhoudsprocedures en configuratiemanagement zorgvuldig vast te leggen. Ook de wijze waarop wijzigingen worden geïnitieerd, al of niet worden goedgekeurd en uiteindelijk worden verwerkt (bij elkaar ook wel samengevat onder de noemer change management) moet zorgvuldig worden beschreven. Documenteren moet als een continu proces gezien worden en niet als een klusje dat na elke activiteit nog even verricht moet worden.

11.2 Aanwijzingen voor de leerling

In dit hoofdstuk bespreken we een methode om het netwerk te documenteren. Na het ontwerp ligt er een compleet pak aan documenten hoe het netwerk is opgebouwd en waarom dit zo gedaan is. Dit is de start voor het zorgvuldig bijhouden van een beschrijving van het netwerk. Dan kan altijd makkelijk opgezocht worden wat waar is, welk probleem zich waar heeft voorgedaan en hoe het moet worden opgelost.

De netwerkdocumentatie bestaat normaal gesproken uit:
- de relevante ontwerpdocumenten;
- een logboek met een beschrijving van alle gebeurtenissen;
- een complete beschrijving van het netwerk met alle configuratiedetails en geschiedenis.

11.3 Praktijkopdracht

Op bijvoorbeeld www.download.com en www.tucows.com staat een groot aantal tools die kunnen helpen bij het documenteren van netwerken. Sommige zijn slechts een uitbreiding voor Visio, maar er zijn ook complete managementpakketten. Een pakket dat ook goed gebruikt kan worden om netwerken te tekenen is DIA. Het is GPL en is te vinden via www.sourceforge.com.

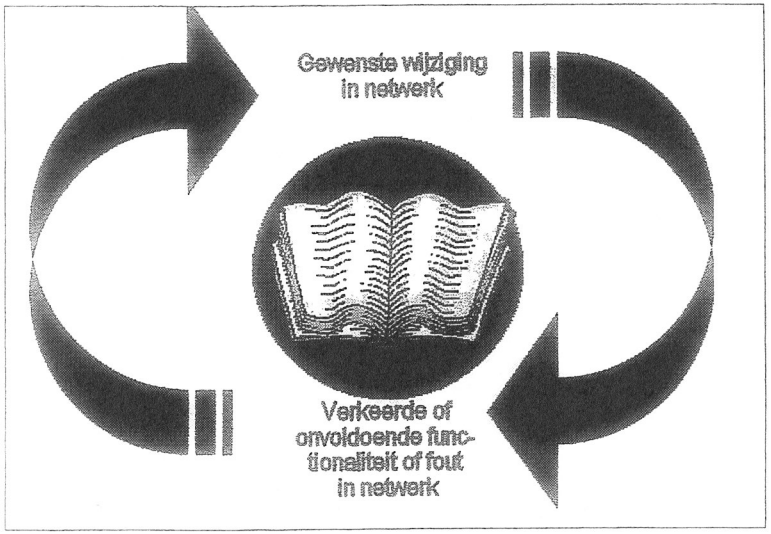
Bespreek in een groepje van drie wat de eisen zijn die je aan een dergelijk pakket stelt en onderzoek minimaal vijf van deze pakketten aan de hand van je eisenpakket. Schrijf er (als groep) een (beredeneerd) advies over voor de directeur ICT.

11.4 Documenteren van netwerken

Een groot deel van het ontwerpproces bestaat uit het onderbouwen en vastleggen van keuzes. Dit hele bouwwerk kan opgevat worden als de start van de netwerkdocumentatie. Gedurende de levensduur moet teruggevonden kunnen worden waarom voor bepaalde (on)mogelijkheden is gekozen.

In deze documenten ligt ook het complete ontwerp vast. In een ideale wereld zou dat voldoende moeten zijn. Een netwerk is in de praktijk echter geen statisch geheel. Al vanaf het begin worden er wijzigingen en aanvullingen op aangebracht. Deze wijzigingen moeten aan de oorspronkelij-

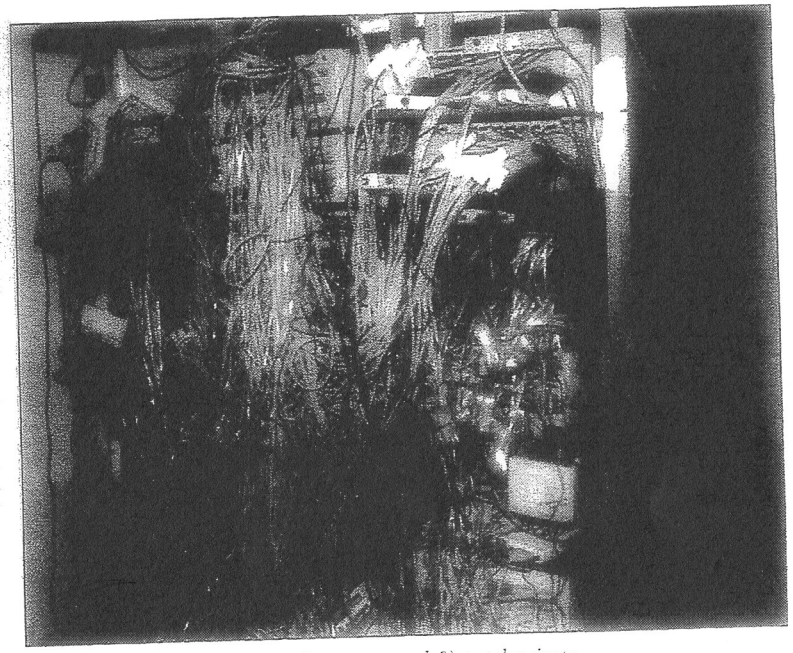
ke documentatie worden toegevoegd. Documenteren moet dan ook als continu proces worden gezien.



Figuur 11.1 Documenteren als continu proces.

Er zijn veel manieren om een netwerk te documenteren. Veel netwerken die op dit moment bij organisaties in gebruik zijn, zijn gegroeid vanuit een relatief eenvoudige situatie, waarbij het beheer door iemand 'erbij' werd gedaan, naar een veel gecompliceerder netwerk, waarbij lang niet alles gedocumenteerd is. Dat is fysiek nog wel op te lossen. Je kunt alsnog een tekening maken van de plaats waar kabels lopen en van de locatie van de apparatuur. Waarom echter bepaalde configuraties zijn zoals ze zijn, is meestal niet meer te achterhalen. In dat soort netwerken weet vaak alleen de beheerder wat waar ligt, waarvoor het dient en hoe het geconfigureerd is. Dat betekent dat als deze 'onder de tram komt' er een echt probleem is.

Andere netwerken zijn goed gedocumenteerd voor wat betreft serverpark en connectie naar buiten, maar niet tot op het niveau van de werkstations. Patchkasten zijn vaak een voorbeeld waar documentatie niet tot op de laatste patch is bijgewerkt. Dat lijkt een klein probleem, maar niet-bijgewerkte documentatie is niet betrouwbaar en daardoor eigenlijk meteen waardeloos.



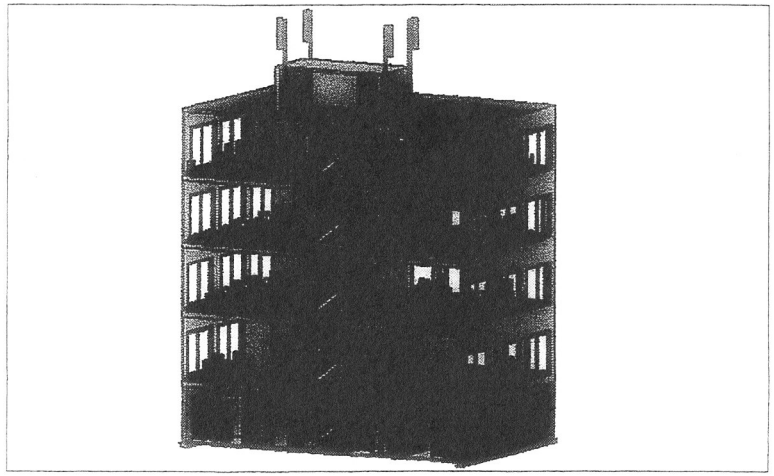
Figuur 11.2 Een volle (ongedocumenteerde?) patchruimte.

Er zijn diverse softwarepakketten in de handel die (een deel van) het documentatieproces uit handen nemen. Vaak kunnen ze via 'in- en uitzoomen' een gedetailleerd beeld van een deel van het netwerk geven, maar ook een globaal beeld zonder dat data vaker moet worden ingegeven. Voorbeelden van dergelijke pakketten zijn:

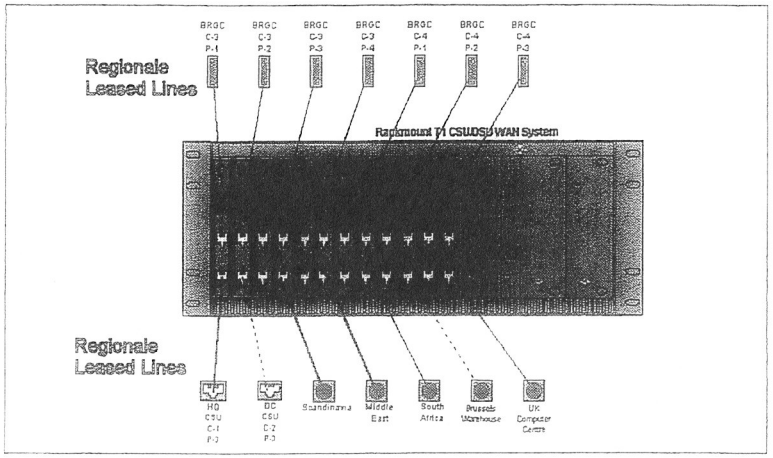
- **NetViz** van NetViz
- **LanMapShot** van Fluke Networks
- **LanFlow** van PaceStar

- Documenteer op verschillende niveaus. Je wilt een 'overview' van het netwerk in je documentatie én je wilt kunnen opzoeken welk kabelnummer op verdieping 8 in kamer 4 ligt én je wilt kunnen zien waar deze is gepatcht.

- Houd je documentatie bij. Verwerk alle veranderingen in het netwerk meteen in de documentatie. Morgen is te laat en volgende week ben je het vergeten. En dan heb je de documentatie juist nodig om die ene fout te vinden! Als in je documentatie de verbinding die de fout veroorzaakt niet bestaat, is het lastig om de fout te vinden.



Figuur 11.5 Beschrijving op het niveau van gebouw en verdieping.



Figuur 11.6 Beschrijving op het niveau van kabel en patch

Bij het standaardiseren van de netwerkdocumentatie is het van belang om intern standaarden vast te stellen. Het is daarbij essentieel dat iedereen binnen de organisatie een eenduidig beeld heeft van wat met een bepaald symbool wordt bedoeld. Gebruik symbolen dus consistent! Het verdient aanbeveling om in een documentatiepakket of een tekenpakket een bibliotheek met standaardafbeeldingen aan te maken.

Het blijft altijd een lastige zaak om te bepalen wat je van apparatuur wel of niet moet documenteren. Er zullen altijd situaties voorkomen waarbij je net dat ene attribuut niet hebt gecatalogiseerd dat je wel nodig hebt. Een (niet uitputtende) lijst attributen om van een **werkstation** te documenteren:

- serienummer;
- fabrikant;
- CPU (type/merk en snelheid);
- ROM-BIOS (source en versie);
- RAM (grootte, snelheid en type);
- diskdrives (aantal floppies, harddisk, cd, dvd, zip; eventueel pen-drive);
- harddisk-capaciteit (in MB of GB, niet beide!);
- adapter cards (display, netwerk, communication);
- adapter card settings (I/O address, IRQ, DMA);
- Network Node Identification (MAC/IP);
- Network Client Software (naam en versie);
- operating system (naam en versie + subversie);
- aanschafdatum (onder meer in verband met upgrades en licenties);
- afloop van de garantie;
- onderhoudsgegevens (per reparatie of call, wat ermee/eraan is gedaan);
- fysieke locatie (gebouw, ruimte, verdieping);
- gebruiker (naam, telefoonnummer e.d.).

Van een **server** sla je het bovenstaande natuurlijk ook op, maar daarbij nog:

- servernaam;
- servertype (file/print/mail e.d.);
- netwerkidentificatie (MAC/IP);
- operating system (versie, subversie en configuratie);
- andere services en hun configuratie;
- protocolstacks (IPX/SPX-IP, NetBIOS, NetBEUI).

patchkast
bekabeling

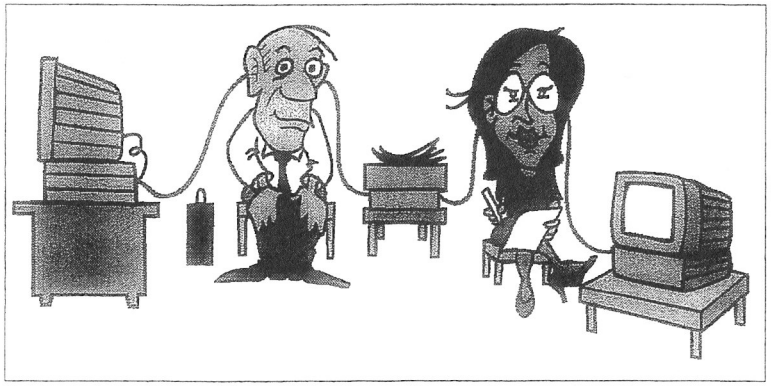
11.5 Documenteren van patchkasten en kabels

Het meeste werk (en eerlijk gezegd ook het meest vervelende) is het documenteren van alle **bekabeling**. Toch is dit een karwei dat goed en zorgvuldig gedaan moet worden. Vaak is er al een kabelnummersysteem in gebruik, dat correspondeert met de nummering in de patchkast. Daarnaast is het dan handig om de volgende zaken te weten:

- LAN-technologie (bijvoorbeeld Ethernet, Token Ring);
- topologie (Frame Relay, 10base2, 1000baseT);
- kabeltype (coax, FTP, SFTP, FDDI).

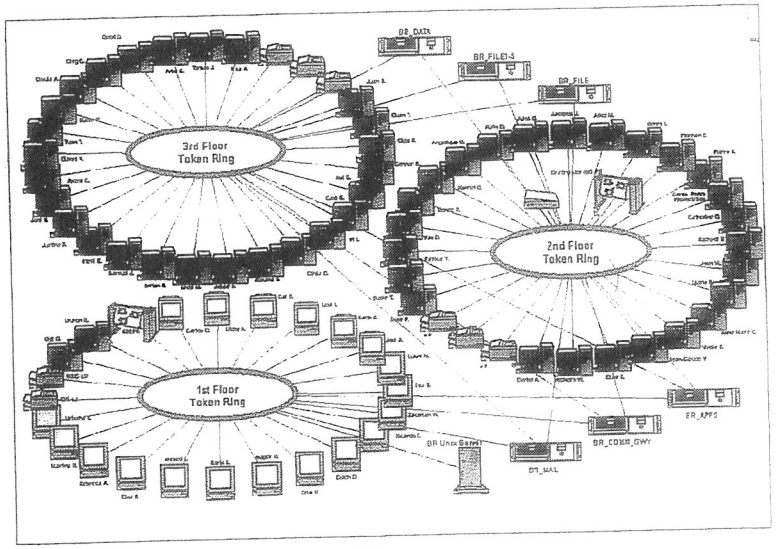
Verder de geografische gegevens:

- kabelnummer;
- van (locatie);
- naar (locatie);
- van apparaat;
- naar apparaat;
- impedantie;
- lengte;
- bandbreedte;



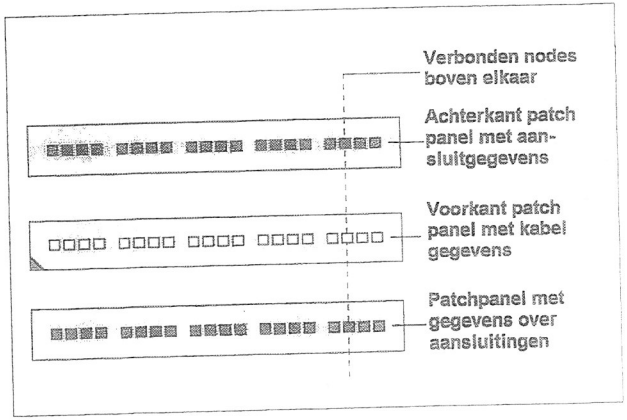
Figuur 11.7 Kabels in LAN's lopen niet altijd even logisch.

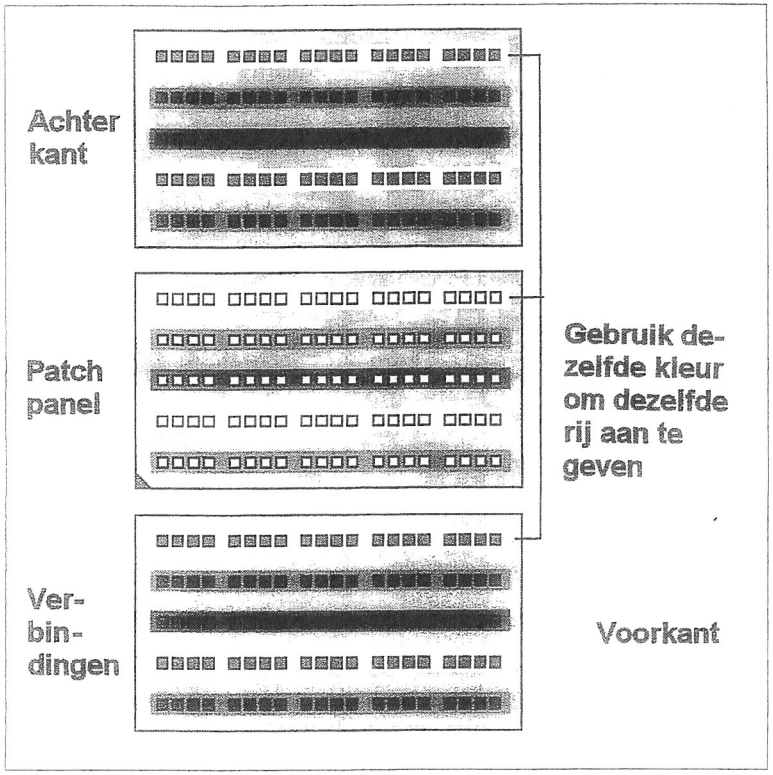
Bijna altijd kan een softwarepakket deze gegevens gebruiken om een 'mooie' grafische 'view' van het netwerk (of deel ervan) te genereren.



Figuur 11.8 Concept-netwerkoverzicht.

Om een patchkast te documenteren zijn diverse technieken voorhanden. Voor welke gekozen wordt, hangt mede af van de mogelijkheden van de gebruikte software. Een manier om patchkasten te documenteren is om van beide kabels – zowel die aan de voorkant als die aan de achterkant – vast te leggen wat er aan de andere kant zit. Daartoe wordt het patchpanel twee keer in de documentatie opgenomen en wordt met kleuren aangegeven welke uiteinden bij elkaar horen. Dit is toegelicht in de figuren 11.9 en 11.10.





Figuur 11.10 Een multi-row patchpanel.

11.6 Conclusie

Als het hele netwerk gedocumenteerd is en deze documentatie ook consequent is bijgehouden en up-to-date is, kunnen beheer en onderhoud sterk vereenvoudigd worden. Het zoeken naar een fout is niet meer te vergelijken met het zoeken naar een speld in een hooiberg, maar wordt een proces van redeneren en controleren. Het aanbrengen van veranderingen in de configuratie is sterk vereenvoudigd. Er hoeft niet eerst uitgebreid gecontroleerd te worden of er geen (ongedocumenteerde) wijziging is aangebracht die de voorgestelde wijziging ongewenst, onnodig of zelfs onmogelijk maakt.

11.7 Opdrachten

1. Voer de praktijkopdracht uit paragraaf 11.3 uit als je dat nog niet hebt gedaan.

2. Naar aanleiding van opdracht 1 heb je een overzicht van vele pakketten. Daarvan is er een het meest geschikt voor je doel. Formuleer voor de andere voor welke situaties/bedrijven/organisaties dat pakket het meest geschikt is. Vat dit samen tot een overzicht.