Afstudeeropdracht:	**Mina-IT @ Groningen**
Document:	procesverslag
Student:	Mina Nabil
Afstudeerbegeleider:	Cobie van der Hoek
Expert:	Nico Huiberts
Datum:	04-10-2010

Referaat

Mina Nabil, afstudeeropdracht, Mina-IT @ Groningen , Mina-IT , Nieuwegein , 4 oktober 2010.

Dit verslag is geschreven als onderdeel van het afstuderen van Mina Nabil voor de opleiding Technische Informatica aan de Haagsche Hogeschool. De afstudeeropdracht “Mina-IT @ Groningen” is uitgevoerd bij het fictieve bedrijf Mina-IT te Nieuwegein, gedurende de periode 8 februari 2010 tot en met 4 oktober 2010.

Descriptoren:

- Afstudeeropdracht
- ASI-Rapport
- Netwerkarchitectuur
- Adviesrapport
- Virtualisatie
- Ontwerpen

Voorwoord

Voor u ligt de scriptie die ter afsluiting dient van mijn opleiding Technische Informatica aan de Haagsche Hogeschool te Den Haag.
De scriptie gaat over IT-netwerken en IT- infrastructuur. Mijn eerste contact met netwerken begon al tijdens mijn MBO opleiding Technische Informatica aan het Mondriaan college te Delft.
Na mijn MBO opleiding besloot ik me te verdiepen in IT-netwerken. Daarom heb ik ervoor gekozen om de opleiding Technische Informatica aan de Haagsche Hogeschool te volgen.
De laatste fase van mijn opleiding is het afstuderen. Helaas kon ik niet afstuderen bij het bedrijf waar ik werkzaam ben omdat wij niet in netwerken zijn gespecialiseerd, maar in Oracle database beheer. Oracle databases zijn helaas geen onderdeel van de opleiding Technische Informatica.
Gelukkig heeft de school mij de kans gegeven om zelf een fictieve opdracht te verzinnen. Dit brengt echter de benodigde moeilijkheden en uitdagingen met zich mee. Het was niet makkelijk om zowel opdrachtgever als uitvoerder te zijn.
Ik wil daarom ook iedereen bedanken die mij heeft geholpen bij het afstuderen, in het bijzonder mijn afstudeercoördinator Michiel Sorber. Michiel stond altijd voor me klaar als ik vragen had en nam altijd de tijd om extra uitleg en feedback te geven.
Ook wil ik mijn verloofde Christina Sadik bedanken. Christina heeft me geholpen met de opmaak van mijn scriptie.
Tenslotte wil ik de Haagsche Hogeschool en de begeleiders bedanken dat zij mij de kans hebben gegeven om een fictieve opdracht te verzinnen en zo toch nog succesvol te kunnen afstuderen.
Ik hoop dat de lezer net zoveel plezier beleeft bij het lezen van mijn scriptie als dat ik heb beleefd bij het samenstellen ervan.

Mina Nabil
oktober 2010

Inleiding

Afstuderen is de laatste fase van mijn TI-opleiding. Tijdens het afstuderen krijgen de studenten de kans om te laten zien wat ze allemaal hebben geleerd tijdens hun opleiding. Samen met de heer Hans de Vreught heb ik besloten om door middel van een fictieve opdracht af te studeren. Hierbij mocht ik van de heer de Vreught zelf bepalen waar de opdracht over ging.
Omdat het van school verplicht is om een opdrachtgever te vermelden, heb ik de naam Mina-IT verzonnen als opdrachtgever.
Aangezien ik netwerken altijd het leukste onderdeel van mijn opleiding heb gevonden, besloot ik om een netwerkopdracht te verzinnen. We hebben op school eerder projecten gehad waarbij er een netwerk ontworpen moest worden. Dit was altijd een klein project, bijvoorbeeld een netwerk voor een basisschool. Ik heb ervoor gekozen om een groot netwerk te ontwerpen. Bij een groot netwerk komen immers veel meer aspecten kijken dan bij een klein netwerk.
Om de afstudeeropdracht nog ingewikkelder te maken, heb ik ervoor gekozen om het te ontwerpen netwerk te koppelen aan de hoofdvestiging van Mina-IT te Nieuwegein (uiteraard is de hoofdvestiging ook verzonnen). Hierdoor werd de opdracht een heel stuk ingewikkelder, omdat ik rekening moest houden met de bestaande architectuur. Ook moest er rekening gehouden worden met de verbindingen tussen beide vestigingen. Dit zijn allemaal aspecten die normaal niet aan bod zouden komen als ik een simpel netwerk zou ontwerpen.
Om mijn adviesvaardigheid te kunnen presenteren, heb ik ervoor gekozen om een adviesrapport te maken voor alle hardware die in het nieuwe netwerk komt. Hierbij zal ik ook de verschillende hardwaremerken en softwareleveranciers met elkaar vergelijken. Tenslotte zal ik ook de verschillende Internet providers met elkaar vergelijken.

Inhoudsopgave

Totstandkoming van het project

In dit hoofdstuk ga ik de huidige situatie beschrijven. Ik besteed aandacht aan de soort omstandigheden waarin dit project zich heeft afgespeeld en de achtergrondinformatie van het bedrijf. Dit zal de lezer helpen om de omstandigheden beter te begrijpen. In dit hoofdstuk kies ik tevens een projectmanagementmethodiek.

Achtergrondinformatie over Mina-IT

Om een reële projectomgeving te creëren, heb ik de onderstaande situatie verzonnen. Deze situatie is grotendeels gebaseerd op de werkzaamheden die ik bij mijn huidige werkgever uitvoer:

Mina-IT is een van de grotere IT dienstverleners in Nederland op het gebied van oracle database beheer. Bij het beheren van een Oracle database omgeving komen veel verschillenden soorten werkzaamheden kijken, zoals:

- Databases aanmaken, wijzigen of verwijderen
- Performance tuning op de databases (zodat de applicaties sneller hun data uit een database kunnen halen).
- Productie verstoringen verhelpen.
- Dagelijkse beheer werkzaamheden zoals databases vergroten of de back-up inrichten.
- Etc

Onze klanten zijn voornamelijk overheidsinstellingen zoals ministeries, waterschappen en gemeentes. Daarnaast hebben wij enkele commerciële klanten zoals banken, hogescholen en Telecom providers.

Mina-IT is zeven jaar geleden opgestart en is sindsdien extreem hard gegroeid. Door de sterke groei van het bedrijf is besloten om een tweede vestiging te openen in Groningen. Het pand waar het bedrijf zich gaat vestigen is net gebouwd en er is nog totaal geen IT infrastructuur aanwezig.

In deze vestiging zullen uiteindelijk 450 werknemers aan de slag gaan. De werknemers worden verdeeld over zeven afdelingen die verspreid zijn over acht verdiepingen. Ongeveer 80 procent van de werknemers gaat zich bezig houden met het uitvoeren van beheerwerkzaamheden op Oracle omgevingen van onze klanten. De overige 20 procent bestaat voornamelijk uit overhead personeel, zoals administratieve medewerkers, receptiemedewerkers, etc.

Projectmanagement methodiek

Omdat dit een complex project betreft, is het van groot belang om een projectmanagement methodiek te gebruiken. Wanneer je een projectmanagement methodiek gebruikt, voorkom je dat het project chaotisch verloopt. Je brengt ook meer structuur aan in het project. Ook zorg je voor meer transparantie en overzichtelijkheid voor alle partijen die bij het project betrokken zijn.

Er bestaan momenteel tientallen verschillende projectmanagement methodieken. Op school heb ik met PRINCE2 en ASI leren werken. Ook heb ik bij mijn vorige werkgever de waterval-methodiek gehanteerd. Omdat ik uit ervaring weet dat alle drie de methodieken geschikt zijn voor mijn project en dat ik ze alle drie beheers, heb ik besloten om niet verder te kijken naar andere methodieken.

Voordat ik uit een van de drie methodieken kan kiezen, moet ik eerst voor mezelf duidelijk hebben wat ik in een projectmanagement methodiek zoek. Ik zou graag een projectmanagement methodiek willen gebruiken die mij kan ondersteunen bij de volgende werkzaamheden:

- De complexiteit van het project vereenvoudigen. Uit ervaring weet ik dat dit het best opgelost kan worden door te faseren. Wanneer je gaat faseren, hak je het project in kleinere stukken die makkelijker uit te voeren zijn. Dit is veel overzichtelijker dan wanneer je het project in één keer uitvoert.
- Het ontwerpen van netwerken.
- Goede documentatie zonder veel overhead rapporten.

Elk van de bovenstaande methodieken heeft zowel voor – als nadelen. Hieronder heb ik deze opgesomd.

ASI

Voordelen :

- Minder voorbereidingstijd omdat ik deze methodiek als beste van de drie methodieken beheers.
- Niet veel overhead documentatie.
- ASI maakt gebruik van fasering.
- Uiterst geschikt voor projecten waarbij netwerken ontworpen moeten worden.

Nadelen:

- Weinig literatuur over deze methodiek te vinden.

PRINCE2

Voordelen:

- Minder voorbereidingstijd omdat ik deze methodiek al beheers.
- Uiterst geschikt voor grote projecten.
- Erg veel theorie beschikbaar.
- PRINCE2 maakt gebruik van fasering.

Nadelen:

- Erg veel overhead documentatie en rapportages zoals: Issue log, Lessons learned log, Daily log, activity log, etc.
- PRINCE2 is niet gespecialiseerd in het ontwerpen van netwerken.

Watervalmethodiek

Voordelen:

- Watervalmethodiek maakt gebruik van fasering en is zeer overzichtelijk voor alle betrokkenen bij het project. Een nieuwe fase wordt pas gestart als de vorige fase volledig naar wens is voltooid. Zo weten de betrokkenen te allen tijde in welke fase zij zich bevinden.
- Omdat het zo bekend is, zullen weinig mensen problemen ondervinden met het gebruik van deze methodiek.

Nadelen:

- Deze methodiek kan niet goed met veranderingen uit vorige fases omgaan. De methodiek is niet flexibel en achteraf wijzigingen doorvoeren is vaak lastig.
- Niet echt geschikt voor kleinere projecten omdat de nadruk op de documentatie gelegd wordt.
- De watervalmethodiek is niet gespecialiseerd in het ontwerpen van netwerken.

Nu ik weet welke methodieken ik kan gaan gebruiken en wat de methodieken voor mij kunnen betekenen, kan ik een keuze maken uit de bovenstaande methodieken.

Als ik kies voor de methodiek PRINCE2, besteed ik erg veel tijd aan de documentatie en het maken van de eerder genoemde logs. Daarnaast is PRINCE2 veel geschikter voor grote projecten waar veel partijen aan samenwerken. Dat is bij mij niet het geval. Daarom vind ik PRINCE2 niet de meest geschikte methodiek voor mijn project.

Omdat dit een complex project betreft, is het mogelijk dat er achteraf wijzigingen gemaakt moeten worden aan de opdracht. Dit kan financiële of technische redenen hebben. Zoals eerder gezegd kan de watervalmethodiek niet goed omgaan met het achteraf doorvoeren van wijzigingen. Daarnaast is het project niet geschikt voor kleinere projecten, omdat ik erg veel tijd bezig zal zijn met het documenteren.

In tegenstelling tot PRINCE2 en de watervalmethodiek is de ASI methode uiterst geschikt voor kleinere projecten. Daarnaast is ASI uitermate geschikt voor het maken van netwerkontwerpen en wordt bij het gebruik van de methodiek niet veel overhead documentatie gemaakt. Zoals eerder genoemd is er niet veel literatuur beschikbaar over deze methodiek. Gelukkig heeft de Haagsche Hogeschool wel de benodigde literatuur (ASI RAPPORT) in huis. Omdat ik deze methodiek bovendien veel gebruikt heb op school, ben ik daar het beste mee bekend.

Om een goede vergelijking te maken heb ik bovenstaande argumenten in een tabel weergegeven. Op deze manier zal het maken van een keuze vergemakkelijkt worden.
In de onderstaande tabel kan elk onderdeel maximaal 3 punten scoren.

	ASI	**PRINCE2**	**Waterval**
Gebruik van fasering	3	3	3
Geschikt voor netwerk ontwerpen	3	1	1
Geschikt voor kleinere projecten	3	1	1
Voorbereidingstijd nodig om methodiek te gebruiken (mijn bekendheid met de methodiek)	3	2	1
Literatuur over methodiek	1	3	2
Totaal aantal punten	**13**	**10**	**8**

Op basis van de bovengenoemde argumenten en resultaten uit het tabel, heb ik besloten om ASI als projectmanagement methodiek te gaan gebruiken.

ASI methodiek

Nu de beslissing is gemaakt om ASI als projectmanagement methodiek te gebruiken, is de volgende stap om de fases in de methodiek te beschrijven.

Fases
Bij het gebruik van ASI als projectmanagement methodiek, komen vier fases aan de orde, namelijk:

- Definitiefase
- Architectuurfase
- Ontwerpfase
- Ontwikkelfase

Definitiefase
In de definitiefase worden de eisen en wensen van de opdrachtgever vastgelegd. Aan de hand van de eerder genoemde eisen en wensen, wordt een blauwdruk gemaakt voor de nieuwe situatie. Daarnaast worden in de definitiefase de randvoorwaarden beschreven en wordt er een voorlopige planning beschreven.

Ik ga tijdens de definitiefase extra aandacht besteden aan het verkrijgen van meer informatie van de opdrachtgever. Op deze manier voorkom ik dat in een later stadium toch fouten ontstaan door gebrek aan informatie of communicatieproblemen.
Het resultaat van deze fase wordt beschreven in een definitierapport.

Architectuurfase
In de architectuurfase worden de eisen en wensen uit de definitiefase verwerkt tot één of meerdere globale schetsen van de technische infrastructuur. Hierbij worden keuzes gemaakt op basis van technologie, technieken en fabrikanten.

Tijdens de architectuurfase wil ik zoveel mogelijk uiteenlopende technieken overwegen. Op deze manier kan ik zowel gebruikmaken van betrouwbare en veel gebruikte technieken, als zeer moderne technieken die nog niet vaak gebruikt worden.
Het resultaat van deze fase wordt beschreven in een architectuurrapport.

Ontwerpfase
In de ontwerpfase wordt de eerder gemaakte schets van de technische infrastructuur uitgewerkt. Wanneer dit compleet is, ontstaat er een technische ontwerp waar alle benodigde details op staan. Tijdens de ontwerpfase is het niet de bedoeling dat er nog vaagheden aanwezig zijn. Alles moet tot in de puntjes kloppen. Dit is tenslotte de laatste fase voordat het product daadwerkelijk gebouwd wordt. Het resultaat van deze fase wordt beschreven in een ontwerprapport.

Ontwikkelfase

In de ontwikkelfase wordt het daadwerkelijke product gebouwd, aan de hand van de eerder opgeleverde ontwerpen uit de ontwerpfase. Omdat ik in dit project het netwerk niet zelf zal aanleggen, ga ik deze fase niet verder behandelen.

Beschrijving van de eisen en wensen

Zoals reeds is beschreven staat de definitiefase in het teken van de eisen en wensen van de opdrachtgever. Wanneer de eisen en wensen van de opdrachtgever bekend zijn, kan er een plan van aanpak gemaakt worden. Ook zal er gedurende deze fase een voorlopige planning gemaakt worden als onderdeel van het plan van aanpak. Het resultaat van deze fase wordt beschreven in een definitierapport.

Doelstelling project

Het doel van dit project is het leveren van een adviesrapport voor de te gebruiken hardware voor het inrichten van het netwerk. In dit adviesrapport zal onder andere advies gegeven worden over de te gebruiken internetverbindingen en de beveiliging van het netwerk.

Daarnaast moet er een compleet netwerkarchitectuur worden opgeleverd. Aan de hand van de opgeleverde producten gaat Mina-IT een extern bedrijf inhuren dat daadwerkelijk de omgeving gaat bouwen volgens ons advies en netwerkarchitectuur.

Doordat ik een dergelijk groot netwerk moet gaan ontwerpen, komen de belangrijkste netwerkcomponenten hier aan te pas. Enige tijd geleden heb ik voor een schoolopdracht een netwerk ontworpen voor een basisschool. Echter, dit was een kleine omgeving en er kwamen geen grote componenten bij kijken zoals een SAN of virtualisatie. Ook hoefde er alleen een IP-plan gemaakt te worden. Daarnaast werd er geen rekening gehouden met de hardware en de beschikbaarheid van het netwerk.

In tegenstelling tot de bovengenoemde schoolopdracht zal ik in dit project wel stilstaan bij bijna alle componenten die bij de meeste grote netwerken gebruikt worden. Denk hierbij aan: switches, routers, SAN, virtualisatie, servers, firewall, wireless, computers, DNS, DHCP, Domain controller, etc.

Scope van het project (eisen)

Om te beginnen is het erg belangrijk om de scope van het project duidelijk te maken voor alle partijen. Ik heb zelf de scope van het project verzonnen. Ik heb wel mijn best gedaan om een netwerkopdracht te realiseren die zo reëel mogelijk is. Hieronder is te zien welke onderdelen binnen de scope van dit project vallen:

- Er dient een gehele netwerkinfrastructuur bedacht te worden voor de 500 medewerkers die verspreid zijn over zeven afdelingen en acht verdiepingen. Initieel zullen er maar 450 medewerkers in de nieuwe vestiging werken, maar de opdrachtgever wil wel dat het netwerk tot maximaal 500 medewerkers uitgebreid kan worden zonder ingrijpende veranderingen aan het netwerk te brengen.

- Er dient een voorstel te komen voor het realiseren van een verbinding die 24x7 verbonden is tussen deze vestiging en het hoofdkantoor te Nieuwegein. Ook moet er een back-up verbinding komen voor het geval dat er storingen optreden met de primaire verbinding.
- Het gehele pand moet voorzien zijn van een beveiligd draadloos netwerk.
- Er dient een voorstel te komen voor de te gebruiken apparatuur zoals werkplekken, servers, back-up units, storage en netwerkapparatuur. Hiervoor is een beperkt budget beschikbaar.
- Er dient een voorstel te komen voor de te gebruiken technieken voor de storage.
- Er dient een voorstel te komen voor de beveiliging van het netwerk.
- Er dient een voorstel te komen voor de installatie van de volgende servers. Hierbij kan gebruik gemaakt worden van virtualisatie:
    - Mailserver
    - Domeinserver
    - FTPserver
    - DNSserver
    - DHCPserver
    - Applicatie servers
    - Database server
- De nieuwe vestiging zal geopend worden op 01-01-2011. Dit betekent dat het project uiterlijk 31-11-2010 afgerond moet zijn, zodat het netwerk in de maand voorafgaand aan de opening gebouwd kan worden door het externe bedrijf.

- Voor het aanschaffen van de apparatuur is een budget van €1.000.000,- beschikbaar gesteld. Dit bedrag is exclusief de kosten voor het bouwen van het netwerk. Dit bedrag is zelf door de opdrachtgever bepaald. Er is eventueel meer geld beschikbaar als dat echt nodig is. Het is echter wel de bedoeling dat we in eerste instantie binnen het budget blijven.

- Er moet een advies komen voor de high availablity van de netwerkapparatuur, servers en de storage. Hierbij moet rekening gehouden worden met het maken van back-ups en het elimineren van single point of failures. Daarnaast moet er gedacht worden aan back-up stroomvoorzieningen zoals UPS.

Ik heb besloten dat onderstaande onderdelen buiten de scope van dit project vallen. De reden hiervan is het feit dat dit een fictieve opdracht is. Mina-IT bestaat in werkelijkheid niet en dit zorgt ervoor dat onderstaande punten onmogelijk uit te voeren zijn in het project. Aan deze punten wordt in het project daarom verder geen aandacht besteed.

- Het daadwerkelijk bouwen van het netwerk.
- De bekabeling van het netwerk. Dit zal door een extern bedrijf uitgevoerd worden.
- Het aannemen en/of opleiden van de ICT afdeling.

- Het inrichten van de helpdesk of het gebruik van ITIL en andere methodieken of processen voor de helpdesk.

Plan van aanpak

Om het project succesvol af te ronden, is een goed plan van aanpak nodig. In het plan van aanpak worden belangrijke keuzes gemaakt en het is daarom erg belangrijk om het plan van aanpak voldoende gedetailleerd te maken. Hierdoor kunnen misverstanden voorkomen worden. Ook kun je met het plan van aanpak je huidige positie in het project bepalen en eventueel tijdig bijsturen.

Aanpak project

Zoals reeds aangegeven zullen twee producten opgeleverd worden aan het eind van dit project:

- Een complete netwerkarchitectuur (architectuurrapport).
- Een adviesrapport over de inrichting van de nieuwe omgeving.

Omdat deze twee eindproducten teveel van elkaar verschillen, ga ik het project in twee delen opsplitsen. Allereerst zal het architectuurdocument opgesteld worden en vervolgens ga ik een advies geven over de overige zaken die te maken hebben met de IT-infrastructuur.

Dit moet in bovenstaande volgorde gebeuren omdat het andersom niet mogelijk zou zijn. Dit omdat van tevoren nog niet bekend is welke netwerktechnieken gebruikt zullen worden en ik dus ook geen advies kan geven over de netwerkapparatuur. Daarom is ervoor gekozen om eerst de netwerkarchitectuur te maken en vervolgens de advies te geven voor het inrichten van de nieuwe omgeving en de hardware.

Extra informatie vergaren

Tijdens het maken van de plan van aanpak is het erg belangrijk om zoveel mogelijk informatie over het project voorhanden te hebben. Dit is nodig om de fases en de planning zo gedetailleerd mogelijk te maken. Omdat er thans nog veel details onbekend zijn, moet ik eerst meer informatie van de opdrachtgever vergaren.

Om meer informatie te vergaren kan ik verschillende methodes gebruiken. De meest gebruikte methodes zijn: een enquête houden, interviewen of zelf onderzoeken.
Omdat enquêtes over het algemeen gebruikt worden voor een groep mensen, zal deze methode voor mij niet geschikt zijn. Er is namelijk maar één persoon waarvan ik meer informatie kan/wil verzamelen. Ook zelf onderzoeken is hier niet mogelijk, omdat de wensen van de opdrachtgever voor mij nog niet duidelijk zijn. De beste manier om informatie in te winnen is daarom door de opdrachtgever te interviewen.

Tijdens het interviewen zou ik open, gesloten of suggestieve vragen kunnen stellen. Omdat ik geïnteresseerd ben in veel verschillende aspecten, is het niet verstandig om voor gesloten of suggestieve vragen te kiezen. Daarom kies ik ervoor om uitsluitend open vragen te stellen. Op deze manier hoop ik zoveel mogelijk informatie van de opdrachtgever in te winnen.

Het feit dat ik zowel de opdrachtgever als de uitvoerder ben in dit project, maakt het interviewen erg lastig. Dit omdat ik in feite mezelf moet interviewen. Om het zo realistisch mogelijk te houden, heb ik ervoor gekozen om iemand met beperkte technische kennis voor de geest te halen. Dit is geen vreemde situatie, omdat de meeste opdrachtgevers daadwerkelijk weinig kennis hebben op dit gebied. Hierdoor krijgt de uitvoerder van een project vaak zelf de kans om belangrijke keuzes te maken en neemt hij de expertrol op zich (zie het interview in de bijlage).

projectverdeling

Na het interview zijn veel details bekend geworden. Nu kan ik verder met het plannen van mijn project. Aan de hand van het eerder afgelegde interview en de informatie die hieruit is voortgevloeid, weet ik nu wat de eisen zijn van het project.

De onderdelen die te maken hebben met het ontwerpen van het netwerk, zal ik in het eerste gedeelte van het project plaatsen. Deze onderdelen zijn bijv. het opstellen van een IP plan of het maken van de architectuur.

De onderdelen in het kader van het adviseren, zal ik in het tweede gedeelte van het project plaatsen. Denk bij deze onderdelen bijvoorbeeld aan het adviseren van een geschikte storage oplossing.

Netwerkarchitectuur

In het eerste gedeelte van het project wordt de netwerkarchitectuur bedacht en opgesteld. Tijdens het opstellen van het architectuurdocument wordt aandacht besteed aan de volgende punten:

- Er moet een logisch IP schema worden opgesteld.
- Er moet rekening gehouden worden met de beveiliging van het netwerk.
- Er moet rekening gehouden worden met de aanwezigheid van een beveiligde draadloze netwerkverbinding in het hele gebouw.
- Er moet rekening gehouden worden met het feit dat er 24x7 een netwerkverbinding aanwezig moet zijn met het hoofdkantoor te Nieuwegein. Ook moet er een back-up verbinding aanwezig zijn, mocht de primaire verbinding uitvallen.

Advies over het inrichten van het nieuwe netwerk

Wanneer het bekend is hoe de architectuur van het netwerk eruit komt te zien, kunnen we verder met het tweede gedeelte van het project: het advies over hoe het nieuwe netwerk ingericht moet worden. Hierbij moet gedacht worden aan de volgende punten:

- Er dient een voorstel te komen voor de te gebruiken apparatuur zoals servers, storage en netwerkapparatuur. Hiervoor is een budget van €1.000.000,- beschikbaar.
- Er dient een voorstel te komen voor de te gebruiken technieken voor de storage.
- Er dient een voorstel te komen voor de beveiliging van het netwerk.
- Er dient een voorstel te komen voor de installatie van de volgende servers. Hierbij kan gebruik gemaakt worden van virtualisatie:
    - Mailserver
    - Domeinserver
    - FTPserver
    - DNSserver
    - DHCPserver
    - Applicatie servers
    - Database server
- Er moet een advies komen voor de high availablity van de netwerkapparatuur, servers en de storage. Hier moet rekening mee gehouden worden met het maken van back-ups en het elimineren van single point of failures. Daarnaast moeten we denken aan back-up stroomvoorzieningen zoals UPS.

  Omdat de meeste onderdelen waarover wordt geadviseerd teveel van elkaar verschillen, ga ik over ieder onderdeel een apart adviesrapport maken. Eerst worden de verschillende oplossingen beschreven, waarbij de voor - en nadelen in beeld worden gebracht. Vervolgens wordt aan de hand hiervan een advies gegeven over het inrichten van het onderdeel.

Planning

Om ervoor te zorgen dat het project geen vertraging oploopt, is het belangrijk om van tevoren goed te plannen. Hieronder staat een planningsschema dat ervoor moet zorgen dat het project succesvol en op tijd afgerond wordt.

Bij het maken van de planning heb ik op basis van eigen ervaringen een schatting gemaakt van de tijd die de verschillende fases in beslag zullen nemen. Om ervoor te zorgen dat bij enige vertraging geen grote problemen ontstaan, heb ik voor een uitloopperiode van een week gekozen. In deze planning is verder te zien welke (sub)producten aan het eind van elke fase opgeleverd dienen te worden.

Als tussenproducten heb ik onder andere het definitierapport, architectuurrapport en het ontwerprapport aangehouden, zoals de ASI methodiek beschrijft.

Actie	**Op te leveren (sub)producten**	**voortgang**
Voorbereiden project	-	1e week
Maken van plan van aanpak	Plan van aanpak (onderdeel van het definitierapport)	3e week
Beschrijven definitie fase	Definitierapport	4e week
Onderzoeken naar verschillende netwerktechnieken	-	5e week
Eerste opzet netwerkarchitectuur	Architectuur rapport	6e week
Uitwerken netwerkarchitectuur	Ontwerp rapport	8e week
Onderzoeken hardware passend bij architectuur	Beschrijving van de uitgevoerde onderzoeken.	9e week
Maken adviesrapport voor hardware	Advies rapport voor hardware	11e week
Uitwerken Procesverslag	Procesverslag	15e week
Uitloop	-	17e week

Beschrijving van de architectuur

Nu de Definitiefase achter de rug is, kunnen we beginnen met de architectuurfase. In deze fase onderzoek ik welke netwerkapparatuur ik nodig heb en waarom. Bij het maken van de keuzes ga ik alleen op de functionaliteiten van de apparatuur letten en niet op het merk of de prijs. Dit gebeurt namelijk in deel twee van dit project tijdens het adviseren. Ook zal ik onderzoeken welke apparatuur redundant uitgevoerd moeten worden.

Omdat ik de ASI methodiek hanteer, ga ik uiteindelijk meerdere netwerkarchitecturen (schetsen) maken en daar de beste van uitkiezen. Het gekozen ontwerp zal in de ontwerpfase verder uitgewerkt worden. Het resultaat van deze fase wordt beschreven in een architectuurrapport.

Netwerkapparatuur

Om te weten wat voor netwerkapparatuur ik nodig heb, heb ik vooraf onderzocht waar de verschillende netwerkcomponenten voor bedoeld zijn. Daarnaast wilde ik weten of deze voor mij van belang waren. Dankzij de Cisco cursus die ik op school heb gevolgd, wist ik al voor een groot deel welke soort apparatuur ik nodig zal hebben. Ik heb tevens op het Internet vele verschillende netwerken nauwkeurig bestudeerd. Op de website www.ratemynetworkdiagram.com zetten veel netwerkarchitecten hun netwerktekening online. Tenslotte heb ik gebruik gemaakt van voorbeelden uit het boek Top-Down Network Design.

Na de bovenstaande zoekactie is duidelijk geworden dat de onderstaande componenten nodig zijn:

- Switches
- Routers
- Firewalls
- Storage
- Draadloze accesspoints
- Servers

Nu ik weet welke netwerkcomponenten ik nodig heb, is het tijd om te beslissen waar de apparatuur aan moet voldoen. Ik zal per netwerkcomponent aangeven waar het aan moet voldoen.

Switches

Tijdens mijn onderzoek ben ik erachter gekomen dat ik voor ons netwerk twee verschillende soorten switches nodig heb, namelijk een backbone-switch en een enduser-switch. De backbone-switch wordt gebruikt om de belangrijkste netwerkcomponenten met elkaar te verbinden, zoals bijv. servers en routers. De enduser-switches worden gebruikt om de gebruikers aan het fysieke netwerk te koppelen met behulp van UTP.

In de afgelopen jaren werden steeds meer applicaties via het web gebruikt, denk aan Webmail, intranet, wiki-portal, etc.) Hierdoor vindt er steeds meer netwerkverkeer plaats. Om te voorkomen dat gebruikers het netwerk als traag ervaren, gaan wij alle enduser switches gigabit (10/100/1000) uitvoeren. Dit werkt niet alleen prettig voor de gebruikers maar maakt het netwerk ook meer futureproof.

Enduser-switches zijn in veel varianten verkrijgbaar. De meest gebruikte switches zijn de 16, 24 en 48 poorts switches. Het voordeel van de 48 poorts switch is de ruimtebesparing in de patchkasten, omdat er minder switches nodig zijn. Dit heeft echter wel een nadeel. Wanneer een switch kapot gaat, zijn er maximaal 48 personen die niet kunnen werken. Wanneer een 16 poorts switch wordt gebruikt, zullen bij een defecte switch maximaal 16 personen gehinderd worden. Er zijn dan echter wel drie keer zoveel patchkasten nodig.

Omdat de beschikbaarheid voor de opdrachtgever erg belangrijk is, wil ik niet de kans lopen dat meer dan 10 procent van de werknemers niet kan werken door een defecte switch (dit is het geval wanneer een 48 poorts switch gebruikt wordt). Vandaar dat ik ervoor kies om 24 poorts switches te gebruiken. Op deze manier kunnen er bij switchproblemen 50 procent meer werknemers werken dan bij een 48 poorts switch. Dit betekent echter wel dat er dubbel zoveel switch patchkasten nodig zijn.

We moeten niet alleen rekening houden met 500 werknemers, maar ook met de overige hardware. Er komen meerdere printers en scanners per verdieping. Voor al deze componenten moeten ook netwerkverbindingen beschikbaar zijn. Als we ervan uit gaan dat er per verdieping drie printers en één scanner aanwezig zijn, hebben we voor acht verdiepingen minimaal 32 extra poorten nodig. In totaal hebben we dus ongeveer 550 poorten nodig voor het hele gebouw. Dit komt overeen met 23 switches (24 poorts).

Meestal worden backbone-switches redundant uitgevoerd omdat ze essentieel zijn. Deze switches mogen dus 24 of 48 poorts zijn. In geval van een storing met de switch zal al het verkeer via de andere switch lopen.

Routers
Routers hebben een belangrijke rol, namelijk het routeren tussen de verschillende netwerksegmenten. Alle routers moeten evenals de switches minimaal gigabit routers zijn.

Firewall
Een firewall houdt ongewenst verkeer buiten ons netwerk. Daarom hebben wij voor ons netwerk ook een firewall nodig. Ook moet ons firewall DMZ ondersteunen (momenteel wordt er geen gebruik van gemaakt, maar in de toekomst wellicht wel).

Storage
Een correcte storage oplossing is onmisbaar in een netwerk. Op je storage komt namelijk alle data te staan. Data is vaak van onschatbare waarde. Voor ons netwerk zal dus een storage oplossing moeten komen.

Draadloze accesspoints
Ik heb uitgezocht wat het bereik is van de meeste accesspoints; dit bleek tussen de 75 en de 100 meter te zijn. Aangezien de verdiepingen niet langer dan 50 meter zijn, is het dus voldoende om op iedere verdieping één draadloze accesspoint te plaatsen.

Servers
Een perfect draaiend netwerk zonder servers is nutteloos. De opdrachtgever heeft aangegeven dat hij vier applicatieservers nodig heeft. Daarnaast zijn er DHCP, FTP, DNS, mail, domein - en database servers vereist. We hebben dus minimaal tien servers nodig. Het is daarom verstandig om rekening te houden met extra servers.

Omdat niet alle servers altijd optimaal benut worden, is het zonde om 10 servers aan te schaffen die sporadisch werken. Virtualisatie kan hier een goede oplossing voor bieden.
Bij virtualisatie is het mogelijk om op èèn host (server) meerdere besturingssystemen naast elkaar installeren. Deze besturingssystemen zullen samen de hardware van de host delen. Ook zijn deze besturingssystemen van elkaar gescheiden en werken ze onafhankelijk van elkaar.

Het is gunstiger om vijf servers te kopen, waar we vervolgens met behulp van virtualisatie 10 virtuele servers op kunnen installeren. Op deze manier halen we het maximale uit ons apparatuur. Door gebruik te maken van virtualisatie worden er veel kosten bespaard, die weer bij andere netwerkcomponenten goed van pas komen.

Redundante hardware

De opdrachtgever heeft aangegeven dat het netwerk moet blijven doordraaien, ook wanneer er een kritieke netwerkcomponent kapot gaat. Met kritieke apparatuur wordt apparatuur bedoeld waarvan bijna de gehele netwerk van afhankelijk is, zoals backbone-switches. Werkstations vallen niet onder kritieke apparatuur.

Het is nu belangrijk om te weten welke apparatuur redundant uitgevoerd moet worden en welke niet. Hieronder heb ik beschreven welke netwerkapparatuur dubbel uitgevoerd moeten worden en waarom.

Firewall
De firewall is het eerste aanspreekpunt voor het netwerk van buitenaf. Dat betekent dat er in het geval van een storing in de firewall, grote problemen kunnen ontstaan tussen netwerkverkeer van buiten naar binnen en vice versa. De firewall zal dus redundant uitgevoerd moeten worden.

Routers
De routers zorgen voor het routeren in een netwerk. Als er een storing optreedt in een router, kan een groot deel van het netwerk onbruikbaar worden. Daarom is het belangrijk dat een router redundant uitgevoerd wordt.

Storage
In de storage staat alle data opgeslagen. In het geval van een storing in de storage, is de data niet meer beschikbaar voor de medewerkers. Om dit te voorkomen, zal dus tevens de storage redundant uitgevoerd moeten worden. Op deze manier creëer je tevens een kopie op de tweede storage. Dit is erg nuttig, omdat het ook meteen een belangrijke back-up mechanisme is voor waardevolle data.

Draadloze accesspoints
Wanneer er op een draadloze accesspoint een storing ontstaat, zullen gebruikers op de betreffende verdieping niet meer optimaal gebruik kunnen maken van het draadloos netwerk. Ze zullen echter wel nog gebruik kunnen maken van de draadloze accesspoint van de verdieping boven of onder hen, omdat het bereik van de accesspoint tussen de 75 en 100 meter is. Mocht dit niet lukken, dan is het nog altijd mogelijk om via UTP verbinding maken met het netwerk. Als we alle accesspoints redundant zouden uitvoeren zou het erg veel kosten met zich mee brengen, terwijl er ook workarounds beschikbaar zijn. Daarom heb ik ervoor gekozen om de accesspoints niet redundant uit te voeren.

Servers

Omdat we eerder hebben aangeven dat de gebruikers intensief gebruik maken van de vier applicatieservers, is het belangrijk dat de servers altijd beschikbaar blijven. Vandaar dat ook de servers redundant uitgevoerd moeten worden. Mochten er storingen optreden met een server, dan kan de redundante server de sessie overnemen.

Zonder een DNS server kunnen gebruikers niet browsen of mailen. Dit is echter wel nodig in hun werkzaamheden. Daarom is het belangrijk om de DNS server redundant uit te voeren.

Omdat het voor de beheerders lastig is om op elk werkstation handmatig een IP adres te configureren, wordt er gebruik gemaakt van een DHCP server. Deze server zorgt ervoor dat elk werkstation het juiste IP adres krijgt. Hierdoor is het noodzakelijk om de DHCP server redundant uit te voeren, want zonder een DHCP server kunnen gebruikers geen IP-adres verkrijgen. Dit zorgt er op zijn beurt weer voor dat er geen verbinding kan worden gemaakt met het netwerk.

Wanneer de domeinserver een storing heeft, kunnen de gebruikers niet op het domein inloggen. Het gevolg hiervan is dat de gebruikers hun werkzaamheden niet kunnen verrichten. Ook hier is het dus van essentieel belang dat de domeinserver redundant wordt uitgevoerd.

Zonder de database-server kunnen de applicaties hun data niet ophalen, waardoor de applicaties onbruikbaar worden. Kennis is macht; indien de data voorgoed verdwijnt, betekent dit dat er ook veel kennis verdwijnt. Ook back-ups zijn niet voor de volle 100 procent te vertrouwen; de back-up jobs kunnen falen of er kunnen hardware problemen met de back-up mechanismen ontstaan. Vandaar dat het erg belangrijk is om de database-server redundant uit te voeren.

Indien er een storing optreedt in de mailserver, kunnen de gebruikers geen gebruik meer maken van hun e-mail. De e-mail is van significante waarde, omdat er tegenwoordig steeds meer via de digitale weg wordt gecommuniceerd. Als de mailserver niet juist werkt, is er een belangrijke communicatiechannel niet meer beschikbaar. Dit kan tot veel problemen leiden voor de medewerkers en de klanten.

Omdat alle bovenstaande servers erg belangrijk zijn, zal ik ze allemaal redundant uitvoeren zodat de gebruikers in geval van serverstoringen kunnen doorwerken zoals ze gewend zijn.

Switches

In een netwerk hebben switches verschillende rollen. Zo zijn er backbone-switches en enduser-switches. De backbone-switches verbinden de primaire netwerkapparatuur met elkaar. Dit zijn bijvoorbeeld de switches die tussen de routers en de enduser switches zitten.

De enduser-switches zijn switches die direct de gebruiker aan het netwerk koppelen. Deze switches zijn vervolgens op de backbone-switches aangesloten.

Wanneer een backbone-switch kapot gaat, is het mogelijk dat alle enduser-switches die daarop aangesloten zijn geen netwerkverkeer meer kunnen doorsturen. Hierdoor kan het gehele netwerk onbruikbaar worden voor de eindgebruikers. Het is dus van cruciaal belang om de backbone-switches redundant uit te voeren.

Wanneer de enduser-switch kapot gaat, kunnen maximaal 24 medewerkers geen gebruik maken van het netwerk. De rest van de organisatie zou wel door kunnen werken. Omdat het werkstation van de gebruikers meestal maar één netwerkaansluiting heeft, kan een werkstation niet op twee switches worden aangesloten. Daarom hoeven de enduser-switches niet redundant uitgevoerd te worden. Wanneer er toch een enduser-switch kapot gaat, zal deze altijd binnen 24 uur vervangen worden door de hardware leverancier omdat daar een servicecontract mee afgesloten is.

De opdrachtgever wil een uptime garantie van 99 procent hebben. Wanneer een enduser-switch kapot gaat, kunnen er op dat moment maximaal 24 gebruikers niet werken. Dat is ongeveer vijf procent van de gebruikers voor één dag. Om de downtime te berekenen, kunnen we de volgende formule gebruiken:

D = Totale downtime (uren)
T = Totale tijd in een jaar (uren)
Downtime (in %) = D/T X 100

Voor ons zou de volgende situatie ontstaan:
D = Totale downtime is 24 uur
T= Totale tijd in een jaar is 8760 uur

Downtime = 24 /8760 x 100 = 0,27% oftewel 99,72%
Dit geldt echter alleen voor 5 procent van de werknemers, omdat er maar één switch kapot gaat. Dit betekent dat de overige 95 procent van de werknemers gewoon door kan werken.

Wanneer één enduser-switch kapot gaat, zullen we ruim onder de norm van 99 procent uptime zitten.

Verschillende ontwerpen

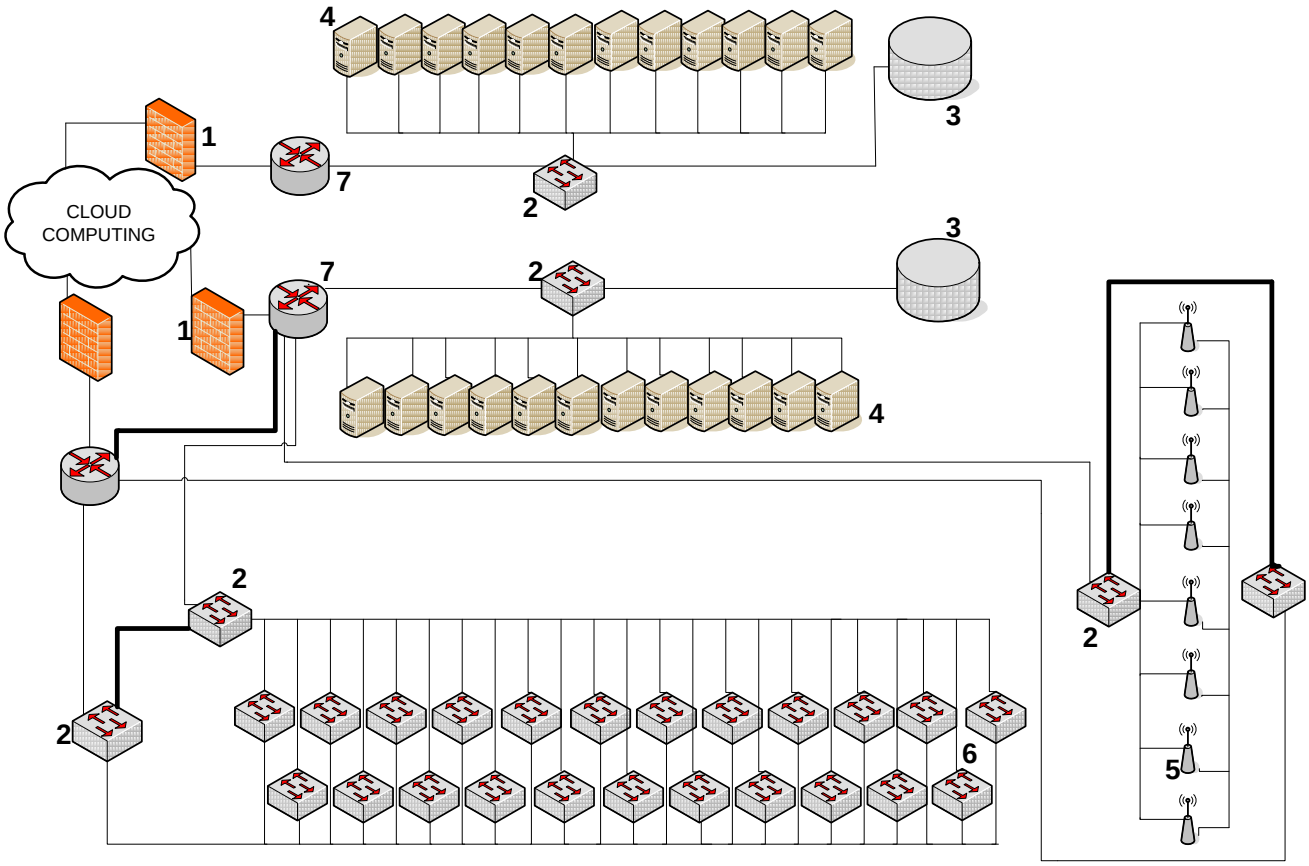
Wanneer je de ASI methodiek hanteert, is het erg verstandig om meerdere ontwerpen (schetsen) te maken. Daarom heb ik meerdere schetsen gemaakt, die ik hierna zal onderbouwen. Omdat de opdrachtgever heeft aangegeven dat alle kritieke componenten redundant uitgevoerd moeten worden, heb ik twee verschillende schetsen met verschillende technieken getoond.

Om tot verschillende schetsen te komen, heb ik besloten om technieken te gebruiken die op verschillende manieren werken. Sinds men bezig is met het redundant uitvoeren van netwerkcomponenten, wordt er gebruik gemaakt van interne redundantie. Interne redundantie houdt in dat meerdere netwerkcomponenten elkaars taken kunnen overnemen in geval van hardware problemen. In dat geval zitten de dezelfde componenten meestal op dezelfde locatie (intern).

Al enkele jaren wordt gebruik gemaakt van externe redundantie. De gebruikte term hiervoor is cloud computing. Cloud computing is een techniek die steeds vaker gebruikt wordt. De nadruk bij cloud computing ligt op het delen van hardware en software via het Internet. Hierbij hoeven de verschillende redundante netwerkcomponenten niet meer op dezelfde locatie te staan, maar kunnen ze ook aan de andere kant van de wereld staan.

Cloud computing

Het grootste voordeel van cloud computing is dat de servers op een hele andere locatie aanwezig kunnen zijn, wat meteen een goede back-up mechanisme is. Dit is ook meteen het grootste nadeel van cloud computing: je bent namelijk beperkt door je Internetverbinding. Wanneer een Internetverbinding niet meer werkt, is het niet mogelijk om bij de servers aan de andere kant van de cloud te komen. Hieronder staat een schets van onze opzet, in het geval we gebruik zouden maken van cloud computing. Bij het maken van deze schets heb ik rekening gehouden met de eisen van de opdrachtgever.



1=firewall
2=Backbone-switch
3=Storage
4 =Servers
5= Accesspoints
6= Enduser-switches
7= Router

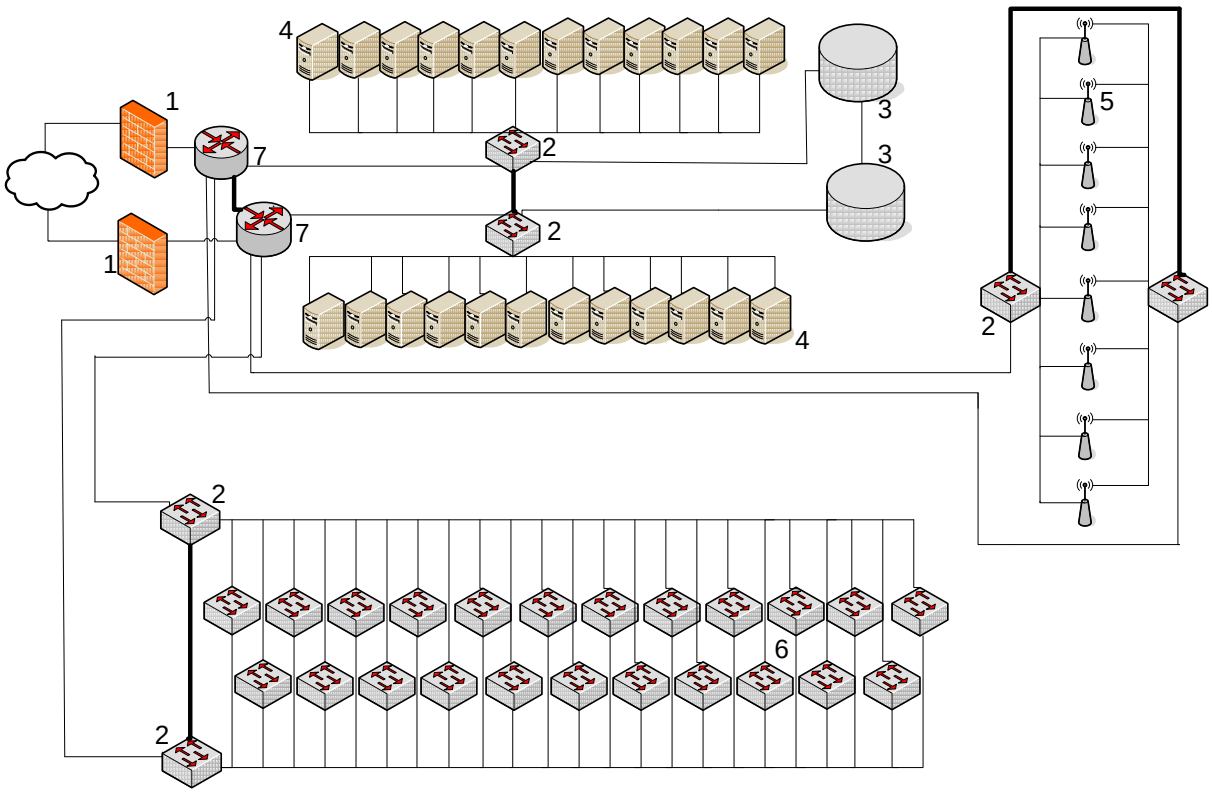
Bij het maken van de bovenstaande schets heb ik zoveel mogelijk aan de eisen van de opdrachtgever voldaan. Zo heb de firewall, router en backbone-switch redundant uitgevoerd op de hoofdvestiging (onderkant van de cloud). Op de uitwijkomgeving (bovenkant van de cloud) staan de standby servers en storage.

De dikgedrukte lijnen dienen voor het gebruik van redundantie. Wanneer bijvoorbeeld een backbone-switch kapot gaat, moet er bij de standby backbone-switch een lampje gaan branden dat hij de taken moet overnemen. Deze protocol wordt ook wel de Spanning Tree Protocol genoemd. Wanneer het protocol vaststelt dat pakketten meerdere keren naar eenzelfde segment worden gerouteerd, wordt een van de paden naar dat segment afgesloten door de desbetreffende switchpoort uit te schakelen.

Ook de dikke verbinding tussen de routers staat voor een failover protocol. Vaak worden voor Cisco routers de Hot Standby Router Protocol (HSRP) geconfigureerd. Een router van een ander merk dan Cisco zou de Virtual Router Redundancy Protocol (VRRP) kunnen gebruiken, want HSRP werkt alleen op Cisco apparatuur. Bij deze protocollen wordt ook de standby router geactiveerd als de primary niet meer benaderbaar is.

Interne redundantie

Bij de tweede schets heb ik gebruik gemaakt van interne redundantie. Dit is in praktijk eigenlijk de meest gebruikte redundantie techniek. Hierbij wordt standby apparatuur naast de primaire apparatuur op dezelfde locatie geplaatst.



1=firewall
2=Backbone-switch
3=Storage
4 =Servers
5= Accesspoints
6= Enduser-switches
7= Router

Ook de tweede schets heb ik zo opgesteld, dat deze voldoet aan de eisen van de opdrachtgever. In de bovenstaande opstelling is de firewall, router, backbone-switch, servers en storage redundant uitgevoerd. Daarnaast worden hier dezelfde failover protocollen gebruikt als op de eerste schets.

Het grootste voordeel van de bovenstaande opstelling is dat je niet afhankelijk bent van je Internetverbinding. Wanneer er geen Internet beschikbaar is, draait intern het netwerk nog door (de applicaties die Internet nodig hebben uiteraard niet).
Het grootste nadeel is dat alles op dezelfde locatie aanwezig is. Wanneer het gebouw door een calamiteit getroffen wordt, bijvoorbeeld een brand, is de kans dat je zowel je primaire als de redundante hardware kwijt bent groter.

Nog een voordeel van deze opstelling is dat er minder apparatuur nodig is om aan de eisen van de opdrachtgever te voldoen. Om precies te zijn is er bij de eerste opstelling een extra firewall en router nodig om dezelfde redundantie te bereiken, die aan de behoefte van de opdrachtgever voldoet.

Cloud computing VS. Interne redundantie

Zowel cloud computing als interne redundantie hebben voor - en nadelen. Hieronder heb ik de voor - en nadelen van beide architecturen op een rijtje gezet:

Interne redundantie architectuur
Voordelen:

- Minder hardware nodig om gewenste redundantie te bereiken.
- Ook zonder Internet draait het interne netwerk normaal door en is het mogelijk om in geval van hardware problemen de stand-by apparatuur gebruiken.
- Er worden kosten bespaard voor het afhuren van een uitwijklocatie.
- De opdrachtgever heeft al aangegeven geen uitwijklocatie te willen. Hiermee houd je meer rekening met de eisen van de opdrachtgever.

Nadelen:

- Wanneer het gehele gebouw onbruikbaar wordt, is men vaak zowel de primaire als de standby apparatuur kwijt. Echter is de kans dat het gehele gebouw onbruikbaar wordt zeer klein.

Cloud computing architectuur
Voordelen:

- Veiliger, aangezien de uitwijkomgeving op een andere locatie aanwezig kan zijn.

Nadelen:

- Meer hardware nodig om gewenste redundantie te bereiken.
- Afhankelijkheid van een Internetverbinding. Wanneer er geen Internet meer tot de beschikking is, kan het ook niet mogelijk zijn om de uitwijklocatie te benaderen. Wanneer je niet bij je uitwijklocatie kan, heeft het dus ook niet veel nut om een uitwijklocatie te hebben.

- Er zijn extra kosten vereist, omdat er een uitwijklocatie nodig is. De opdrachtgever had al aangegeven geen uitwijklocatie te willen. Dit houdt in dat het eindproduct niet aan de eisen van de opdrachtgever voldoet, wanneer er voor deze oplossing gekozen zou worden.

Omdat interne redundantie ten opzichte van cloud computing meer voordelen heeft, kies ik ervoor om deze methode te gebruiken. Op deze manier bereiken we alsnog de gewenste redundantie en hoeft de opdrachtgever geen uitwijklocatie te huren.

Nu wij een degelijke architectuur voor ons ontwerp hebben opgesteld, is hiermee het eind van de architectuurfase bereikt. Het architectuurrapport is in de bijlage toegevoegd.

Beschrijving van het ontwerp

Volgens ASI wordt in de ontwerpfase de eerder gekozen architectuur tot in de kleine details uitgewerkt. Een onderdeel van deze fase is het ontwerpen van een juist IP plan voor onze architectuur. Wanneer er een IP plan aanwezig is, wordt de architectuur nogmaals uitgebreid ontworpen met alle gekozen details. Het resultaat van deze fase is een ontwerprapport en het uiteindelijke netwerkontwerp. Aan de hand van dit ontwerp zou een derde partij de infrastructuur kunnen aanleggen.

IP plan

Nu bekend is hoe onze architectuur eruit komt te zien, is het hoog tijd om een IP plan te maken. Een goed IP-plan is cruciaal voor een netwerk. Wanneer er een verkeerde keuze wordt gemaakt bij het bedenken van een IP-plan, kan dit ervoor zorgen dat er na een bepaalde periode geen interne adressen meer beschikbaar zijn. Hierdoor moet het netwerk opnieuw ingericht worden. Om dit te voorkomen, ga ik eerst onderzoeken wat de mogelijkheden zijn. Hieronder staat een plan beschreven voor het vinden van de ideale IP-adressen en subnetmasks:

1. Eerst moet ik achterhalen hoeveel subnetten ik wil hebben in mijn netwerk.
2. Zodra ik weet hoeveel subnetten ik in mijn netwerk wil hebben, moet ik gaan bepalen hoeveel hosts er maximaal per subnet aanwezig zullen zijn.
3. Zodra ik weet hoeveel subnetten ik nodig heb en hoeveel hosts per subnet aanwezig zijn, kan ik gaan kiezen tussen de verschillende networkclasses.
4. Als de bovenstaande informatie allemaal bekend is, kan ik bepalen wat de subnetmask wordt van zowel de overkoepelende als de kleinere subnetten.

Waarom subnetten?

Voordat ik ga beginnen met het achterhalen van het aantal subnetten dat ik nodig heb, zal ik eerst moeten uitzoeken waarom ik meerdere subnetten nodig heb.

Er zijn meerdere redenen om subnetten te gebruiken. De belangrijkste redenen zijn beveiliging en groeperingen.

Wanneer een netwerk twee subnetten heeft, kunnen hosts op subnet A niet direct naar de hosts op subnet B. Om dit wel mogelijk te maken, moeten ze via de router gerouteerd worden. Het voordeel hiervan is dat je door middel van de router kan analyseren, loggen, filteren en dus beveiligen.

De tweede reden is het groeperen. Wanneer je iedereen in een enkele subnet zou plaatsen, zou het veel beheer kosten om een bepaalde groep gebruikers anders in te richten dan de

rest (bijv. andere rechten). Als je de verschillende groepen in verschillende subnets zet, kun je volledige groepen hetzelfde gaan behandelen. Hierdoor hoef je niet meer iedere gebruiker apart te beheren, maar je beheert de gehele groep in één keer op dezelfde manier.

Aantal subnetten

Nu ik weet waarom ik subnetten nodig heb, kan ik de hoeveelheid subnetten achterhalen die ik nodig heb. Uit veiligheid is het verstandig om de servers in een aparte subnet te zetten. Zo zou ik, als het nodig is, verkeer van medewerkers kunnen blokkeren naar de servers.

Gebruikers kunnen op twee manieren verbinding maken met het netwerk: via de UTP, of door middel van inloggen via het draadloos netwerk. Het lijkt mij dan ook uitermate handig om zowel het draadloze gedeelte als het UTP gedeelte in een aparte subnet te zetten. Op deze manier zouden we het verkeer beter kunnen analyseren of beveiligen, bijvoorbeeld omdat sommige gebruikers om veiligheidsredenen beperkt gebruik mogen maken van het draadloos netwerk.

Omdat wij het netwerk graag futureproof willen maken, is het handig om een extra subnet te reserveren voor toekomstig gebruik.

In totaal hebben we dus vier subnetten nodig, namelijk:
- Servers
- Draadloos netwerk
- Fysiek netwerk
- Gereserveerde voor toekomstige gebruik.

Aantal hosts per subnet

We hebben eerder aangegeven dat we rekening gaan houden met 500 medewerkers. Om toch op de toekomst voorbereid te zijn, is het zeer handig om toch ervan uit te gaan dat het netwerk meer kan gaan groeien dan nu wordt verwacht. Op deze manier voorkomen we in de toekomst veel problemen. Voor het gemak zal ik van het dubbele aantal medewerkers uit gaan. Dit betekent dat de subnet van het draadloos netwerk en van het fysieke netwerk voor 1000 medewerkers beschikbaar moet zijn.

Omdat we niet weten hoeveel servers erbij zullen komen, is het moeilijk om in te schatten wat de maximale grootte is van de subnet. Ik zou de subnet van de servers kunnen verhogen naar 100 servers, maar omdat ik niet weet hoeveel servers in de toekomst nodig zullen zijn, is het niet verstandig om dit een lage waarde te geven. Voor de zekerheid ga ik ervan uit dat de subnet van de servers ook 1000 hosts zou kunnen hebben.

Omdat ik nog niet weet waar de gereserveerde subnet voor gebruikt zal worden, kan ik ook heel moeilijk aangeven hoeveel hosts in de subnet gaan komen. Vandaar dat ik het aantal gelijk houd aan de overige subnetten.

Dit betekent dat ik rekening moet houden met 1000 hosts per subnet.

Network class

Nu ik weet hoeveel subnetten ik nodig heb en hoeveel hosts er maximaal in de subnets zitten, kan ik de juiste networkclass kiezen. Er bestaan vijf networkclasses, namelijk A, B, C, D en E. Networkclass D is gereserveerd voor Multicasting en networkclass E is gereserveerd voor toekomstig gebruik. D en E kunnen we dus niet gebruiken. We kunnen alleen networkclass A, B en C gebruiken:

Networkclass	Netwerk ID	Max. Hosts	Max. Subnetten
A	*a*.0.0.0	16777214	4194304
B	*a.b*.0.0	65534	16384
C	a.b.c.0	254	64

De systeembeheerder van de hoofdvestiging heeft al eerder aangegeven dat de hoofdvestiging gebruik maakt van de 10.10.0.0/19 range (B CLASS). Daarnaast valt de hele organisatie onder de 10.10.0.0./18 reeks.

Wij hebben zelf een range nodig die hieronder valt en die 4000 hosts kan bevatten. Omdat de 10.10.0.0/19 reeks reeds in gebruik is door de hoofdvestiging, kunnen wij de adressen 10.10.0.0 t/m 10.10.31.255 niet gebruiken. De range die minimaal 4000 hosts kan bevatten is de 10.10.32.0/20 range. Deze range kan maximaal 4096 hosts bevatten en is dus prima voor ons.

Deze ip-range zal in de routetabel van de routers van de hoofdvestiging opgenomen worden. Dat betekent dat alle verkeer van de hoofdvestiging naar de nieuwe vestiging, naar de 10.10.32.0/20 wordt gerouteerd. Als ik ervoor zou kiezen om de vier subnetten allemaal in de routetabel van de hoofdvestiging te plaatsen, zou het beheer wel lastiger worden. Het is makkelijker om de 10.10.32.0/20 subnet te gebruiken, omdat alle subnetten toch binnen dezelfde range vallen en er dus maar één aanspreekpunt is.

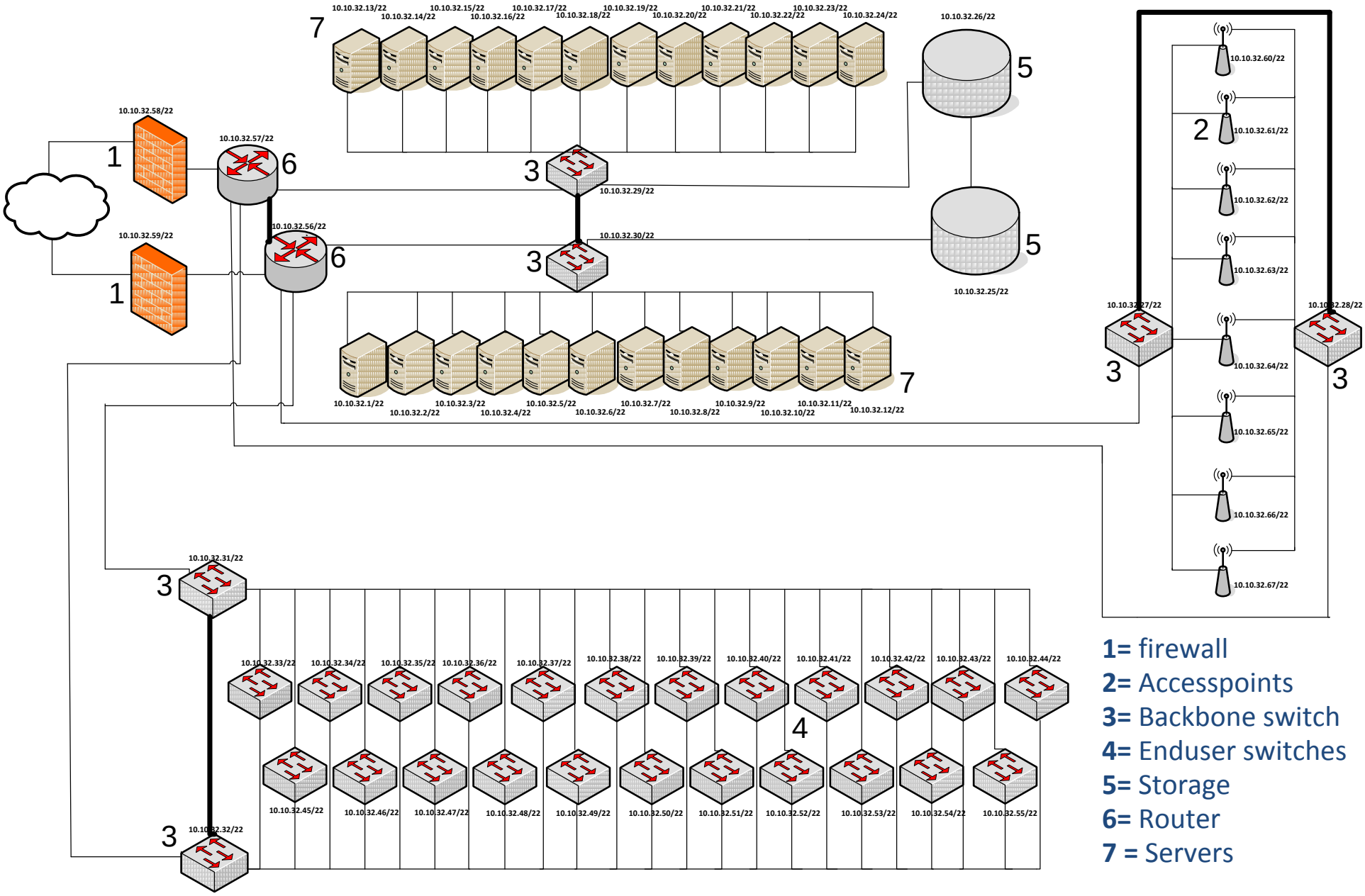
In de 10.10.32.0/20 subnet kunnen maximaal 4096 hosts aanwezig zijn; dit is voldoende voor ons. Onder de 10.10.32.0/20 subnet zullen onze vier subnetten komen die in de 10.10.0.0/22 range zitten. Deze subnetten kunnen maximaal 1024 host per subnet bevatten. Dat is prima, omdat ik eigenlijk van maximaal 1000 hosts per subnet ben uitgegaan. Het geheel ziet er als volgt uit:

Subnet naam	Subnet	IP range	Aantal adressen
Gehele organisatie	10.10.0.0/18	10.10.0.0 – 10.10.63.255	16384 Adressen
Hoofdvestiging	10.10.0.0/19	10.10.0.0 – 10.10.31.255	8192 Adressen
Mina-IT Groningen	10.10.32.0/20	10.10.32.0 – 10.10.47.255	4096 Adressen
Servers	10.10.32.0/22	10.10.32.0 – 10.10.35.255	1024 Adressen
Draadloos netwerk	10.10.36.0/22	10.10.36.0 – 10.10.39.255	1024 Adressen
Fysiek netwerk	10.10.40.0/22	10.10.40.0 – 10.10.43.255	1024 Adressen
Gereserveerde	10.10.44.0/22	10.10.44.0 – 10.10.47.255	1024 Adressen

Nu we weten wat voor apparatuur we nodig hebben en wat het IP-plan is, kunnen we het gekozen IP plan in ons ontwerp implementeren. Op de volgende pagina is het uiteindelijke netwerkarchitectuur zichtbaar.

Hiermee ben ik aan het eind gekomen van mijn ontwerpfase. In de bijlage staat het ontwerprapport. Ook is de complete netwerkarchitectuur in de bijlage toegevoegd.

Hiermee kom ik tevens aan het einde van het eerste gedeelte van het project. In het tweede gedeelte van het project zal ik de geschikte hardware voor mijn ontwerp kiezen.



1= firewall
2= Accesspoints
3= Backbone switch
4= Enduser switches
5= Storage
6= Router
7 = Servers

Netwerkontwerp Mina-IT

Het maken van een adviesrapport

Inleiding

Nu het eerste gedeelte van het project erop zit, weet ik precies wat voor soort hardware ik nodig heb voor het netwerk. Ook is bekend hoeveel ik van elk component nodig zal hebben. In dit gedeelte van het project moet ik zien te achterhalen welke producten het meest geschikt zijn voor het netwerk.

Hardware

Om het juiste hardware component te vinden, moet ik belangrijke afwegingen maken met betrekking tot de uptime, specificaties, performance, kosten, etc.
Ik geef per product aan wat de verschillende mogelijkheden en belangrijkste verschillen zijn. Tevens zal ik per product de argumenten onderbouwen waarom ik vind dat de gekozen product het best past bij het netwerk.

Ik geef advies over de volgende producten:

- Werkstations
- Firewalls
- Routers
- Enduser-switches
- Backbone-switches
- Storage
- Accesspoints
- Servers
- Backup Units
- UPS
- Primary en backup verbindingen naar hoofdkantoor

Budget

De opdrachtgever heeft aangegeven dat er een budget van €1.000.000 gereserveerd is voor de werkstations en de netwerkapparatuur. Hij heeft tevens aangegeven dat dit bedrag verhoogd kan worden indien dat noodzakelijk is. Het is echter wel de bedoeling dat we in eerste instantie binnen het budget te blijven.

Hardware leveranciers

Bij het kiezen van de juiste hardware leveranciers, moeten er meerdere keuzes gemaakt worden. Om te beginnen wil ik weten of het beter is om alle hardware die ik nodig heb bij één hardware leverancier te kopen, of juist bij verschillende leveranciers.

Alle hardware bij één hardware leverancier kopen, heeft zowel nadelen als voordelen. De grootste nadelen als wij alle hardware zouden kopen bij één leverancier:

- Je beperkt je tot het assortiment van de leverancier. Echter is het wel zo dat bijna alle grote hardware leveranciers in Nederland aan de meeste hardware kunnen komen als ze die niet standaard in hun assortiment hebben.
- Je zal misschien iets duurder uit zijn als je alles bij één hardware leverancier koopt, omdat bij andere leveranciers bepaalde producten wellicht goedkoper zijn.

De grootste voordelen als wij alle hardware zouden kopen bij één leverancier:

- Mogelijk meer korting, omdat je erg veel producten koopt in één keer.
- Het beheren van je bestelling is makkelijker, omdat je alles bij één leverancier koopt.
- Het maken van toekomstige bestellingen is makkelijker omdat de leverancier precies weet wat voor apparatuur je in je netwerk hebt. Zo kan de leverancier een advies geven over toekomstige bestellingen.
- De opdrachtgever heeft eerder aangegeven dat hij een onderhoudscontract gaat afsluiten met de hardware leverancier. Wanneer er meerdere leveranciers zijn, moet hij ook meerdere contracten afsluiten. Wanneer alle apparatuur bij één leverancier wordt ingekocht, sluit je maar één beheerscontract af. Dit zal het beheer van de contracten en de administratie een stuk makkelijker maken.

Aan de hand van bovenstaande punten raad ik de opdrachtgever aan om alle hardware bij één hardware leverancier aan te schaffen. De belangrijkste reden om niet alle hardware bij één leverancier te kopen, zijn de eventuele hogere kosten. Maar als ik alles bij één hardware leverancier aanschaf, krijg ik wel meer korting. Hierdoor kom ik uiteindelijk op dezelfde prijs uit, of zelfs goedkoper.

Nu ik besloten heb dat alle hardware bij één hardware leverancier wordt aangeschaft, moet ik kiezen uit de vele hardware leveranciers in Nederland. Om een zo goed mogelijke keuze hierin te kunnen maken, is het belangrijk om beoordelingscriteria vast te stellen. Het gaat dan om de volgende criteria: prijs, voorraad, service, assortiment, betrouwbaarheid en levertijd.

Om tot een goede keuze te komen, ga ik de vier grootste hardware leveranciers in Nederland (volgens Tweakers.net) met elkaar vergelijken. Ik heb de site Tweakers.net gekozen omdat deze onafhankelijk is en omdat bijna elke hardware leverancier in Nederland

bij hen ingeschreven staat. Om de test zo eerlijk mogelijk te laten verlopen, ga ik vijf producten vergelijken bij de vier leveranciers. Zo kan ik zien welke leverancier over het algemeen het goedkoopst is, welke het grootste assortiment heeft en welke de meeste producten op voorraad heeft. Vervolgens ga ik de levertijden met elkaar vergelijken, om te zien welke leverancier het snelst levert. Omdat de service en de betrouwbaarheid bij de verschillende leveranciers erg dynamisch zijn, is het niet mogelijk om deze aspecten met elkaar te vergelijken.

Volgens Tweakers.net behoren de volgende leveranciers tot de grootste in Nederland:

- Misco
- Scholten awater
- Central point
- Conrad

Ik ga de volgende producten met elkaar vergelijken (volgens Tweakers.net worden deze producten het meest gebruikt in grote netwerken):

- Cisco Catalyst Express 520-24PC
- HP ProCurve Switch 1810-24G
- HP Compaq Business Desktop dc7900 - Core 2 Duo E8400 3 GHz
- NETGEAR ProSafe VPN Firewall 50 FVS338
- HP ProCurve MSM323 Access Point WW

Hardware	**Misco**	**Scholten awater**	**Central point**	**Conrad**
Cisco Catalyst Express 520-24PC	€699	€1387	Niet in assort.	Niet in assort.
HP ProCurve Switch 1810-24G	€349	**€265**	**€274**	Niet in assort.
HP Compaq Business Desktop dc7900	€595	€1049	€642	Niet in assort.
NETGEAR ProSafe VPN Firewall 50 FVS338	€149	€141	€151	€265
HP ProCurve MSM323 Access Point WW	**€549**	€677	€647	Niet in assort.
Totaal	€2341	€3519	Ongeschikt	Ongeschikt

Bij Central point en Conrad waren sommige componenten niet aanwezig in het assortiment. Dit geeft aan dat er te weinig keus is, waardoor ik mezelf teveel zou beperken tot het kleine assortiment.

Bij Misco en Scholten awater waren alle producten in het assortiment aanwezig. Beide leveranciers hadden echter elk één product niet op voorraad (vetgedrukt hierboven). Omdat Misco en Scholten awater ongeveer hetzelfde assortiment en voorraad hebben, maakt dat de prijs doorslaggevend. Misco is in totaal €1178 goedkoper. Misco komt dus als de grote winnaar uit de bus.

Advies over de hardware componenten

In de volgende hoofdstukken beschrijf ik het proces die ik doorlopen heb bij het adviseren van de hardware componenten voor het nieuwe netwerk.

Voor het geven van een advies zal eerst per product een onderzoek gedaan worden. Zowel functionaliteiten als prijzen worden dan met elkaar vergeleken. Aan het eind wordt de gemaakte keuze met argumenten onderbouwd.

Onderzoekmethoden

Er bestaan verschillende onderzoekmethoden waar ik gebruik van kan maken, zoals: literatuuronderzoek, experimenteel onderzoek, surveyonderzoek, etc.

De meeste onderzoekmethoden kunnen in twee groepen onderverdeeld worden, namelijk kwalitatieve methoden en kwantitatieve methoden.

De kwalitatieve methoden worden over het algemeen gebruikt bij onderzoeken waar men meningen, opinies of kennis over een bepaald onderwerp probeert te achterhalen. Hierbij wordt vaak onderzoek gedaan onder een kleine groep mensen. Kwantitatieve onderzoeken worden vaak gebruikt voor het verzamelen van statistieken. Hierbij wordt een grote groep mensen betrokken.

Omdat ik geïnteresseerd ben in informatie over een bepaald onderwerp, zal ik gebruik maken van een kwalitatieve onderzoekmethode. De meest gebruikte kwalitatieve onderzoekmethoden zijn observatieonderzoeken, open interviews en literatuuronderzoeken.

Bij een observatieonderzoek wordt gebruikt gemaakt van systematische waarneming van bepaalde gedragingen van over het algemeen kleine groepen. Hierbij wordt enkel gelet op gedragingen die voor het onderzoek interessant zijn. Omdat ik niet geïnteresseerd ben in het observeren van het gedrag van een groep mensen, zal ik niet voor deze methode kiezen.

Een open interview wordt vaak gehouden tussen twee personen. Het doel van een interview is vaak om de belevingen of motieven van een geinterviewde te achterhalen. Omdat ik onderzoeken doe naar hardware componenten is deze methode niet geschikt voor mij.

Een literatuuronderzoek is wel geschikt voor mij. Over de werking van netwerkonderdelen is namelijk veel literatuur te vinden in zowel boeken als op het internet. Daarom kies ik ervoor om deze onderzoekmethode te gebruiken.

Werkstations

Via de werkstations zullen de werknemers al hun werkzaamheden moeten uitvoeren. Dit betekent dat een goed werkstation een must is. Als ik een werkstation kies dat te langzaam is voor de werknemers, zal dit voor vertragingen en irritaties zorgen. Het is echter ook niet de bedoeling om een werkstation te kiezen dat extreem snel is en waar uiteindelijk geen gebruik wordt gemaakt van alle resources dat het werkstation kan leveren. Dit is dan eigenlijk geldverspilling.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande werkstations in aanmerking gekomen:

Werkstation	Geheugen	CPU	Hardeschijf	Prijs
HP Compaq Business dc7900	2gb + 2gb extra	3 GHz	160 Gb	€655,-
HP Compaq 6000 Pro	2gb + 2gb extra	3 GHz	250 Gb	€589,-
Acer Veriton M670G	2gb + 2gb extra	3.16GHz	320 Gb	€655,-
Dell OptiPlex 780DT	4 gb standaard	3.16GHz	250 Gb	€659,-

Bovenstaande machines voldoen allemaal aan de gestelde eisen. Bijna alle werkstations kosten ongeveer hetzelfde, behalve de HP Compaq 6000; deze is ongeveer €70,- goedkoper. Omdat ze allemaal voldoen aan de eisen, is het zonde om meer geld te investeren in hardware als niet het maximale eruit wordt gehaald. Vandaar dat ik de opdrachtgever ga adviseren om de HP Compaq 6000 pro aan te schaffen.
Omdat bovenstaande werkstations zonder schermen geleverd worden, ga ik de opdrachtgever adviseren om de bijpassende schermen aan te schaffen. Dit is de HP LA1951G 19-inch. Dit scherm kost €144,- euro. In totaal kost een werkplek dus €733,-

Voor de 450 werkplekken zal uiteindelijk een bedrag van 450 x 733 =
€ 329.850,- betaald moeten worden. Hiermee houden we nog €670.150,- over van ons budget.

Firewall

Een firewall wordt voornamelijk gebruikt om te voorkomen dat (ongewenst) netwerkverkeer van het ene netwerksegment terecht komt in een ander netwerksegment. Hiermee wordt de veiligheid binnen het netwerk verhoogd. Meestal wordt een firewall ingezet om het interne netwerk te beveiligen tegen het Internet. Zo minimaliseer je de kans dat vanuit het Internet virussen of hackers in het netwerk binnendringen.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande firewalls in aanmerking gekomen:

Product	DMZ	Aantal VPN verbindingen	snelheid	Aantal gebruikers	prijs
Cisco ASA 5550	Ja	500	1024 mb/s	650000	€11.999,-
SonicWALL NSA/E6500 Multi-Core UTM	Ja	6000	1024 mb/s	6000	€12.395,-
SonicWALL (NSA) E5500	Ja	4000	3900 mb/s	4000	€8133,-
DC-Networks firewall: DCFW-1800E-V2 Firewall	Ja	2000	1024 mb/s	1.000.000	€4490,-
D-Link ENTERPRISE FIREWALL	Ja	2500	1024 mb/s	1000	€5331,-

Er is in principe een firewall nodig die maximaal 500 gebruikers kan ondersteunen en 500 VPN verbindingen tegelijkertijd kan maken. Daarnaast moet de firewall een snelheid van minimaal 1024 mb/s hebben.

De Cisco ASA 5550 is een van de duurdere firewalls uit de lijst. Deze switch kan 650.000 medewerkers ondersteunen. Wij hebben echter maar 500 medewerkers. Omdat deze firewall verder geen bijzonderheden biedt, zal deze dus afvallen.

De SonicWALL NSA/E6500 is de duurste firewall uit de lijst. Deze firewall kan de meeste VPN verbindingen maken, namelijk 6000. Omdat wij alleen 500 medewerkers hebben, is deze dure feature dus overbodig. De SonicWALL NSA/E6500 valt ook af.

De SonicWALL (NSA) E5500 is nu de duurste firewall die over is gebleven. Wat deze firewall duurder maakt, is het feit dat hij bijna vier keer zo snel is als de overige firewalls. Echter, wij hebben genoeg aan een firewall die 1024 mb/s kan doorvoeren. Het zou dus geldverspilling zijn om een snellere firewall aan te schaffen en daar het maximale niet uit te halen.

Nu blijven twee firewalls over: de DC-Networks DCFW-1800E en de D-Link ENTERPRISE FIREWALL. De DC-Networks firewall kan 1.000.000 gebruikers ondersteunen. Dat is 990.000 keer meer dan de D-Link. De D-Link ENTERPRISE kan 2500 VPN verbindingen beheren; dat is 500 meer dan de DC-Networks. Echter, beide extra features zijn niet interessant voor ons

omdat ze allebei al prima voldoen aan onze eisen. Ik zal de opdrachtgever adviseren om twee DC-Networks DCFW-1800E-V2 Firewalls aan te schaffen. Samen kosten deze firewalls €8980,- . Hiermee houden we nog €661.170,- over van ons budget.

De DC-Network is een nieuw merk op de markt en heeft zich in een korte tijd zeer goed bewezen. Ik ben ervan overtuigd dat deze prima zal bevallen.

Routers

Een router zorgt voor het routeren tussen verschillende netwerken. Een router gebruikt hiervoor zijn eigen routetabel, waarin staat wat de kortste routes zijn naar de verschillende nodes in een netwerk. Omdat ons netwerk meerdere subnetten heeft, is er een router nodig om tussen de subnetten te routeren.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande routers in aanmerking gekomen:

Product	MTBF	Protocollen	Uitbreidbaar	Snelheid	Prijs
Cisco 2851	19 jaar	Allemaal	Ja 4 slots	1 Gb/s	€4.199,-
Cisco 2821	12 jaar	Allemaal	Ja 4 slots	1 Gb/s	€2.799,-
Juniper J2320	7 jaar	Allemaal	Ja 3 slots	1 Gb/s	€1.259,-

Alle bovenstaande routers voldoen aan ons eisen. De Juniper router is het goedkoopst van de drie. Echter heeft deze minder uitbreidingsmogelijkheden. Ook is het de minst betrouwbare router van de drie, omdat het de laagste MTBF-waarde heeft. De Juniper valt dus af, omdat deze qua niveau ver onder de overige routers zit.

Nu de Juniper is afgevallen, blijven de Cisco 2851 en de Cisco 2821 over. De grote verschillen tussen deze routers is de MTBF en de prijs. De Cisco 2851 gaat volgens Cisco 19 jaar mee, voordat er problemen ontstaan. Bij de Cisco 2821 is dat 12 jaar. De Cisco 2851 is echter wel €1400,- duurder.

Omdat wij de routers redundant zullen uitvoeren, moet een MTBF van 12 jaar meer dan voldoende zijn. Dit omdat de standby router in geval van problemen de taken overneemt van de primary router. Daarom is het niet verstandig om €1400,- extra te betalen per router, terwijl we geen optimaal gebruik gaan maken van de extra betrouwbaarheid.

Ik zal de opdrachtgever adviseren om twee Cisco 2851 routers aan te schaffen. De kosten hiervan zijn samen €8.398,- . Hiermee blijft er nog €652.772,- over van ons budget.

Enduser-switches

Een enduser-switch zorgt ervoor dat de data bij de juiste persoon wordt geleverd. Het grote verschil tussen bijvoorbeeld een switch en een hub, is dat een hub alle data naar alle poorten stuurt. Een switch kan echter achterhalen voor welke node een bepaalde data packet bestemd is en stuurt het vervolgens alleen naar deze node. Hiermee overlaad je de rest van de nodes niet met data die niet voor hen bestemd is.

Elk werkstation, netwerkprinter, netwerkscanner, etc., wordt door middel van een switch aan het netwerk gehangen. Zoals reeds aangegeven, is het de bedoeling dat er meer dan 500 netwerkapparaten aan het netwerk worden hangen. Dit komt neer op 23 switches van 24 poorten.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande enduser-switches in aanmerking gekomen:

Product	VLAN	Routering	Protocollen	Prijs
3Com Baseline Plus Switch 2928 PWR	Ja	Ja	Allemaal	€449,-
Linksys SPS2024	Ja	Ja	Allemaal	€449,-
Cisco Small Business Pro 520 Ethernet Switch 24-poorts 10/100/1000 met PoE	Ja	Ja	Allemaal	€1.399,-
HP ProCurve Switch 2910al-24G	Ja	Ja	Allemaal	€1.599,-
3Com Switch 4500G 24-Poorten	Ja	Ja	Allemaal	€1.799,-

Bovenstaande switches voldoen allemaal aan onze eisen.
De 3Com 4500G switch is de duurste van allemaal. Deze is zelfs vier keer zo duur dan de 3Com 2928 PWR switch. Echter heeft deze switch wel een functionaliteit die de rest niet heeft, namelijk twee upload poorten van 10 gb/s. Dit was echter geen eis van ons. De eis was een snelheid van 1 gb/s. Het is dan ook niet verantwoord om vier keer zoveel te betalen voor een switch waar we niet het maximale uit kunnen halen. Daarom valt de 3Com 4500G switch af.
De Cisco small business en de HP ProCurve switch zijn ruim drie keer zo duur dan de 3Com Baseline of de Linksys SPS2024. De reden dat deze switches duurder zijn, is het feit dat ze meer protocollen ondersteunen. Echter, wij gaan geen gebruik maken van al deze extra features. Het is dan ook geldverspilling als we meer geld gaan uitgeven aan features die we niet gaan gebruiken. De Cisco small business en de HP ProCurve switch vallen dus ook allebei af.

Nu blijven de 3Com Baseline en de Linksys SPS2024 over. Deze twee switches ondersteunen allebei VLAN, ROUTERING en ze hebben 24 x 1gb/s poorten. Ook de prijs van deze twee switches is hetzelfde. Omdat deze twee switches zo erg op elkaar lijken, moet ik dieper ingaan op de verschillen. Op deze manier kan ik zien welke switch meer te bieden heeft.

Als ik de specificaties van beide switches beter ga bekijken, zie ik een duidelijk verschil in de ondersteunde protocollen.

Dit zijn de protocollen die de 3Com switch ondersteunt:
Datatransport, Layer 3-omschakeling, Layer 2-omschakeling, DHCP-ondersteuning, automatische onderhandeling, ARP-ondersteuning, VLAN-ondersteuning, IGMP-spionage, Weighted Round Robin (WRR) queuing, opslaan en verder, Quality of Service (QoS), Jumbo Frames ondersteuning.

Dit zijn de protocollen die de Cisco switch ondersteunt:
Datatransport, Layer 2-omschakeling, DHCP-ondersteuning, automatische onderhandeling, BOOTP-ondersteuning, VLAN-ondersteuning, auto-uplink (auto MDI/MDI-X), IGMP-spionage, gespiegelde poorten, DiffServ-ondersteuning, Weighted Round Robin (WRR) queuing, opslaan en verder, MAC adresfiltering, Broadcast Storm Control, IPv6-ondersteuning, SNTP-ondersteuning, DHCP-spionage, Trivial File Transfer Protocol (TFTP) ondersteuning, Access Control List (ACL)-ondersteuning, Quality of Service (QoS), SSH-ondersteuning, Jumbo Frames ondersteuning, Dynamic ARP Inspection (DAI).

Zoals hierboven te zien is, ondersteunt de Cisco switch twee keer zoveel protocollen dan de 3Com switch. Een ander verschil dat ik heb ontdekt is het aantal beheerprotocollen.

Dit zijn de beheerprotocollen die 3Com switch ondersteunt:
SNMP 1, SNMP 2, RMON, SNMP 3, HTTPS

Dit zijn de beheerprotocollen die de Cisco switch ondersteunt:
SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, SSH.

Aan de hand van bovenstaande gegevens ga ik de opdrachtgever adviseren om de Linksys SPS2024 aan te schaffen. De Linksys SPS2024 kost €449,- per stuk. We hebben 23 stuks nodig. Dit betekent dat we totaal €10.327,- kwijt zijn aan de enduser-switches. Hiermee houden we nog €642.445,- over van het budget.

Backbone-switches

Backbone-switches voeren in principe dezelfde taken uit als de enduser-switches. Echter, backbone-switches moeten sneller zijn omdat daar veel meer verkeer doorheen gaat dan een enduser-switch. Tevens moeten de backbone-switches betrouwbaarder zijn, omdat de impact bij een defect vele malen groter is dan bij een enduser-switch.

In onze omgeving worden alle enduser-switches aan het netwerk gehangen door middel van backbone-switches . Dit betekent dat wanneer de backbone-switches kapot gaan, alle gebruikers zonder netwerk zitten. Daarom heb ik in onze omgeving de backbone-switches redundant uitgevoerd, om te voorkomen dat de hele productieomgeving uitvalt wanneer de backbone-switch kapot gaat.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande backbone-switches in aanmerking gekomen:

Product	Poorten	Snelheid	Redundante hardware	Prijs
Cisco N5000 2RU CHASSIS 5 FAN	40	10 gb/s	Ja	€17.623,22
Cisco N5000 1RU Chassis 2 Fan 20p	20	10 gb/s	Ja	€9.425,21
HP 2408 24-10GBE W/8-8GB	24	10 gb/s	Nee	€ 42.065,00

De HP switch is de duurste van de drie en heeft 24 poorten. Deze switch heeft echter geen redundante stroomvoorziening en FAN. Omdat ik liever niet op betrouwbaarheid inlever, valt deze switch af.

De overgebleven switches zijn van hetzelfde merk en model, alleen heeft de Cisco N5000 2RU twee keer zoveel poorten. Omdat deze switch de enige is die geschikt is voor het aansluiten van de 23 enduser-switches, is deze switch ideaal.

Ik zou ook de Cisco N5000 2RU CHASSIS 5 FAN switch kunnen gebruiken voor het serverpark en de accesspoints. Echter heb ik niet zoveel poorten nodig voor de andere twee segmenten. Het zou daarom geldverspilling zijn als we een 40 poorten switch aanschaffen, aangezien we bij de twee segmenten respectievelijk 8 en 13 poorten gaan gebruiken.

Voor het serverpark en de accesspoints zou ik de Cisco N5000 1RU kunnen gebruiken. Deze switch is net zo betrouwbaar als de N5000 2RU maar heeft 20 poorten in plaats van 40 poorten. Daarnaast kost deze switch de helft van de prijs van de N5000 2RU CHASSIS 5 FAN switch. Dat maakt deze switch ideaal voor het serverpark en de accesspoints.

Ik zal de opdrachtgever adviseren om tweemaal de N5000 2RU en viermaal de Cisco N5000 1RU aan te schaffen. Deze switches kosten bij elkaar €72.947,28. Hiermee blijft er nog €569.498,- over van het budget.

Storage

Storage is een van de belangrijkste componenten in de gehele IT-infrastructuur. Op storage wordt data opgeslagen. Data is zo waardevol, dat in geval van dataverlies er vaak een ramp ontstaat binnen het bedrijf (wanneer er geen back-ups gemaakt worden).

Zonder data kun je vaak het bedrijf niet meer runnen. Wanneer bijvoorbeeld alle administratie en financiële data verdwenen is, kun je vaak niet meer achterhalen welke klanten wel of niet betaald hebben. Gegevens over de medewerkers zoals salarissen, bonussen en afspraken raken dan ook vaak kwijt. Dergelijke fouten zijn al vaker ontstaan en bedrijven die dit hebben meegemaakt zijn vaak onderuit gegaan. Data gaat vaak gepaard met kennis en kennis is macht. Vandaar dat ik voor dit bedrijf een zeer goede storage oplossing nodig heb.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande storages in aanmerking gekomen:

Product	Snelheid	Capaciteit	Type	Prijs
Netgear ReadyNAS 4200 19 Rackmount, 10GB via CX-4	10 gb/s	24 TB	Schijven	€8.644,95
Netgear ReadyNAS 4200 19 Rackmount	1 gb/s	24 TB	Schijven	€7.992,95
HP StorageWorks All-in-One Storage System 1200r 3TB SATA	1 gb/s	3 TB	Schijven	€6.349,95
Thecus N8800 Network Storage Server 8 BAY NAS 16TB	1 gb/s	16 TB	Schijven	€3.020,95
Intel X25-E SATA II SSD 64GB	10 gb/s	64 GB	SSD	€584,95

Omdat ik een zeer snelle storage oplossing wil hebben, heb ik besloten dat de schijven een minimale overdrachtsnelheid moeten hebben van 10 gb/s. De Netgear ReadyNAS 4200 19 Rackmount, de HP StorageWorks All-in-One Storage en de Thecus storage hebben allemaal een verbinding met een maximale overdrachtsnelheid van 1 gb/s. Dit is voor ons te laag en daarom vallen deze drie storage oplossingen al af.

Nu blijven twee storage oplossingen over: de Netgear ReadyNAS 4200 19 Rackmount, 10GB via CX-4 en de Intel X25-E SATA II SSD 64GB. Het grootste verschil tussen deze storage oplossingen is het type. De Intel schijf is Solid state disk. Het genoemde bedrag is per 64 GB module. Eerder is aangegeven dat ik een storage wil hebben van 20 TB. Dit betekent dat ik 20 TB/64 Gb = 320 schijven nodig zal hebben. Samen zullen de schijven dan 320 x €584,95 = €187.184,- kosten. Dit is exclusief de kosten van de server waarin de schijven gehangen zullen worden. De netgear kost echter maar €8.644,95 en daar krijg je 24 TB voor, inclusief de storageserver. Dat is ruim €180.000,- euro goedkoper.

De voornaamste reden om de Intel SSD te nemen is de betrouwbaarheid. Echter, ik heb in ons netwerk twee storage servers gehangen: één primary en één standby storage. Dit betekent dat de data te allen tijde op twee verschillende storage schijven zijn opgeslagen. Ook zullen er regelmatig back-ups gemaakt worden van ons systeem, waardoor de betrouwbaarheid alleen maar toeneemt. Omdat de data dus altijd op twee verschillende plekken opgeslagen is plus de back-up, is de keuze voor de Netgear storage snel gemaakt.

Een tweede reden om voor de Netgear storage te gaan, is de prijs. Omdat er twee storage dozen nodig zijn, betekent dit een besparing van €360.000,- . Als ik voor de Intel SSD zou kiezen, zouden we hoogwaarschijnlijk in geldproblemen komen omdat er nog veel netwerkcomponenten aangeschaft moeten worden.

Om deze redenen zal ik de opdrachtgever adviseren om twee Netgear ReadyNAS 4200 19 Rackmount, 10GB via CX-4 aan te schaffen die samen €17.289,90 kosten. Hiermee blijft er nog €552.209,- over van het budget.

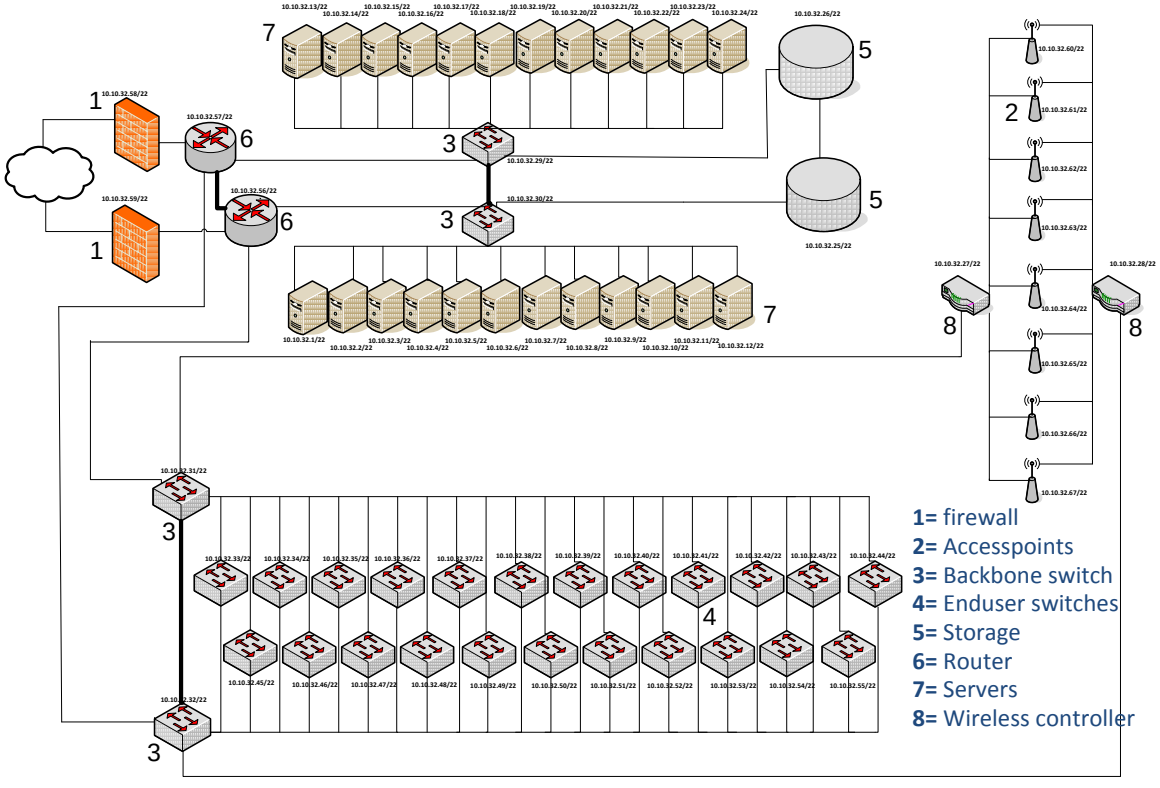
Accesspoints

Accesspoints zorgen ervoor dat werknemers gebruik kunnen maken van het netwerk via het draadloze netwerk. Omdat sommige medewerkers, ook in de toekomst, gebruik zullen maken van laptops, moet op alle verdiepingen een draadloos netwerk beschikbaar zijn. Zoals ik eerder heb uitgezocht, is het bereik van de accesspoints ruim voldoende om een gehele verdieping van een draadloos netwerk te voorzien.

Voordat ik bij de hardware leverancier ga kijken wat ze te bieden hebben, moet ik eerst weten waar ik op moet letten om de juiste keuze te kunnen maken. Om dat te achterhalen, heb ik me eerst moeten verdiepen in accesspoints en de werking daarvan.

Tijdens mijn onderzoek (zie bijlage) ben ik erachter gekomen dat ik een ontwerpfout heb gemaakt. Ik heb bij het maken van het netwerkontwerp aangegeven dat de accesspoints op een backbone-switch aangesloten moeten worden. Dit zou echter geen juiste oplossing zijn. Ik heb namelijk gemerkt dat de accesspoints verbonden moeten worden met een wireless controller en niet met een backbone-switch. De wireless controller zorgt voor de juiste werking van de accesspoints en zorgt er ook voor dat gebruikers probleemloos gebruik kunnen maken van de verschillende accesspoints, zonder dat ze daar iets van merken.

Nu ik weet dat er geen zes, maar vier backbone-switches nodig zijn, zal ik de opdrachtgever adviseren om twee Cisco N5000 1RU switches aan te schaffen en geen vier. Hiermee gaat er €18.850,- minder van het budget af. Het budget bedraagt nu €571.059,- .



Netwerkontwerp Mina-IT aangepast

Zoals op de vorige pagina is weergegeven heb ik de architectuur tekening aangepast. Deze is ook in de bijlage te vinden (Netwerkontwerp-Mina-IT_aangepast.vsd).

Nu moet ik eerst twee geschikte wireless controllers vinden voor het netwerk, voordat ik een geschikte accesspoint ga zoeken. Om een juiste netwerkcontroller te vinden, moet ik eerst weten waar ik op moeten letten bij het maken van de juiste keuze. Ik ga daarom eerst onderzoek verrichten naar wireless controllers en de werking daarvan.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande wireless-controllers in aanmerking gekomen:

Product	Snelheid	Aantal AP's	Gebruikers	beveiliging	prijs
Cisco 4400 Series WLAN Controller of up to 12 Lightweight APs	1 gb/s	12	2000	Ja	€4.999,-
HP ProCurve MSM730 Access Controller	100mb/s	40	500	Ja	€1.999,-
Netgear ProSafe Wirelless Controller incl. 8 10/100 PoE poorten	100mb/s	16	256	Ja	€1.559,-

Zoals bekend is, moet de overdrachtsnelheid van de wireless controllers minimaal 1 gb/s zijn. Er is maar één wireless controller die hier aan voldoet, namelijk de Cisco wireless controller. Ook kan deze wireless controller het meeste aantal gebruikers ondersteunen en biedt het de beste beveiliging van de drie, namelijk: RSA, RC4, MD5, AES, 128-bits WEP, SSL, TLS 1.0, 104-bits WEP, TKIP, WPA, WPA2, PKI en AES-CCMP.
Deze wireless controller voldoet prima aan de eisen voor het netwerk. Ik ga daarom de opdrachtgever adviseren om hier twee van aan te schaffen. Dat komt neer op €9998,-. Hiermee blijft er nog €561.061,- over van het budget.

Voor het aansluiten van de wireless controller en de accesspoints hebben we geen extra backbone-switches nodig. Ik heb eerder de opdrachtgever geadviseerd om twee backbone-switches aan te schaffen voor de enduser-switches. Echter hebben deze backbone-switches 40 poorten, terwijl er maar 23 enduser-switches zijn. Dit betekent dat beide backbone-switches nog 17 poorten vrij hebben. Deze poorten zijn dus ruim voldoende voor het aansluiten van de twee wireless controllers en acht accesspoints.

Nu ik weet welke wireless controller ik ga gebruiken, kan ik verder gaan met het zoeken naar een geschikte accesspoint.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande accesspoints in aanmerking gekomen:

Product	Snelheid	Ethernet poorten	Prijs
HP ProCurve MSM335 WW Access Point	54 mb/s	1	€649,-
HP ProCurve MSM323 WW Access Point	54 mb/s	2	€549,-
D-LINK (DNK) DWL-8500AP 802.11A/G	108 mb/s	1	€369,-

De D-LINK accesspoint is de snelste van de drie. Ook is deze accesspoint het goedkoopst van de drie. Echter, deze accesspoint heeft maar één ethernet poort. Dat betekent dat deze accesspoint ongeschikt is voor het netwerk.

De twee HP accesspoints zijn bijna identiek aan elkaar. Alleen heeft de HP ProCurve MSM335 maar één ethernet poort terwijl de HP ProCurve MSM323 twee ethernet poorten heeft. Ook is deze accesspoint goedkoper dan de andere HP ProCurve MSM335. Deze accesspoint is eigenlijk de enige die geschikt is voor het netwerk. Ik ga de opdrachtgever daarom adviseren om hier acht van aan te schaffen. Bij elkaar kosten deze acht accesspoints €4.392,- . Dat betekent dat er nu nog €556.669,- over is van ons budget.

Servers

Het is erg belangrijk om een snel en betrouwbaar netwerk te hebben. Een netwerk is niets meer dat een medium. Het gene waar het uiteindelijk om gaat is de services waar je gebruik van kunt maken. Deze services worden door de servers geleverd. In alle netwerken zijn servers onmisbaar, of het nu om een applicatieserver gaat of om een database server. Omdat servers zo belangrijk zijn voor ons, moeten we ervoor zorgen dat we de juiste servers voor onze omgeving vinden.

We hebben eerder aangegeven dat we gebruik zullen gaan maken van virtualisatie, omdat niet alle servers altijd erg hard zullen werken. Daarom is het zonde om twaalf fysieke servers aan te schaffen waar we niet het maximale uit gaan halen. Zoals eerder afgesproken gaan we zes zware servers kopen en daarop zullen we twaalf virtuele servers installeren. Ook voor de standby omgeving hebben we de zelfde opstelling nodig. In totaal hebben we dus 12 fysieke servers nodig waar 24 virtuele servers op geïnstalleerd kunnen worden.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande servers in aanmerking gekomen:

Server	Processor	Geheugen	GB Ethernet	Type	Prijs
HP ProLiant BL680c G5	2 x Quad Core Xeon E7340 (2.4GHz)	8 GB (max 64 GB)	4	Blade	€8.199,-
IBM BladeCenter LS42 7902	2 x AMD Opteron 8431 / 2.4 GHz (6-core)	4 GB (max 128 GB)	2	Blade	€7.899,-
HP ProLiant DL180 G6	2 x Intel Xeon E5540 / 2.53 GHz (Quad-Core)	12GB(max 96 GB)	2	Blade	€3.299,-
HP ProLiant DL165 G6	2 x AMD Opteron 2435 / 2.6 GHz (6-core)	8 GB (max 32 GB)	2	Blade	€2.749,-
Dell PowerEdge R710	1 x Intel Xeon E5530 2.4 Ghz (Quad-Core)	12 Gb(max 144 GB)	2	Blade	€2.199,-
Lenovo ThinkServer RD220	1 x Intel Xeon E5520 / 2.26 GHz (Quad-Core)	2 Gb (max 128 GB)	2	Blade	€2.049,-

Tijdens mijn onderzoek ben ik erachter gekomen dat IBM en HP de grootste spelers op de markt zijn op het gebied van servers. De HP ProLiant BL680c G5 server is de duurste en biedt vier Gb ethernet poorten. Wij hebben echter maar twee Gb ethernet poorten nodig. Als wij deze server zouden kiezen dan zouden we niet het maximale uit de server kunnen halen. Het zal daarom geldverspilling zijn als we deze server zouden aanschaffen. Daarom valt deze server af.

Zoals reeds aangegeven willen we per virtuele server minimaal twee cores hebben van 2,5Ghz. Dit betekent dat we dus minimaal een quadcore van 2.5 Ghz. nodig hebben. Daarom vallen tevens de Dell en lenove servers uit de selectie.

De IBM server is de duurste van de overgebleven drie servers. Echter is deze zeker niet de beste. De HP ProLiant DL165 G6 is de goedkoopste van de drie en heeft meer geheugen. In de IBM server is maximaal 128 GB aan geheugen te plaatsen. Zoveel geheugen zouden wij nooit nodig hebben, daarom is het niet financieel verantwoord om voor deze server te kiezen. Deze server valt zodoende ook af.

Nu blijven de HP ProLiant DL180 G6 en de HP ProLiant DL165 G6 over. De HP ProLiant DL180 heeft 4 Gb geheugen meer ter beschikking en kan maximaal 96 GB aan geheugen hebben, in tegenstelling tot de HP ProLiant DL165 die maar 32 GB aan geheugen kan dragen.

Het laatste grote verschil tussen deze twee servers is de processor. De AMD processor heeft 6 cores. De Xeon processor heeft 4 cores. Echter is de Xeon processor in praktijk sneller. Hieronder zijn de resultaten van een benchmark (toms hardware) die dit bevestigt.

Model	Speed (GHz)	Max. clock 4 cores busy (GHz)	L2 Cache (KB)	L3 Cache (MB)	Interconnect Bandwidth in One Direction
AMD Opteron 2435	2.6	2.6	6 x 512 KB	6 MB	9.8 GB/s
Intel Xeon E5540	2.53	2.66	4 x 256 KB	8 MB	11.7 GB/s

Hiermee is de HP ProLiant DL180 G6 wederom beter. Ook is het verschil in prijs onder de 500 euro. Je krijgt dus veel meer waar voor je geld.

Ik zal daarom de opdrachtgever aanraden om twaalf HP ProLiant DL180 G6 servers aan te schaffen. Bij elkaar kosten deze servers €39.588,- (exclusief de schijven).
Dit betekent dat er nog €517.081,- van ons budget over blijft.

Voor High Availability doeleinden zullen de servers in twee clusters geplaatst moeten worden. Zo kunnen de servers elkaars services overnemen in geval van calamiteiten. Echter zal de systeembeheerder hier zelf zorg voor moet dragen, omdat clustering buiten de scope van het project valt. Ik zal hier daarom niet verder op ingaan.

Op verzoek van mevrouw Van der Hoek en de heer Huiberts zal ik de komende hoofdstukken niet uitgebreid behandelen omdat de nadruk van het project daar niet op ligt. Bij het uitbrengen van een advies over de Backup Units, UPS en de verbindingen naar het hoofdkantoor, zal ik alleen aangeven welke producten ik adviseer aan de opdrachtgever en waarom.

Back-up Units

Ik heb voor een storage oplossing gekozen waarbij de data te allen tijde op twee storage stations staan opgeslagen. Beide storage stations staan echter wel in hetzelfde gebouw. Dit betekent dat wanneer het gebouw bijvoorbeeld afbrandt, alle data alsnog kwijt zullen raken. Om dit probleem te voorkomen, zullen de data ook buiten het gebouw bewaard moeten worden. Hiervoor zijn de juiste back-up units nodig. De data kunnen we bijvoorbeeld op tapes opslaan, die vervolgens dagelijks of wekelijks worden bewaard in de hoofdvestiging.

Daarnaast zou er gebruik gemaakt kunnen worden van de 'MEDIA, TRANSPORT EN OPSLAG' service van Getronics. Hierbij komen Getronics medewerkers de tapes dagelijks ophalen, waarna deze naar kluizen worden gebracht. Zo ben je er altijd zeker van dat de data ook in geval van calamiteiten buiten het gebouw veilig is.

Om te kunnen achterhalen wat de meest geschikte back-up unit is, moet ik eerst weten hoeveel data de back-up unit moet kunnen bewaren. Omdat dit een fictieve opdracht is, zal het niet mogelijk zijn om te weten hoeveel data uiteindelijk gebackupt moet worden. Ik kies daarom voor een fictieve waarde van 10 TB.

Toen ik op het Internet zocht naar de beste back-up oplossingen, kwam ik al snel bij HP uit. HP is één van de grootste spelers op het gebied van back-up units en tapes.
Ik heb bij Misco uitgezocht wat in dit geval de beste back-up oplossing is en ik kwam uit op de HP StorageWorks MSL2024 1 Ultrium 960 Drive Library. Deze back-up unit kost €6.226,95 en kan maximaal 19.2 TB aan gecomprimeerde data opslaan, en 9.6 TB aan data van oorspronkelijk formaat. In deze tape unit kunnen maximaal 24 tapes geplaatst worden. Hiermee kan deze back-up unit meer data opslaan dan elke ander back-up unit die de leverancier kan leveren. Ook is dit een financieel bewuste keuze, omdat er ook duurdere back-up units leverbaar zijn, die minder snel zijn en minder data kunnen opslaan. Al met al is dit dus een ideale back-up unit voor Mina-IT.

Ik zal de opdrachtgever adviseren om deze back-up unit aan te schaffen. Hiermee blijft er nog €510.854 over van het budget.

UPS

Wanneer er een stroomstoring optreedt en de servers meteen uitvallen, kan dit voor grote problemen zorgen. Dit omdat componenten van de server hierdoor defect kunnen raken. Om in geval van een stroomstoring de servers netjes te kunnen afsluiten, is er een UPS (Uninterruptible Power Supply) nodig. Hiermee krijgen de beheerders een paar extra minuten de tijd om de servers netjes af te sluiten. De servers zijn ook zo in te stellen dat ze automatisch afsluiten wanneer er een stroomstoring optreedt, en dat de UPS vervolgens de stroom levert in plaats van de gebruikelijke netstroom.

Een tweede belangrijke functie van UPS is het beschermen van je hardware tegen hoge stroompieken. Wanneer er hoge stroompieken optreden, zal de UPS deze opvangen waardoor ze geen gevaar meer vormen voor de servers.

Om de juiste UPS te vinden moet ik eerst weten hoeveel stroom de servers verbruiken. Met deze gegevens kan ik zoeken naar de UPS die aan de behoeften van de servers voldoet.

Eerder heb ik de opdrachtgever geadviseerd om twaalf HP ProLiant DL180 G6 servers aan te schaffen. Ik heb bij HP uitgezocht hoeveel stroom deze servers verbruiken en dat bleek 470 watt per server te zijn. Dat betekent dat de twaalf servers bij elkaar 470 x 12 = 5640 watt verbruiken.

Nu ik weet hoe sterk de UPS moet zijn, heb ik gekeken naar het aanbod van Misco. Ik heb de verschillende UPS units met elkaar vergeleken en uiteindelijk kwam ik bij de APC Smart-UPS VT 10kVA 400V terecht. Deze UPS levert 8000 watt, wat meer dan voldoende is, en heeft daarnaast een zeer acceptabele prijs van €6.599. APC is de marktleider op het gebied van UPS’s en ik ben er daarom zeker van dat dit een prima keuze is voor het netwerk.

Ik ga de opdrachtgever adviseren om deze UPS aan te schaffen. Hiermee blijft er nog €504.255,- over van het budget.

Verbindingen naar het hoofdkantoor

De opdrachtgever zal veel beheertaken op de nieuwe vestiging laten uitvoeren door de beheerders van de hoofdvestiging. Hiervoor moet er een snelle verbinding tussen de vestigingen beschikbaar zijn. Ook moet er een tweede verbinding aanwezig zijn in geval van een storing met de primaire verbinding, zodat de beheerders altijd hun taken kunnen uitvoeren bij storingen. Deze verbinding hoeft echter niet zo snel te zijn, zodat er niet op de kosten wordt gedrukt.

Toen ik op het Internet zocht naar de verbindingen die daaraan kunnen voldoen, kwam ik erachter dat het alleen met glasvezelverbindingen mogelijk is. Echter zijn glasvezelverbindingen erg duur. De opdrachtgever heeft aangegeven dat hij niet meer dan €2.500, - per maand aan de verbindingen wil uitgeven.

Ik heb op het Internet naar leveranciers gezocht en ik kwam uiteindelijk uit bij dataweb.nl. Dataweb.nl kan een 100MB/s glasvezelverbinding over VPN tussen beide vestigingen leveren. Deze verbinding kost €1500,- per maand en is snel genoeg voor de beheertaken en bestandsoverdracht tussen beide vestigingen.

Ook kan het bedrijf een kleinere back-up verbinding leveren. Deze verbinding is ook een glasvezelverbinding over VPN maar heeft een snelheid van 4 MB/s. en kost €500,- per maand. Deze back-up verbinding zal via een andere Internet provider lopen, om zo optimale veiligheid te kunnen bieden. Met deze verbindingen samen garandeert dataweb.nl een uptime van 99.98 procent.

Samen kosten deze verbindingen €2000,- per maand en dat is onder het maximum bedrag van €2500,- dat de opdrachtgever heeft vastgesteld. Ik ga de opdrachtgever adviseren om bovengenoemde verbindingen af te nemen van dataweb.nl .

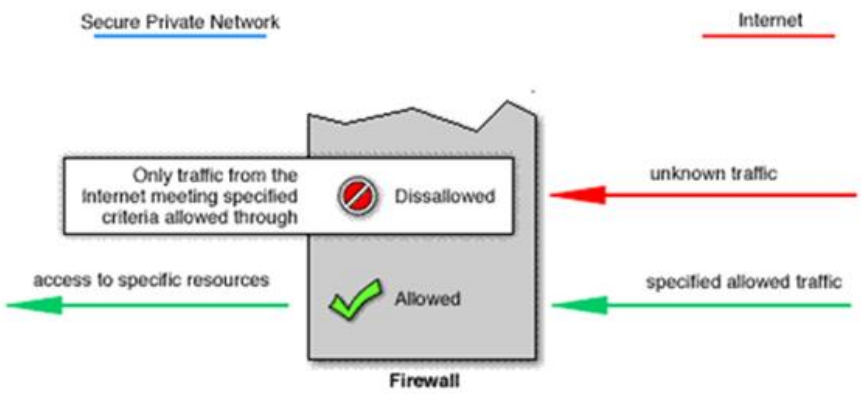
Hiermee is een eind gekomen aan het adviesrapport. In totaal heb ik producten geadviseerd die samen €495.745,- kosten. De opdrachtgever heeft aangegeven dat hij maximaal €1.000.000,- wil uitgeven aan de hardware. Het is uiteindelijk gelukt om het voor minder dan de helft van dit bedrag te doen.

Advies over de beveiliging van het netwerk

Mocht er iemand in ons netwerk willen inbreken, dan kan hij waardevolle data meenemen of vernietigen. Nu wij precies weten welke hardware componenten wij precies gaan gebruiken, is het belangrijk om te weten hoe wij ons netwerk met deze componenten gaan beveiligen.

Allereerst moeten wij achterhalen wat ons zwakke punten in het netwerk zijn. Ons netwerk is op drie manieren toegankelijk voor hackers: van buitenaf door de primaire of de back-up verbinding, door het draadloze netwerk en van binnenuit (bijvoorbeeld medewerkers met slechte bedoelingen).

Beveiligen van de primaire en back-up verbinding
Zowel de primaire verbinding als de back-up verbinding moeten eerst langs de firewalls. De beveiliging zal derhalve door de firewall uitgevoerd moeten worden. In de firewall kan door middel van acceslist aangegeven worden welk verkeer wel of niet toegelaten mag worden tot het interne netwerk. Wanneer een hacker probeert binnen te dringen door middel van een bepaalde IP of poort waar geen goedkeuring voor is, dan zal dat door de firewall tegen gehouden worden. Hieronder staat grafisch uitgelegd hoe het proces in elkaar steekt.



Mijn advies aan de netwerkbeheerders is dan ook om de firewall door middel van accesslists te configureren. Hiermee kunnen ze zelf bepalen welk verkeer wel of niet tot het netwerk toegelaten mag worden. Op deze manier worden hackers buiten de deur gehouden zonder dat het normale verkeer belemmerd wordt.

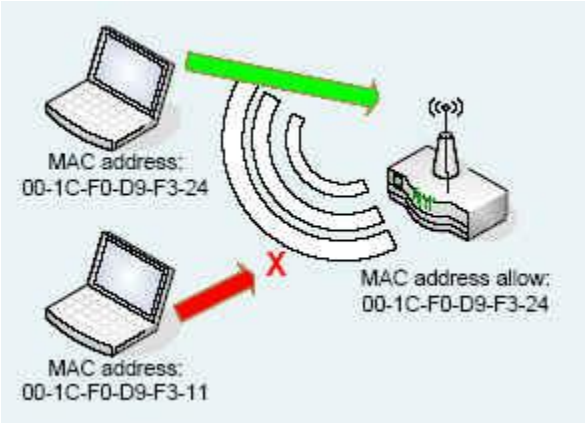
Beveiligen van het draadloze netwerk

Het draadloos netwerk vormt een groot risico omdat het niet vereist is om fysiek met het netwerk verbonden te zijn om in te kunnen breken. Dit kan ook simpelweg met een laptop buiten het gebouw gebeuren. Dit kunnen we voorkomen door het draadloos netwerk te beveiligen.

De beveiliging in ons draadloos netwerk zal door de wireless controller uitgevoed worden. Ons wireless controller kent vele vormen van beveiliging. De bekendste drie zijn WEP, WPA2 en MAC filtering.

Bij WEP is een verouderde versie van encryptie van toepassing, die relatief snel te kraken is. WPA2 is een nieuwere encryptie methode. Met WPA2 kunnen veel ingewikkeldere wachtwoorden gebruikt worden. Daarnaast worden deze wachtwoorden continue automatisch veranderd, zodat ze bijna onmogelijk te kraken zijn.

De derde methodiek is het gebruik van MAC filtering. Hiermee is het noodzaak dat de systeembeheerder alle MAC adressen van de draadloze apparatuur in de MAC filter van de wireless controller invoert. De wireless controller zal dan alleen draadloos apparatuur tot het netwerk toestaan die hij in zijn filter kent. Hiermee voorkom je dat hackers met hun laptop toegang krijgen tot het netwerk. Nog een voordeel dat je hiermee bereikt, is dat ook medewerkers hun privé laptop niet kunnen gebruiken op het netwerk. Hiermee houd je het netwerk veiliger (omdat eventuele virussen en spyware op hun privé laptop hierdoor niet in het netwerk terecht kunnen komen).

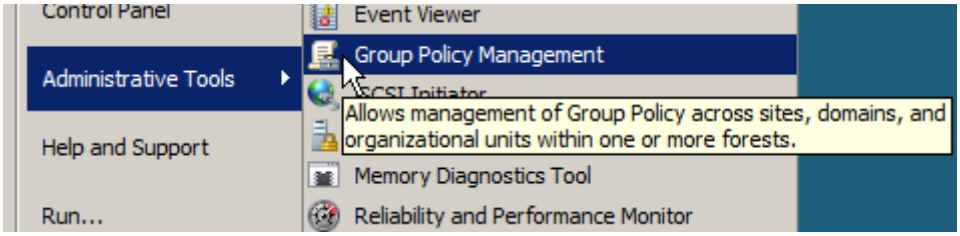


Ik raad de netwerkbeheerders aan om zowel gebruik te maken van WPA2 als MAC filtering. Op deze manier bescherm je het draadloos netwerk maximaal tegen hack-pogingen, afkomstig van zowel buiten als binnen het gebouw.

Beveiligen van het netwerk van binnenuit

Om te voorkomen dat medewerkers met kwade bedoelingen data proberen te stelen of te vernietigen, dient het netwerk ook voor intern verkeer goed beveiligen te worden. MAC filtering zal hier niet veel kunnen helpen, omdat gebruikers vanuit hun eigen werkstation kunnen hacken.

Wanneer iemand wil hacken, zal hij op de plekken willen hacken die waardevolle data bevatten. Vaak zijn dat de servers. Alle servers die gebruikt worden door Mina-IT zijn Windows servers. Standaard zouden alle normale gebruikers ook op de servers moeten kunnen inloggen. Om dit te voorkomen dien je in de Active Directory “Domain Controller Group Policy” te configureren. Hiermee voorkom je dat alle AD gebruikers op de servers kunnen inloggen. Je geeft dan alleen aan de beheerders de rechten om op de servers in te loggen.



Soms dien je een enduser gebruiker toegang te geven tot een server (bijvoorbeeld een programmeur die zijn script wilt testen op de applicatie server). Ook hier is het mogelijk om met de “Domain Group Policy” te voorkomen dat de gebruiker op andere servers gaat inloggen. Daarnaast zou je zijn rechten op de server kunnen beperken zodat hij bijvoorbeeld programma’s niet kan installeren of verwijderen. Hiermee geef je dus iedereen restricties op maat.

Hiermee kom ik aan het eind van het adviesrapport. Ik ben ervan overtuigd dat alle gegeven adviezen samen zullen zorgen voor een snelle, betrouwbare en een veilig netwerk voor Mina-IT.

Evaluatie

Met het overhandigen van het netwerkarchitectuurrapport en het adviesrapport aan de opdrachtgever heb ik dit project afgerond. Tijdens dit hoofdstuk zal ik mijn gemaakte producten evalueren. Ook zal ik het proces dat ik doorlopen heb evalueren. Tenslotte zal ik mijn competenties onderbouwen.

Evaluatie van de producten

Netwerk architectuurrapport
Hoewel dit een fictieve opdracht is, ben ik er toch in geslaagd om een hoogwaardig netwerkarchitectuurrapport te maken. In dit architectuurrapport zitten alle componenten die ook in andere grote netwerken aanwezig zijn.

Bij het maken van de architectuur is veel nagedacht over de functie van de componenten, de keuze uit de verschillende technieken en de redundantie van het ontwerp. Hiermee werd de complexiteit aanzienlijk verhoogd, omdat alle componenten ook onderling met elkaar goed moeten kunnen communiceren.

Adviesrapport
Het adviseren van de vele onderdelen van het netwerk heeft aanzienlijk meer tijd gekost dan ik had verwacht, met name omdat ik in de architectuurfase een ontwerpfout had gemaakt. Ik heb eerst het ontwerp moeten aanpassen voordat ik verder kon met het adviesrapport.

De manier waarop ik het adviesrapport heb gemaakt was voor mij nieuw. Ik heb namelijk eerst de criteria moeten vaststellen, zodat ik kon achterhalen waar ik naar op zoek was. Zodra de criteria duidelijk waren, kon ik op zoek naar de producten die aan mijn criteria voldeden. Deze producten heb ik aan de hand van de criteria met elkaar vergeleken om te zien welke het beste bij mijn ontwerp past. Dit was niet alleen voor mij overzichtelijk, maar ook voor de lezer. Ik zal in de toekomst deze methode vaker gebruiken bij het maken van keuzes.

Evaluatie van het proces

Het hanteren van projectmanagement methodiek

Het hanteren van een projectmanagement methodiek heeft me erg veel geholpen bij het uitvoeren van dit project. Ik ben dan ook zeer tevreden over de ASI methodiek. Ik heb bij het maken van de architectuur een fout gemaakt bij het ontwerp. Ik kwam daar pas achter tijdens het adviseren.

Omdat ik ASI als methodiek heb gebruikt, kon ik mijn fout in een eerder stadium herstellen zonder het project in gevaar te brengen. Als ik bijvoorbeeld de watervalmethodiek had gebruikt, was ik wel in problemen gekomen. Zoals reeds aangegeven is de watervalmethodiek niet ontworpen om achteraf wijzigingen aan te brengen in een gesloten fase.

Een ander groot voordeel van ASI is de duidelijke structuur die de methodiek biedt. Van begin tot eind kon ik mijn project uiterst gestructureerd voortzetten. Ik vind het jammer dat er weinig literatuur over ASI beschikbaar is. Als er meer literatuur over ASI te vinden was, zou ASI wellicht in praktijk veel vaker gebruikt worden.

Doelstellingen

Zoals eerder aangegeven in de opdrachtomschrijving, bestaat het resultaat van mijn project uit de volgende producten:

- Een compleet netwerkarchitectuur
- Een adviesrapport over het inrichten van het netwerk.

Ik heb beide producten met volle tevredenheid opgeleverd.

Competenties tonen

Hieronder zijn de competenties te vinden, zoals deze in het afstudeerplan beschreven zijn. Ik zal hierna onderbouwen waarom ik aan deze competenties heb voldaan:

- C9 - Ontwerpen van een infrastructuur
- J12 - Adviesproces uitvoeren

Ontwerpen van een infrastructuur

Om deze competentie te behalen heb ik de volgende taken uitgevoerd:

- Het maken van een ontwerp dat rekening houdt met operationele eisen, zoals: performance, beschikbaarheid, veiligheid, betrouwbaarheid, etc.
- Het maken van verschillende architecturen en het onderbouwen daarvan. Uiteindelijk onderbouwen waarom een bepaalde architectuur is gekozen.
- Het maken van een gedetailleerde infrastructuur inclusief IP adressering.
- Uitleg en onderbouwing van de verschillende gebruikte protocollen en functies.

Adviesproces uitvoeren

Om deze competentie te behalen heb ik de volgende taken uitgevoerd:

- De gegeven adviezen zijn onderbouwd.
- De gegeven adviezen zijn uitermate geschikt voor deze organisatie
- De adviezen zijn zoveel mogelijk SMART gedefinieerd.
- Een volledig adviesrapport met alle vooraf gedefinieerde eisen van de opdrachtgever.

Moeilijkheidsgraad bepalen

Om de complexiteit van het project te meten, zal ik het “Niveau bepalingsmodel” van de Haagsche Hogeschool gebruiken.

		Ja	Nee
Opdrachtsituatie			
1	In je opdracht heb je te maken met conflicterende (product)eisen.		X
2	Je werkt onder behoorlijke tijdsdruk.	X	
3	Je hebt meerdere (informele) opdrachtgevers die allen andere wensen/eisen kunnen hebben.		X
4	Er liggen zware kwaliteitseisen op de producten die ik aflever. Ik moet de kwaliteit duidelijk aantoonbaar maken.	X	
5	Mijn werk ligt politiek nogal gevoelig.		X
6	Deze opdracht mag absoluut niet mislukken.		X
7	Als ik mijn opdracht verknal, kost dat de afdeling klanten.		X
8	Er is veel geld gemoeid met deze opdracht.		X
9	Er zullen veel mensen te maken krijgen met mijn werk.	X	
10	Er zal veel veranderen op de afdeling/bij de klant als mijn werk af is.		X
11	De resultaten van mijn opdracht heeft het management nodig om te beslissen hoe het in de toekomst verder moet.	X	
12	Ik moet veel methoden/technieken leren voor deze klus die ik vanuit de opleiding niet ken.		X
13	Ik moet me met vakgebieden van de informatica gaan bezighouden, die niet bij mijn major horen.		X
14	Ik heb veel nieuwe business kennis nodig voor deze opdracht.		X
15	Goh, er gaat een wereld voor me open….		X
16	Er zitten allerlei vaktechnische ingewikkelheden in deze opdracht.		X

≤ 2 : Simpel
> 2 en ≤ 4 : Lastig
> 4 : Complex

In het model zijn voor mij vier van de zestien punten van toepassing. Dit betekent dat het projectniveau complex is. Ik heb in korte tijd veel verschillende onderzoeken moeten doen en adviezen moeten geven. Ook heb ik onder veel tijdsdruk (door uitloop van verschillende onderzoeken) een complete netwerkarchitectuur moeten ontwerpen. Daarnaast moest ik aan de hand van mijn producten duidelijk maken hoe ik de kwaliteitseisen van de opdrachtgever heb kunnen waarborgen. De eindproducten van mijn project zijn uiterst nauwkeurig en betrouwbaar. Aan de hand van deze producten zou een compleet netwerk ingericht kunnen worden. Door alle bovenstaande punten kom ik uit op niveau Complex. Dit wordt tevens door het beoordelingstabel bevestigd.

Het niveau van mijn positie in het project zou geleid, zelfstandig of sturend kunnen zijn. Wanneer ik kijk naar het gehele proces, komt mijn positie uit op sturend.
Dit komt doordat ik zowel opdrachtgever als uitvoerder was. Dit heeft het project voor mij extra lastig gemaakt. Tijdens het interview heb ik bijvoorbeeld de keuze gemaakt dat de opdrachtgever weinig technische kennis bezit. Op deze manier kon ik als uitvoerder zelf keuzes maken en onderbouwen. Wanneer de opdrachtgever veel technische kennis zou bezitten, zou mijn positie waarschijnlijk geleid zijn en dat was niet mijn uitgangspunt. Maar aangezien ik tijdens het project bijna alle keuzes zelf heb gemaakt, is mijn positie in het project sturend geweest.

Ik ben ervan overtuigd dat alle 500 medewerkers erg veel baat zouden hebben gehad bij het gebruik van het door mij ontworpen netwerk infrastructuur en de gegeven adviezen, indien dit project een reële opdracht was geweest.

Tot slot

Ik vond het zeer interessant en leerzaam om aan dit project te mogen werken. Ik ben veel uitdagingen tegengekomen, zowel op organisatorisch niveau als op technisch niveau. Ik was voor het eerst de opdrachtgever voor een grote project als deze. Daarnaast heb ik veel verschillende technieken gehanteerd, waar ik nooit eerder gebruik van had gemaakt.

Ik vond het uiterst leerzaam om een geheel netwerk van A tot Z te mogen ontwerpen. Ik heb veel met netwerken gedaan maar dit was voor mij wel een hele nieuwe ervaring. Ook heb ik nooit eerder een ontwerpadvies mogen maken voor een bedrijf van een dergelijk formaat. Wederom was dit erg leerzaam.

Tijdens dit project heb ik veel aspecten kunnen combineren zoals leiderschap (opdrachtgever), het bedenken en opzetten van een project en vervolgens het individueel uitvoeren van het project door middel van ASI als projectmanagement methodiek. Al met al ben ik zeer tevreden over het opgeleverde werk en ik heb er met veel plezier aan gewerkt en tot een succesvol eind gebracht.

Bijlage

In de bijlage treft u de volgende documenten:

- Interview met de opdrachtgever
- IP plan
- Definitierapport
- Architectuurrapport
- Ontwerprapport
- Hardware onderzoeken.
- Adviesrapport
- Netwerkarchitectuur

Bronnen

Ik heb tijdens het uitvoeren van mijn project gebruik gemaakt van de volgende bronnen:

- www.ratemynetworkdiagram.com
- www.misco.nl
- www.tweakers.net
- www.dataweb.nl
- ASI rapport (geleverd door de Haagsche Hogeschool)
- Ccnp Cisco Networking Academy Program (Mark McGregor, ISBN-13 : 9781587130281)
- Feilloos adviseren (Peter Block , ISBN-13: 9789052613383)
- Top-Down Network Design (Priscilla Oppenheimer , ISBN-13: 9781578700691)

Afstudeeropdracht:	**Mina-IT @ Groningen**
Document:	Interview
Student:	Mina Nabil
Afstudeerbegeleider:	Cobie van der Hoek
Expert:	Nico Huiberts
Datum:	04-10-2010

Hieronder heb ik een lijst met vragen opgesteld. Per vraag zal ik toelichten waarom deze vraag gesteld wordt en waarom het belangrijk is voor de uitvoerder om daar een antwoord op te hebben. Onder de vraag heb ik aangegeven wat het antwoord van de opdrachtgever is.

Moet er een verbinding gerealiseerd worden die altijd in verbinding is met het hoofdkantoor?

- Dit wil ik weten zodat ik zowel de hardware als de leverancier kan kiezen die dit ondersteunen.

Antwoord:

De opdrachtgever wilt inderdaad dat er 24x7 een directe verbinding aanwezig is met het hoofdkantoor. Tevens wil hij een back-up verbinding die met het hoofdkantoor verbonden is. Dit in het geval van falen van de primaire verbinding. Het altijd verbonden blijven met het hoofdkantoor is essentieel omdat een groot gedeelte van het nieuwe netwerk beheerd zal worden door beheerders op het hoofdkantoor.

Is er een voorkeur voor een vaste verbinding en back-up verbinding naar het hoofdkantoor?

- Het is erg belangrijk om te weten hoe de nieuwe vestiging verbonden moet worden met de hoofdvestiging. Hier zijn veel methodes voor, die erg veel van elkaar verschillen. Ook speelt het budget hier een belangrijke rol in, omdat de ene oplossing vele malen duurder is dan de andere. Dit geldt ook voor de backup-verbinding. De opdrachtgever zou voor een goedkopere backup-verbinding kunnen kiezen, om zo geld te besparen.

Antwoord:

- Door de beperkte technische kennis van de opdrachtgever kan hij hierin geen keuze maken. De opdrachtgever wil echter niet meer dan €2500,- per maand aan de verbindingen uitgeven.

Is er een voorkeur voor bepaalde types hardware die we moeten gebruiken ?

- Dit is belangrijk om te weten omdat ik gericht naar bepaalde modellen hardware moet zoeken als de opdrachtgever dat specifiek aangeeft.

Antwoord:

- Door de beperkte technische kennis van de opdrachtgever heeft hij geen voorkeur voor een bepaalde hardware type of fabrikant. Ik zal zelf dus moeten uitzoeken welk type het meest geschikt is voor het nieuwe netwerk. Voor het aanschaffen van de apparatuur is een budget van €1.000.000,- beschikbaar gesteld. Dit bedrag is exclusief de kosten voor het bouwen van het netwerk. Dit bedrag is zelf door de opdrachtgever bepaald. Er is eventueel meer geld beschikbaar als dat echt nodig is, maar het is in principe wel de bedoeling dat we binnen het budget blijven.

Is al bekend hoe het netwerk beveiligd zal worden?

- Dit wil ik weten zodat ik mijn hardware op het bestaande beveiligingsplan kan afstemmen. Als er nog niet over de beveiliging is nagedacht, kan ik zelf een beveiligingsplan maken en de nieuwe hardware daarop afstemmen.

Antwoord:

- De opdrachtgever heeft aangegeven dat hij zelf niet over de technische kennis beschikt om de beveiliging van het netwerk te bedenken. Ik zal daarom zelf moeten uitzoeken hoe ik het nieuwe netwerk het beste kan beveiligen.

Wanneer zal het nieuwe gebouw in gebruik genomen worden en wat is de deadline van dit project?

- Dit wil ik weten om mijn planning te kunnen maken. Ook is dit belangrijk om te weten zodat ik rekening kan houden met de levertijden van hardware en Internetverbindingen.

Antwoord:

- De nieuwe vestiging zal geopend worden op 01-01-2011. Dit betekent dat het project uiterlijk 31-11-2010 afgerond moet zijn, zodat het netwerk in de resterende maand gebouwd kan worden door het externe bedrijf.

Moet er rekening gehouden worden met High availablity?

- Dit is van belang om de juiste hardware te kunnen adviseren en om de netwerkarchitectuur daarop af te stemmen.

Antwoord:

- Er moet een advies komen voor de high availablity van de netwerkapparatuur, servers en de storage. Hierbij moet rekening gehouden worden met het maken van back-ups en het elimineren van single point of failures. Daarnaast moet er gedacht worden aan back-up stroomvoorzieningen zoals UPS.

Hoeveel downtime mag er per jaar voorkomen?

- Dit is erg belangrijk om te weten, omdat dit voor een groot gedeelte zal bepalen welke netwerkapparatuur je gaat gebruiken en hoe de architectuur eruit komt te zien. Ook zal er meer redundante apparatuur aanwezig moeten zijn als de downtime erg kort is.

Antwoord:

De opdrachtgever wil dat zijn netwerk minimaal een uptime van 99% heeft. Dit betekent dat de downtime 1% is, oftewel 3,5 dagen per jaar. De hoofdvestiging heeft ook dezelfde uptime garantie en dit bevalt de opdrachtgever prima. Het is voor hem dan ook niet noodzakelijk om meer geld te investeren in een hogere uptime.

Voorkeur voor ip-adressen structuur?

- De opdrachtgever heeft al aangegeven dat beide netwerken 24x7 met elkaar verbonden moeten zijn. Het is dus cruciaal om te weten wat voor ip-adressen er worden gebruikt, om conflicten te voorkomen. Ook kan het een wens van de opdrachtgever zijn om een bepaalde IP-reeks te gebruiken.

Antwoord:

Door de beperkte technische kennis van de opdrachtgever heeft hij hier geen antwoord op kunnen geven. Wel heeft hij bij de systeembeheerder nagevraagd wat ze nu zelf gebruiken en dat bleek de 10.10.0.0/19 reeks te zijn. Ook heeft de systeembeheerder aangegeven dat de hele organisatie onder de 10.10.0.0/18 reeks valt, dus ook de nieuwe vestiging. Ik zal zelf onderzoeken wat de meest geschikte reeks is voor de opdrachtgever, en deze vervolgens gebruiken.

Voorkeur voor aantal poorten switch?

- Dit heeft met meerdere factoren te maken; onder andere het formaat van de patchkasten. Wanneer de werkgever over weinig patchkasten beschikt, is het beter om switches te kopen met meer poorten zodat er minder patchkasten nodig zijn. Echter, wanneer een 48 poorts switch kapot gaat, kunnen er maximaal 48 mensen niet werken. Wanneer een 16 poorts switch gebruikt wordt, is de schade veel beperkter.

Antwoord:

- De opdrachtgever heeft geen voorkeur voor het aantal poorten dat een switch moet bieden. Ik zal zelf onderzoeken wat voor de opdrachtgever de beste oplossing is.

Voorkeur bereik draadloos netwerk?

- Wilt de werkgever op iedere verdieping een draadloos netwerk hebben? Dit is belangrijk om te weten omdat er meer apparatuur nodig is wanneer hij meer bereik wenst.

Antwoord:

- De opdrachtgever heeft aangegeven dat er op iedere verdieping een draadloos netwerk aanwezig dient te zijn.

Voorkeur beveiliging draadloos netwerk?

- Draadloze netwerken kunnen op meerdere manieren beveiligd worden. Het is belangrijk om te weten of de opdrachtgever een voorkeur heeft voor een bepaalde methode. Als dat niet het geval is, zal ik zelf een beveiligingstechniek kiezen.

Antwoord:

- De opdrachtgever heeft geen voorkeur voor een bepaalde beveiligingsmethode. Ik zal zelf uitzoeken wat de beste beveiligingsmethode is voor de opdrachtgever.

Moet het netwerk probleemloos door draaien bij een storing aan elk netwerkcomponent?

- Omdat netwerkapparatuur nu eenmaal niet 100 procent betrouwbaar is, moeten we rekening houden met storingen en defecte netwerkapparatuur. Het is erg belangrijk om te weten hoeveel downtime de opdrachtgever accepteert. Downtime kan geminimaliseerd worden door netwerkapparatuur dubbel uit te voeren (redundantie). Hierdoor moet er wel meer hardware aangeschaft worden die misschien nooit gebruikt zal worden. Dit is een belangrijke keuze die de opdrachtgever moet maken.

Antwoord:

- De opdrachtgever heeft aangegeven dat alle bedrijfskritieke onderdelen van het netwerk één klap mogen hebben en toch nog 100 procent moet functioneren. Onder de bedrijfkritieke onderdelen worden de onderdelen verstaan die de totale productie kunnen stoppen bij een defect. De opdrachtgever wil niet het risico lopen dat zijn productie stil komt te liggen door het falen van bedrijfskritieke onderdelen.

Uitwijklocatie nodig?

- Het is belangrijk om te weten of de opdrachtgever na een calamiteit nog binnen een voorafgestelde tijd weer operationeel wilt zijn. Als dit het geval is, zal er een uitwijklocatie nodig zijn. Ook kan ervoor gekozen worden om de hoofdvestiging als uitwijklocatie te gebruiken. Wanneer er wordt gekozen om een uitwijklocatie te bouwen, zal er ook extra hardware aangeschaft moeten worden.

Antwoord:

- De opdrachtgever heeft ervoor gekozen om **geen** uitwijklocatie in te richten. Bij calamiteiten zullen de belangrijkste taken door het hoofdkantoor overgenomen worden.

Hoeveel servers nodig?

- Het is belangrijk om te weten hoeveel servers de opdrachtgever verwacht te installeren. Dit heeft invloed op het type servers dat aangeschaft moet worden. Wanneer er een groot aantal servers gebruikt gaat worden, is het wellicht beter om voor blade servers te kiezen omdat deze minder ruimte innemen.

Antwoord:

- De opdrachtgever kon niet vertellen hoeveel servers er nodig waren. Hij wist me wel te vertellen dat ze vier grote applicaties gebruiken die elk een eigen server hebben.

Wil je gebruik maken van virtualisatie?

- Tegenwoordig is virtualisatie erg populair in de IT. De opdrachtgever kan ervoor kiezen om de meeste servers te gaan virtualiseren en daarmee minder hardware te kopen.

Antwoord:

- De opdrachtgever kon hier geen keuze in maken. Hij heeft mij gevraagd om te onderzoeken wat voor hem de beste methode is.

Voorkeur voor storage?

- Er zijn erg veel verschillende storage oplossingen beschikbaar. Het is belangrijk om te weten wat de voorkeur van de opdrachtgever is. Als de opdrachtgever hier geen voorkeur voor heeft, dan zal ik zelf onderzoeken wat de beste oplossing is voor de opdrachtgever.

Antwoord:

- Door de beperkte technische kennis van de opdrachtgever heeft hij hier geen keuze in kunnen maken. De opdrachtgever heeft mij verzocht zelf een storage oplossing te kiezen na dit onderzocht te hebben.

Moet er rekening mee worden gehouden dat het aantal medewerkers gaat groeien? Tot hoeveel?

- Dit is erg esssentieel om te weten, zodat we de netwerkapparatuur daarop kunnen afstemmen. Het is beter om het netwerk futureproof te maken, zodat er geen ingrijpende netwerkmigraties hoeven plaats te vinden in de toekomst. Daarnaast zal de inkoop goedkoper zijn wanneer de netwerkapparatuur in één keer wordt ingekocht. Tenslotte hoeft er dan geen apart budget voor aangevraagd te worden.

Antwoord:

- De opdrachtgever heeft aangegeven dat het aantal medewerkers in deze vestiging kan groeien tot maximaal 500 medewerkers. Ook zou hij graag alle IT-voorzieningen voor 500 werknemers willen inrichten.

Wil je extra standby netwerkapparatuur?

- De opdrachtgever kan er voor kiezen om extra netwerkapparatuur te kopen en die op te slaan, om bij storingen snel zelf de apparatuur te kunnen verwisselen en op deze manier maar zeer kort down te zijn. De opdrachtgever kan er echter ook voor kiezen om een onderhoudscontract te nemen bij een grote leverancier, die garandeert dat de apparatuur binnen een paar uur op locatie afgeleverd wordt.

Antwoord:

- De opdrachtgever wil geen extra netwerkapparatuur aanschaffen, omdat hij een onderhoudscontract met de leverancier heeft waardoor er binnen 24 uur een nieuw apparaat geleverd wordt. Ook zullen de belangrijkste componenten redundant uitgevoerd moeten worden. Vandaar dat het dan overbodig luxe is om extra hardware aan te schaffen.

Afstudeeropdracht:	**Mina-IT @ Groningen**
Document:	Onderzoeken
Student:	Mina Nabil
Afstudeerbegeleider:	Cobie van der Hoek
Expert:	Nico Huiberts
Datum:	04-10-2010

Onderzoek naar een werkstation.

Om het juiste werkstation te vinden, moet ik eerst achterhalen hoeveel resources de werknemers nodig hebben. Hier kom ik achter door uit te zoeken wat voor applicaties de werknemers gaan gebruiken en hoeveel resources deze vragen van het systeem. Ook is het van belang om te weten of de gebruikers constant hun e-mail en Internetbrowser gebruiken. Tenslotte is het belangrijk om te weten wat voor OS er op de machine zal draaien.

Omdat de systemen die in de nieuwe vestiging komen reeds gebruikt worden in de hoofdvestiging, neem ik contact op met de systeembeheerder zodat ik meer te weten kan komen over het gebruik van de applicaties.

Ik heb de systeembeheerder van de hoofdvestiging de volgende vragen gesteld:
Wat zijn de systeemeisen van de applicaties?
Welke OS zal uiteindelijk op het werkstation draaien?
Gebruiken de werknemers regelmatig hun e-mail en het Internet?

Van de systeembeheerder heb ik de volgende antwoorden gekregen:
Wat zijn de systeemeisen van de applicaties?
De systeembeheerder heeft aangegeven dat drie applicaties ongeveer evenveel resources gebruiken. De vierde applicatie gebruikt bijna twee keer zoveel resources dan de overige drie. Hieronder staan de resources die elke applicatie gebruikt:

- 400 MB geheugen
- Ongeveer 300 mhz (dit is berekend door het percentage van de taskmanager te verdelen over de totale beschikbare processorkracht).
- 2 GB harde schijfruimte.

Welke OS zal uiteindelijk op het werkstation draaien?
De systeembeheerder heeft aangegeven dat Windows 7 zal draaien op de nieuwe machines. Dit is op de hoofdvestiging inmiddels getest en het werkt prima met alle applicaties. Ik heb uitgezocht wat de systeemeisen van Windows 7 zijn:

- 1,0 GHz-processor (32-bits CPU)
- 1GB RAM-geheugen (32-bits)
- 16 GB vrije schijfruimte (32-bits)

Gebruiken de werknemers regelmatig hun e-mail en het Internet?
De systeembeheerder heeft aangegeven dat de gebruikers de hele dag Outlook 2007 open hebben staan. Ook maken ze regelmatig gebruik van Internet Explorer 7.

Ik heb uitgezocht hoeveel resources Internet Explorer 7 nodig heeft. Dit bleek 32 Mb te zijn bij normaal gebruik en 150 mhz bij intensief gebruik. Voor Outlook is 64 Mb aan geheugen nodig en 100 mhz aan cpu kracht bij intensief gebruik. Voor de installatie van beide applicaties is ongeveer 1,5 GB aan schijfruimte nodig.

Nu ik weet hoeveel applicaties er gebruikt worden, moet ik alle resources bij elkaar optellen om erachter te komen wat we uiteindelijk nodig hebben.

Applicatie	**Geheugen**	**CPU**	**Schijfruimte**
Windows 7 (32-bit)	1 Gb	1,0 ghz	16 GB
Applicatie 1	400 MB	300 mhz	2 GB
Applicatie 2	400 MB	300 mhz	2 GB
Applicatie 3	400 MB	300 mhz	2 GB
Applicatie 4	800 MB	600 mhz	4 GB
Internet Explorer 7	32 MB	150 mhz	750 MB
Microsoft Outlook 2007	64 MB	100 mhz	750 MB
Totaal	3096 MB	2750 mhz	27,5 GB

De minimale systeemeisen voor het werkstation zullen zijn:

- 3096 Mb geheugen.
- 2750 mhz cpu.
- 27,5 Gb hardeschijf.

Omdat ik graag futureproof werkstations wil hebben, zal ik iets krachtigere systemen nemen dan nu in eerste instantie nodig is. Dit zodat we in de toekomst bij uitbreiding van applicaties niet meteen nieuwe werkstation hoeven aan te schaffen. Hieronder de eisen waar het futureproof werkstation aan moet voldoen:

- 4 GB geheugen
- 3 GHZ CPU
- 80 Gb Harde schijf (dit is gebaseerd op de minimale grootte van een harde schijf die momenteel te verkrijgen is).

Nu ik weet wat het werkstation moet kunnen, is het tijd om te kijken wat Misco te bieden heeft. Ik heb meerdere werkstations gevonden die voor mij interessant zijn:

HP Compaq Business Desktop dc7900
- Core 2 Duo E8400 3 GHz
- 2 Gb geheugen (+ 2gb geheugen is €60 extra)
- 160 Gb hardeschijf

Prijs €595 + €60 (extra geheugen) = €655,-

HP Compaq 6000 Pro
- Core 2 Duo E8400 3 GHz
- 2 Gb geheugen (+ 2gb geheugen is €60 extra)
- 250 Gb hardeschijf

Prijs €529 + €60 (extra geheugen) = €589,-

Acer Veriton M670G
- Core 2 Duo E8500 3.16 GHz
- 2 Gb geheugen (+ 2gb geheugen is €60 extra)
- 320 Gb hardeschijf

Prijs €595 + €60 (extra geheugen) = €655,-

Dell OptiPlex 780DT
- Core 2 Duo E8500 3.16GHz
- 4GB geheugen
- 250 Gb hardeschijf

Prijs €659,-

Werkstation	Geheugen	CPU	Hardeschijf	Prijs
HP Compaq Business dc7900	2gb + 2gb extra	3 GHz	160 Gb	€655,-
HP Compaq 6000 Pro	2gb + 2gb extra	3 GHz	250 Gb	€589,-
Acer Veriton M670G	2gb + 2gb extra	**3.16GHz**	320 Gb	€655,-
Dell OptiPlex 780DT	4 gb standaard	**3.16GHz**	**250** Gb	€659,-

Onderzoek naar een accesspoint

Tijdens dit onderzoek ben ik erachter gekomen dat onderstaande punten het meest van belang zijn bij het aanschaffen van een accesspoint:

- Bereik van de accesspoint
- Overdrachtsnelheid
- Ethernet verbindingen
- Prijs

De bovenstaande aspecten zijn gebaseerd op eigen ervaringen en voorbeelden uit het boek Top-Down Network Design.

Het bereik van de meeste accesspoints is boven de 75 meter. Het is wel belangrijk om de accesspoints op de juiste locatie te installeren voor de maximale performance. Het is daarom niet handig om de accesspoints op elke verdieping op dezelfde plek te installeren. De accesspoints kunnen beter geïnstalleerd worden waar de meeste gebruikers aan het werk zijn.

Ik heb uitgezocht wat de wireless snelheden zijn en ik ben erachter gekomen dat bijna alle accesspoints een maximale snelheid hebben van 54 mb/s. Het is algemeen bekend dat draadloze netwerken vele malen langzamer werken dan ethernet netwerken. Onze accesspoints moeten dus een snelheid hebben van minimaal 54 mb/s.

Omdat accesspoints op twee wireless controllers aangesloten zullen worden, is het een eis dat alle accesspoints minimaal twee ethernet poorten hebben (geen beheerpoorten).

Net zoals bij de rest van de componenten is het ook hier belangrijk om een prijsbewuste keuze te maken.

In het volgende schema is te zien welke accesspoints de hardware leverancier levert, die voor ons interessant zijn:

Product	Snelheid	Ethernet poorten	Prijs
HP ProCurve MSM335 WW Access Point	54 mb/s	1	€649,-
HP ProCurve MSM323 WW Access Point	54 mb/s	2	€549,-
D-LINK (DNK) DWL-8500AP 802.11A/G	108 mb/s	1	€369,-

Onderzoek naar een backbone-switch

Om te weten waar ik op moet letten bij het kiezen van de juiste backbone-switch, heb ik onderzoek gedaan naar de eigenschappen van een backbone-switch. Hieronder staan de belangrijkste criteria opgesomd waarop de switch beoordeeld wordt.

- Redundante stroomvoorziening
- Aantal poorten
- Overdrachtssnelheid
- prijs

De onderstaande aspecten zijn gebaseerd op eigen ervaringen en voorbeelden uit het boek Top-Down Network Design.

Tijdens dit onderzoek ben ik erachter gekomen dat de stroomvoorziening en de FAN meestal de zwakste onderdelen zijn van de switch. Wanneer de FAN kapot gaat, kan de switch niet meer gekoeld worden. Het gevolg hiervan is dat de switch uiteindelijk oververhit raakt en kapot gaat. Om dit probleem te voorkomen, wordt bij sommige switches de stroomvoorziening en de FAN dubbel uitgevoerd. Dit is een eigenschap die ik ook wil hebben in de backbone-switch.

Volgens ons ontwerp moeten de backbone-switches die de enduser-switches aan het netwerk gaan koppelen, minimaal 23 poorten hebben. De backbone-switch die het serverpark aan het netwerk gaat koppelen, moet minimaal 13 poorten hebben. De backbone-switch die de wireless accesspoints aan het netwerk moet koppelen, moet minimaal 8 poorten hebben.

Ik heb aangegeven dat alle enduser-switches minimaal 1 gb/s snelheid moeten hebben. Bij de backbone-switch moet er vele malen meer verkeer doorheen. Ik heb uitgezocht wat momenteel sneller is dan 1 gb/s en ik kwam bij de 10 gb/s uit. Veel sneller dan dit is momenteel nog niet verkrijgbaar voor middelgrote netwerken. Zodoende wil ik dat onze switch minimaal 24 x 10 gb/s poorten heeft.

Nu ik weet waar ik precies naar op zoek ben, ga ik bij Misco kijken wat ze te bieden hebben.

Hieronder staan de backbone-switches die het meest voldoen aan onze eisen.

product	**Poorten**	**Snelheid**	**Redundante hardware**	**Prijs**
Cisco N5000 2RU CHASSIS 5 FAN	40	10 gb/s	Ja	€17.623,22
Cisco N5000 1RU Chassis 2 Fan 20p	20	10 gb/s	Ja	€9.425,21
HP 2408 24-10GBE W/8-8GB	24	10 gb/s	Nee	€ 42.065,00

Onderzoek naar een enduser-switch

Om te kunnen achterhalen welke enduser-switch het meest geschikt is voor ons netwerk, moet ik eerst weten welke factoren hier van belang zijn. Tijdens het onderzoek naar de werking van switches, heb ik vastgesteld dat onderstaande punten het belangrijkst zijn:

- Overdrachtssnelheid
- Remote beheerbaar
- Protocollen die gebruikt worden
- Prijs

De onderstaande aspecten zijn gebaseerd op eigen ervaringen en voorbeelden uit het boek Top-Down Network Design.

Zoals reeds aangegeven wil ik graag dat al onze netwerkapparatuur minimaal een overdrachtssnelheid heeft van 1 gb/s. Dit geldt dus ook voor de enduser-switch. Veel switches hebben twee uploadpoorten van 1 gb/s en resterende poorten van 10/100 mb/s. Echter, ik wil dat alle poorten in de switches 1 gb/s (10/100/1000) poorten zijn.

Omdat voor het beheer van de nieuwe omgeving veel beheertaken uitgevoerd gaan worden door de beheerders in de hoofdvestiging, is het erg belangrijk dat de beheerders de switches remote kunnen beheren. Het is dan ook van belang dat de switches remote beheerbaar zijn.

Net als bij routers maakt de switch gebruik van meerdere protocollen. Na mijn onderzoek ben ik erachter gekomen dat de onderstaande protocollen het belangrijkst zijn:

- VLAN-ondersteuning
- Routering
- Quality of Service (QoS)

Omdat wij werken met meerdere subnetten, is het erg belangrijk dat de switch VLAN kan ondersteunen. Hiermee is per poort aan te geven in welk segment deze zit. Zo kan men heel dynamisch met subnetten omgaan.

Omdat de switch op meerdere verschillende subnetten kan werken, is het belangrijk dat de switch kan routeren tussen deze verschillende netwerksegmenten. Switches die kunnen routeren worden ook wel layer3 switches genoemd. Ze hebben deze naam gekregen omdat ze op laag 2 en laag 3 van het OSI model werken (switchen en routeren).

QoS is een soort verkeersregelaar in een netwerk. Wanneer bedrijfskritieke processen zoals VoIP gebruikt worden naast minder bedrijfskritieke processen, is het erg handig om gebruik te maken van QoS. Met QoS kun je verschillende groepen verschillende prioriteiten geven. Zo kun je bijvoorbeeld VoIP belverkeer voorrang geven boven e-mailen. Dat betekent dat wanneer een netwerk zwaar belast wordt, VoIP altijd verkeersvoorrang krijgt op bijvoorbeeld e-mail. Op deze manier kunnen gebruikers nog steeds bellen zonder vertragingen. Dat een e-mail een paar seconden later bezorgd wordt, is vaak minder erg. Natuurlijk moet het budget ook in gedachten worden gehouden. De switch die ik wil hebben, moet ook betaalbaar zijn. Ik heb 23 switches nodig, dus een klein prijsverschil per switch kan uiteindelijk in het geheel een groot prijsverschil maken.

Product	**VLAN**	**Routering**	**Protocollen**	**Prijs**
3Com Baseline Plus Switch 2928 PWR	Ja	Ja	Allemaal	€449,-
Cisco 24-poorts Gigabit Switch L2	Ja	Ja	Allemaal	€449,-
Cisco Small Business Pro 520 Ethernet Switch 24-poorts 10/100/1000 met PoE	Ja	Ja	Allemaal	€1.399,-
HP ProCurve Switch 2910al-24G	Ja	Ja	Allemaal	€1.599,-
3Com Switch 4500G 24-Poorten	Ja	Ja	Allemaal	€1.799,-

Onderzoek naar een firewall

Tijdens dit onderzoek heb ik ontdekt dat er meerdere types firewall op de markt zijn, die verschillende eigenschappen hebben. Hieronder staan de bekendste soorten opgesomd:

- packet filtering firewall
- application layer firewall
- personal firewall
- network firewall

De onderstaande aspecten zijn gebaseerd op eigen ervaringen en voorbeelden uit het boek Top-Down Network Design.

Packet filtering firewalls hebben een tabel met daarin de regels die de firewall moet hanteren. In deze regels staan welke pakketten naar welke host moeten. Hierbij wordt gebruik gemaakt van de ip-header in het data packet. Deze firewall werkt snel en efficiënt, maar biedt minder bescherming tegen virussen en spam.

Application layer firewalls hebben een ingebouwd stukje software, die voor elk gebruikte protocol bepaalt of een pakketje doorgelaten of geblokkeerd moet worden. Omdat deze firewall constant beslissingen moet nemen, is hij langzamer dan een Packet filtering firewall. Wel is deze firewall veiliger voor het netwerk, omdat hij erg goed is in het blokkeren van spam en virussen. Meestal worden Application layer firewalls ingezet in de vorm van een proxy server.

Een personal firewall zal alleen de computer beschermen waarop de firewall geïnstalleerd is. Personal firewalls kunnen meerdere technieken gebruiken om hun regels op te bouwen. De nieuwere types kunnen zelf een applicatie aan een poort koppelen. Hiermee kan bijvoorbeeld alleen outlook.exe gebruik maken van poort 25. Hiermee voorkom je dat andere applicaties ongewenst mail gaan versturen vanuit je machine.

Network firewalls worden voornamelijk gebruikt om meerdere netwerken van elkaar te scheiden. In deze firewalls is vaak een DMZ (demilitarized zone) aanwezig. In het DMZ gedeelte van het netwerk, kunnen verschillende netwerken met elkaar communiceren. Vaak wordt hier bijvoorbeeld de Webserver geplaatst, zodat deze kan communiceren met zowel het Internet, als het interne netwerk.

Omdat ik een advies wil schrijven over het beveiligen van het netwerk, zal ik voor een network firewall kiezen. Om de juiste firewall te vinden, moet ik eerst weten waar ik op moet letten bij het maken van mijn keuze. Na een onderzoek heb ik geconstateerd dat de onderstaande eigenschappen het belangrijkst zijn bij het kiezen van een network firewall:

- aanwezigheid DMZ Functie
- aanwezigheid VPN functie
- Aantal VPN verbindingen
- Overdrachtssnelheid
- uptime
- Aantal gebruikers die gelijktijdig gebruik kunnen maken van de firewall
- Prijs

In de huidige situatie wordt er geen gebruik gemaakt van de DMZ functie. Het bedrijf zal dit in de toekomst wellicht gaan gebruiken bij het hosten van een website.

Omdat sommige medewerkers thuis zullen werken, moet het mogelijk zijn om een VPN verbinding voor alle medewerkers mogelijk te maken. Zo kunnen alle medewerkers thuis werken als dat nodig is, bijvoorbeeld in het geval van een calamiteit in het gebouw (gaslek , waterschade, etc.).

Omdat bijna al onze apparatuur minimaal 1 GB/s kan ondersteunen, moet de firewall minstens net zo snel zijn. Hiermee voorkom je dat de firewall het gehele netwerk vertraagt.

Nu ik weet wat ik nodig heb, ga ik kijken bij Misco wat ze te bieden hebben. Onderstaande firewalls voldoen aan onze eisen:

Product	**DMZ**	**Aantal VPN verbindingen**	**snelheid**	**Aantal gebruikers**	**prijs**
Cisco ASA 5550	Ja	500	1024 mb/s	650000	€11.999,-
SonicWALL NSA/E6500 Multi-Core UTM	Ja	6000	1024 mb/s	6000	€12.395,-
SonicWALL (NSA) E5500	Ja	4000	3900 mb/s	4000	€8133,-
DC-Networks firewall: DCFW-1800E-V2 Firewall	Ja	2000	1024 mb/s	1.000.000	€4490,-
D-Link ENTERPRISE FIREWALL	Ja	2500	1024 mb/s	1000	€5331,-

Onderzoek naar een wireless controller

Tijdens het onderzoek naar een geschikte wireless controller, heb ik vastgesteld dat onderstaande punten het belangrijkst zijn bij het maken van de keuze:

- Aantal accesspoint aansluitingen
- Overdrachtssnelheid
- Beveiliging
- Aantal gebruikers die gelijktijdig gebruik kunnen maken van het wireless netwerk.
- Prijs

De bovenstaande aspecten zijn gebaseerd op eigen ervaringen en voorbeelden uit het boek Top-Down Network Design.

Eerder is aangegeven dat er acht accesspoints gebruikt gaan worden in het netwerk. Dit betekent dat de wireless controller minimaal acht accesspoints moet ondersteunen. Aangezien er in de toekomst geen verdiepingen meer bij zullen komen, hoeven we ook geen wireless controller te hebben die uitbreidbaar is of meerdere poorten heeft.
Aangezien alle componenten in ons netwerk minimaal een snelheid hebben van 1 gb/s, mag de wireless controller geen bottleneck vormen. Daarom moet ook de wireless controller een snelheid hebben van minimaal 1 gb/s.

Tevens moet de wireless controller voor het netwerk de mogelijkheid hebben om het wireless verkeer te beveiligen. Juist omdat draadloos makkelijker toegankelijk is voor hackers, moet het goed beveiligd worden.

Het gehele netwerk moet zoals gezegd voor 500 gebruikers worden ingericht. Mocht de opdrachtgever in de toekomst besluiten om met laptops te gaan werken in plaats van met werkstations, dan moet het netwerk deze mogelijkheid bieden. Vandaar dat de wireless controller de mogelijkheid moet hebben om 500 medewerkers tegelijkertijd te kunnen ondersteunen.

Uiteraard is ook hier de prijs een belangrijke factor. Ik hoef niet per se de beste wireless controller op de markt, maar ik wil wel een wireless controller die aan de eisen voldoet. Vandaar dat ook hier de prijs een belangrijk punt is.

Product	Snelheid	Aantal AP's	Gebruikers	beveiliging	prijs
Cisco 4400 Series WLAN Controller of up to 12 Lightweight APs	1 gb/s	12	2000	Ja	€4.999,-
HP ProCurve MSM730 Access	100mb/s	40	500	Ja	€1.999,-

Controller					
Netgear ProSafe Wirelless Controller incl. 8 10/100 PoE poorten	100mb/s	16	256	Ja	€1.559,-

Onderzoek naar een router

Om de meest geschikte router te kiezen, moet ik eerst weten op welke criteria ik ga beoordelen. Tijdens dit onderzoek heb ik bepaald dat de volgende criteria het belangrijkst zijn:

- Overdrachtssnelheid
- Mean time between failures (de tijd dat de router zonder problemen blijft werken)
- Aantal slots en uitbreidingsmogelijkheid
- Ondersteunde protocollen
- Prijs

De onderstaande aspecten zijn gebaseerd op eigen ervaringen en voorbeelden uit het boek Top-Down Network Design.

Zoals ik eerder heb aangegeven moet alle netwerkapparatuur een snelheid van minimaal 1 GB/s hebben. De overdrachtssnelheid van de router moet dus ook minimaal 1Gb/s zijn. Omdat de kans bestaat dat het netwerk in de toekomst zal groeien, neem ik een router die tot minimaal zes segmenten uit te breiden is. Momenteel zijn er vijf segmenten die met elkaar verbonden moeten worden (vier interne subnetten en externe verkeer, bijvoorbeeld Internet/hoofdvestiging).

Tevens moet de router de nodige protocollen ondersteunen. Bijna alle routers in dit segment bieden de standaard protocollen. Tijdens mijn onderzoek heb ik ontdekt dat onderstaande protocollen erg belangrijk zijn:

- HSRP (Hot Standby Router Protocol)
- VRRP (Virtual Router Redundancy Protocol)
- OSPF (Open Shortest Path First)
- CDP (Cisco Discovery Protocol)

De HSRP (Hot Standby Router Protocol) zorgt ervoor dat wanneer er een tweede router in het netwerk aanwezig is, deze altijd klaarstaat om het werk van de primary router over te nemen wanneer deze het begeeft. Omdat we in het netwerk de routers redundant hebben uitgevoerd, is dit een erg belangrijk protocol. De HSRP protocol is echter eigendom van Cisco. Als we dit protocol als eis zouden hebben, zouden wij hiermee alle andere merken behalve Cisco buiten beschouwing laten.

Gelukkig is er ook een alternatief voor de HSRP protocol, namelijk de VRRP protocol (Virtual Router Redundancy Protocol). Dit protocol is geen eigendom van Cisco en mag wel gebruikt worden door alle fabrikanten.
Een ander belangrijk protocol is de OSPF (Open Shortest Path First) protocol. Door middel van dit protocol wordt constant bijgehouden welke interfaces up zijn. Op deze manier wordt constant berekend wat het kortste (goedkoopste) pad is. Op deze manier weet de router welke route hij moet gebruiken voor het routeren.

Nog een handig protocol is de CDP (Cisco Discovery Protocol) protocol. Dit protocol is eigendom van Cisco en zorgt ervoor dat de router automatisch zijn Cisco buren herkent. Dit geldt niet alleen voor routers maar ook voor andere Cisco apparatuur die op andere netwerklagen werkt, bijvoorbeeld Switches en hubs. CDP apparatuur stuurt ieder minuut zijn huidige CDP tabel door naar zijn buren. Wanneer de buren langer dan drie minuten niet reageren, worden ze uit het informatietabel verwijderd. Zo weet de router altijd welke apparatuur binnen het netwerk hij kan gebruiken voor het routeren.

De CDP is echter alleen interessant als we meerdere Cisco apparatuur in ons netwerk hebben. Dit protocol is dus geen eis. De OSPF en HSRP of VRRP protocollen zijn wel een eis.

Product	**MTBF**	**Protocollen**	**Uitbreidbaar**	**Snelheid**	**Prijs**
Cisco 2851	19 jaar	Allemaal	Ja 4 slots	1 Gb/s	€4.199,-
Cisco 2821	12 jaar	Allemaal	Ja 4 slots	1 Gb/s	€2.799,-
Juniper J2320	7 jaar	Allemaal	Ja 3 slots	1 Gb/s	€1.259,-

Onderzoek naar een server

Omdat ik niet erg veel verstand heb van servers, was het noodzaak dat ik eerst ging onderzoeken hoe servers in elkaar zitten en waar ik op moet letten bij het maken van de keuze voor de juiste server. Tijdens dit onderzoek ben ik erachter gekomen dat onderstaande punten het belangrijkst zijn bij het maken van een beslissing:

- Type server (tower, blade, etc.)
- Processor
- Geheugen (uitbreidingsmogelijkheid)
- Harde schijf
- Ethernetkaart

De onderstaande aspecten zijn gebaseerd op eigen ervaringen en voorbeelden uit het boek Top-Down Network Design.

Het type server is voor ons niet heel erg belangrijk, echter gaat mijn voorkeur toch uit naar de blade servers. Reden hiervoor is hun ruimtebesparing. Omdat blade servers zo compact zijn, zouden ze allemaal in één patchkast passen.

Het feit dat het hier om een fictieve opdracht gaat, maakt het voor mij erg lastig om te achterhalen hoe snel de processor moet zijn en hoeveel geheugen gewenst is. De meeste bedrijven gebruiken een standaard serverconfiguratie. Deze configuratie kan indien gewenst speciaal toegepast worden op speciale servers. Ik kies ervoor om alle serverconfiguraties gelijk te houden. Mocht een bepaalde server bijvoorbeeld meer geheugen nodig hebben, dan kan dat achteraf altijd gewijzigd worden.

Om te achterhalen wat de meest gangbare configuratie is heb ik twee senior systeembeheerders geïnterviewd. Tijdens het interview is mij verteld dat 4 GB per virtuele server bijna altijd genoeg is voor alle gangbare servers. Voor de meest gangbare servers is ook een dual-core processor van minimaal 2,5 Ghz ruim voldoende.

Over de grootte van de schijf wisten ze me niet heel veel te vertellen, omdat dit echt aan het type server ligt. Een database server heeft bijvoorbeeld tien keer zoveel ruimte nodig als een DNS server. Ik heb bij de hardware leverancier gekeken en ik zag dat bijna alle servers zonder schijven geleverd worden. Daarom zullen we ook niet beoordelen op de schijfruimte, omdat we niet weten hoeveel schijfruimte elke server nodig heeft. Omdat dit een fictieve opdracht is, kan ik het me veroorloven om met de bovenstaande waarden te werken. Het gaat tenslotte niet om de waarden, maar om het onderzoek dat ik ga uitvoeren.

Zoals eerder aangegeven is het netwerk niet meer dan een medium. We moeten er dus voor zorgen dat de servers een snelle ethernet verbinding hebben. Op deze manier voorkomen we dat de servers de bottleneck op ons netwerk vormen. De servers moeten daarom minimaal 1 gb/s netwerk poorten hebben.

Nu we weten waar we op moeten letten bij het selecteren van de juiste server kunnen we gaan kijken wat de hardware leverancier ons te bieden heeft. Dat levert het volgende schema op.

Server	Processor	Geheugen	GB Ethernet	Type	Prijs
HP ProLiant BL680c G5	2 x Quad Core Xeon E7340 (2.4GHz)	8 GB (max 64 GB)	4	Blade	€8.199,-
IBM BladeCenter LS42 7902	2 x AMD Opteron 8431 / 2.4 GHz (6-core)	4 GB (max 128 GB)	2	Blade	€7.899,-
HP ProLiant DL180 G6	2 x Intel Xeon E5540 / 2.53 GHz (Quad-Core)	12GB(max 96 GB)	2	Blade	€3.299,-
HP ProLiant DL165 G6	2 x AMD Opteron 2435 / 2.6 GHz (6-core)	8 GB (max 32 GB)	2	Blade	€2.749,-
Dell PowerEdge R710	1 x Intel Xeon E5530 2.4 Ghz (Quad-Core)	12 Gb(max 144 GB)	2	Blade	€2.199,-
Lenovo ThinkServer RD220	1 x Intel Xeon E5520 / 2.26 GHz (Quad-Core)	2 Gb (max 128 GB)	2	Blade	€2.049,-

Onderzoek naar een storage oplossing

Om de juiste storage te vinden, moet ik eerst weten waar ik op moet letten bij het maken van de juiste keuze. Om dat te kunnen achterhalen, heb ik onderzoek moeten doen naar storage oplossingen. Tijdens dit onderzoek ben ik tot de volgende belangrijkste criteria gekomen:

- Overdrachtssnelheid
- Type storage (schijven of solid state disks)
- Capaciteit van de storage
- Prijs

De bovenstaande aspecten zijn gebaseerd op eigen ervaringen en voorbeelden uit het boek Top-Down Network Design.

Omdat de schijven door honderden mensen tegelijkertijd geraadpleegd worden, moet de storage een zeer hoge overdrachtssnelheid hebben. Wanneer de storage niet snel genoeg is, zal dit het netwerk vertragen. Het doel was om een zeer stabiel en snel netwerk te maken. Ik heb van alle componenten een uiterst hoge snelheid geëist. De storage is hier geen uitzondering in. Na mijn onderzoek ben ik tot de conclusie gekomen dat de betere schijven op de markt een overdrachtssnelheid hebben tussen de 4 gb/s en de 10 gb/s.
Ik wil dan ook graag dat onze storage minimaal een snelheid van 10 gb/s heeft. Op deze manier vormt de snelheid van de storage geen issue binnen het netwerk.

Tot een paar jaar terug waren alleen IDE, Sata of SCSI schijven het medium waarop bestanden opgeslagen konden worden (voor grote netwerken). Nu zijn er echter ook nieuwere technieken beschikbaar, zoals de Solid State Disks. De solid state disk lijkt erg op een grote SD kaart. Het bevat geen draaiende onderdelen, in tegenstelling tot de normale schijven. Hierdoor is de kans op storingen en defecten veel kleiner. Ook zijn Solid state disks vaak sneller dan normale schijven. Een nadeel is dat de solid state disk niet ver ontwikkeld is. Ook is het in vergelijking met normale storage vele malen duurder. Dit is vaak de reden dat veel mensen daar (nog) niet voor kiezen.

Een van de belangrijkste punten waar ik op moet letten bij het kiezen van de schijven, is de capaciteit. Omdat dit een fictieve opdracht is, is het erg lastig om te achterhalen hoeveel ruimte de schijven nodig zullen hebben. Ook is dit niet erg relevant voor mijn afstudeeropdracht. Het belangrijkste van mijn afstudeeropdracht is dat ik kan laten zien hoe ik tot mijn keuze kom, en welke beslissingen ik heb gemaakt en waarom. Of ik 10 TB of 30 TB aan schijven nodig zal hebben, is niet erg relevant omdat ik in beide gevallen toch hetzelfde

onderzoek zal uitvoeren. Om toch wel een reële grootte te kiezen, heb ik met een senior systeembeheerder van een soortgelijk bedrijf gesproken. Hij heeft aangegeven dat voor een bedrijf van deze omvang ongeveer 20 TB aan storage nodig is. Dit lijkt in eerste instantie veel, maar omdat er ook regelmatig back-ups worden gemaakt, zullen deze veel ruimte in beslag nemen. Overigens kun je op deze manier je storage ook futureproof maken.

Uiteraard is ook hier de prijs een belangrijke factor. Daarom ga ik zorgvuldig uitzoeken of elke oplossing wel financieel verantwoord is.

Nu ik weet wat ik nodig heb en waar de storage aan moet voldoen, ga ik uitzoeken wat onze hardware leverancier ons kan bieden. Uit mijn onderzoek kwam het volgende lijstje naar voren:

Product	Snelheid	Capaciteit	Type	Prijs
Netgear ReadyNAS 4200 19 Rackmount, 10GB via CX-4	**10 gb/s**	**24 TB**	**Schijven**	€8.644,95
Netgear ReadyNAS 4200 19 Rackmount	**1 gb/s**	**24 TB**	**Schijven**	€7.992,95
HP StorageWorks All-in-One Storage System 1200r 3TB SATA	**1 gb/s**	**3 TB**	**Schijven**	€6.349,95
Thecus N8800 Network Storage Server 8 BAY NAS 16TB	**1 gb/s**	**16 TB**	**Schijven**	€3.020,95
Intel X25-E SATA II SSD 64GB	**10 gb/s**	**64 GB**	**SSD**	€584,95

Afstudeeropdracht:	**Mina-IT @ Groningen**
Document:	Definitierapport
Student:	Mina Nabil
Afstudeerbegeleider:	Cobie van der Hoek
Expert:	Nico Huiberts
Datum:	04-10-2010

Inleiding

In dit rapport worden de eisen en wensen van de opdrachtgever beschreven. Zodra de eisen en wensen duidelijk zijn, kan er een plan van aanpak opgezet worden. Tevens zal er gedurende deze fase een voorlopige planning gemaakt worden als onderdeel van het plan van aanpak.

Inhoudsopgave

Doelstelling project

Het doel van dit project is het leveren van een adviesrapport voor de te gebruiken hardware voor het inrichten van het netwerk. In dit adviesrapport zal onder andere advies gegeven worden over de te gebruiken Internetverbindingen en de beveiliging van het netwerk.

Daarnaast moet er een compleet netwerkarchitectuur worden opgeleverd. Aan de hand van de opgeleverde producten zal Mina-IT een extern bedrijf kunnen inhuren dat daadwerkelijk de omgeving gaat bouwen volgens ons advies en netwerkarchitectuur.

Scope van het project (eisen)

Om te beginnen is het erg belangrijk om de scope van het project duidelijk te maken voor alle partijen. Ik heb zelf de scope van het project verzonnen. Ik heb wel mijn best gedaan om een netwerkopdracht te realiseren die zo reëel mogelijk is. Hieronder is te zien welke onderdelen binnen de scope van dit project vallen:

- Er dient een gehele netwerkinfrastructuur bedacht te worden voor de 500 medewerkers die verspreid zijn over zeven afdelingen en acht verdiepingen. Initieel zullen er maar 450 medewerkers in de nieuwe vestiging werken, maar de opdrachtgever wil wel dat het netwerk tot maximaal 500 medewerkers uitgebreid kan worden zonder ingrijpende veranderingen aan het netwerk te brengen.
- Er dient een voorstel te komen voor het realiseren van een verbinding die 24x7 verbonden is tussen deze vestiging en het hoofdkantoor te Nieuwegein. Ook moet er een back-up verbinding komen voor het geval dat er storingen optreden met de primaire verbinding.
- Het gehele pand moet voorzien zijn van een beveiligd draadloos netwerk.
- Er dient een voorstel te komen voor de te gebruiken apparatuur zoals werkplekken, servers, back-up units, storage en netwerkapparatuur. Hiervoor is een beperkt budget beschikbaar.
- Er dient een voorstel te komen voor de te gebruiken technieken voor de storage.
- Er dient een voorstel te komen voor de beveiliging van het netwerk.
- Er dient een voorstel te komen voor de installatie van de volgende servers. Hierbij kan gebruik gemaakt worden van virtualisatie:
    - Mailserver
    - Domeinserver
    - FTPserver
    - DNSserver
    - DHCPserver
    - Applicatie servers

    - Database server

- De nieuwe vestiging zal geopend worden op 01-01-2011. Dit betekent dat het project uiterlijk 31-11-2010 afgerond moet zijn, zodat het netwerk in de maand voorafgaand aan de opening gebouwd kan worden door het externe bedrijf.

- Voor het aanschaffen van de apparatuur is een budget van €1.000.000,- beschikbaar gesteld. Dit bedrag is exclusief de kosten voor het bouwen van het netwerk. Dit bedrag is zelf door de opdrachtgever bepaald. Er is eventueel meer geld beschikbaar als dat echt nodig is. Het is echter wel de bedoeling dat we in eerste instantie binnen het budget blijven.

  Er moet een advies komen voor de high availablity van de netwerkapparatuur, servers en de storage. Hierbij moet rekening gehouden worden met het maken van back-ups en het elimineren van single point of failures. Daarnaast moet er gedacht worden aan back-up stroomvoorzieningen zoals UPS.

Plan van aanpak

Om het project succesvol af te ronden, is een goed plan van aanpak nodig. In het plan van aanpak worden belangrijke keuzes gemaakt. Het is daarom erg belangrijk om het plan van aanpak voldoende gedetailleerd te maken. Hierdoor kunnen misverstanden voorkomen worden. Ook kan je met het plan van aanpak je huidige positie in het project bepalen en eventueel bijsturen.

Aanpak project

Zoals eerder beschreven zullen twee producten opgeleverd worden aan het eind van dit project:

- Een complete netwerkarchitectuur (architectuurrapport).
- Een adviesrapport over de inrichting van de nieuwe omgeving.

Omdat deze twee eindproducten teveel van elkaar verschillen heb ik het project in twee delen opgesplitst. Eerst zal het architectuurdocument opgesteld worden en daarna ga ik een advies geven over de overige zaken die te maken hebben met de IT-infrastructuur.

Dit moet in deze volgorde gebeuren omdat het andersom niet mogelijk zou zijn. Dit omdat van tevoren nog niet bekend is welke netwerktechnieken gebruikt zullen worden en ik dus ook geen advies kan geven over de netwerkapparatuur. Daarom is ervoor gekozen om eerst de netwerkarchitectuur te maken en vervolgens de advies te geven voor het inrichten van de nieuwe omgeving en de hardware.

Extra informatie vergaren

Tijdens het maken van de plan van aanpak is het erg belangrijk om zoveel mogelijk informatie over het project te beschikken. Omdat er nu nog veel details onbekend zijn heb ik eerst meer informatie van de opdrachtgever moeten vergaren.

Om meer informatie te vergaren zou ik verschillende methodes kunnen gebruiken. De meeste gebruikte methodes zijn: enquête houden , Interviewen of zelf onderzoeken. Omdat enquêtes over het algemeen gebruikt worden voor een groep mensen zal deze methode voor mij niet geschikt zijn. Ik heb namelijk maar een persoon waarvan ik meer informatie kan/wil verzamelen. Ook zelf onderzoeken is hier niet mogelijk omdat ik niet weet wat de opdrachtgever precies wilt hebben. Ik zal er dus voor kiezen om de opdrachtgever te interviewen en op deze manier meer informatie proberen te winnen.

Ik zou tijdens het interviewen open , gesloten of suggestieve vragen kunnen stellen. Omdat ik geïnteresseerd ben in veel informatie is het niet verstandig om voor gesloten of suggestieve vragen te kiezen. Daarom kies ik ervoor om uitsluitend openvragen te stellen. Op deze manier hoop ik zoveel mogelijk informatie van de opdrachtgever te winnen.

Omdat ik de opdrachtgever ben heb ik besloten om de interview met mij zelf te houden.
Ik heb tijdens het interview net gedaan alsof ik zeer beperkt technische kennis had.
Dit is geen vreemd situatie want meestal is dat ook zo in werkelijkheid. Op deze manier krijgt de uitvoerder van dit project zelf de kans om belangrijke keuzes te maken. Op deze manier neemt de uitvoerder de expert rol op zich (zie de interview in de bijlage).

projectverdeling

Na het interview zijn veel details nu bekend geworden. Nu kan ik verder met het plannen van mijn project. Aan de hand van de eerder afgelegde interview en de geleverde eisen weet ik nu wat de eisen zijn van het project.

De onderdelen die te maken hebben met het ontwerpen van het netwerken heb ik in het eerste gedeelte van het project geplaatst. Deze onderdelen zijn bijv. het opstellen van een IP plan of het maken van de architectuur.

De onderdelen die over het adviseren gaan heb ik in het tweede gedeelte van het project geplaatst. Bij deze onderdelen moet je bijvoorbeeld denken aan het adviseren van een geschikte storage oplossing.

Netwerkarchitectuur

In het eerste gedeelte van het project zal de netwerkarchitectuur bedacht en opgesteld worden. Tijdens het opstellen van het architectuurdocument moest aandacht besteed worden aan de volgende punten:

- Er moet een logisch IP schema worden opgesteld.
- Er moet rekening gehouden worden met de beveiliging van het netwerk.
- Er moet rekening gehouden worden met de aanwezigheid van een beveiligde draadloze netwerkverbinding in het hele gebouw.
- Er moet rekening gehouden worden met het feit dat er 24x7 een netwerkverbinding aanwezig moet zijn met het hoofdkantoor te Nieuwegein. Ook moet er een back-up verbinding aanwezig zijn, mocht de primaire verbinding uitvallen.

Advies over het inrichten van het nieuwe netwerk

Wanneer het bekend is hoe de architectuur van het netwerk eruit komt te zien, kunnen we verder met het tweede gedeelte van het project: het advies over hoe het nieuwe netwerk ingericht moet worden. Hierbij moet gedacht worden aan de volgende punten:

- Er dient een voorstel te komen voor de te gebruiken apparatuur zoals servers, storage en netwerkapparatuur. Hiervoor is een budget van €1.000.000,- beschikbaar.
- Er dient een voorstel te komen voor de te gebruiken technieken voor de storage.
- Er dient een voorstel te komen voor de beveiliging van het netwerk.
- Er dient een voorstel te komen voor de installatie van de volgende servers. Hierbij kan gebruik gemaakt worden van virtualisatie:
    - Mailserver
    - Domeinserver
    - FTPserver
    - DNSserver
    - DHCPserver
    - Applicatie servers
    - Database server
- Er moet een advies komen voor de high availablity van de netwerkapparatuur, servers en de storage. Hier moet rekening mee gehouden worden met het maken van back-ups en het elimineren van single point of failures. Daarnaast moeten we denken aan back-up stroomvoorzieningen zoals UPS.

  Omdat de meeste onderdelen waarover wordt geadviseerd teveel van elkaar verschillen, ga ik over ieder onderdeel een apart adviesrapport maken. Eerst worden de verschillende oplossingen beschreven, waarbij de voor - en nadelen in beeld worden gebracht. Vervolgens wordt aan de hand hiervan een advies gegeven over het inrichten van het onderdeel.

Planning

Om ervoor te zorgen dat het project geen vertraging oploopt, is het belangrijk om van tevoren goed te plannen. Hieronder staat een planningsschema dat ervoor moet zorgen dat het project succesvol en op tijd afgerond wordt.

Bij het maken van de planning heb ik op basis van eigen ervaring een schatting gemaakt voor de verschillende fases. Om ervoor te zorgen dat bij enige vertraging geen grote problemen zullen ontstaan, heb ik voor een uitloopperiode van een week gekozen. In deze planning is verder te zien welke (sub)producten aan het einde van elke fase opgeleverd dienen te worden.

Zoals ASI beschrijft heb ik onder andere als tussenproducten de: Definitierapport , Architectuurrapport en het ontwerprapport.

Actie	**Op te leveren (sub)producten**	**voortgang**
Voorbereiden project	-	1e week
Maken van plan van aanpak	Plan van aanpak	3e week
Beschrijven definitie fase	Definitierapport	4e week
Onderzoeken naar verschillende netwerktechnieken	-	5e week
Eerste opzet netwerkarchitectuur	Architectuur rapport	6e week
Uitwerken netwerkarchitectuur	Ontwerp rapport	8e week
Onderzoeken hardware passend bij architectuur	Beschrijving van de uitgevoerde onderzoeken.	9e week
Maken adviesrapport voor hardware	Advies rapport voor hardware	11e week
Uitwerken Procesverslag	Procesverslag	15e week
Uitloop	-	17e week

Conclusie

In dit rapport heb ik de eisen van de opdrachtgever beschreven. Ook heb ik een plan van aanpak gemaakt. Dit plan van aanpak is belangrijk voor het gehele traject. Het plan van aanpak wordt niet alleen gebruikt om te weten hoe je in het project staat, maar ook om het project ermee te sturen en eventueel te corrigeren.

Afstudeeropdracht:	**Mina-IT @ Groningen**
Document:	Architectuurrapport
Student:	Mina Nabil
Afstudeerbegeleider:	Cobie van der Hoek
Expert:	Nico Huiberts
Datum:	04-10-2010

Inleiding

In dit rapport presenteer ik mijn architectuur. Ik geef aan wat voor soort apparatuur ik nodig heb voor mijn architectuur en waarom ik gebruik ga maken van redundantie.

Omdat ik de ASI methodiek hanteer, zal ik verschillende netwerkarchitecturen (schetsen) vergelijken en de beste daarvan kiezen. De gekozen architectuur zal in de ontwerpfase verder uitgewerkt worden.

Inhoudsopgave

Netwerkapparatuur

Om te weten wat voor netwerkapparatuur ik nodig heb, heb ik vooraf onderzocht waar de verschillende netwerkcomponenten voor bedoeld zijn. Daarnaast wilde ik weten of deze voor mij van belang waren. Dankzij de Cisco cursus die ik op school heb gevolgd, wist ik al voor een groot deel welke soort apparatuur ik nodig zal hebben. Ik heb tevens op het Internet vele verschillende netwerken nauwkeurig bestudeerd. Op de website www.ratemynetworkdiagram.com zetten veel netwerkarchitecten hun netwerktekening online. Tenslotte heb ik gebruik gemaakt van voorbeelden uit het boek Top-Down Network Design.

Na de bovenstaande zoekactie is duidelijk geworden dat de onderstaande componenten nodig zijn:

- Switches
- Routers
- Firewalls
- Storage
- Draadloze accesspoints
- Servers

Nu ik weet welke netwerkcomponenten ik nodig heb, is het tijd om te beslissen waar de apparatuur aan moet voldoen. Ik zal per netwerkcomponent aangeven waar het aan moet voldoen.

Switches

Tijdens mijn onderzoek ben ik erachter gekomen dat ik voor ons netwerk twee verschillende soorten switches nodig heb, namelijk een backbone-switch en een enduser-switch. De backbone-switch wordt gebruikt om de belangrijkste netwerkcomponenten met elkaar te verbinden, zoals bijv. servers en routers. De enduser-switches worden gebruikt om de gebruikers aan het fysieke netwerk te koppelen met behulp van UTP.

In de afgelopen jaren werden steeds meer applicaties via het web gebruikt, denk aan Webmail, intranet, wiki-portal, etc.) Hierdoor vindt er steeds meer netwerkverkeer plaats. Om te voorkomen dat gebruikers het netwerk als traag ervaren, gaan wij alle enduser switches gigabit (10/100/1000) uitvoeren. Dit werkt niet alleen prettig voor de gebruikers maar maakt het netwerk ook meer futureproof.

Enduser-switches zijn in veel varianten verkrijgbaar. De meest gebruikte switches zijn de 16, 24 en 48 poorts switches. Het voordeel van de 48 poorts switch is de ruimtebesparing in de patchkasten, omdat er minder switches nodig zijn. Dit heeft echter wel een nadeel. Wanneer een switch kapot gaat, zijn er maximaal 48 personen die niet kunnen werken. Wanneer een 16 poorts switch wordt gebruikt, zullen bij een defecte switch maximaal 16 personen gehinderd worden. Er zijn dan echter wel drie keer zoveel patchkasten nodig.

Omdat de beschikbaarheid voor de opdrachtgever erg belangrijk is, wil ik niet de kans lopen dat meer dan 10 procent van de werknemers niet kan werken door een defecte switch (dit is het geval wanneer een 48 poorts switch gebruikt wordt). Vandaar dat ik ervoor kies om 24 poorts switches te gebruiken. Op deze manier kunnen er bij switchproblemen 50 procent meer werknemers werken dan bij een 48 poorts switch. Dit betekent echter wel dat er dubbel zoveel switch patchkasten nodig zijn.

We moeten niet alleen rekening houden met 500 werknemers, maar ook met de overige hardware. Er komen meerdere printers en scanners per verdieping. Voor al deze componenten moeten ook netwerkverbindingen beschikbaar zijn. Als we ervan uit gaan dat er per verdieping drie printers en één scanner aanwezig zijn, hebben we voor acht verdiepingen minimaal 32 extra poorten nodig. In totaal hebben we dus ongeveer 550 poorten nodig voor het hele gebouw. Dit komt overeen met 23 switches (24 poorts).

Meestal worden backbone-switches redundant uitgevoerd omdat ze essentieel zijn. Deze switches mogen dus 24 of 48 poorts zijn. In geval van een storing met de switch zal al het verkeer via de andere switch lopen.

Routers
Routers hebben een belangrijke rol, namelijk het routeren tussen de verschillende netwerksegmenten. Alle routers moeten evenals de switches minimaal gigabit routers zijn.

Firewall
Een firewall houdt ongewenst verkeer buiten ons netwerk. Daarom hebben wij voor ons netwerk ook een firewall nodig. Ook moet ons firewall DMZ ondersteunen (momenteel wordt er geen gebruik van gemaakt, maar in de toekomst wellicht wel).

Storage
Een correcte storage oplossing is onmisbaar in een netwerk. Op je storage komt namelijk alle data te staan. Data is vaak van onschatbare waarde. Voor ons netwerk zal dus een storage oplossing moeten komen.

Draadloze accesspoints
Ik heb uitgezocht wat het bereik is van de meeste accesspoints; dit bleek tussen de 75 en de 100 meter te zijn. Aangezien de verdiepingen niet langer dan 50 meter zijn, is het dus voldoende om op iedere verdieping één draadloze accesspoint te plaatsen.

Servers
Een perfect draaiend netwerk zonder servers is nutteloos. De opdrachtgever heeft aangegeven dat hij vier applicatieservers nodig heeft. Daarnaast zijn er DHCP, FTP, DNS, mail, domein - en database servers vereist. We hebben dus minimaal tien servers nodig. Het is daarom verstandig om rekening te houden met extra servers.

Omdat niet alle servers altijd optimaal benut worden, is het zonde om 10 servers aan te schaffen die sporadisch werken. Virtualisatie kan hier een goede oplossing voor bieden.
Bij virtualisatie is het mogelijk om op èèn host (server) meerdere besturingssystemen naast elkaar installeren. Deze besturingssystemen zullen samen de hardware van de host delen. Ook zijn deze besturingssystemen van elkaar gescheiden en werken ze onafhankelijk van elkaar.

Het is gunstiger om vijf servers te kopen, waar we vervolgens met behulp van virtualisatie 10 virtuele servers op kunnen installeren. Op deze manier halen we het maximale uit ons apparatuur. Door gebruik te maken van virtualisatie worden er veel kosten bespaard, die weer bij andere netwerkcomponenten goed van pas komen.

Redundante hardware

De opdrachtgever heeft aangegeven dat het netwerk moet blijven doordraaien, ook wanneer er een kritieke netwerkcomponent kapot gaat. Met kritieke apparatuur wordt apparatuur bedoeld waarvan bijna de gehele netwerk van afhankelijk is, zoals backbone-switches. Werkstations vallen niet onder kritieke apparatuur.

Het is nu belangrijk om te weten welke apparatuur redundant uitgevoerd moet worden en welke niet. Hieronder heb ik beschreven welke netwerkapparatuur dubbel uitgevoerd moeten worden en waarom.

Firewall

De firewall is het eerste aanspreekpunt voor het netwerk van buitenaf. Dat betekent dat er in het geval van een storing in de firewall, grote problemen kunnen ontstaan tussen netwerkverkeer van buiten naar binnen en vice versa. De firewall zal dus redundant uitgevoerd moeten worden.

Routers

De routers zorgen voor het routeren in een netwerk. Als er een storing optreedt in een router, kan een groot deel van het netwerk onbruikbaar worden. Daarom is het belangrijk dat een router redundant uitgevoerd wordt.

Storage

In de storage staat alle data opgeslagen. In het geval van een storing in de storage, is de data niet meer beschikbaar voor de medewerkers. Om dit te voorkomen, zal dus tevens de storage redundant uitgevoerd moeten worden. Op deze manier creëer je tevens een kopie op de tweede storage. Dit is erg nuttig, omdat het ook meteen een belangrijke back-up mechanisme is voor waardevolle data.

Draadloze accesspoints

Wanneer er op een draadloze accesspoint een storing ontstaat, zullen gebruikers op de betreffende verdieping niet meer optimaal gebruik kunnen maken van het draadloos netwerk. Ze zullen echter wel nog gebruik kunnen maken van de draadloze accesspoint van de verdieping boven of onder hen, omdat het bereik van de accesspoint tussen de 75 en 100 meter is. Mocht dit niet lukken, dan is het nog altijd mogelijk om via UTP verbinding maken met het netwerk. Als we alle accesspoints redundant zouden uitvoeren zou het erg veel kosten met zich mee brengen, terwijl er ook workarounds beschikbaar zijn. Daarom heb ik ervoor gekozen om de accesspoints niet redundant uit te voeren.

Servers

Omdat we eerder hebben aangeven dat de gebruikers intensief gebruik maken van de vier applicatieservers, is het belangrijk dat de servers altijd beschikbaar blijven. Vandaar dat ook de servers redundant uitgevoerd moeten worden. Mochten er storingen optreden met een server, dan kan de redundante server de sessie overnemen.

Zonder een DNS server kunnen gebruikers niet browsen of mailen. Dit is echter wel nodig in hun werkzaamheden. Daarom is het belangrijk om de DNS server redundant uit te voeren.

Omdat het voor de beheerders lastig is om op elk werkstation handmatig een IP adres te configureren, wordt er gebruik gemaakt van een DHCP server. Deze server zorgt ervoor dat elk werkstation het juiste IP adres krijgt. Hierdoor is het noodzakelijk om de DHCP server redundant uit te voeren, want zonder een DHCP server kunnen gebruikers geen IP-adres verkrijgen. Dit zorgt er op zijn beurt weer voor dat er geen verbinding kan worden gemaakt met het netwerk.

Wanneer de domeinserver een storing heeft, kunnen de gebruikers niet op het domein inloggen. Het gevolg hiervan is dat de gebruikers hun werkzaamheden niet kunnen verrichten. Ook hier is het dus van essentieel belang dat de domeinserver redundant wordt uitgevoerd.

Zonder de database-server kunnen de applicaties hun data niet ophalen, waardoor de applicaties onbruikbaar worden. Kennis is macht; indien de data voorgoed verdwijnt, betekent dit dat er ook veel kennis verdwijnt. Ook back-ups zijn niet voor de volle 100 procent te vertrouwen; de back-up jobs kunnen falen of er kunnen hardware problemen met de back-up mechanismen ontstaan. Vandaar dat het erg belangrijk is om de database-server redundant uit te voeren.

Indien er een storing optreedt in de mailserver, kunnen de gebruikers geen gebruik meer maken van hun e-mail. De e-mail is van significante waarde, omdat er tegenwoordig steeds meer via de digitale weg wordt gecommuniceerd. Als de mailserver niet juist werkt, is er een belangrijke communicatiechannel niet meer beschikbaar. Dit kan tot veel problemen leiden voor de medewerkers en de klanten.

Omdat alle bovenstaande servers erg belangrijk zijn, zal ik ze allemaal redundant uitvoeren zodat de gebruikers in geval van serverstoringen kunnen doorwerken zoals ze gewend zijn.

Switches

In een netwerk hebben switches verschillende rollen. Zo zijn er backbone-switches en enduser-switches. De backbone-switches verbinden de primaire netwerkapparatuur met elkaar. Dit zijn bijvoorbeeld de switches die tussen de routers en de enduser switches zitten. De enduser-switches zijn switches die direct de gebruiker aan het netwerk koppelen. Deze switches zijn vervolgens op de backbone-switches aangesloten.

Wanneer een backbone-switch kapot gaat, is het mogelijk dat alle enduser-switches die daarop aangesloten zijn geen netwerkverkeer meer kunnen doorsturen. Hierdoor kan het gehele netwerk onbruikbaar worden voor de eindgebruikers. Het is dus van cruciaal belang om de backbone-switches redundant uit te voeren.

Wanneer de enduser-switch kapot gaat, kunnen maximaal 24 medewerkers geen gebruik maken van het netwerk. De rest van de organisatie zou wel door kunnen werken. Omdat het werkstation van de gebruikers meestal maar één netwerkaansluiting heeft, kan een werkstation niet op twee switches worden aangesloten. Daarom hoeven de enduser-switches niet redundant uitgevoerd te worden. Wanneer er toch een enduser-switch kapot gaat, zal deze altijd binnen 24 uur vervangen worden door de hardware leverancier omdat daar een servicecontract mee afgesloten is.

De opdrachtgever wil een uptime garantie van 99 procent hebben. Wanneer een enduser-switch kapot gaat, kunnen er op dat moment maximaal 24 gebruikers niet werken. Dat is ongeveer vijf procent van de gebruikers voor één dag. Om de downtime te berekenen, kunnen we de volgende formule gebruiken:

D = Totale downtime (uren)
T = Totale tijd in een jaar (uren)
Downtime (in %) = D/T X 100

Voor ons zou de volgende situatie ontstaan:
D = Totale downtime is 24 uur
T= Totale tijd in een jaar is 8760 uur

Downtime = 24 /8760 x 100 = 0,27% oftewel 99,72%
Dit geldt echter alleen voor 5 procent van de werknemers, omdat er maar één switch kapot gaat. Dit betekent dat de overige 95 procent van de werknemers gewoon door kan werken.

Wanneer één enduser-switch kapot gaat, zullen we ruim onder de norm van 99 procent uptime zitten.

Verschillende ontwerpen

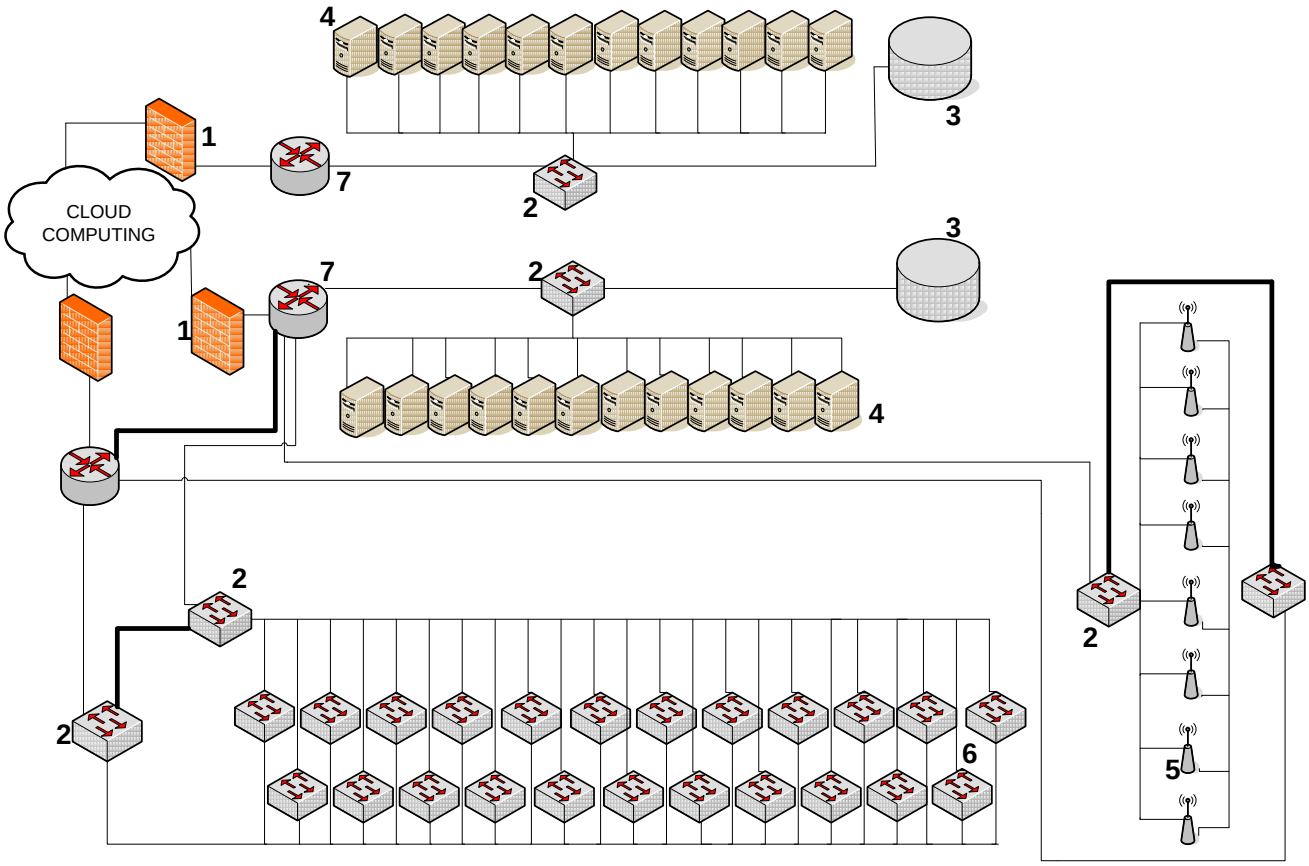
Wanneer je de ASI methodiek hanteert, is het erg verstandig om meerdere ontwerpen (schetsen) te maken. Daarom heb ik meerdere schetsen gemaakt, die ik hierna zal onderbouwen. Omdat de opdrachtgever heeft aangegeven dat alle kritieke componenten redundant uitgevoerd moeten worden, heb ik twee verschillende schetsen met verschillende technieken getoond.

Om tot verschillende schetsen te komen, heb ik besloten om technieken te gebruiken die op verschillende manieren werken. Sinds men bezig is met het redundant uitvoeren van netwerkcomponenten, wordt er gebruik gemaakt van interne redundantie. Interne redundantie houdt in dat meerdere netwerkcomponenten elkaars taken kunnen overnemen in geval van hardware problemen. In dat geval zitten de dezelfde componenten meestal op dezelfde locatie (intern).

Al enkele jaren wordt gebruik gemaakt van externe redundantie. De gebruikte term hiervoor is cloud computing. Cloud computing is een techniek die steeds vaker gebruikt wordt. De nadruk bij cloud computing ligt op het delen van hardware en software via het Internet. Hierbij hoeven de verschillende redundante netwerkcomponenten niet meer op dezelfde locatie te staan, maar kunnen ze ook aan de andere kant van de wereld staan.

Cloud computing

Het grootste voordeel van cloud computing is dat de servers op een hele andere locatie aanwezig kunnen zijn, wat meteen een goede back-up mechanisme is. Dit is ook meteen het grootste nadeel van cloud computing: je bent namelijk beperkt door je Internetverbinding. Wanneer een Internetverbinding niet meer werkt, is het niet mogelijk om bij de servers aan de andere kant van de cloud te komen. Hieronder staat een schets van onze opzet, in het geval we gebruik zouden maken van cloud computing. Bij het maken van deze schets heb ik rekening gehouden met de eisen van de opdrachtgever.



1=firewall
2=Backbone-switch
3=Storage
4 =Servers
5= Accesspoints
6= Enduser-switches
7= Router

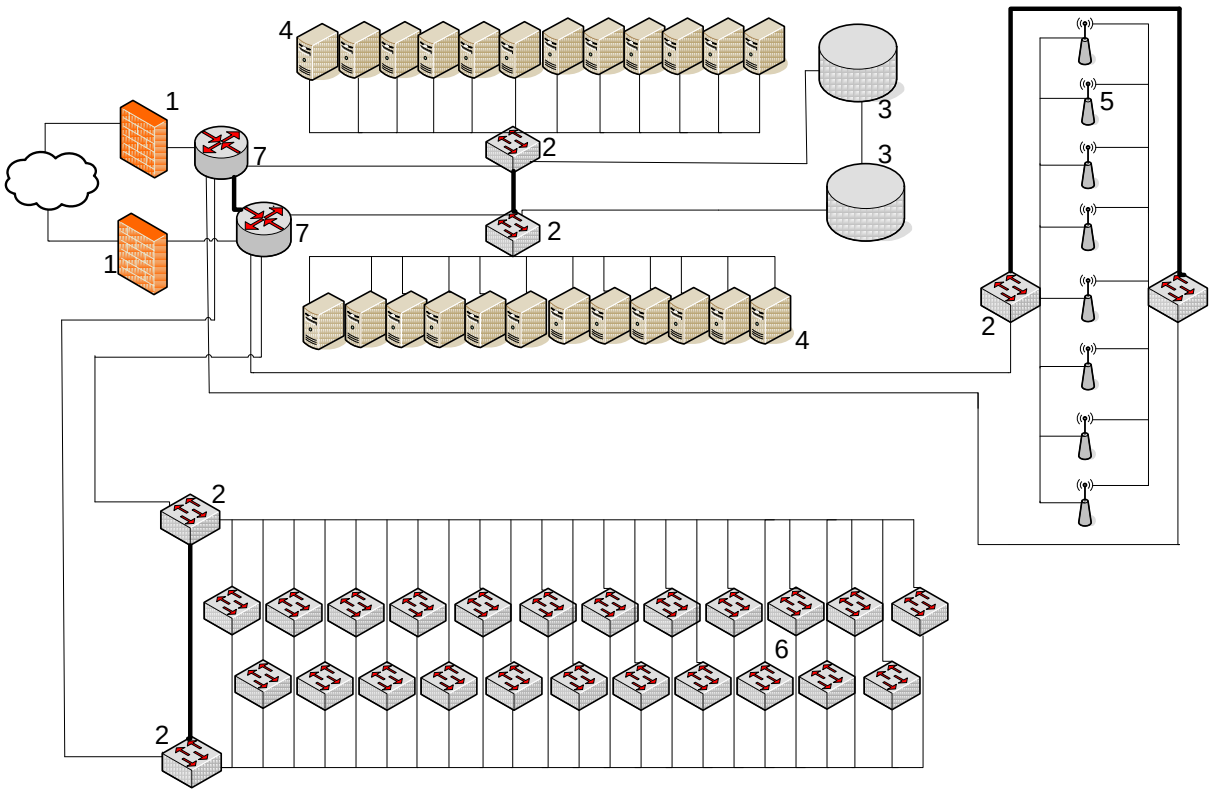
Bij het maken van de bovenstaande schets heb ik zoveel mogelijk aan de eisen van de opdrachtgever voldaan. Zo heb de firewall, router en backbone-switch redundant uitgevoerd op de hoofdvestiging (onderkant van de cloud). Op de uitwijkomgeving (bovenkant van de cloud) staan de standby servers en storage.

De dikgedrukte lijnen dienen voor het gebruik van redundantie. Wanneer bijvoorbeeld een backbone-switch kapot gaat, moet er bij de standby backbone-switch een lampje gaan branden dat hij de taken moet overnemen. Deze protocol wordt ook wel de Spanning Tree Protocol genoemd. Wanneer het protocol vaststelt dat pakketten meerdere keren naar eenzelfde segment worden gerouteerd, wordt een van de paden naar dat segment afgesloten door de desbetreffende switchpoort uit te schakelen.

Ook de dikke verbinding tussen de routers staat voor een failover protocol. Vaak worden voor Cisco routers de Hot Standby Router Protocol (HSRP) geconfigureerd. Een router van een ander merk dan Cisco zou de Virtual Router Redundancy Protocol (VRRP) kunnen gebruiken, want HSRP werkt alleen op Cisco apparatuur. Bij deze protocollen wordt ook de standby router geactiveerd als de primary niet meer benaderbaar is.

Interne redundantie

Bij de tweede schets heb ik gebruik gemaakt van interne redundantie. Dit is in praktijk eigenlijk de meest gebruikte redundantie techniek. Hierbij wordt standby apparatuur naast de primaire apparatuur op dezelfde locatie geplaatst.



1=firewall
2=Backbone-switch
3=Storage
4 =Servers
5= Accesspoints
6= Enduser-switches
7= Router

Ook de tweede schets heb ik zo opgesteld, dat deze voldoet aan de eisen van de opdrachtgever. In de bovenstaande opstelling is de firewall, router, backbone-switch, servers en storage redundant uitgevoerd. Daarnaast worden hier dezelfde failover protocollen gebruikt als op de eerste schets.

Het grootste voordeel van de bovenstaande opstelling is dat je niet afhankelijk bent van je Internetverbinding. Wanneer er geen Internet beschikbaar is, draait intern het netwerk nog door (de applicaties die Internet nodig hebben uiteraard niet).
Het grootste nadeel is dat alles op dezelfde locatie aanwezig is. Wanneer het gebouw door een calamiteit getroffen wordt, bijvoorbeeld een brand, is de kans dat je zowel je primaire als de redundante hardware kwijt bent groter.

Nog een voordeel van deze opstelling is dat er minder apparatuur nodig is om aan de eisen van de opdrachtgever te voldoen. Om precies te zijn is er bij de eerste opstelling een extra firewall en router nodig om dezelfde redundantie te bereiken, die aan de behoefte van de opdrachtgever voldoet.

Cloud computing VS. Interne redundantie

Zowel cloud computing als interne redundantie hebben voor - en nadelen. Hieronder heb ik de voor - en nadelen van beide architecturen op een rijtje gezet:

Interne redundantie architectuur

Voordelen:

- Minder hardware nodig om gewenste redundantie te bereiken.
- Ook zonder Internet draait het interne netwerk normaal door en is het mogelijk om in geval van hardware problemen de stand-by apparatuur gebruiken.
- Er worden kosten bespaard voor het afhuren van een uitwijklocatie.
- De opdrachtgever heeft al aangegeven geen uitwijklocatie te willen. Hiermee houd je meer rekening met de eisen van de opdrachtgever.

Nadelen:

- Wanneer het gehele gebouw onbruikbaar wordt, is men vaak zowel de primaire als de standby apparatuur kwijt. Echter is de kans dat het gehele gebouw onbruikbaar wordt zeer klein.

Cloud computing architectuur

Voordelen:

- Veiliger, aangezien de uitwijkomgeving op een andere locatie aanwezig kan zijn.

Nadelen:

- Meer hardware nodig om gewenste redundantie te bereiken.
- Afhankelijkheid van een Internetverbinding. Wanneer er geen Internet meer tot de beschikking is, kan het ook niet mogelijk zijn om de uitwijklocatie te benaderen. Wanneer je niet bij je uitwijklocatie kan, heeft het dus ook niet veel nut om een uitwijklocatie te hebben.

- Er zijn extra kosten vereist, omdat er een uitwijklocatie nodig is. De opdrachtgever had al aangegeven geen uitwijklocatie te willen. Dit houdt in dat het eindproduct niet aan de eisen van de opdrachtgever voldoet, wanneer er voor deze oplossing gekozen zou worden.

Omdat interne redundantie ten opzichte van cloud computing meer voordelen heeft, kies ik ervoor om deze methode te gebruiken. Op deze manier bereiken we alsnog de gewenste redundantie en hoeft de opdrachtgever geen uitwijklocatie te huren.

Nu wij een degelijke architectuur voor ons ontwerp hebben opgesteld, is hiermee het eind van de architectuurfase bereikt. Het architectuurrapport is in de bijlage toegevoegd.

Conclusie

In dit rapport heb ik aangegeven welke hardware componenten we nodig hebben en waarom. Ook heb ik laten zien welke hardware redundant uitgevoerd moet worden en wat de reden daarvan is. Nadat ik twee verschillende netwerkarchitecturen met elkaar heb vergeleken, is uiteindelijk voor de architectuur gekozen die ons maximale performance en availablility biedt, met het minst apparatuur.

Afstudeeropdracht:	**Mina-IT @ Groningen**
Document:	Ontwerprapport
Student:	Mina Nabil
Afstudeerbegeleider:	Cobie van der Hoek
Expert:	Nico Huiberts
Datum:	04-10-2010

Inleiding

In dit rapport beschrijf ik hoe ik in de ontwerpfase de gekozen architectuur uit de architectuurfase tot in de kleinste details heb uitgewerkt. Een onderdeel van deze fase was het ontwerpen van een juist IP plan voor onze architectuur. Wanneer er een IP plan aanwezig is, wordt de architectuur nogmaals uitgebreid ontworpen met alle gekozen details. Het resultaat van deze fase is het uiteindelijke netwerkontwerp. Aan de hand van dit ontwerp zou een derde partij de infrastructuur kunnen aanleggen.

Inhoudsopgave

IP plan

Een goed IP-plan is cruciaal voor een netwerk. Wanneer er een verkeerde keuze wordt gemaakt bij het bedenken van een IP-plan, kan dit ervoor zorgen dat er na een bepaalde periode geen interne adressen meer beschikbaar zijn. Hierdoor moet het netwerk opnieuw ingericht worden.

Voor het ontwerpen van het netwerk heb ik besloten om meerdere subnetten te gebruiken. Hier zijn verschillende redenen voor. De belangrijkste redenen zijn beveiliging en groeperingen. Ik heb ervoor gekozen om de volgende subnetten te gebruiken:

- Een subnet voor de servers; om veiligheidsredenen is het verstandig om de servers in een aparte subnet te zetten. Zo zou de beheerder, als dat nodig is, verkeer van medewerkers kunnen blokkeren naar de servers.

- Een subnet voor voor het draadloos netwerk; gebruikers kunnen verbinding maken met het draadloos netwerk. Wanneer het draadloos netwerk in een aparte subnet wordt geplaatst, is het mogelijk om het verkeer beter te analyseren of te beveiligen, bijvoorbeeld omdat sommige gebruikers om veiligheidsredenen beperkt gebruik mogen maken van het draadloos netwerk.

- Een subnet voor de UTP; gebruikers kunnen verbinding maken met het netwerk via de UTP. Ook hier geldt dat wanneer de UTP in een aparte subnet wordt geplaatst, het mogelijk is om het verkeer beter te analyseren of te beveiligen, bijvoorbeeld omdat sommige gebruikers om veiligheidsredenen beperkt gebruik mogen maken van het draadloos netwerk.

Omdat wij het netwerk graag futureproof willen maken, heb ik besloten om een extra subnet te reserveren voor toekomstig gebruik.

In totaal hebben we dus vier subnetten nodig, namelijk:
- Servers
- Draadloos netwerk
- Fysiek netwerk
- Gereserveerde voor toekomstige gebruik.

Aantal hosts per subnet

We hebben eerder aangegeven dat we rekening gaan houden met 500 medewerkers. Om toch op de toekomst voorbereid te zijn, heb ik besloten om rekening te houden met meer medewerkers. Op deze manier voorkomen we in de toekomst veel problemen. Voor het gemak zal ik van het dubbele aantal medewerkers uit gaan. Dit betekent dat de subnet van het draadloos netwerk en van het fysieke netwerk voor 1000 medewerkers beschikbaar moet zijn.

Omdat ik niet weten hoeveel servers erbij zullen komen, is het moeilijk om in te schatten wat de maximale grootte is van de subnet. Ik zou de subnet van de servers kunnen verhogen naar 100 servers, maar omdat ik niet weet hoeveel servers in de toekomst nodig zullen zijn, is het niet verstandig om dit een lage waarde te geven. Voor de zekerheid ga ik ervan uit dat de subnet van de servers ook 1000 hosts zou kunnen hebben.

Omdat ik nog niet weet waar de gereserveerde subnet voor gebruikt zal worden, kan ik ook heel moeilijk aangeven hoeveel hosts in de subnet gaan komen. Vandaar dat ik het aantal gelijk houd aan de overige subnetten.

Dit betekent dat ik rekening moet houden met 1000 hosts per subnet.

Network class

Nu ik weet hoeveel subnetten ik nodig heb en hoeveel hosts er maximaal in de subnets zitten, kan ik de juiste networkclass kiezen. Er bestaan vijf networkclasses, namelijk A, B, C, D en E. Networkclass D is gereserveerd voor Multicasting en networkclass E is gereserveerd voor toekomstig gebruik. D en E kunnen we dus niet gebruiken. We kunnen alleen networkclass A, B en C gebruiken:

Networkclass	Netwerk ID	Max. Hosts	Max. Subnetten
A	*a*.0.0.0	16777214	4194304
B	*a.b*.0.0	65534	16384
C	a.b.c.0	254	64

De systeembeheerder van de hoofdvestiging heeft al eerder aangegeven dat de hoofdvestiging gebruik maakt van de 10.10.0.0/19 range (B CLASS). Daarnaast valt de hele organisatie onder de 10.10.0.0./18 reeks.

Wij hebben zelf een range nodig die hieronder valt en die 4000 hosts kan bevatten. Omdat de 10.10.0.0/19 reeks reeds in gebruik is door de hoofdvestiging, kunnen wij de adressen 10.10.0.0 t/m 10.10.31.255 niet gebruiken. De range die minimaal 4000 hosts kan bevatten is de 10.10.32.0/20 range. Deze range kan maximaal 4096 hosts bevatten en is dus prima voor ons.

Deze ip-range zal in de routetabel van de routers van de hoofdvestiging opgenomen worden. Dat betekent dat alle verkeer van de hoofdvestiging naar de nieuwe vestiging, naar de 10.10.32.0/20 wordt gerouteerd. Als ik ervoor zou kiezen om de vier subnetten allemaal in de routetabel van de hoofdvestiging te plaatsen, zou het beheer wel lastiger worden. Het is makkelijker om de 10.10.32.0/20 subnet te gebruiken, omdat alle subnetten toch binnen dezelfde range vallen en er dus maar één aanspreekpunt is.

In de 10.10.32.0/20 subnet kunnen maximaal 4096 hosts aanwezig zijn; dit is voldoende voor ons. Onder de 10.10.32.0/20 subnet zullen onze vier subnetten komen die in de 10.10.0.0/22 range zitten. Deze subnetten kunnen maximaal 1024 host per subnet bevatten. Dat is prima, omdat ik eigenlijk van maximaal 1000 hosts per subnet ben uitgegaan. Het geheel ziet er als volgt uit:

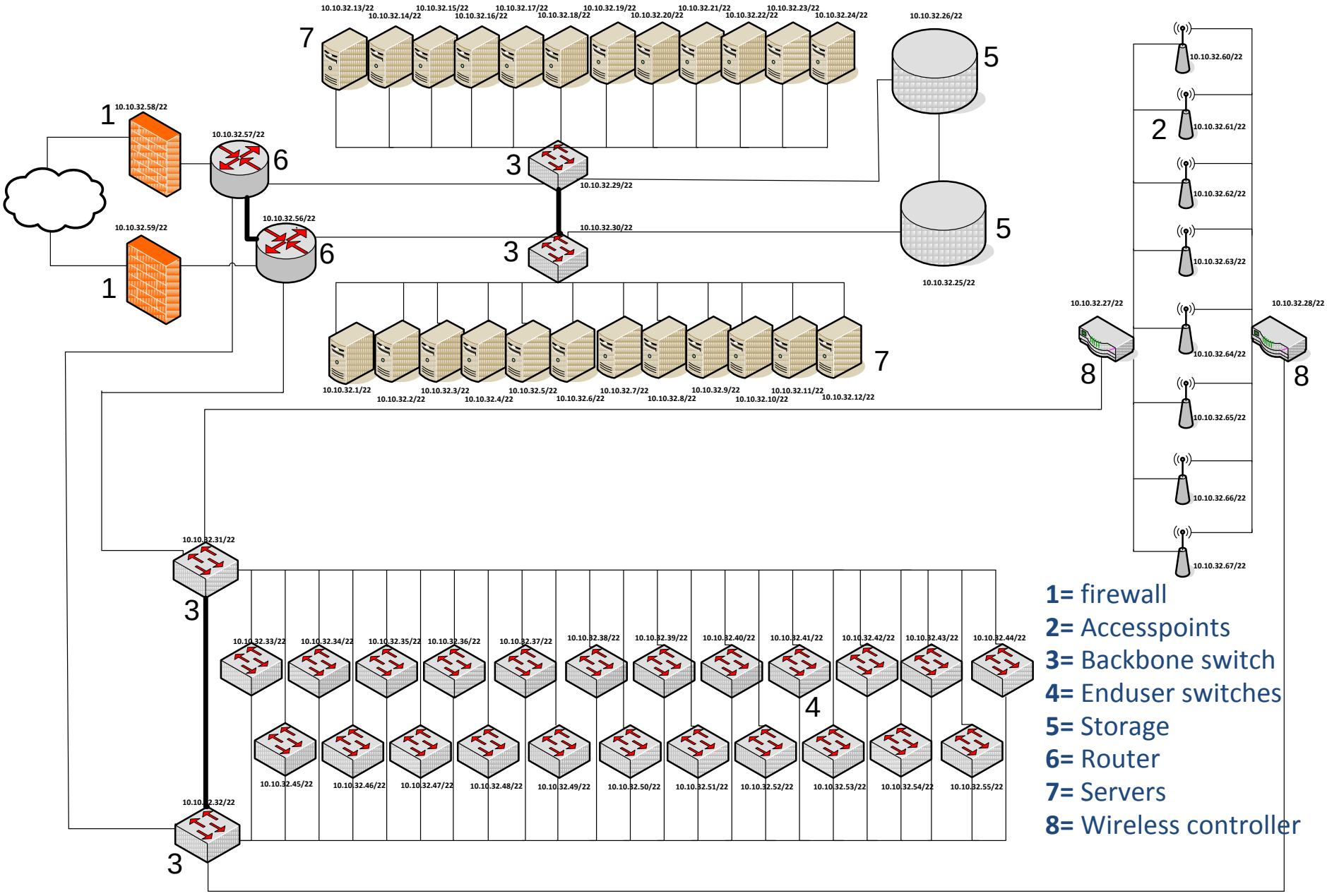
Subnet naam	Subnet	IP range	Aantal adressen
Gehele organisatie	10.10.0.0/18	10.10.0.0 – 10.10.63.255	16384 Adressen
Hoofdvestiging	10.10.0.0/19	10.10.0.0 – 10.10.31.255	8192 Adressen
Mina-IT Groningen	10.10.32.0/20	10.10.32.0 – 10.10.47.255	4096 Adressen
Servers	10.10.32.0/22	10.10.32.0 – 10.10.35.255	1024 Adressen
Draadloos netwerk	10.10.36.0/22	10.10.36.0 – 10.10.39.255	1024 Adressen
Fysiek netwerk	10.10.40.0/22	10.10.40.0 – 10.10.43.255	1024 Adressen
Gereserveerde	10.10.44.0/22	10.10.44.0 – 10.10.47.255	1024 Adressen

Hieronder is de uiteindelijke IP tabel en het netwerk architectuur.

IP tabel

Netwerkcomponent	Naam	Adres	Rol
Firewall	Firewall1	10.10.32.58/22	Primary
Firewall	Firewall1_standby	10.10.32.59/22	Standby
Server	Server1	10.10.32.1/22	Primary
Server	Server2	10.10.32.2/22	Primary
Server	Server3	10.10.32.3/22	Primary
Server	Server4	10.10.32.4/22	Primary
Server	Server5	10.10.32.5/22	Primary
Server	Server6	10.10.32.6/22	Primary
Server	Server7	10.10.32.7/22	Primary
Server	Server8	10.10.32.8/22	Primary
Server	Server9	10.10.32.9/22	Primary
Server	Server10	10.10.32.10/22	Primary
Server	Server11	10.10.32.11/22	Primary
Server	Server12	10.10.32.12/22	Primary
Server	Server1_standby	10.10.32.13/22	Standby
Server	Server2_standby	10.10.32.14/22	Standby
Server	Server3_standby	10.10.32.15/22	Standby
Server	Server4_standby	10.10.32.16/22	Standby
Server	Server5_standby	10.10.32.17/22	Standby
Server	Server6_standby	10.10.32.18/22	Standby
Server	Server7_standby	10.10.32.19/22	Standby
Server	Server8_standby	10.10.32.20/22	Standby
Server	Server9_standby	10.10.32.21/22	Standby
Server	Server10_standby	10.10.32.22/22	Standby
Server	Server10_standby	10.10.32.23/22	Standby
Server	Server10_standby	10.10.32.24/22	Standby
Storage	Storage1	10.10.32.25/22	Primary
Storage	Storage2_standby	10.10.32.26/22	Standby
Router	Router1	10.10.32.56/22	Primary
Router	Router1_standby	10.10.32.57/22	Standby
Backbone switch	Backboneswitch1	10.10.32.29/22	Primary
Backbone switch	Backboneswitch2	10.10.32.32 /22	Primary
Wirelesscontroller	wirelesscontroller	10.10.32.27 /22	Primary
Backbone switch	Backboneswitch1_standby	10.10.32.30/22	Standby
Backbone switch	Backboneswitch2_standby	10.10.32.31/22	Standby
Wirelesscontroller	wirelesscontroller _standby	10.10.32.28/22	Standby

Enduser-switch	Enduser-switch1	10.10.32.33/22	Primary
Enduser-switch	Enduser-switch2	10.10.32.34/22	Primary
Enduser-switch	Enduser-switch3	10.10.32.35/22	Primary
Enduser-switch	Enduser-switch4	10.10.32.36/22	Primary
Enduser-switch	Enduser-switch5	10.10.32.37/22	Primary
Enduser-switch	Enduser-switch6	10.10.32.38/22	Primary
Enduser-switch	Enduser-switch7	10.10.32.39/22	Primary
Enduser-switch	Enduser-switch8	10.10.32.40/22	Primary
Enduser-switch	Enduser-switch9	10.10.32.41/22	Primary
Enduser-switch	Enduser-switch10	10.10.32.42/22	Primary
Enduser-switch	Enduser-switch11	10.10.32.43/22	Primary
Enduser-switch	Enduser-switch12	10.10.32.44/22	Primary
Enduser-switch	Enduser-switch13	10.10.32.45/22	Primary
Enduser-switch	Enduser-switch14	10.10.32.46/22	Primary
Enduser-switch	Enduser-switch15	10.10.32.47/22	Primary
Enduser-switch	Enduser-switch16	10.10.32.48/22	Primary
Enduser-switch	Enduser-switch17	10.10.32.49/22	Primary
Enduser-switch	Enduser-switch18	10.10.32.50/22	Primary
Enduser-switch	Enduser-switch19	10.10.32.51/22	Primary
Enduser-switch	Enduser-switch20	10.10.32.52/22	Primary
Enduser-switch	Enduser-switch21	10.10.32.53/22	Primary
Enduser-switch	Enduser-switch22	10.10.32.54/22	Primary
Enduser-switch	Enduser-switch23	10.10.32.55/22	Primary
Accesspoint	Accesspoint1	10.10.32.60/22	Primary
Accesspoint	Accesspoint2	10.10.32.61/22	Primary
Accesspoint	Accesspoint3	10.10.32.62/22	Primary
Accesspoint	Accesspoint4	10.10.32.63/22	Primary
Accesspoint	Accesspoint5	10.10.32.64/22	Primary
Accesspoint	Accesspoint6	10.10.32.65/22	Primary
Accesspoint	Accesspoint7	10.10.32.66/22	Primary
Accesspoint	Accesspoint8	10.10.32.67/22	Primary



1= firewall
2= Accesspoints
3= Backbone switch
4= Enduser switches
5= Storage
6= Router
7= Servers
8= Wireless controller

Conclusie

In dit rapport heb ik beschreven wat subnetten zijn en hoe ik ze gebruikt heb. Tevens heb ik een complete netwerkarchitectuur inclusief IP tabel gemaakt. Aan de hand van deze documenten kan de opdrachtgever een bedrijf inhuren dat het netwerk voor hem kan inrichten volgens het geleverde ontwerp.

Afstudeeropdracht:	**Mina-IT @ Groningen**
Document:	adviesrapport
Student:	Mina Nabil
Afstudeerbegeleider:	Cobie van der Hoek
Expert:	Nico Huiberts
Datum:	04-10-2010

Inleiding

Een van de doelstellingen van dit project is om een adviesrapport te maken voor de te gebruiken hardware. In dit adviesrapport heb ik een advies gegeven over de verschillende hardware componenten die nodig zijn in ons netwerk.

Om advies te kunnen geven over een component, heb ik vooraf onderzoek moeten doen naar dat component en de werking ervan. Op deze manier kon ik mijn criteria bepalen. Zodra de criteria vastgesteld waren, kon ik op zoek gaan naar de verschillende componenten die aan mijn criteria voldeden. Vervolgens heb ik de verschillende componenten met elkaar vergeleken om de meest geschikte te selecteren. Bij de vergelijking is rekening gehouden met verschillende aspecten zoals performance, beschikbaarheid, prijs en kwaliteit.

Aan het eind van dit rapport heb ik een advies gegeven over de beveiliging van het netwerk. Ook hier heb ik de verschillende beveiligingstechnieken met elkaar vergeleken en de beste techniek gekozen.

Inhoudsopgave

Hardware

Om het juiste hardware component te vinden, moet ik belangrijke afwegingen maken met betrekking tot de uptime, specificaties, performance, kosten, etc.
Ik geef per product aan wat de verschillende mogelijkheden en belangrijkste verschillen zijn. Tevens zal ik per product de argumenten onderbouwen waarom ik vind dat de gekozen product het best past bij het netwerk.

Ik geef advies over de volgende producten:

- Werkstations
- Firewalls
- Routers
- Enduser-switches
- Backbone-switches
- Storage
- Accesspoints
- Servers
- Backup Units
- UPS
- Primary en backup verbindingen naar hoofdkantoor

Budget

De opdrachtgever heeft aangegeven dat er een budget van €1.000.000 gereserveerd is voor de werkstations en de netwerkapparatuur. Hij heeft tevens aangegeven dat dit bedrag verhoogd kan worden indien dat noodzakelijk is. Het is echter wel de bedoeling dat we in eerste instantie binnen het budget te blijven.

Advies over de hardware componenten

In de volgende hoofdstukken beschrijf ik het proces die ik doorlopen heb bij het adviseren van de hardware componenten voor het nieuwe netwerk.

Werkstations

Via de werkstations zullen de werknemers al hun werkzaamheden moeten uitvoeren. Dit betekent dat een goed werkstation een must is. Als ik een werkstation kies dat te langzaam is voor de werknemers, zal dit voor vertragingen en irritaties zorgen. Het is echter ook niet de bedoeling om een werkstation te kiezen dat extreem snel is en waar uiteindelijk geen gebruik wordt gemaakt van alle resources dat het werkstation kan leveren. Dit is dan eigenlijk geldverspilling.
Uit mijn onderzoek (zie bijlage) zijn de onderstaande werkstations in aanmerking gekomen:

Werkstation	Geheugen	CPU	Hardeschijf	Prijs
HP Compaq Business dc7900	2gb + 2gb extra	3 GHz	160 Gb	€655,-
HP Compaq 6000 Pro	2gb + 2gb extra	3 GHz	250 Gb	€589,-
Acer Veriton M670G	2gb + 2gb extra	3.16GHz	320 Gb	€655,-
Dell OptiPlex 780DT	4 gb standaard	3.16GHz	250 Gb	€659,-

Bovenstaande machines voldoen allemaal aan de gestelde eisen. Bijna alle werkstations kosten ongeveer hetzelfde, behalve de HP Compaq 6000; deze is ongeveer €70,- goedkoper. Omdat ze allemaal voldoen aan de eisen, is het zonde om meer geld te investeren in hardware als niet het maximale eruit wordt gehaald. Vandaar dat ik de opdrachtgever ga adviseren om de HP Compaq 6000 pro aan te schaffen.
Omdat bovenstaande werkstations zonder schermen geleverd worden, ga ik de opdrachtgever adviseren om de bijpassende schermen aan te schaffen. Dit is de HP LA1951G 19-inch. Dit scherm kost €144,- euro. In totaal kost een werkplek dus €733,-

Voor de 450 werkplekken zal uiteindelijk een bedrag van 450 x 733 = € 329.850,- betaald moeten worden. Hiermee houden we nog €670.150,- over van ons budget.

Firewall

Een firewall wordt voornamelijk gebruikt om te voorkomen dat (ongewenst) netwerkverkeer van het ene netwerksegment terecht komt in een ander netwerksegment. Hiermee wordt de veiligheid binnen het netwerk verhoogd. Meestal wordt een firewall ingezet om het interne netwerk te beveiligen tegen het Internet. Zo minimaliseer je de kans dat vanuit het Internet virussen of hackers in het netwerk binnendringen.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande firewalls in aanmerking gekomen:

Product	DMZ	Aantal VPN verbindingen	snelheid	Aantal gebruikers	prijs
Cisco ASA 5550	Ja	500	1024 mb/s	650000	€11.999,-
SonicWALL NSA/E6500 Multi-Core UTM	Ja	6000	1024 mb/s	6000	€12.395,-
SonicWALL (NSA) E5500	Ja	4000	3900 mb/s	4000	€8133,-
DC-Networks firewall: DCFW-1800E-V2 Firewall	Ja	2000	1024 mb/s	1.000.000	€4490,-
D-Link ENTERPRISE FIREWALL	Ja	2500	1024 mb/s	1000	€5331,-

Er is in principe een firewall nodig die maximaal 500 gebruikers kan ondersteunen en 500 VPN verbindingen tegelijkertijd kan maken. Daarnaast moet de firewall een snelheid van minimaal 1024 mb/s hebben.

De Cisco ASA 5550 is een van de duurdere firewalls uit de lijst. Deze switch kan 650.000 medewerkers ondersteunen. Wij hebben echter maar 500 medewerkers. Omdat deze firewall verder geen bijzonderheden biedt, zal deze dus afvallen.

De SonicWALL NSA/E6500 is de duurste firewall uit de lijst. Deze firewall kan de meeste VPN verbindingen maken, namelijk 6000. Omdat wij alleen 500 medewerkers hebben, is deze dure feature dus overbodig. De SonicWALL NSA/E6500 valt ook af.

De SonicWALL (NSA) E5500 is nu de duurste firewall die over is gebleven. Wat deze firewall duurder maakt, is het feit dat hij bijna vier keer zo snel is als de overige firewalls. Echter, wij hebben genoeg aan een firewall die 1024 mb/s kan doorvoeren. Het zou dus geldverspilling zijn om een snellere firewall aan te schaffen en daar het maximale niet uit te halen.

Nu blijven twee firewalls over: de DC-Networks DCFW-1800E en de D-Link ENTERPRISE FIREWALL. De DC-Networks firewall kan 1.000.000 gebruikers ondersteunen. Dat is 990.000 keer meer dan de D-Link. De D-Link ENTERPRISE kan 2500 VPN verbindingen beheren; dat is

500 meer dan de DC-Networks. Echter, beide extra features zijn niet interessant voor ons omdat ze allebei al prima voldoen aan onze eisen. Ik zal de opdrachtgever adviseren om twee DC-Networks DCFW-1800E-V2 Firewalls aan te schaffen. Samen kosten deze firewalls €8980,- . Hiermee houden we nog €661.170,- over van ons budget.

De DC-Network is een nieuw merk op de markt en heeft zich in een korte tijd zeer goed bewezen. Ik ben ervan overtuigd dat deze prima zal bevallen.

Routers

Een router zorgt voor het routeren tussen verschillende netwerken. Een router gebruikt hiervoor zijn eigen routetabel, waarin staat wat de kortste routes zijn naar de verschillende nodes in een netwerk. Omdat ons netwerk meerdere subnetten heeft, is er een router nodig om tussen de subnetten te routeren.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande routers in aanmerking gekomen:

Product	MTBF	Protocollen	Uitbreidbaar	Snelheid	Prijs
Cisco 2851	19 jaar	Allemaal	Ja 4 slots	1 Gb/s	€4.199,-
Cisco 2821	12 jaar	Allemaal	Ja 4 slots	1 Gb/s	€2.799,-
Juniper J2320	7 jaar	Allemaal	Ja 3 slots	1 Gb/s	€1.259,-

Alle bovenstaande routers voldoen aan ons eisen. De Juniper router is het goedkoopst van de drie. Echter heeft deze minder uitbreidingsmogelijkheden. Ook is het de minst betrouwbare router van de drie, omdat het de laagste MTBF-waarde heeft. De Juniper valt dus af, omdat deze qua niveau ver onder de overige routers zit.

Nu de Juniper is afgevallen, blijven de Cisco 2851 en de Cisco 2821 over. De grote verschillen tussen deze routers is de MTBF en de prijs. De Cisco 2851 gaat volgens Cisco 19 jaar mee, voordat er problemen ontstaan. Bij de Cisco 2821 is dat 12 jaar. De Cisco 2851 is echter wel €1400,- duurder.

Omdat wij de routers redundant zullen uitvoeren, moet een MTBF van 12 jaar meer dan voldoende zijn. Dit omdat de standby router in geval van problemen de taken overneemt van de primary router. Daarom is het niet verstandig om €1400,- extra te betalen per router, terwijl we geen optimaal gebruik gaan maken van de extra betrouwbaarheid.

Ik zal de opdrachtgever adviseren om twee Cisco 2851 routers aan te schaffen. De kosten hiervan zijn samen €8.398,- . Hiermee blijft er nog €652.772,- over van ons budget.

Enduser-switches

Een enduser-switch zorgt ervoor dat de data bij de juiste persoon wordt geleverd. Het grote verschil tussen bijvoorbeeld een switch en een hub, is dat een hub alle data naar alle poorten stuurt. Een switch kan echter achterhalen voor welke node een bepaalde data packet bestemd is en stuurt het vervolgens alleen naar deze node. Hiermee overlaad je de rest van de nodes niet met data die niet voor hen bestemd is.

Elk werkstation, netwerkprinter, netwerkscanner, etc., wordt door middel van een switch aan het netwerk gehangen. Zoals reeds aangegeven, is het de bedoeling dat er meer dan 500 netwerkapparaten aan het netwerk worden hangen. Dit komt neer op 23 switches van 24 poorten.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande enduser-switches in aanmerking gekomen:

Product	VLAN	Routering	Protocollen	Prijs
3Com Baseline Plus Switch 2928 PWR	Ja	Ja	Allemaal	€449,-
Linksys SPS2024	Ja	Ja	Allemaal	€449,-
Cisco Small Business Pro 520 Ethernet Switch 24-poorts 10/100/1000 met PoE	Ja	Ja	Allemaal	€1.399,-
HP ProCurve Switch 2910al-24G	Ja	Ja	Allemaal	€1.599,-
3Com Switch 4500G 24-Poorten	Ja	Ja	Allemaal	€1.799,-

Bovenstaande switches voldoen allemaal aan onze eisen.

De 3Com 4500G switch is de duurste van allemaal. Deze is zelfs vier keer zo duur dan de 3Com 2928 PWR switch. Echter heeft deze switch wel een functionaliteit die de rest niet heeft, namelijk twee upload poorten van 10 gb/s. Dit was echter geen eis van ons. De eis was een snelheid van 1 gb/s. Het is dan ook niet verantwoord om vier keer zoveel te betalen voor een switch waar we niet het maximale uit kunnen halen. Daarom valt de 3Com 4500G switch af.

De Cisco small business en de HP ProCurve switch zijn ruim drie keer zo duur dan de 3Com Baseline of de Linksys SPS2024. De reden dat deze switches duurder zijn, is het feit dat ze meer protocollen ondersteunen. Echter, wij gaan geen gebruik maken van al deze extra features. Het is dan ook geldverspilling als we meer geld gaan uitgeven aan features die we niet gaan gebruiken. De Cisco small business en de HP ProCurve switch vallen dus ook allebei af.

Nu blijven de 3Com Baseline en de Linksys SPS2024 over. Deze twee switches ondersteunen allebei VLAN, ROUTERING en ze hebben 24 x 1gb/s poorten. Ook de prijs van deze twee switches is hetzelfde. Omdat deze twee switches zo erg op elkaar lijken, moet ik dieper ingaan op de verschillen. Op deze manier kan ik zien welke switch meer te bieden heeft.

Als ik de specificaties van beide switches beter ga bekijken, zie ik een duidelijk verschil in de ondersteunde protocollen.

Dit zijn de protocollen die de 3Com switch ondersteunt:
Datatransport, Layer 3-omschakeling, Layer 2-omschakeling, DHCP-ondersteuning, automatische onderhandeling, ARP-ondersteuning, VLAN-ondersteuning, IGMP-spionage, Weighted Round Robin (WRR) queuing, opslaan en verder, Quality of Service (QoS), Jumbo Frames ondersteuning.

Dit zijn de protocollen die de Cisco switch ondersteunt:
Datatransport, Layer 2-omschakeling, DHCP-ondersteuning, automatische onderhandeling, BOOTP-ondersteuning, VLAN-ondersteuning, auto-uplink (auto MDI/MDI-X), IGMP-spionage, gespiegelde poorten, DiffServ-ondersteuning, Weighted Round Robin (WRR) queuing, opslaan en verder, MAC adresfiltering, Broadcast Storm Control, IPv6-ondersteuning, SNTP-ondersteuning, DHCP-spionage, Trivial File Transfer Protocol (TFTP) ondersteuning, Access Control List (ACL)-ondersteuning, Quality of Service (QoS), SSH-ondersteuning, Jumbo Frames ondersteuning, Dynamic ARP Inspection (DAI).

Zoals hierboven te zien is, ondersteunt de Cisco switch twee keer zoveel protocollen dan de 3Com switch. Een ander verschil dat ik heb ontdekt is het aantal beheerprotocollen.

Dit zijn de beheerprotocollen die 3Com switch ondersteunt:
SNMP 1, SNMP 2, RMON, SNMP 3, HTTPS

Dit zijn de beheerprotocollen die de Cisco switch ondersteunt:
SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, SSH.

Aan de hand van bovenstaande gegevens ga ik de opdrachtgever adviseren om de Linksys SPS2024 aan te schaffen. De Linksys SPS2024 kost €449,- per stuk. We hebben 23 stuks nodig. Dit betekent dat we totaal €10.327,- kwijt zijn aan de enduser-switches. Hiermee houden we nog €642.445,- over van het budget.

Backbone-switches

Backbone-switches voeren in principe dezelfde taken uit als de enduser-switches. Echter, backbone-switches moeten sneller zijn omdat daar veel meer verkeer doorheen gaat dan een enduser-switch. Tevens moeten de backbone-switches betrouwbaarder zijn, omdat de impact bij een defect vele malen groter is dan bij een enduser-switch.

In onze omgeving worden alle enduser-switches aan het netwerk gehangen door middel van backbone-switches . Dit betekent dat wanneer de backbone-switches kapot gaan, alle gebruikers zonder netwerk zitten. Daarom heb ik in onze omgeving de backbone-switches redundant uitgevoerd, om te voorkomen dat de hele productieomgeving uitvalt wanneer de backbone-switch kapot gaat.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande backbone-switches in aanmerking gekomen:

Product	Poorten	Snelheid	Redundante hardware	Prijs
Cisco N5000 2RU CHASSIS 5 FAN	40	10 gb/s	Ja	€17.623,22
Cisco N5000 1RU Chassis 2 Fan 20p	20	10 gb/s	Ja	€9.425,21
HP 2408 24-10GBE W/8-8GB	24	10 gb/s	Nee	€ 42.065,00

De HP switch is de duurste van de drie en heeft 24 poorten. Deze switch heeft echter geen redundante stroomvoorziening en FAN. Omdat ik liever niet op betrouwbaarheid inlever, valt deze switch af.

De overgebleven switches zijn van hetzelfde merk en model, alleen heeft de Cisco N5000 2RU twee keer zoveel poorten. Omdat deze switch de enige is die geschikt is voor het aansluiten van de 23 enduser-switches, is deze switch ideaal.

Ik zou ook de Cisco N5000 2RU CHASSIS 5 FAN switch kunnen gebruiken voor het serverpark en de accesspoints. Echter heb ik niet zoveel poorten nodig voor de andere twee segmenten. Het zou daarom geldverspilling zijn als we een 40 poorten switch aanschaffen, aangezien we bij de twee segmenten respectievelijk 8 en 13 poorten gaan gebruiken.

Voor het serverpark en de accesspoints zou ik de Cisco N5000 1RU kunnen gebruiken. Deze switch is net zo betrouwbaar als de N5000 2RU maar heeft 20 poorten in plaats van 40 poorten. Daarnaast kost deze switch de helft van de prijs van de N5000 2RU CHASSIS 5 FAN switch. Dat maakt deze switch ideaal voor het serverpark en de accesspoints.

Ik zal de opdrachtgever adviseren om tweemaal de N5000 2RU en viermaal de Cisco N5000 1RU aan te schaffen. Deze switches kosten bij elkaar €72.947,28. Hiermee blijft er nog €569.498,- over van het budget.

Storage

Storage is een van de belangrijkste componenten in de gehele IT-infrastructuur. Op storage wordt data opgeslagen. Data is zo waardevol, dat in geval van dataverlies er vaak een ramp ontstaat binnen het bedrijf (wanneer er geen back-ups gemaakt worden).

Zonder data kun je vaak het bedrijf niet meer runnen. Wanneer bijvoorbeeld alle administratie en financiële data verdwenen is, kun je vaak niet meer achterhalen welke klanten wel of niet betaald hebben. Gegevens over de medewerkers zoals salarissen, bonussen en afspraken raken dan ook vaak kwijt. Dergelijke fouten zijn al vaker ontstaan en bedrijven die dit hebben meegemaakt zijn vaak onderuit gegaan. Data gaat vaak gepaard met kennis en kennis is macht. Vandaar dat ik voor dit bedrijf een zeer goede storage oplossing nodig heb.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande storages in aanmerking gekomen:

Product	Snelheid	Capaciteit	Type	Prijs
Netgear ReadyNAS 4200 19 Rackmount, 10GB via CX-4	10 gb/s	24 TB	Schijven	€8.644,95
Netgear ReadyNAS 4200 19 Rackmount	1 gb/s	24 TB	Schijven	€7.992,95
HP StorageWorks All-in-One Storage System 1200r 3TB SATA	1 gb/s	3 TB	Schijven	€6.349,95
Thecus N8800 Network Storage Server 8 BAY NAS 16TB	1 gb/s	16 TB	Schijven	€3.020,95
Intel X25-E SATA II SSD 64GB	10 gb/s	64 GB	SSD	€584,95

Omdat ik een zeer snelle storage oplossing wil hebben, heb ik besloten dat de schijven een minimale overdrachtsnelheid moeten hebben van 10 gb/s. De Netgear ReadyNAS 4200 19 Rackmount, de HP StorageWorks All-in-One Storage en de Thecus storage hebben allemaal een verbinding met een maximale overdrachtsnelheid van 1 gb/s. Dit is voor ons te laag en daarom vallen deze drie storage oplossingen al af.

Nu blijven twee storage oplossingen over: de Netgear ReadyNAS 4200 19 Rackmount, 10GB via CX-4 en de Intel X25-E SATA II SSD 64GB. Het grootste verschil tussen deze storage oplossingen is het type. De Intel schijf is Solid state disk. Het genoemde bedrag is per 64 GB module. Eerder is aangegeven dat ik een storage wil hebben van 20 TB. Dit betekent dat ik 20 TB/64 Gb = 320 schijven nodig zal hebben. Samen zullen de schijven dan 320 x €584,95 = €187.184,- kosten. Dit is exclusief de kosten van de server waarin de schijven gehangen zullen worden. De netgear kost echter maar €8.644,95 en daar krijg je 24 TB voor, inclusief de storageserver. Dat is ruim €180.000,- euro goedkoper.

De voornaamste reden om de Intel SSD te nemen is de betrouwbaarheid. Echter, ik heb in ons netwerk twee storage servers gehangen: één primary en één standby storage. Dit betekent dat de data te allen tijde op twee verschillende storage schijven zijn opgeslagen. Ook zullen er regelmatig back-ups gemaakt worden van ons systeem, waardoor de

betrouwbaarheid alleen maar toeneemt. Omdat de data dus altijd op twee verschillende plekken opgeslagen is plus de back-up, is de keuze voor de Netgear storage snel gemaakt.

Een tweede reden om voor de Netgear storage te gaan, is de prijs. Omdat er twee storage dozen nodig zijn, betekent dit een besparing van €360.000,- . Als ik voor de Intel SSD zou kiezen, zouden we hoogwaarschijnlijk in geldproblemen komen omdat er nog veel netwerkcomponenten aangeschaft moeten worden.

Om deze redenen zal ik de opdrachtgever adviseren om twee Netgear ReadyNAS 4200 19 Rackmount, 10GB via CX-4 aan te schaffen die samen €17.289,90 kosten. Hiermee blijft er nog €552.209,- over van het budget.

Wireless controller

Om de accesspoints aan te sturen wil ik gebruik maken van wireless controllers. Een wireless controller zorgt ook voor de beveiliging van het draadloos netwerk.

Om een geschikte netwerkcontroller te vinden, moet ik eerst weten waar ik op moeten letten bij het maken van de juiste keuze. Ik heb daarom eerst onderzocht waar een goede wireless controller aan moet voldoen.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande wireless-controllers in aanmerking gekomen:

Product	Snelheid	Aantal AP's	Gebruikers	beveiliging	prijs
Cisco 4400 Series WLAN Controller of up to 12 Lightweight APs	1 gb/s	12	2000	Ja	€4.999,-
HP ProCurve MSM730 Access Controller	100mb/s	40	500	Ja	€1.999,-
Netgear ProSafe Wirelless Controller incl. 8 10/100 PoE poorten	100mb/s	16	256	Ja	€1.559,-

Zoals bekend is, moet de overdrachtsnelheid van de wireless controllers minimaal 1 gb/s zijn. Er is maar één wireless controller die hier aan voldoet, namelijk de Cisco wireless controller. Ook kan deze wireless controller het meeste aantal gebruikers ondersteunen en biedt het de beste beveiliging van de drie, namelijk: RSA, RC4, MD5, AES, 128-bits WEP, SSL, TLS 1.0, 104-bits WEP, TKIP, WPA, WPA2, PKI en AES-CCMP.

Deze wireless controller voldoet prima aan de eisen voor het netwerk. Ik ga daarom de opdrachtgever adviseren om hier twee van aan te schaffen. Dat komt neer op €9998,-. Hiermee blijft er nog €561.061,- over van het budget.

Accesspoints

Accesspoints zorgen ervoor dat werknemers gebruik kunnen maken van het netwerk via het draadloze netwerk. Omdat sommige medewerkers, ook in de toekomst, gebruik zullen maken van laptops, moet op alle verdiepingen een draadloos netwerk beschikbaar zijn. Zoals ik eerder heb uitgezocht, is het bereik van de accesspoints ruim voldoende om een gehele verdieping van een draadloos netwerk te voorzien.

Voordat ik bij de hardware leverancier ga kijken wat ze te bieden hebben, moet ik eerst weten waar ik op moet letten om de juiste keuze te kunnen maken. Om dat te achterhalen, heb ik me eerst moeten verdiepen in accesspoints en de werking daarvan.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande accesspoints in aanmerking gekomen:

Product	Snelheid	Ethernet poorten	Prijs
HP ProCurve MSM335 WW Access Point	54 mb/s	1	€649,-
HP ProCurve MSM323 WW Access Point	54 mb/s	2	€549,-
D-LINK (DNK) DWL-8500AP 802.11A/G	108 mb/s	1	€369,-

De D-LINK accesspoint is de snelste van de drie. Ook is deze accesspoint het goedkoopst van de drie. Echter, deze accesspoint heeft maar één ethernet poort. Dat betekent dat deze accesspoint ongeschikt is voor het netwerk.

De twee HP accesspoints zijn bijna identiek aan elkaar. Alleen heeft de HP ProCurve MSM335 maar één ethernet poort terwijl de HP ProCurve MSM323 twee ethernet poorten heeft. Ook is deze accesspoint goedkoper dan de andere HP ProCurve MSM335. Deze accesspoint is eigenlijk de enige die geschikt is voor het netwerk.

Ik ga de opdrachtgever daarom adviseren om hier acht van aan te schaffen. Bij elkaar kosten deze acht accesspoints €4.392,- . Dat betekent dat er nu nog €556.669,- over is van ons budget.

Servers

Het is erg belangrijk om een snel en betrouwbaar netwerk te hebben. Een netwerk is niets meer dat een medium. Het gene waar het uiteindelijk om gaat is de services waar je gebruik van kunt maken. Deze services worden door de servers geleverd. In alle netwerken zijn servers onmisbaar, of het nu om een applicatieserver gaat of om een database server. Omdat servers zo belangrijk zijn voor ons, moeten we ervoor zorgen dat we de juiste servers voor onze omgeving vinden.

We hebben eerder aangegeven dat we gebruik zullen gaan maken van virtualisatie, omdat niet alle servers altijd erg hard zullen werken. Daarom is het zonde om twaalf fysieke servers aan te schaffen waar we niet het maximale uit gaan halen. Zoals eerder afgesproken gaan we zes zware servers kopen en daarop zullen we twaalf virtuele servers installeren. Ook voor de standby omgeving hebben we de zelfde opstelling nodig. In totaal hebben we dus 12 fysieke servers nodig waar 24 virtuele servers op geïnstalleerd kunnen worden.

Uit mijn onderzoek (zie bijlage) zijn de onderstaande servers in aanmerking gekomen:

Server	Processor	Geheugen	GB Ethernet	Type	Prijs
HP ProLiant BL680c G5	2 x Quad Core Xeon E7340 (2.4GHz)	8 GB (max 64 GB)	4	Blade	€8.199,-
IBM BladeCenter LS42 7902	2 x AMD Opteron 8431 / 2.4 GHz (6-core)	4 GB (max 128 GB)	2	Blade	€7.899,-
HP ProLiant DL180 G6	2 x Intel Xeon E5540 / 2.53 GHz (Quad-Core)	12GB(max 96 GB)	2	Blade	€3.299,-
HP ProLiant DL165 G6	2 x AMD Opteron 2435 / 2.6 GHz (6-core)	8 GB (max 32 GB)	2	Blade	€2.749,-
Dell PowerEdge R710	1 x Intel Xeon E5530 2.4 Ghz (Quad-Core)	12 Gb(max 144 GB)	2	Blade	€2.199,-
Lenovo ThinkServer RD220	1 x Intel Xeon E5520 / 2.26 GHz (Quad-Core)	2 Gb (max 128 GB)	2	Blade	€2.049,-

Tijdens mijn onderzoek ben ik erachter gekomen dat IBM en HP de grootste spelers op de markt zijn op het gebied van servers. De HP ProLiant BL680c G5 server is de duurste en biedt vier Gb ethernet poorten. Wij hebben echter maar twee Gb ethernet poorten nodig. Als wij deze server zouden kiezen dan zouden we niet het maximale uit de server kunnen halen. Het zal daarom geldverspilling zijn als we deze server zouden aanschaffen. Daarom valt deze server af.

Zoals reeds aangegeven willen we per virtuele server minimaal twee cores hebben van 2,5Ghz. Dit betekent dat we dus minimaal een quadcore van 2.5 Ghz. nodig hebben. Daarom vallen tevens de Dell en lenove servers uit de selectie.

De IBM server is de duurste van de overgebleven drie servers. Echter is deze zeker niet de beste. De HP ProLiant DL165 G6 is de goedkoopste van de drie en heeft meer geheugen. In de IBM server is maximaal 128 GB aan geheugen te plaatsen. Zoveel geheugen zouden wij nooit nodig hebben, daarom is het niet financieel verantwoord om voor deze server te kiezen. Deze server valt zodoende ook af.

Nu blijven de HP ProLiant DL180 G6 en de HP ProLiant DL165 G6 over. De HP ProLiant DL180 heeft 4 Gb geheugen meer ter beschikking en kan maximaal 96 GB aan geheugen hebben, in tegenstelling tot de HP ProLiant DL165 die maar 32 GB aan geheugen kan dragen.

Het laatste grote verschil tussen deze twee servers is de processor. De AMD processor heeft 6 cores. De Xeon processor heeft 4 cores. Echter is de Xeon processor in praktijk sneller. Hieronder zijn de resultaten van een benchmark (toms hardware) die dit bevestigt.

Model	Speed (GHz)	Max. clock 4 cores busy (GHz)	L2 Cache (KB)	L3 Cache (MB)	Interconnect Bandwidth in One Direction
AMD Opteron 2435	2.6	2.6	6 x 512 KB	6 MB	9.8 GB/s
Intel Xeon E5540	2.53	2.66	4 x 256 KB	8 MB	11.7 GB/s

Hiermee is de HP ProLiant DL180 G6 wederom beter. Ook is het verschil in prijs onder de 500 euro. Je krijgt dus veel meer waar voor je geld.

Ik zal daarom de opdrachtgever aanraden om twaalf HP ProLiant DL180 G6 servers aan te schaffen. Bij elkaar kosten deze servers €39.588,- (exclusief de schijven).
Dit betekent dat er nog €517.081,- van ons budget over blijft.

Voor High Availability doeleinden zullen de servers in twee clusters geplaatst moeten worden. Zo kunnen de servers elkaars services overnemen in geval van calamiteiten. Echter zal de systeembeheerder hier zelf zorg voor moet dragen, omdat clustering buiten de scope van het project valt. Ik zal hier daarom niet verder op ingaan.

Op verzoek van mevrouw Van der Hoek en de heer Huiberts zal ik de komende hoofdstukken niet uitgebreid behandelen omdat de nadruk van het project daar niet op ligt. Bij het uitbrengen van een advies over de Backup Units, UPS en de verbindingen naar het hoofdkantoor, zal ik alleen aangeven welke producten ik adviseer aan de opdrachtgever en waarom.

Back-up Units

Ik heb voor een storage oplossing gekozen waarbij de data te allen tijde op twee storage stations staan opgeslagen. Beide storage stations staan echter wel in hetzelfde gebouw. Dit betekent dat wanneer het gebouw bijvoorbeeld afbrandt, alle data alsnog kwijt zullen raken. Om dit probleem te voorkomen, zullen de data ook buiten het gebouw bewaard moeten worden. Hiervoor zijn de juiste back-up units nodig. De data kunnen we bijvoorbeeld op tapes opslaan, die vervolgens dagelijks of wekelijks worden bewaard in de hoofdvestiging.

Daarnaast zou er gebruik gemaakt kunnen worden van de 'MEDIA, TRANSPORT EN OPSLAG' service van Getronics. Hierbij komen Getronics medewerkers de tapes dagelijks ophalen, waarna deze naar kluizen worden gebracht. Zo ben je er altijd zeker van dat de data ook in geval van calamiteiten buiten het gebouw veilig is.

Om te kunnen achterhalen wat de meest geschikte back-up unit is, moet ik eerst weten hoeveel data de back-up unit moet kunnen bewaren. Omdat dit een fictieve opdracht is, zal het niet mogelijk zijn om te weten hoeveel data uiteindelijk gebackupt moet worden. Ik kies daarom voor een fictieve waarde van 10 TB.

Toen ik op het Internet zocht naar de beste back-up oplossingen, kwam ik al snel bij HP uit. HP is één van de grootste spelers op het gebied van back-up units en tapes.
Ik heb bij Misco uitgezocht wat in dit geval de beste back-up oplossing is en ik kwam uit op de HP StorageWorks MSL2024 1 Ultrium 960 Drive Library. Deze back-up unit kost €6.226,95 en kan maximaal 19.2 TB aan gecomprimeerde data opslaan, en 9.6 TB aan data van oorspronkelijk formaat. In deze tape unit kunnen maximaal 24 tapes geplaatst worden. Hiermee kan deze back-up unit meer data opslaan dan elke ander back-up unit die de leverancier kan leveren. Ook is dit een financieel bewuste keuze, omdat er ook duurdere back-up units leverbaar zijn, die minder snel zijn en minder data kunnen opslaan. Al met al is dit dus een ideale back-up unit voor Mina-IT.

Ik zal de opdrachtgever adviseren om deze back-up unit aan te schaffen. Hiermee blijft er nog €510.854 over van het budget.

UPS

Wanneer er een stroomstoring optreedt en de servers meteen uitvallen, kan dit voor grote problemen zorgen. Dit omdat componenten van de server hierdoor defect kunnen raken. Om in geval van een stroomstoring de servers netjes te kunnen afsluiten, is er een UPS (Uninterruptible Power Supply) nodig. Hiermee krijgen de beheerders een paar extra minuten de tijd om de servers netjes af te sluiten. De servers zijn ook zo in te stellen dat ze automatisch afsluiten wanneer er een stroomstoring optreedt, en dat de UPS vervolgens de stroom levert in plaats van de gebruikelijke netstroom.

Een tweede belangrijke functie van UPS is het beschermen van je hardware tegen hoge stroompieken. Wanneer er hoge stroompieken optreden, zal de UPS deze opvangen waardoor ze geen gevaar meer vormen voor de servers.

Om de juiste UPS te vinden moet ik eerst weten hoeveel stroom de servers verbruiken. Met deze gegevens kan ik zoeken naar de UPS die aan de behoeften van de servers voldoet.

Eerder heb ik de opdrachtgever geadviseerd om twaalf HP ProLiant DL180 G6 servers aan te schaffen. Ik heb bij HP uitgezocht hoeveel stroom deze servers verbruiken en dat bleek 470 watt per server te zijn. Dat betekent dat de twaalf servers bij elkaar 470 x 12 = 5640 watt verbruiken.

Nu ik weet hoe sterk de UPS moet zijn, heb ik gekeken naar het aanbod van Misco. Ik heb de verschillende UPS units met elkaar vergeleken en uiteindelijk kwam ik bij de APC Smart-UPS VT 10kVA 400V terecht. Deze UPS levert 8000 watt, wat meer dan voldoende is, en heeft daarnaast een zeer acceptabele prijs van €6.599. APC is de marktleider op het gebied van UPS's en ik ben er daarom zeker van dat dit een prima keuze is voor het netwerk.

Ik ga de opdrachtgever adviseren om deze UPS aan te schaffen. Hiermee blijft er nog €504.255,- over van het budget.

Verbindingen naar het hoofdkantoor

De opdrachtgever zal veel beheertaken op de nieuwe vestiging laten uitvoeren door de beheerders van de hoofdvestiging. Hiervoor moet er een snelle verbinding tussen de vestigingen beschikbaar zijn. Ook moet er een tweede verbinding aanwezig zijn in geval van een storing met de primaire verbinding, zodat de beheerders altijd hun taken kunnen uitvoeren bij storingen. Deze verbinding hoeft echter niet zo snel te zijn, zodat er niet op de kosten wordt gedrukt.

Toen ik op het Internet zocht naar de verbindingen die daaraan kunnen voldoen, kwam ik erachter dat het alleen met glasvezelverbindingen mogelijk is. Echter zijn glasvezelverbindingen erg duur. De opdrachtgever heeft aangegeven dat hij niet meer dan €2.500, - per maand aan de verbindingen wil uitgeven.

Ik heb op het Internet naar leveranciers gezocht en ik kwam uiteindelijk uit bij dataweb.nl. Dataweb.nl kan een 100MB/s glasvezelverbinding over VPN tussen beide vestigingen leveren. Deze verbinding kost €1500,- per maand en is snel genoeg voor de beheertaken en bestandsoverdracht tussen beide vestigingen.

Ook kan het bedrijf een kleinere back-up verbinding leveren. Deze verbinding is ook een glasvezelverbinding over VPN maar heeft een snelheid van 4 MB/s. en kost €500,- per maand. Deze back-up verbinding zal via een andere Internet provider lopen, om zo optimale veiligheid te kunnen bieden. Met deze verbindingen samen garandeert dataweb.nl een uptime van 99.98 procent.

Samen kosten deze verbindingen €2000,- per maand en dat is onder het maximum bedrag van €2500,- dat de opdrachtgever heeft vastgesteld. Ik ga de opdrachtgever adviseren om bovengenoemde verbindingen af te nemen van dataweb.nl .

Hiermee is een eind gekomen aan het adviesrapport. In totaal heb ik producten geadviseerd die samen €495.745,- kosten. De opdrachtgever heeft aangegeven dat hij maximaal €1.000.000,- wil uitgeven aan de hardware. Het is uiteindelijk gelukt om het voor minder dan de helft van dit bedrag te doen.

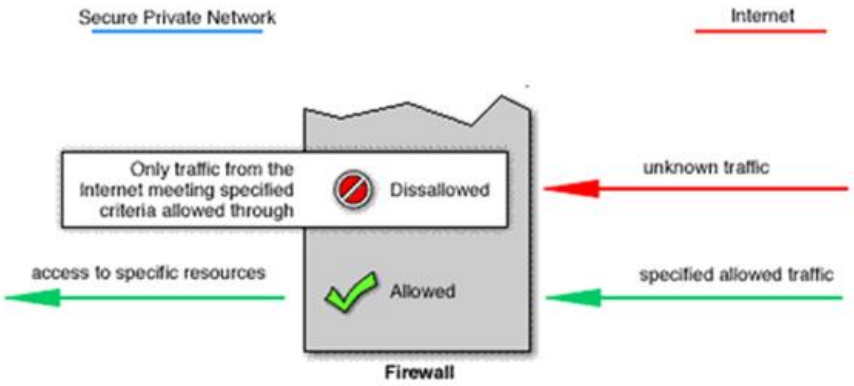
Advies over de beveiliging van het netwerk

Mocht er iemand in ons netwerk willen inbreken, dan kan hij waardevolle data meenemen of vernietigen. Nu wij precies weten welke hardware componenten wij precies gaan gebruiken, is het belangrijk om te weten hoe wij ons netwerk met deze componenten gaan beveiligen.

Allereerst moeten wij achterhalen wat ons zwakke punten in het netwerk zijn. Ons netwerk is op drie manieren toegankelijk voor hackers: van buitenaf door de primaire of de back-up verbinding, door het draadloze netwerk en van binnenuit (bijvoorbeeld medewerkers met slechte bedoelingen).

Beveiligen van de primaire en back-up verbinding

Zowel de primaire verbinding als de back-up verbinding moeten eerst langs de firewalls. De beveiliging zal derhalve door de firewall uitgevoerd moeten worden. In de firewall kan door middel van acceslist aangegeven worden welk verkeer wel of niet toegelaten mag worden tot het interne netwerk. Wanneer een hacker probeert binnen te dringen door middel van een bepaalde IP of poort waar geen goedkeuring voor is, dan zal dat door de firewall tegen gehouden worden. Hieronder staat grafisch uitgelegd hoe het proces in elkaar steekt.



Mijn advies aan de netwerkbeheerders is dan ook om de firewall door middel van accesslists te configureren. Hiermee kunnen ze zelf bepalen welk verkeer wel of niet tot het netwerk toegelaten mag worden. Op deze manier worden hackers buiten de deur gehouden zonder dat het normale verkeer belemmerd wordt.

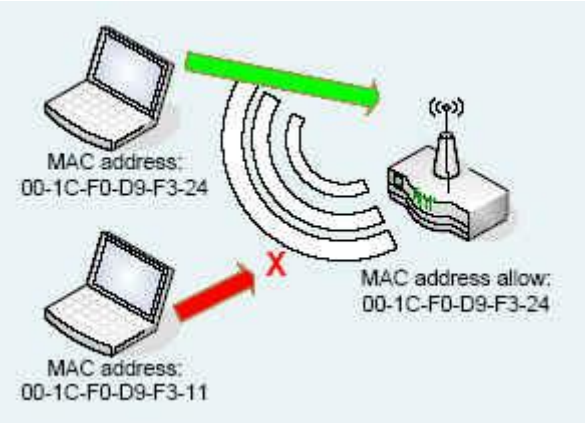
Beveiligen van het draadloze netwerk

Het draadloos netwerk vormt een groot risico omdat het niet vereist is om fysiek met het netwerk verbonden te zijn om in te kunnen breken. Dit kan ook simpelweg met een laptop buiten het gebouw gebeuren. Dit kunnen we voorkomen door het draadloos netwerk te beveiligen.

De beveiliging in ons draadloos netwerk zal door de wireless controller uitgevoed worden. Ons wireless controller kent vele vormen van beveiliging. De bekendste drie zijn WEP, WPA2 en MAC filtering.

Bij WEP is een verouderde versie van encryptie van toepassing, die relatief snel te kraken is. WPA2 is een nieuwere encryptie methode. Met WPA2 kunnen veel ingewikkeldere wachtwoorden gebruikt worden. Daarnaast worden deze wachtwoorden continue automatisch veranderd, zodat ze bijna onmogelijk te kraken zijn.

De derde methodiek is het gebruik van MAC filtering. Hiermee is het noodzaak dat de systeembeheerder alle MAC adressen van de draadloze apparatuur in de MAC filter van de wireless controller invoert. De wireless controller zal dan alleen draadloos apparatuur tot het netwerk toestaan die hij in zijn filter kent. Hiermee voorkom je dat hackers met hun laptop toegang krijgen tot het netwerk. Nog een voordeel dat je hiermee bereikt, is dat ook medewerkers hun privé laptop niet kunnen gebruiken op het netwerk. Hiermee houd je het netwerk veiliger (omdat eventuele virussen en spyware op hun privé laptop hierdoor niet in het netwerk terecht kunnen komen).

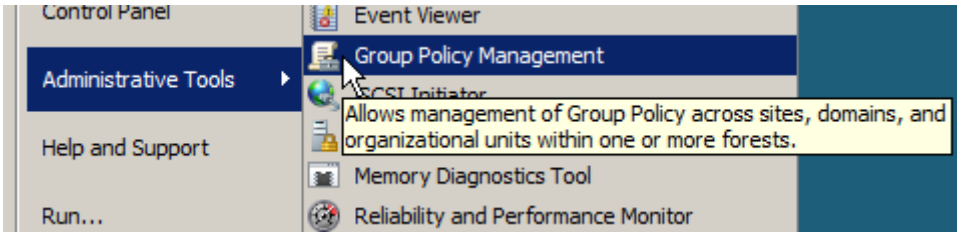


Ik raad de netwerkbeheerders aan om zowel gebruik te maken van WPA2 als MAC filtering. Op deze manier bescherm je het draadloos netwerk maximaal tegen hack-pogingen, afkomstig van zowel buiten als binnen het gebouw.

Beveiligen van het netwerk van binnenuit

Om te voorkomen dat medewerkers met kwade bedoelingen data proberen te stelen of te vernietigen, dient het netwerk ook voor intern verkeer goed beveiligen te worden. MAC filtering zal hier niet veel kunnen helpen, omdat gebruikers vanuit hun eigen werkstation kunnen hacken.

Wanneer iemand wil hacken, zal hij op de plekken willen hacken die waardevolle data bevatten. Vaak zijn dat de servers. Alle servers die gebruikt worden door Mina-IT zijn Windows servers. Standaard zouden alle normale gebruikers ook op de servers moeten kunnen inloggen. Om dit te voorkomen dien je in de Active Directory “Domain Controller Group Policy” te configureren. Hiermee voorkom je dat alle AD gebruikers op de servers kunnen inloggen. Je geeft dan alleen aan de beheerders de rechten om op de servers in te loggen.



Soms dien je een enduser gebruiker toegang te geven tot een server (bijvoorbeeld een programmeur die zijn script wilt testen op de applicatie server). Ook hier is het mogelijk om met de “Domain Group Policy” te voorkomen dat de gebruiker op andere servers gaat inloggen. Daarnaast zou je zijn rechten op de server kunnen beperken zodat hij bijvoorbeeld programma’s niet kan installeren of verwijderen. Hiermee geef je dus iedereen restricties op maat.

Hiermee kom ik aan het eind van het adviesrapport. Ik ben ervan overtuigd dat alle gegeven adviezen samen zullen zorgen voor een snelle, betrouwbare en een veilig netwerk voor Mina-IT.

Totale uitgave

Hiermee komen we aan het eind van de adviesrapport voor de hardware componenten, de verbindingen en de beveiliging van het netwerk. In de onderstaande tabel is de totale kosten weergegeven:

Component	Prijs per stuk	aantaal	Totale prijs
HP Compaq 6000 pro + monitor	€733	450	€329.850
DC-Networks DCFW-1800E-V2 Firewall	€4.490	2	€8.980
Cisco 2851 router	€4.199	2	€8.398
Linksys SPS2024 (enduser switch)	€449	23	€10.327
Cisco N5000 2RU (backbone switch)	€17.623	2	€35.246
Cisco N5000 1RU (backbone switch)	€9.425	2	€18.850
Netgear ReadyNAS 4200 19 Rackmount	€8.644	2	€17.289
Cisco 4400 Series WLAN Controller	€4.999	2	€9.998
HP ProCurve MSM323	€549	8	€4.392
HP ProLiant DL180 G6	€3.299	12	€39.588
HP StorageWorks MSL2024 1 Ultrium 960	€6.226	1	€6.226
APC Smart-UPS VT 10kVA 400V	€6.599	1	€6.599
Totale prijs			**€495.743**

In totaal heb ik producten geadviseerd die samen €495.743,- kosten (dit bedrag is exclusief de korting die Misco nog gaat geven). De opdrachtgever heeft aangegeven dat hij maximaal €1.000.000,- wil uitgeven aan de hardware. Het is uiteindelijk gelukt om het voor minder dan de helft van dit bedrag te doen.

Tot slot

Ik heb in dit adviesrapport bijna alle componenten beschreven die bij het bouwen van een dergelijk netwerk aan de orde komen. Alle gekozen componenten en services zijn pas gekozen na intensieve research. Ik ben ervan overtuigd dat alle gegeven adviezen samen zullen zorgen voor een snel, betrouwbaar en veilig netwerk voor Mina-IT.

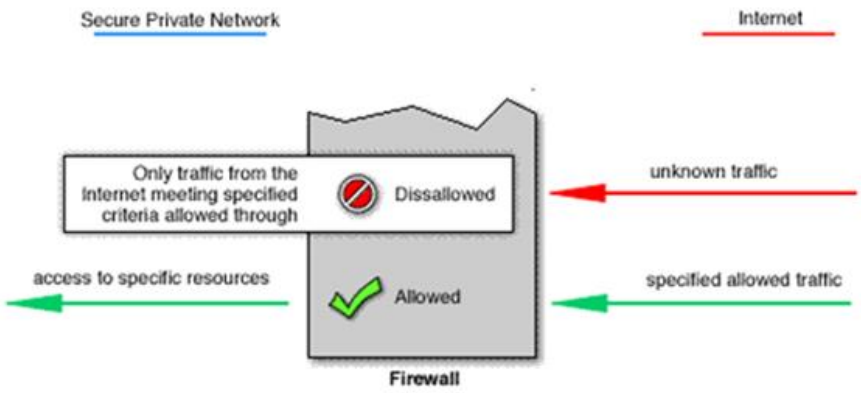
Advies over de beveiliging van ons netwerk

Mocht er iemand in ons netwerk willen inbreken dan kan hij waardevolle data meenemen of vernietigen. Nu wij precies weten welke hardware componenten wij precies gaan gebruiken is het belangrijk om te weten hoe wij ons netwerk met deze componenten gaan beveiligen.

Eerst moeten wij achterhalen wat ons zwakke punten in het netwerk zijn. Ons netwerk is op drie manier toegankelijk voor hackers. Namelijk : vanaf buitenaf door de primaire of de back-up verbinding, door het draadloze netwerk en van binnen uit (bijv. medewerkers met slechte bedoelingen).

Beveiligen van de primaire en back-up verbinding

Zowel de primaire verbinding als de back-up verbinding moeten eerst langs de firewalls. De beveiliging zal dus door de firewall uitgevoerd moeten worden. In de firewall kan door middel van acceslist aangegeven worden welke soort verkeer wel of niet toegelaten mag worden tot het interne netwerk. Wanneer een hacker probeert binnen te dringen door middel van een bepaalde IP of poort waar geen goedkeuring voor is dan zal dat door de firewall tegen gehouden worden. Hieronder staat grafische uitgelegd hoe het werkt:



Mijn advies aan de netwerk beheerders is dan ook om de firewall door middel van accesslists te configureren. Hiermee kunnen ze zelf bepalen welke verkeer wel of niet tot het netwerk toegelaten mag worden. Op deze manier kunnen ze hackers buiten houden zonder dat het normale verkeer belemmert wordt.

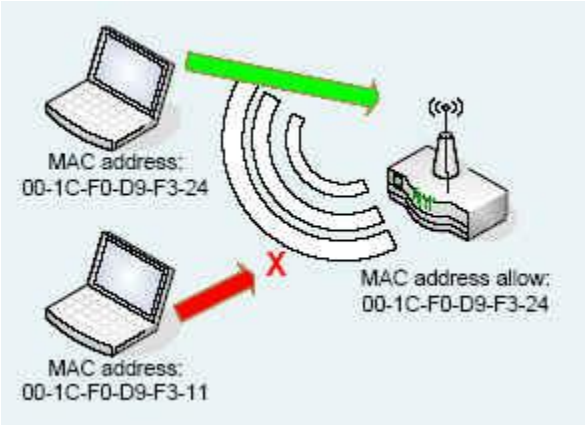
Beveiligen van het draadloze netwerk

Het draadloze netwerk vormt een grote risico omdat je niet fysiek met netwerk verbonden hoeft te zijn om in te kunnen breken. Dit kan ook gewoon simpelweg met een laptop buiten het gebouw gebeuren. Dit kunnen we voorkomen door het draadloze netwerk te beveiligen.

De beveiliging in ons draadloos netwerk zal door de wireless controller uitgevoed worden. Ons wireless controller kent vele vormen van beveiliging. De bekendste drie zijn : WEP , WPA2 en MAC filtering.

Bij WEP is een verouderde versie van encryptie en is relatief snel te kraken. WPA2 is een nieuwere encryptie methode. Met WPA2 kunnen veel ingewikkeldere wachtwoorden gebruikt worden. Ook worden deze wachtwoorden continue automatisch veranderd zodat ze bijna onmogelijk te kraken zijn.

De derde methodiek is het gebruik van MAC filtering. Hiermee moet je in de wireless controller alle MAC adressen van de draadloze apparatuur invoeren. De wireless controller zal dan alleen draadloos apparatuur tot het netwerk toestaan die hij in zijn filter kent. Hiermee voorkom je dat hackers met hun laptop toegang krijgen tot het netwerk. Nog een voordeel wat je hiermee bereikt is dat ook medewerkers hun privé laptop niet kunnen gebruiken op het netwerk. Hiermee hou je het netwerk veiliger (omdat eventuele virussen en spyware op hun privé laptop niet in het netwerk komt).

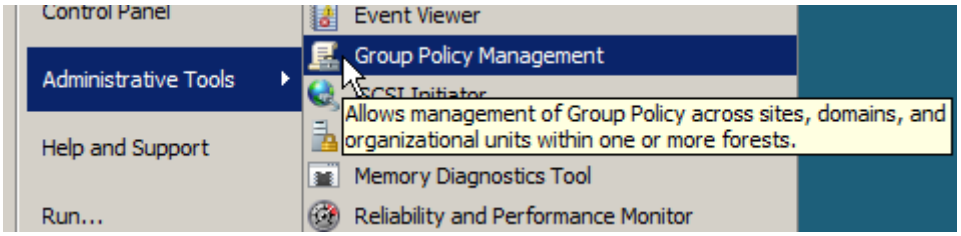


Ik raad de netwerk beheerders aan om zowel gebruik te maken van WPA2 als MAC filtering. Op deze manier bescherm je je draadloze netwerk maximaal tegen hack pogingen van zowel buiten als binnenuit het gebouw.

Beveiligen van het netwerk van binnenuit

Omdat te voorkomen dat medewerkers met kwade bedoelingen data proberen te stelen of te vernietigen dien je het netwerk ook voor intern verkeer goed te beveiligen. MAC filtering zal hier niet heel veel kunnen helpen omdat gebruikers vanuit hun eigen werkstation zouden kunnen proberen te hacken.

Wanneer iemand wil hacken dan zal hij op de plekken willen hacken die waardevolle data bevatten. Vaak zijn dat de servers. Alle servers die gebruikt worden door Mina-IT zullen allemaal Windows servers. Standaard zouden alle normale gebruikers ook op de servers kunnen inloggen. Om dit te voorkomen dien je in de Active Directory “Domain Controller Group Policy” te configureren. Hiermee voorkom je dat alle AD gebruikers op de servers kunnen inloggen. Je geeft dan alleen aan de beheerders die rechten om op de servers in te loggen.

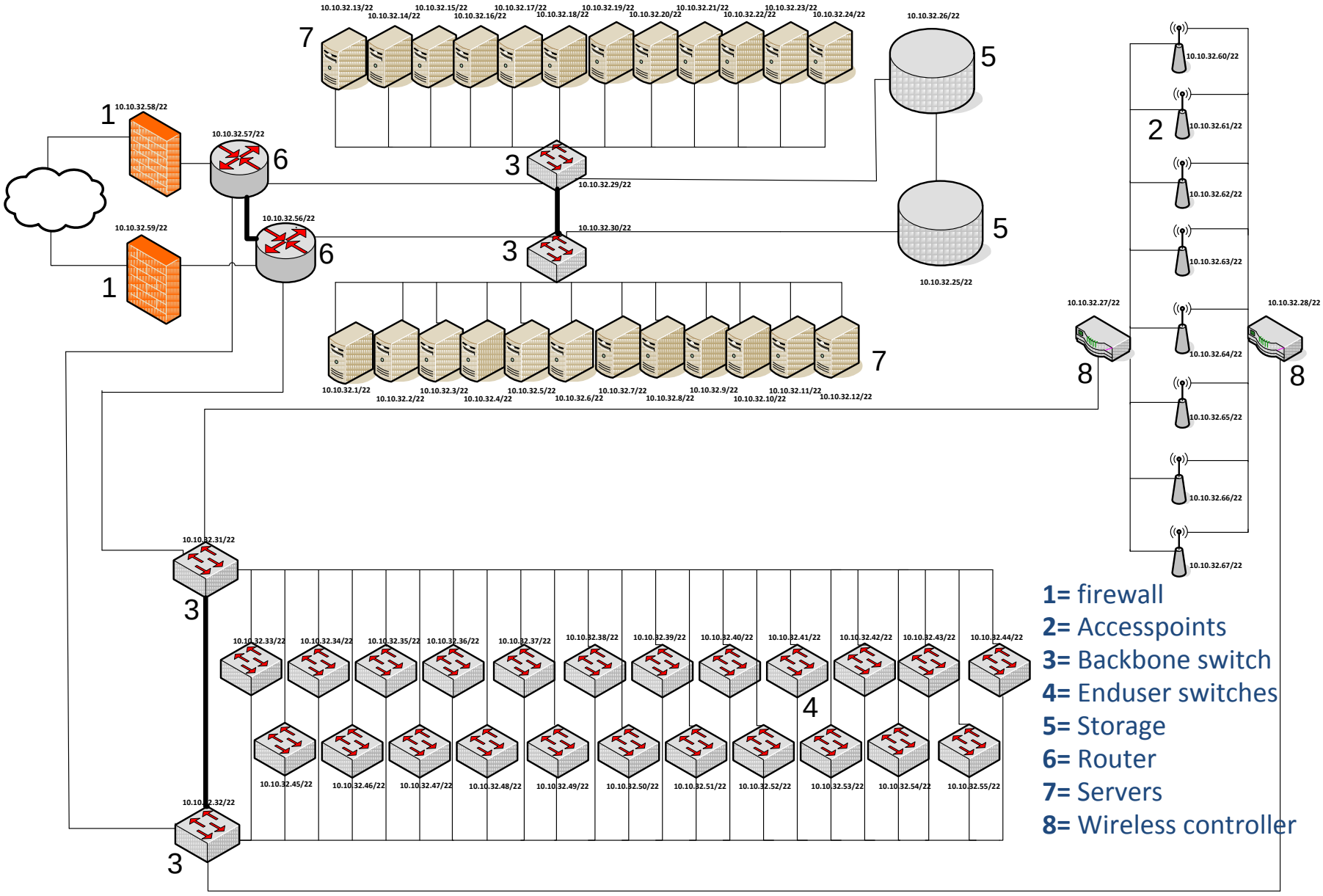


Soms dien je een enduser gebruiker toegang te geven to een server (bijv. een programmeur die zijn script wilt testen op de applicatie server). Ook hier kan je met de “Domain Group Policy” voorkomen dat hij op andere servers gaat inloggen. Ook zou je zijn rechten op de server kunnen beperken zodat hij bijv. programma’s niet kan installeren of verwijderen. Hiermee geef je dus iedereen restricties op maat.

Tot slot

Ik heb in dit adviesrapport bijna alle componenten beschreven die in bij het bouwen van een dergelijk netwerk aan te pas komen. Alle gekozen componenten en services zijn pas gekozen na intensieve research. Ik ben ervan overtuigt dat alle gegeven adviezen samen zullen zorgen voor een snelle , betrouwbare en een veilige netwerk voor Mina-IT.

Afstudeeropdracht:	**Mina-IT @ Groningen**
Document:	Architectuurrapport
Student:	Mina Nabil
Afstudeerbegeleider:	Cobie van der Hoek
Expert:	Nico Huiberts
Datum:	04-10-2010



1= firewall
2= Accesspoints
3= Backbone switch
4= Enduser switches
5= Storage
6= Router
7= Servers
8= Wireless controller

Netwerkontwerp Mina-IT aangepast