

Procesverslag



“Onderzoek voor verbetering van het netwerk binnen de BOAL Group”

23-04-2012 t/m 24-09-2012

Projectdetails:

De Haagse Hogeschool

Datum:	24 september 2012
Opdrachtgever:	Lex Erades
Begeleiders BOAL:	Lex Erades
Begeleidende docenten:	Rutger Spaans Madelon Nieuwland
Opleiding:	Technische Informatica

Uitvoerende Student:

Naam:	Henk van Tol
Studentnummer:	20051121

Referaat

Henk van Tol, Afstudeeropdracht, Onderzoek voor verbetering van het netwerk binnen de BOAL Group, BOAL Group te De Lier, 24 september 2012.

Dit verslag is geschreven voor het afstuderen van Henk van Tol, die onderzoek heeft gedaan voor het verbeteren van het netwerk binnen de BOAL Group. Het is geschreven in het kader van de opleiding Technische Informatica, aan de Haagse Hogeschool te Den Haag. De opdracht is uitgevoerd bij de BOAL Group te De Lier van 23 april 2012 tot en met 24 september 2012.

Descriptoren:

- Afstudeerverslag
- Procesverslag
- Risicoanalyse netwerk
- ASI methode
- Definitierapport
- Architectuurrapport
- Ontwerprapport
- Adviesrapport

Voorwoord

Dit verslag is geschreven in het kader van het afstuderen van Henk van Tol voor de opleiding Technische Informatica aan de Haagse Hogeschool te Den Haag. De afstudeeropdracht is uitgevoerd voor en bij de BOAL Group, waarbij ik de opdracht *“Onderzoek voor het verbeteren van het netwerk binnen de BOAL Group”* van 23 april 2012 tot en met 24 september 2012 heb uitgevoerd.

Het verslag is geschreven voor studenten in een ICT richting en voor mensen die werken in een zelfde richting. Enige voorkennis van netwerkapparatuur en protocollen is een pre. In dit verslag wordt de ASI methode gebruikt, om mijn opdracht tot een succes te voltooien.

Ik wil bij deze mijn dank uitspreken voor iedereen die mij geholpen heeft met de totstandkoming van de opgeleverde producten en procesverslag, maar in het bijzonder dank ik mijn begeleider en opdrachtgever Lex Erades. Hij heeft mij van de nodige informatie voorzien als opdrachtgever en als begeleider heeft hij mij tijdens de gehele duur van de opdracht van ondersteuning voorzien.

Ik dank ook de docenten van de Haagse Hogeschool, Rutger Spaans en Madelon Nieuwland, voor het advies wat zij gegeven hebben, met name het proces, tijdens het uitvoeren van de opdracht.

Inhoudsopgave

1. Inleiding	6
2. De Achtergrond	7
2.1 Extrusie.....	7
2.2 Het bedrijf	8
2.3 Bedrijfsstructuur.....	9
2.4 ICT-afdeling	11
3. Het prepareren van de opdracht	12
3.1 Initiële opdracht	12
3.2 Concrete opdrachtformulering	12
3.3 Afbakening.....	14
4. Het kiezen van een methode	15
4.1 Formuleren van criteria.....	15
4.2 Maken van een keuze	15
4.3 Beschrijven van de gekozen methode	16
5. Het opstellen van het plan van aanpak	17
5.1 Formuleren van activiteiten	17
5.2 Inventariseren van benodigde mensen en middelen	18
5.3 Opzetten van de initiële planning	18
5.4 Opzetten van het initiële risicolog.....	19
6. Fase 1: De definitiefase.....	20
6.1 Vaststellen eisen en wensen	20
6.2 In kaart brengen huidige technische infrastructuur	23
6.3 LAN netwerk onderzoeken	26
6.4 WAN netwerk onderzoeken.....	30
6.5 Remote Access onderzoeken	32
6.6 Opstellen van risicoanalyse.....	33
6.7 Opleveren van definitierapport	37
6.8 Planning bewaken	37
7. Fase 2: De architectuurfase.....	38
7.1 Maken van een globaal LAN ontwerp	38
7.2 Maken van een globaal WAN ontwerp	45
7.3 Voorstel voor remote access	50
7.4 Bespreken van de ontwerpen.....	52
7.5 Scherpstellen eisen en wensen.....	52
7.6 Opleveren van architectuurrapport.....	52
7.7 Planning bewaken	53

8. Fase 3: De ontwerpfase	54
8.1 Het LAN netwerk gedetailleerd uitwerken	54
8.2 Het WAN netwerk gedetailleerd uitwerken.....	61
8.3 Selectie van toe te passen producten	62
8.4 Opleveren ontwerprapport.....	64
8.5 Planning bewaken	64
9. Fase 4: De ontwikkelfase	65
9.1 Testplan opstellen	65
9.2 Advies implementatie ontwerpen	65
9.3 Opleveren adviesrapport	66
9.4 Planning bewaken	66
10. Evaluatie	67
10.1 Product Evaluatie	67
10.2 Proces Evaluatie.....	68
10.3 Competenties	70
10.4 Tot slot	71
Literatuurlijst.....	72
Bijlagen	72
Figuren.....	72
Tabellen	73

1. Inleiding

De BOAL Group is gespecialiseerd in extrusie van aluminium profielen en de verwerking, van deze profielen, in kasconstructies. Steeds meer productieprocessen worden automatisch aangestuurd, waarbij het netwerk een belangrijke rol speelt. De leveranciers van deze geautomatiseerde productieprocessen, eisen en eigen lokaal netwerk en externe toegang om support te kunnen leveren. Daardoor heeft het bedrijf steeds meer te maken met gebruikers, die extern toegang nodig hebben tot het interne netwerk.

Het proces wordt in dit verslag beschreven, naar mijn onderzoek over de verbetering van het netwerk van de BOAL Group. Uit dit onderzoek is een o.a. ontwerp- en adviesrapport gekomen hoe het netwerk verbeterd kan worden. Zo kan het netwerk gereed gemaakt worden voor de toekomst.

Dit document bestaat uit de volgende onderdelen:

- De achtergrond met het extrusie proces en het bedrijf
- De opdrachtformulering, keuze van methode en plan van aanpak
- Definitiefase, beschrijving van de huidige situatie en risicoanalyse
- Architectuurfase, globale ontwerpen
- Ontwerpfase, gedetailleerde uitwerking van het gekozen ontwerp
- Ontwikkelfase, advies, hoe het ontwerp te implementeren
- Evaluatie over product, proces en competenties

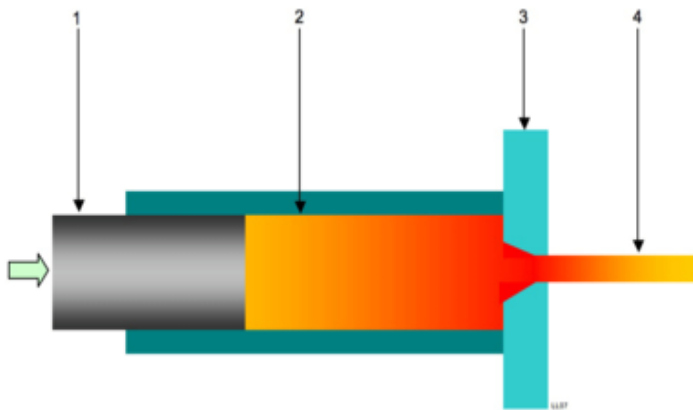
2. De Achtergrond

In dit hoofdstuk wordt beschreven wat extrusie is en wat voor een bedrijf de BOAL Group is.

2.1 Extrusie

Extrusie¹ is een materiaal op hoge druk, eventueel verwarmd, door een matrijs heen persen, zodat het materiaal smelt en de vorm van de matrijs aanneemt. De BOAL Group houdt zich bezig met het extruderen van aluminium profielen waar altijd verwarming voor nodig is.

Hieronder een beeld van het extrusie proces:



Figuur 1: Extrusie proces

1. Pers
2. Verhitte aluminium staaf
3. Matrijs
4. Aluminium profiel gevormd door matrijs

Het aluminium wordt in cilinder gevormde staven aangeleverd van zo'n 20 meter lang. Een externe partij levert het aluminium aan met een door BOAL bepaalde legering. De legering is zeer belangrijk in het extrusie proces, omdat het de sterkte van het profiel naderhand bepaald. Een staaf gaat de oven in om een temperatuur te krijgen van zo'n 450 graden en wordt daarna op gedeelte van zo'n 1 meter.



Figuur 2: Links: aluminium staven bij de oven; Rechts: een matrijs met de vorm van het profiel

Het aluminium wordt door de matrijs heen geperst en neemt de vorm van de matrijs aan, tegelijkertijd wordt het profiel eruit getrokken door een "Puller" om het profiel recht te houden. Door het samen persen van het materiaal komt er extra warmte vrij wat betekent dat het aluminium op zo'n 500 graden uit de pers komt. Het profiel wordt na 30 meter afgezaagd en op een gecontroleerde manier afgekoeld, zodat het zijn uiteindelijke vorm aanneemt.

¹ Bron: [Extrusie](#)



Figuur 3: Links: De “Puller”; Rechts: de profielen liggen klaar om te worden ingepakt

De profielen worden op maat gezaagd naar de wens van de klant, waarna ze de oven in gaan om de chemische reactie te versnellen, hierdoor krijgt het profiel zijn uiteindelijke sterkte. Nadat de profielen zijn afgekoeld gaan ze door naar de inpaktafels waar ze met de hand worden ingepakt. Vanaf dat moment worden de profielen naar de klant gestuurd. Tijdens mijn afstudeeropdracht is er een nieuwe inpaklijn geïnstalleerd bij BOAL Profielen, waardoor het inpakken van de profielen automatisch aangestuurd wordt.

2.2 Het bedrijf

De BOAL Group is een bedrijf met meerdere fabrieken, maar met één eigenaar Ronald Boers. Dit betekent dat het geen beursgenoteerd bedrijf is en volledig privé wordt gefinancierd. Op strategisch gebied kunnen er op lange termijn beslissingen genomen worden, omdat er geen verantwoording naar aandeelhouders afgelegd hoeft te worden. Het streven, van het management, is de afdelingen ervan bewust maken dat er geen overhaaste investeringen op korte termijn gedaan moeten worden, wat die lange termijn een desinvestering kunnen blijken.

BOAL Systemen is 40 jaar geleden begonnen met kasbouwconstructies en kwam erachter dat er een markt was voor extrusie van aluminium profielen en daardoor is BOAL Profielen opgericht in De Lier. Sindsdien hebben zij veel ervaring opgedaan in het extruderen van aluminium profielen. In de loop der jaren zijn er meer vestigingen geopend in België en het Verenigd Koninkrijk, die dezelfde werkzaamheden uitvoeren als BOAL Profielen. Inmiddels zijn er ongeveer 300 werknemers werkzaam bij de BOAL Group.

Er wordt een groei verwacht in de sector, omdat het dieptepunt van de crisis voorbij is en de BOAL Group over een flink aantal patenten beschikt op het gebied van aluminium profielen. Het bedrijf kan snel schakelen in het productie proces, zodat ze de klant snel kleine orders kunnen leveren. BOAL Systemen levert veel orders uit naar Zuid-Amerika en Azië waar de crisis minder erg is als in Europa en dit heeft tot gevolg dat het bedrijf op volle toeren kan werken.

De doelstelling van het bedrijf is om alles te automatiseren, indien technisch en financieel haalbaar, om sneller en accurater te produceren. Het netwerk speelt een belangrijke rol bij een geautomatiseerd productieproces, omdat het netwerk een transport medium is dat ervoor zorgt dat de PLC's², zonder vertraging, de informatie verkrijgen.

Momenteel zijn er 4 vestigingen:

- BOAL Profielen BV (BP) De Lier, Nederland
- BOAL Systemen BV (BS) 's-Gravenzande, Nederland
- BOAL Belgium NV (BB) Moorsele, België
- BOAL UK Ltd (BUK) Shepshed, Verenigd Koninkrijk

² Bron: [PLC](#)

BOAL Profielen (BP) De Lier, Nederland

De vestiging in De Lier beschikt over een extrusiepers van 1600 ton (7 inch) en een extrusiepers van 2200 ton (8 inch). BOAL Profielen is de meest ervaren extrusiesite van de BOAL Groep en onderscheidt zich door de kwaliteiten in profiel- en matrijsontwerp. De commerciële activiteiten van BOAL Profielen richten zich voornamelijk op de Nederlandse en Duitse markt.

BOAL Systemen (BS) 's-Gravenzande, Nederland

40 jaar geleden was BOAL Systemen de grondlegger van de aluminium kasconstructie. Sindsdien hebben de dek- en gevelsystemen van BOAL altijd bekend gestaan om hun sterkte, betrouwbaarheid en duurzaamheid. Met een jaarlijkse distributie van 250 hectare kasdek is BOAL Systemen marktleider in de aluminium kassystemen.

BOAL Belgium (BB) Moorsele, België

De vestiging in Moorsele beschikt over twee extrusiepersen van 1600 ton (beide 7 inch). Deze productielocatie onderscheidt zich door haar jarenlange ervaring in het produceren van hoogwaardige profielen met zeer strenge kwaliteitseisen. BOAL België heeft een inrolmachine waarmee zij profielen kunnen inrollen. Hierbij worden met een kunststof verbindingstuk twee profielen aan elkaar gekoppeld, net name voor thermisch onderbreken.

De commerciële activiteiten van BOAL België richten zich voornamelijk op de Belgische en Franse markt.

BOAL UK (BUK) Shepshed, Verenigd Koninkrijk

De vestiging in Shepshed beschikt over een extrusiepers van 1600 ton (7 inch) en een extrusiepers van 3250 ton (9 inch). Het extrusieproces van BOAL UK is uniek in de wereld (long aging) en bij uitstek geschikt voor het efficiënt produceren van grotere profielen in grotere volumes met korte doorlooptijden. Door de moderne processen en optimale logistiek kunnen wij dagelijks klanten zeer positief verrassen bij bedrijfsbezoeken in Shepshed.

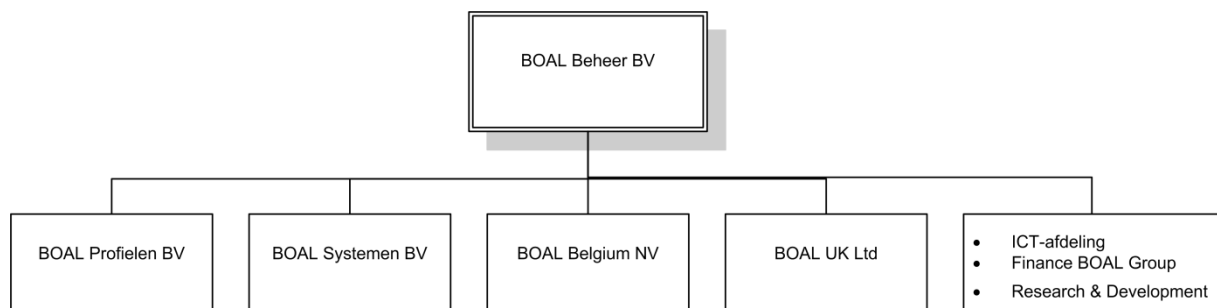
De commerciële activiteiten van BOAL UK richten zich vooral op de Engelse, Ierse, Schotse en Scandinavische markt. Ook wordt door BOAL UK veel in opdracht van BOAL Profielen geproduceerd (grotere profielen).

2.3 Bedrijfsstructuur

BOAL Beheer B.V. is de holding voor alle vestigingen (Figuur 4) en onder BOAL Beheer vallen de volgende afdelingen:

- ICT-afdeling
- Financiële afdeling gehele BOAL Group
- R&D, Research en Development

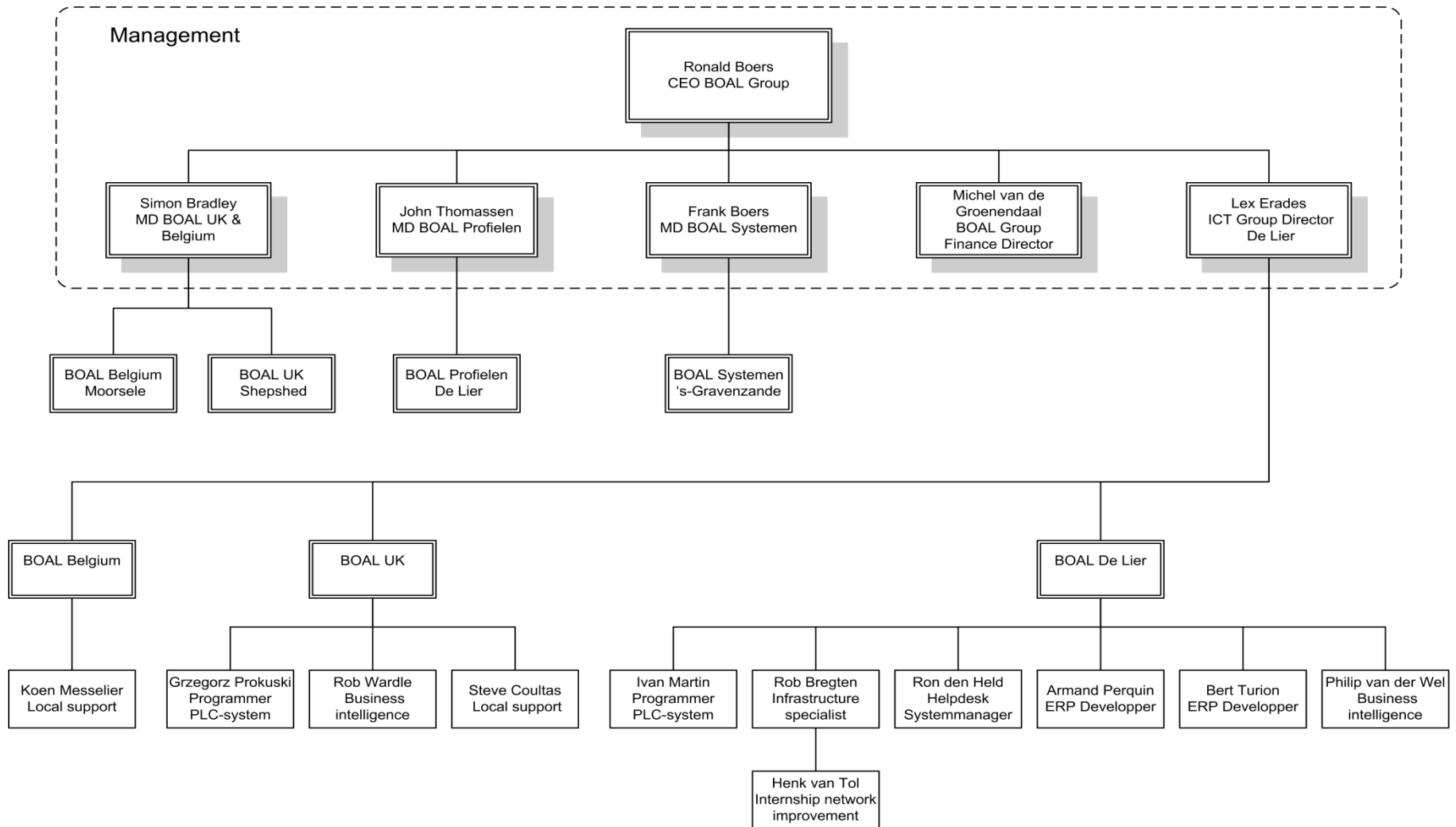
Deze afdelingen opereren voor de gehele BOAL Group en opereren vanuit De Lier. BOAL Beheer B.V. is eigenaar van alle ICT-producten per vestiging behalve de bekabeling.



Figuur 4: Bedrijfsstructuur

Op de volgende pagina (Figuur 5) staat het organigram van de BOAL Group met de ICT-afdeling gedetailleerd uitgewerkt.

BOAL Group organization



Figuur 5: Organigram BOAL Group

2.4 ICT-afdeling

De ICT-afdeling beheert alle clients, printers, servers, telefooncentrales en netwerkapparatuur voor alle vestigingen.

ICT Director

Lex Erades is de ICT Director van de BOAL Group, hij is verantwoordelijk voor de ICT-afdeling en zit in het strategisch management van het bedrijf. Hij is tot een hoog bedrag tekenbevoegd en dat maakt het makkelijk om snel beslissingen te nemen binnen de ICT-afdeling. Tevens is Lex mijn begeleider tijdens mijn afstudeeropdracht.

Beheer en Helpdesk

Rob Bregten is verantwoordelijk voor de gehele ICT-infrastructuur binnen de BOAL Group. Tevens is hij hoofd systeembeheerder en 2^e lijns helpdesk bij BOAL Beheer. Hij is al 12 jaar werkzaam bij de organisatie en kent de infrastructuur door en door. Tijdens mijn afstudeeropdracht zal ik veel met hem te maken hebben.

Ron den Held is een 1^e lijns helpdeskmedewerker en doet het alledaagse systeembeheer. Dit houdt in dat hij de backups controleert en alle accounts beheert. Tevens verzorgt hij nieuwe installaties op de werkstations en beheert hij ook de Microsoft Server³ en Citrix⁴ omgeving.

PLC programmeurs

Er werken twee PLC programmeurs bij de BOAL Group, Ivan Martin(BP) en Grzegorz Prokuski(BUK). Ivan Martin werkt al jaren aan de PLC's en heeft een zeer groot deel geprogrammeerd en tevens verantwoordelijk voor de industriële installaties van alle vestigingen. Bij hem zal ik de informatie over het industriële (PLC) netwerk kunnen verkrijgen.

³ Bron: [Microsoft Server](#)

⁴ Bron: [Citrix](#)

3. Het prepareren van de opdracht

In dit hoofdstuk beschrijf ik hoe ik vanuit de initiële opdrachtformulering tot een concrete opdracht met op te leveren producten ben gekomen. De voorbereiding dient als input voor de rest van dit document en is de basis van de uit te voeren opdracht.

3.1 Initiële opdracht

In de vacature van BOAL Group waar ik op gereageerd heb werden de volgende doelstellingen voor de opdracht omschreven:

- *Creëren van topologie tekeningen:*
 - *Netwerk infrastructuur*
 - *WAN netwerk*
 - *LAN netwerk*
- *Server infrastructuur*
 - *Fysieke infrastructuur*
 - *Logische infrastructuur (gevirtualiseerde omgeving)*
- *Applicatie topologie*

Bovenstaande is van toepassing voor een viertal productie locaties in drie landen (NL, BE & UK). BOAL heeft gekozen voor een sterk gecentraliseerde ICT infrastructuur en maakt gebruik van een Power7 (AS400) voor het ERP-systeem en een ESX servers infrastructuur in combinatie met VMware. De locatie in De Lier en een Tier 1 carrier Data Centre (Rotterdam) vormen de backbone van BOAL, locaties zijn via een MPLS netwerk aangesloten.

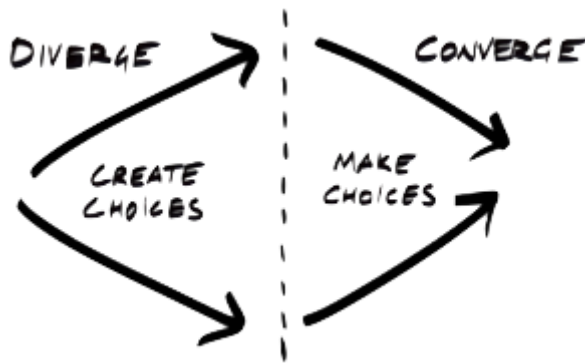
De stagiaire zal nauw samenwerken met een MBO (niveau 4) stagiaire die meer de praktische zaken van het bovenstaande voor zijn/haar rekening zal moeten nemen.

Na hierover te hebben gesproken met de opdrachtgever zijn wij gezamenlijk tot de conclusie gekomen dat de opdracht passend is bij mijn ambities en aansluit op mijn opleiding. Het werd hier ook direct duidelijk dat deze vacature voort is gekomen uit een groter probleem met het netwerk. Naar aanleiding hiervan ben ik bij BOAL Group aan de slag gegaan.

3.2 Concrete opdrachtformulering

De initiële opdracht en het eerste gesprek zijn een goed uitgangspunt om de voorbereidingen voor mijn opdracht op te baseren. Voor een concrete opdrachtformulering was het echter allereerst van belang, om tot een meer gedetailleerde beschrijving te komen van de probleemstelling en de achtergrond. Het scherpstellen van de opdrachtformulering heb ik aangepakt doormiddel van een brainstormsessie met de opdrachtgever en infrastructuur specialist. Hierbij heb ik ernaar gestreefd om onderstaande vragen beantwoord te krijgen. Ik heb de sessie opgedeeld in de onderwerpen probleemstelling (divergeren) en scherpstellen opdracht (convergeren). Hierbij is het thema van het BOAL Group netwerk centraal gebleven om niet te ver af te wijken van de oorspronkelijke vraag. Ik heb de volgende vragen behandeld tijdens de sessie:

- **Probleemstelling**
 - Waar zit de pijn op dit moment;
 - Wat is de oorzaak van het probleem.
- **Scherpstellen opdracht**
 - Hoe kunnen we het probleem concreet maken en vertalen in acties;
 - Welke van deze acties kan ik gedurende mijn stageperiode uitvoeren.



Figuur 6: Divergeren en convergeren⁵

Probleemstelling

Op basis van de antwoorden die ik heb verzameld tijdens de brainstormsessie heb ik een uitwerking gemaakt. Deze uitwerking heb ik allereerst voorgelegd aan mijn opdrachtgever alvorens verder te verwerken. De probleemstellingen heb ik geformuleerd in de volgende punten:

- **Er zijn momenteel geen netwerkdiagrammen aanwezig.** Dit betekent dat het moeilijk is om uit te zoeken waar het probleem zich bevindt, in geval van storingen op het netwerk. Tevens is het niet duidelijk wat de risico's en impact zijn, bij uitval van netwerkapparatuur. De beheersbaarheid is dus niet in orde. Er is een grote noodzaak aan een heldere topologie tekening, voor zowel het LAN als WAN netwerk.
- **LAN netwerk onderzoeken.** De BOAL Group gebruikt voor veel gebruikers Citrix technologie, die veel bandbreedte nodig heeft op het LAN netwerk. Op sommige momenten schiet de capaciteit tekort. Daarnaast is er toekomstige behoefte om videoconferentie en VoIP te introduceren. Dit betekent dat er onderzocht moet worden welke mogelijkheden er zijn om de snelheid van het LAN netwerk te verhogen. De leveranciers van de geautomatiseerde productieprocessen vereisen een eigen LAN netwerk, om verstoringen van het PLC verkeer te voorkomen. Er moet onderzocht worden wat de mogelijkheden hiervoor zijn.
- **Synchronisatie van het ERP systeem.** Er zijn recent nieuwe servers aangeschaft voor het ERP systeem. Deze servers gaan in de vestigingen BOAL Profielen en BOAL UK draaien i.p.v. het Data Centre in Rotterdam. Op deze manier kan het gebruik van het Data Centre opgeheven worden. Dit houdt in dat er onderzocht moet worden of het huidige netwerk (LAN en WAN) geschikt is, om de synchronisatie, voor disaster recovery, tussen de ERP servers te ondersteunen. Indien dit niet het geval is moet er een advies worden uitgebracht hoe deze situatie behandeld dient te worden.
- **WAN netwerk onderzoeken.** Alle vestigingen van de BOAL Group zijn met elkaar verbonden d.m.v. een MPLS netwerk. Op dit moment gaat al het Internet verkeer, via dit netwerk, naar het Data Centre in Rotterdam en vanaf daar het Internet op. Deze lijnen zijn kostbaar en 'traag' volgens de opdrachtgever. Al het verkeer van de BOAL Group vestigingen in Nederland, België en de UK gaat via dit netwerk. Ook het verkeer waarvoor het minder logisch is (lokaal internetverkeer) en onwenselijk omdat het veel bandbreedte kost die nuttiger ingezet kan worden. Bovendien is er geen inzicht in de het type verkeer dat de lijn traag maakt en de afkomst daarvan. Er dient hier een advies uitgebracht te worden welke stappen er kunnen worden ondernomen om dit probleem te verlichten en hoe er inzicht verkregen kan worden in het type verkeer dat over de lijnen gaat.

⁵ Bron: <http://blog.bartlensink.nl/projects/prospectie>

Opdrachtformulering en doelstellingen

Met behulp van de uitwerking van de probleemstelling, heb ik de opdracht in de volgende punten uitgewerkt:

- Gezien het niet beschikbaar zijn van de MBO stagiaire zal ik het complete LAN en WAN netwerk in kaart brengen en uitwerken in een topologie tekening. Deze tekening presenteer ik tussentijds aan mijn opdrachtgever en stel ik samen aan de hand van de fysieke hardware in de server ruimtes en dataruimtes. Tevens zal ik uitzoeken wat de beperkingen van het huidige LAN netwerk zijn. Dit is een te complex aangelegenheid voor een MBO student, omdat diegene niet over voldoende netwerkkennis beschikt, op het gebied van switching en routing.
- Risico's van de opzet van het huidige LAN netwerk van BOAL Profielen in De Lier in kaart brengen. Hierbij focus ik me op de risico's op uitval en de impact die dit kan hebben, op de bedrijfsvoering van BOAL Group.
- Onderzoeken in hoeverre de bestaande netwerkverbindingen en capaciteit hebben, om aan de eisen te kunnen voldoen. Om dit inzichtelijk te maken monitor ik het verkeer op het LAN en WAN netwerk, die de verschillende toepassingen, zoals het ERP systeem, genereren.
- Onderzoeken naar de mogelijkheden voor het scheiden van het LAN netwerk om de geautomatiseerde productieprocessen niet te verstoren, zoals het scheiden van het kantoor- en productieverkeer, waar de laatste zeer gevoelig kan zijn voor latency⁶.
- Verwerken van bovenstaande punten in een advies voor een nieuwe topologie. De wensen en eisen, die op de wijzigingen van toepassing zijn, bespreek ik tussentijds met mijn opdrachtgever en formuleer ik op basis van beschikbaar budget wat ik met mijn opdrachtgever zal overleggen.

3.3 Afbakening

De opdracht moet worden afgebakend, zodat de opdracht binnen de gestelde tijd, van de stageperiode, afgerond kan worden. In overleg met mijn opdrachtgever ben ik tot de volgende afbakening gekomen die buiten de scope van de opdracht vallen:

- Er wordt geen implementatie uitgevoerd van het ontwerp
- De ontwerpen worden niet getest, omdat daar apparatuur voor aangeschaft moet worden. De opdrachtgever geeft mij geen toestemming tot het aanschaffen van de benodigde apparatuur.
- Mijn onderzoek rondom het LAN netwerk zal zich beperken tot de vestiging van BOAL Profielen te De Lier. Al mijn bevindingen rondom het LAN netwerk die in dit document terugkomen zijn daar dan ook op gericht, maar zal tevens gebruikbaar zijn als uitgangspunt voor de andere vestigingen
- Er wordt geen risicoanalyse uitgevoerd op het WAN netwerk

⁶ Bron: [Latency](#)

4. Het kiezen van een methode

Nu de opdracht duidelijk is zal ik een keuze maken welke aanpak ik ga volgen om het traject in goede banen te leiden, waarbij ik mijn opdracht als een project zal uitvoeren. Ik kies ervoor om een projectmethodiek in te zetten om gestructureerd te kunnen werken en de planning met behulp van mijlpalen inzichtelijk te krijgen. In dit hoofdstuk beschrijf ik de criteria die ik heb gehanteerd bij de keuze voor een projectmethodiek en beschrijf ik de methodieken waaruit ik een keuze heb gemaakt. Ik sluit af door te beschrijven hoe ik mijn opdracht structureer aan de hand van de gekozen methodiek.

4.1 Formuleren van criteria

Voor het kiezen van een projectmethode heb ik een aantal criteria opgesteld aan de hand waarvan ik een selectie zal maken uit de beschikbare opties. In onderstaande punten heb ik beschreven waar de projectmethode, die ik kan gebruiken voor mijn opdracht, aan moet voldoen:

- **Technische infrastructuur.** De projectmethode moet specifiek geschikt zijn voor het ontwerpen van een technische infrastructuur. Het product van de opdracht is een ontwerp en advies opleveren voor verbetering van het netwerk. De methodiek moet hierin ondersteunend zijn door fasering te bieden, zodat ik gestructureerd naar een einddoel kan toewerken. Aangezien mijn opdracht het opstellen van een ontwerp is, vallen alle ontwikkelmethodes bij voorbaat af, omdat deze bij software ontwikkeling toegepast worden.
- **Een klein project.** De methode moet geen overhead creëren op het gebied van projectmanagement. De producten worden alleen door mij, als de uitvoerende, opgesteld en opgeleverd. Daardoor zijn meerdere rollen overbodig.
- **Duidelijke fasering.** De projectmethode moet een duidelijke fasering hebben met mijlpalen, die de fasen afsluit. De opdracht heeft een vaste einddatum wat betekent dat er een planning gemaakt kan worden met de einddatum als eindpunt van de opdracht. Deze planning zal rondom de fasering worden opgesteld.
- **Flexibel toepasbaar.** Door precies de stappen te volgen van een ontwerpmethode, is het niet reëel te denken dat er vanzelf een goed ontwerp uit de koker komt rollen. Het moet mogelijk zijn om zelf de keuze te hebben om bepaalde stappen uit te voeren binnen een fase zonder hiermee de complete projectmethodiek overboord te gooien.
- **Beschikbare informatie.** Er moet genoeg informatie en/of documentatie over de methodiek beschikbaar zijn, zodat ik de methodiek eenvoudig en zelfstandig kan toepassen.

4.2 Maken van een keuze

Op basis van de beschreven criteria heb ik een selectie gemaakt uit enkele methoden die toepasbaar zijn. Ik heb hierbij gekozen voor de twee methodes (ASI en PRINCE2), waar ik op school mee gewerkt heb en twee methodes (InFraMe en PMW) die ik niet eerder heb gevolgd. Deze heb ik met behulp van Wikipedia en Google gevonden. Hierbij heb ik voor twee methodetypes gekozen:

- **Ontwerpmethodes.** Dit type methode ondersteunt en beschrijft het proces dat concreet gevolgd dient te worden om als specifiek eindproduct tot een ontwerp te komen. Ik heb de volgende ontwerpmethodes geselecteerd:
 - **ASI.** De ASI methode is uitermate geschikt voor het ontwerpen van een technische infrastructuur en kan in grote en kleine projecten toegepast worden. Het gaat uit van een gefaseerde aanpak met 4 fasen. Een fase kan pas beginnen als de voorgaande fase is afgerond. Tevens is het ASI-rapport flexibel in het toepassen van de verschillende stappen per fase. Van de ASI-methode is niet heel veel te vinden, behalve het ASI-rapport dat zeer duidelijk alle fasen beschrijft.
 - **InFraMe.** Deze methode is ontwikkeld door Sogeti en is geschikt voor het ontwerpen van een technische infrastructuur. Het is minder geschikt voor het onderzoeken van de huidige situatie. Er wordt gewerkt vanuit 4 fasen, maar er is weinig informatie beschikbaar over deze methode waardoor ik niet kon vinden of het flexibel toepasbaar is.

- **Projectmanagementmethodes.** Dit type methode is meer algemeen en beschrijft de algemene structuur aan de hand waarvan een project vormgegeven dient te worden. Het eindproduct hoeft geen ontwerp te zijn. Deze methodes kunnen ingezet worden voor een breed scala aan projecten. Ik heb de volgende projectmanagementmethodes geselecteerd:
 - **Prince2.** Deze methodiek is bedoeld voor allerlei soorten projecten en niet alleen gespitst op ICT. Het wordt voornamelijk voor grote projecten gebruikt en er wordt vanuit verschillende rollen gewerkt, waar veel documentatie mee gemoeid is. Het is uitgebreid gedocumenteerd, op het Internet en in boeken, vanuit 6 fasen om allemaal te doorlopen te worden. Het is flexibel toepasbaar, omdat het een methode is die geschikt is voor allerlei projecten.
 - **PMW.** PMW staat voor ProjectMatig Werken en is net als PRINCE2 voor allerlei types projecten, niet alleen op het gebied van ICT. PMW kan voor grote en kleine projecten worden toegepast. Het is in 5 fasen opgedeeld waarover niet heel veel informatie te vinden is op het Internet. In boeken is er veel meer te vinden over PMW. Het is flexibel toepasbaar, omdat het een methode is die geschikt is voor allerlei projecten.

Bovenstaande methodieken heb ik gescoord op basis van de eerder genoemde criteria. Hierbij hanteer ik de scores **1 matig**, **2 voldoende** en **3 goed**. De totaalscore tel ik bij elkaar op.

Methode	Huidige situatie	Technische infrastructuur	Klein project	Duidelijke fasering	Flexibel toepasbaar	Beschikbare Informatie	Totaal
ASI	3	3	3	3	2	2	16
InFraMe	1	3	3	2	2	1	12
PRINCE2	3	1	1	3	1	3	12
PMW	2	1	3	3	1	2	12

Tabel 1: Methodieken scoren

Uit bovenstaande tabel blijkt dat de ASI methode het meest geschikt is voor de opdracht, om een ontwerp te maken voor het netwerk van de BOAL Group. Ik zal deze methode toepassen tijdens mijn opdracht.

4.3 Beschrijven van de gekozen methode

De ASI methode voorziet in de volgende vier fasen:

- **Definitiefase.** In de definitiefase wordt alle informatie verzameld over de huidige situatie. Vervolgens worden de eisen en wensen geïnventariseerd die op de gewenste situatie van toepassing zijn en worden er oplossingsrichtingen geformuleerd om tot de gewenste situatie te komen. Dit resulteert in een globaal plan van aanpak voor het vervolg.
- **Architectuurfase.** In de architectuurfase wordt een globale opzet van de uiteindelijke technische infrastructuur (gewenste situatie) uitgewerkt. Hiervoor worden enkele alternatieven uitgewerkt en voorzien van een invoeringsscenario en overzicht van kosten. Aan de hand van het eisenpakket dat in de definitiefase is geformuleerd wordt een keuze gemaakt voor één van de alternatieven.
- **Ontwerpfase.** In de ontwerpfase wordt een gedetailleerde uitwerking van technische infrastructuur gemaakt. Alle componenten van de architectuur worden voorzien van logische, fysieke en organisatorische specificaties.
- **Ontwikkelfase.** In de ontwikkelfase wordt een gedetailleerde voorbereiding op de technische en organisatorische invoering uitwerkt. Aan het eind van deze fase is het ontwerp een beproefd en te realiseren product.

5. Het opstellen van het plan van aanpak

De ASI methodiek biedt een goed raamwerk voor het uitvoeren van mijn opdracht. Om ten volle te kunnen profiteren van de methodiek zal ik in dit hoofdstuk concreet maken hoe ik de ASI fasen concreet aan mijn opdracht koppel en welke activiteiten ik per fase uitvoer. Daarbij zal ik de initiële planning, benodigde mensen en middelen en het initiële risicolog uitwerken.

5.1 Formuleren van activiteiten

De volgende activiteiten voer ik uit gedurende de respectievelijke ASI fasen:

Definitiefase

In de Definitiefase voer ik de volgende activiteiten uit:

- Het vaststellen van eisen en wensen
- Het in kaart brengen van de huidige technische infrastructuur
- LAN netwerk onderzoeken
- WAN netwerk onderzoeken
- Remote Access onderzoeken
- Opstellen van risicoanalyse
- Het opleveren van een definitierapport.
- Planning bewaken.

Architectuurfase

In de Architectuurfase voer ik de volgende activiteiten uit:

- Het maken van een globaal ontwerp maken voor het netwerk (LAN & WAN) aan de hand van de eisen en wensen.
- Het in kaart brengen van een alternatief scenario.
- Het bespreken van de ontwerpen met de opdrachtgever en het selecteren van een definitief ontwerp.
- Het scherpstellen van de eisen en wensen met mijn opdrachtgever.
- Het opleveren van een architectuurrapport met de uitwerking van bovenstaande punten.

Ontwerpfase

In de Ontwerpfase voer ik de volgende activiteiten uit:

- Het gedetailleerd uitwerken van het definitieve LAN ontwerp.
- Het gedetailleerd uitwerken van het definitieve WAN ontwerp.
- Selectie van toe te passen producten.
- Het opleveren van een ontwerprapport met de uitwerking van bovenstaande punten.

Ontwikkelfase

In de Ontwikkelfase voer ik de volgende activiteiten uit:

- Testplan opstellen voor het LAN en WAN netwerk
- Het uitwerken van een concreet voorstel voor de implementatie van het LAN netwerk ontwerp
- Het uitwerken van een concreet voorstel voor de implementatie van het WAN netwerk ontwerp
- Het opleveren van een adviesrapport met de uitwerking van bovenstaande punten

5.2 Inventariseren van benodigde mensen en middelen

De volgende mensen en middelen heb ik nodig voor mijn opdracht:

Benodigde mensen

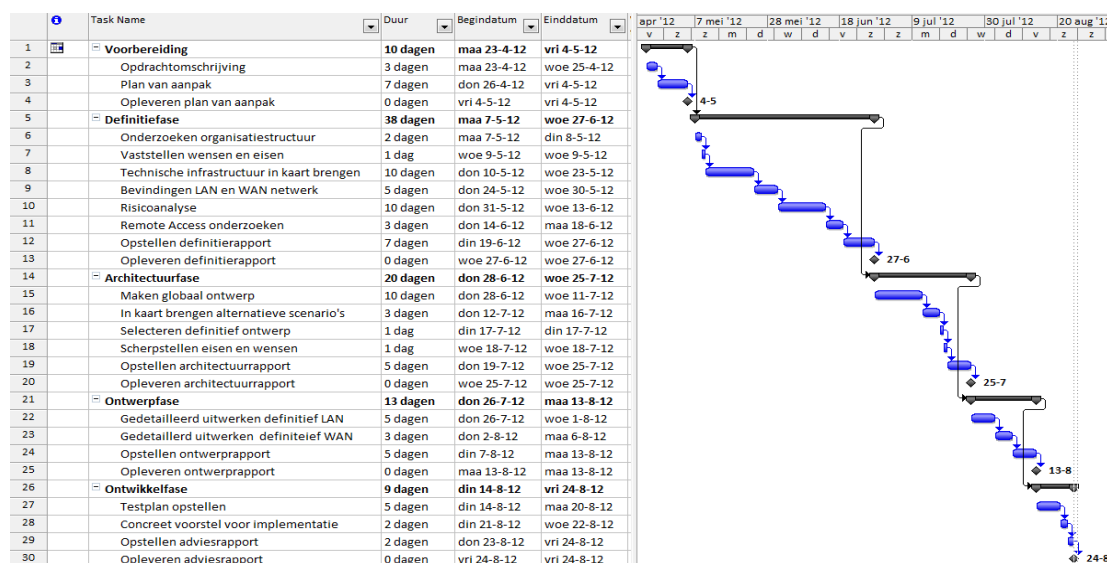
- ICT Director BOAL Group, opdrachtgever en begeleider.
- Infrastructuur specialist BOAL Group en 2e begeleider
- PLC Programmeur voor het Industriële netwerk
- Begeleidende docenten Haagse Hogeschool.

Benodigde middelen

- Werkplek met toegang tot het BOAL Group netwerk.
- Microsoft Word, Excel, Powerpoint en Visio.
- Toegang tot alle dataruimtes en netwerkapparatuur.
- Eventuele gesprekken met externe partijen.

5.3 Opzetten van de initiële planning

De initiële planning heb ik uitgewerkt in Microsoft Project. Dit geeft een goed beeld van de mijlpalen en afhankelijkheden. Bij afwijkingen op de planning kan ik dit eenvoudig verwerken in Project, en worden de implicaties van de afwijkingen direct inzichtelijk. De einddatum is 31 augustus en de planning loopt t/m 24 augustus. Ik houd dus 5 dagen speling in mijn planning



Figuur 7: Initiële planning

5.4 Opzetten van het initiële risicolog

Op basis van de informatie die ik beschikbaar had bij de start van mijn opdracht heb ik een aantal risico's geformuleerd. Deze risico's heb ik ingedeeld aan de hand van een de kans dat het risico zich voordoet, de impact die het risico heeft op mijn opdracht en daarmee de prioriteit die het risico krijgt. Mocht een risico zich voordoen, dan moet ik actie ondernemen met de bijkomende maatregelen

Ik heb de volgende risico's vastgesteld voor mijn opdracht:

Risico:	1. De benodigde mensen en middelen schieten te kort.
Kans:	Klein
Impact:	Gemiddeld
Maatregel:	Eerst zal de afstudeer in gesprek gaan met de begeleiders vanuit de BOAL Group en anders zal er een beroep worden gedaan op de begeleid(ende) docent(en), om tot een oplossing te komen.

Risico:	2. Langdurige ziekte/uitval van afstudeerder
Kans:	Klein
Impact:	Groot
Maatregel:	Er zal een beroep worden gedaan op de begeleid(ende) docent(en), om tot een oplossing te komen.

Risico:	3. Uitloop op de planning
Kans:	Gemiddeld
Impact:	Gemiddeld
Maatregel:	Bij het opstellen van de planning zal er een zo nauwkeurig mogelijke schatting worden gemaakt van de benodigde tijd per deelproduct. Hierbij zal er rekening gehouden worden met eventuele uitloop van activiteiten. Tevens kan er gekozen om een bepaalde activiteit te laten vervallen.

Risico:	4. Onvoldoende informatie
Kans:	Klein
Impact:	Gemiddeld
Maatregel:	De afstudeerder moet extra informatie vergaren bij de begeleiders vanuit de BOAL Group.

Risico:	5. Onvoldoende kennis
Kans:	Gemiddeld
Impact:	Klein
Maatregel:	Er moet documentatie worden geraadpleegd of externe partijen worden ingeschakeld.

6. Fase 1: De definitiefase

In de definitiefase wordt alle informatie verzameld over de huidige situatie. Vervolgens worden de eisen en wensen geïnventariseerd die op de gewenste situatie van toepassing zijn en worden er oplossingsrichtingen geformuleerd om tot de gewenste situatie te komen. Dit resulteert in een globaal plan van aanpak voor het vervolg. Ik heb een aantal concrete activiteiten aan de definitiefase gekoppeld. Deze activiteiten zal ik in dit hoofdstuk beschrijven.

De activiteiten die ik zal uitwerken zijn als volgt:

- Het vaststellen van eisen en wensen
- Het in kaart brengen van de huidige technische infrastructuur
- LAN netwerk onderzoeken
- WAN netwerk onderzoeken
- Remote Access onderzoeken
- Opstellen van risicoanalyse
- Het opleveren van een definitierapport.
- Planning bewaken.

6.1 Vaststellen eisen en wensen

Om de eisen en wensen vast te kunnen stellen heb ik een wederom een brainstormsessie georganiseerd met mijn opdrachtgever en de hoofd systeembeheerder om de probleemstelling die ik eerder heb geformuleerd uit te diepen. De probleemstellingen leverden enkele overlappende wensen en eisen op. Gesorteerd per bovenliggende probleemstelling heeft de sessie de volgende punten opgeleverd:

Probleemstelling

- Er zijn momenteel geen netwerkdiagrammen aanwezig. Dit betekent dat het moeilijk is om uit te zoeken waar het probleem zich bevindt, in geval van storingen op het netwerk. Tevens is het niet duidelijk wat de risico's en impact zijn, bij uitval van netwerkkapparatuur. De beheersbaarheid is dus niet in orde. Er is een grote noodzaak aan een heldere topologie tekening, voor zowel het LAN als WAN netwerk.

Wensen en eisen

- Het huidige LAN en WAN netwerk in kaart brengen.
- De risico's van het huidige LAN netwerk in kaart brengen.

Probleemstelling

- De BOAL Group gebruikt Citrix technologie die constante bandbreedte nodig heeft op het LAN netwerk. Op sommige momenten schiet de capaciteit van het huidige LAN en WAN netwerk te kort. Daarnaast is er toekomstige behoefte om videoconferentie en VoIP mogelijk te maken. Dit betekent dat er onderzocht moet worden welke mogelijkheden er zijn om de capaciteit van het LAN en WAN netwerk te verhogen.

Wensen en eisen

- Hogere beschikbaarheid garanderen d.m.v. impact verlaging.
- Het LAN en WAN netwerk geschikt maken voor videoconferentie en VoIP.
- LAN netwerk logisch scheiden.

Probleemstelling

- **Synchronisatie van het ERP systeem.** Er zijn recent nieuwe servers aangeschaft voor het ERP systeem. Deze servers gaan in de vestigingen BOAL Profielen en BOAL UK draaien i.p.v. het Data Centre in Rotterdam. Op deze manier kan het gebruik van het Data Centre opgeheven worden. Dit houdt in dat er onderzocht moet worden of het huidige netwerk (LAN en WAN) geschikt is, om de synchronisatie, voor disaster recovery, tussen de ERP servers te ondersteunen. Indien dit niet het geval is moet er een advies worden uitgebracht hoe deze situatie behandeld dient te worden.

Wensen en eisen

- Hogere beschikbaarheid garanderen d.m.v. impact verlaging.
- LAN netwerk scheiden.
- Het WAN netwerk moet snel genoeg zijn voor het ERP systeem.

Probleemstelling

- Alle vestigingen van de BOAL Group zijn met elkaar verbonden d.m.v. een MPLS netwerk. Op dit moment gaat al het verkeer via dit netwerk naar het Data Centre in Rotterdam en vanaf daar het Internet op. Deze lijnen zijn kostbaar en ‘traag’ volgens de opdrachtgever. Al het verkeer van de BOAL Group vestigingen in Nederland, België en de UK gaat via dit netwerk. Ook het verkeer waarvoor het minder logisch is (lokaal internetverkeer) en onwenselijk omdat het veel bandbreedte kost die nuttiger ingezet kan worden. Bovendien is er geen inzicht in de het type verkeer dat de lijn traag maakt en de afkomst daarvan. Er dient hier een advies uitgebracht te worden welke stappen er kunnen worden ondernomen om dit probleem te verlichten en hoe er inzicht verkregen kan worden in het type verkeer dat over de lijnen gaat.

Wensen en eisen

- LAN netwerk scheiden.
- Lokaal internetverkeer direct bij een vestiging het internet op.

Probleemstelling

- De leveranciers van de geautomatiseerde productieprocessen eisen een eigen LAN-netwerk, om verstoringen van het PLC verkeer te voorkomen. Er moet onderzocht worden wat de mogelijkheden hiervoor zijn.

Wensen en eisen

- LAN netwerk scheiden.

Naar aanleiding van het doornemen van de probleemstellingen zijn er enkele nieuwe wensen en eisen naar boven gekomen, die van belang zijn voor de BOAL Group. Deze zijn als volgt:

Wensen en eisen

- Remote Access onderzoeken.
- Het netwerk geschikt maken voor wireless.
- Geen desinvestering.
- Beheer eenvoudig houden.

Uitwerken eisen en wensen

Aan de hand van de brainstormsessie heb ik de probleemstellingen kunnen vertalen naar concrete eisen en wensen, welke ik hieronder verder uit zal werken.

- **Het huidige LAN en WAN netwerk in kaart brengen.** Het in kaart brengen van het huidige LAN en WAN netwerk zal ik als onderdeel van de definitiefase afronden. Het overzicht stelt mij in staat de risico's van de huidige situatie te bepalen en de inzetbaarheid van de huidige apparatuur te beoordelen. Zonder het beschrijven van de huidige situatie kan ik niet meetbaar maken voor mijn opdrachtgever welk effect een eventuele nieuwe situatie zal hebben.
- **De risico's van het huidige LAN netwerk in kaart brengen.** Het is niet duidelijk waar de risico's binnen het huidige netwerk liggen. Hierbij zijn vooral de beveiligingsrisico's en het risico op verstoring van het netwerk door incorrect gebruik (en het niet reguleren daarvan) van belang. Zo is het voorgekomen dat een medewerker een eigen router op het netwerk aansloot, die doormiddel van de DHCP server in het apparaat het netwerk verstoort. Ik zal de beveiliging onderzoeken en hier rekening mee houden in de nieuwe ontwerpen. Tevens zal ik een risicoanalyse maken op uitval van netwerkapparatuur.
- **Hogere beschikbaarheid garanderen.** De eis voor hogere beschikbaarheid komt voort uit de behoefte aan een betrouwbaar LAN netwerk. Door een risicoanalyse toe te passen op de ontwerpen, zal ik in staat zijn om de verhoging van de beschikbaarheid meetbaar te maken.
- **Het netwerk geschikt maken voor videoconferentie en VoIP.** Het netwerk moet voldoende capaciteit hebben om deze diensten te ondersteunen. Daarbij mag het (eventueel intensieve) gebruik hiervan, geen negatieve impact hebben op de overige diensten, zoals het verkeer van het ERP systeem, PLC's en Citrix. Aan de hand van de aanwezige apparatuur en infrastructuur zal ik bepalen of het huidige netwerk hier geschikt voor is.
- **LAN netwerk scheiden.** Het LAN netwerk dient gescheiden te worden om de snelheid, veiligheid en beschikbaarheid sterk te verbeteren. De leveranciers van de PLC aangestuurde productieprocessen eisen een gescheiden netwerk, om de beschikbaarheid te garanderen. Het fysiek scheiden van het netwerk is volgens de opdrachtgever geen optie, omdat de investering te hoog is om dit te realiseren. Dit houdt in dat het LAN netwerk logisch gesegmenteerd dient te worden. De huidige of aan te schaffen netwerkapparatuur dient geschikt te zijn voor het logisch scheiden en routeren van het LAN netwerk. Hier zal ik rekening mee houden in de nieuwe ontwerpen.
- **Het WAN netwerk moet voldoende capaciteit hebben voor de synchronisatie van het ERP systeem.** Er zijn bij mijn opdrachtgever zorgen over de snelheid van het huidige WAN netwerk (geleverd door Verizon). De nieuwe ERP systemen brengen een extra behoefte tot bandbreedte met zich mee. Er moet onderzocht worden of hier problemen mee verwacht worden. Dit zal ik in mijn onderzoek meenemen of dit problemen gaat geven op het huidige WAN netwerk.
- **Internetverkeer, bij een vestiging, het internet op via lokale provider.** Het Internetverkeer van alle vestigingen gaat nu via het MPLS netwerk van de BOAL Group naar de Colocatie⁷ in Rotterdam alvorens het Internet op te gaan. Dit brengt ongemakken voor de gebruikers met zich mee, zoals het gebrek aan lokale (Rotterdam) zoekresultaten (bv Google zal standaard de Nederlandse versie gebruiken). Daarnaast worden op dit moment Social Media en sites waar filmpjes in verwerkt zitten geblokkeerd, zodat de capaciteit van het WAN netwerk geen hinder ondervindt van deze bandbreedte verslindende verkeerstromen. Dit is volgens de opdrachtgever geen optimale situatie voor de gebruikers. Ik zal hier rekening mee houden in de nieuwe ontwerpen.

⁷ Bron: [Colocatie](#)

- **Remote Access onderzoeken.** De huidige manier van remote access via Citrix Access verplicht de externe gebruiker tot het installeren van software en beperkt de toegang die een externe gebruiker kan krijgen. Remote access wordt steeds meer gebruikt en gevraagd door zowel medewerkers van de BOAL Group als leveranciers van (netwerk)apparatuur of productieprocessen. Er is behoefte aan de mogelijkheid tot het opzetten van een web based remote access, die zonder het installeren van extra software toegang tot het netwerk van de BOAL Group biedt. Hier zal ik rekening mee houden in de nieuwe ontwerpen.
- **Het netwerk geschikt maken voor wireless.** Op dit moment is er enkel een wireless verbinding beschikbaar die niet in verbinding staat met het LAN netwerk. De wens is om het wireless netwerk een integraal onderdeel van het volledige LAN netwerk te maken, waardoor netwerkcomponenten niet enkel meer afhankelijk zijn van de bedrade verbindingen. Hier zal ik rekening mee houden in de nieuwe ontwerpen.
- **Geen desinvestering.** De apparatuur dient, die nieuw aangeschaft moet worden, gereed te zijn voor expansie van het netwerk en netwerkverkeer. Dit betekent dat ik bij de nieuwe ontwerpen rekening zal houden met uitbreiding van het netwerk(verkeer) en de gevolgen die het heeft voor de netwerkapparatuur. Het is bij mijn opdrachtgever bekend dat het Verizon netwerk relatief duur is. Gekeken moet worden of deze kosten inderdaad gemaakt moeten worden, of dat er betere en/of goedkopere alternatieven zijn. De opdrachtgever verplicht, indien mogelijk, mij tot het gebruik van Juniper producten. Dit is strategisch besloten, omdat de BOAL Group met kortingen Juniper apparatuur kan aanschaffen.
- **Beheer eenvoudig houden.** Het beheer van het netwerk dient zo eenvoudig mogelijk te zijn, zodat er zo min mogelijk kans is op menselijke fouten en dat er niet veel opleiding vereist is, om het dagelijkse beheer uit te voeren. Omdat het beheer van het netwerk tussen de locaties is uitbesteed zal ik de ervaringen met de support van de externe partij meewegen.
- **Testplan opstellen.** Er moet een testplan opgesteld worden, zodat de ICT-afdeling dit kan voor de implementatie van de nieuwe ontwerpen. Ik heb aangegeven dat dit mogelijk komt te vervallen i.v.m. de planning. Er is bepaald dat dit een wens wordt en bij voldoende tijd er invulling aan geven kan worden.

6.2 In kaart brengen huidige technische infrastructuur

Het vertrekpunt voor de definitiefase, en één van de eisen en wensen van mijn opdrachtgever, is het in kaart brengen van de technische infrastructuur. Op het moment van mijn binnenkomst was er geen enkele omschrijving of tekening beschikbaar met een overzicht van de aanwezige netwerkapparatuur.

Inventarisatie van het LAN netwerk

Volgens de opdrachtgever waren er geen netwerkdiagrammen beschikbaar over het netwerk van de BOAL Group. Tijdens een gesprek, met de infrastructuur specialist, over het netwerk heb ik hem gevraagd waarom dit niet aanwezig was en zijn antwoord was:

- Tijd gebrek
- Andere prioriteiten.

Ik heb toegang moeten verkrijgen tot de dataruimtes, om de mijn inventarisatie te starten. De infrastructuur specialist had het tijdens die periode erg druk met andere projecten en kon mij daardoor geen ondersteuning bieden. Na enig aandringen heb ik een Excel lijst (IP Plan) met het de IP adressen en de sleutel van de dataruimtes gekregen.

Met deze lijst als uitgangspunt ben ik de vestigingen van de BOAL Group in De Lier, 's Gravenzande en België afgegaan om de apparatuur te inventariseren en in kaart te brengen. Tevens heb ik de Colocatie in Rotterdam bezocht om te zien hoe een datacentrum van binnen is geregeld.

Aan de hand van mijn handmatige inventarisatie en de lijst van IP adressen heb ik een aantal netwerkdiagrammen opgesteld van het LAN en WAN netwerk. Zoals bepaald in de scope heb ik me voor het LAN netwerk beperkt tot vestiging De Lier. Voor het WAN heb ik de lijnen tussen iedere vestiging beschreven. Voor het maken van de tekeningen heb ik Microsoft Visio gebruikt. Uit ervaring weet ik dat Visio geschikt is voor dit doel en de licenties waren al aanwezig bij de BOAL Group.

Fysiek onderzoeken dataruimtes

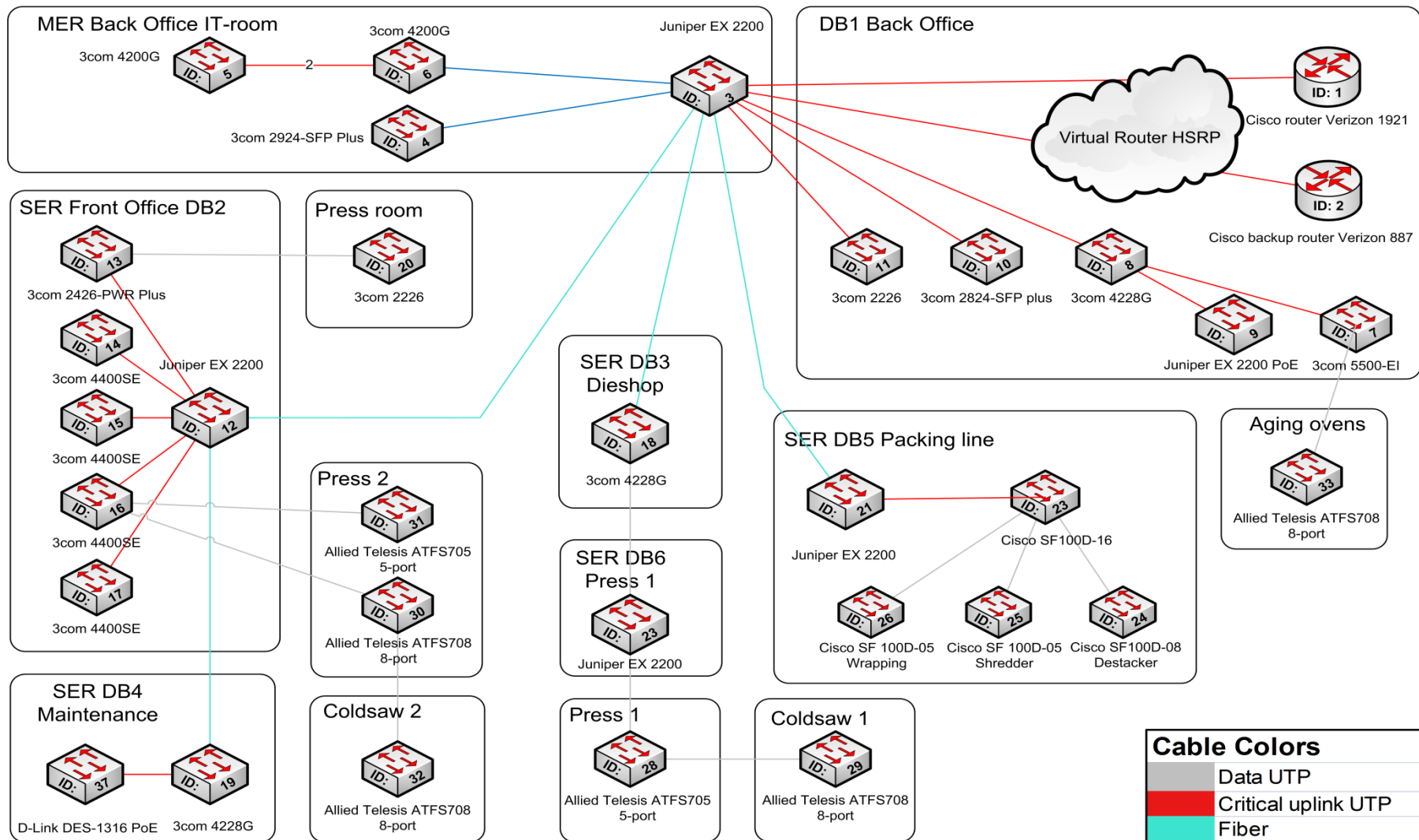
De volgende punten zijn mij opgevallen aan de dataruimtes en IP plan:

- **Kleuren van kabels.** In principe gebruikt de ICT-afdeling van de BOAL Group verschillende kleuren UTP-kabels om onderscheid te kunnen maken tussen verschillende toepassingen, zoals verbindingen tussen netwerkapparatuur en patch kabels van werkplekken. Dit is echter niet consequent doorgevoerd waardoor het risico bestaat dat er bij onderhoud onduidelijk is welk doel de kabels dienen. Dit schept extra risico op menselijke fouten en daarmee de beschikbaarheid van (delen van) het netwerk.
- **Labels.** Het blijkt dat de infrastructuur op sommige plekken niet goed gelabeld is. Wat veel tijd kan kosten op het moment dat er wat in de infrastructuur gewijzigd moet worden.
- **IP plan is niet up to date.** De lijst met IP adressen is verouderd en hier heb ik correcties op uitgevoerd, zodat het IP plan weer up to date is gemaakt.
- **Geen PoE switch.** Er zijn beveiligingscamera's op een switch aangesloten dat een Power over Ethetnet (PoE) zou moeten zijn. Dit bleek niet het geval en daardoor waren er 4 beveiligingscamera's buiten gebruik.
- **Single Point of Failure (SPOF).** De Core van het netwerk is niet redundant uitgevoerd en zijn daardoor een Single Point of Failure. Dit vormt een zeer groot risico voor het netwerk, omdat de gehele fabriek afhankelijk is van de core switch (zie figuur 8 id:3) op netwerk.

Deze bevindingen zal ik terug laten komen in het adviesrapport.

In figuur 8 en 9 zijn netwerkdiagrammen te vinden van het LAN en WAN netwerk. Meer gedetailleerde netwerkdiagrammen zijn te vinden in de bijlagen van het definitierapport. Na de voltooiing, van het in kaart brengen van het netwerk, heb ik de netwerkdiagrammen gepresenteerd aan de opdrachtgever en infrastructuur specialist , waar ze met enthousiasme ontvangen werden.

BOAL Profielen De Lier LAN Switches/Routers



Figuur 8: Netwerkdigram LAN netwerk

6.3 LAN netwerk onderzoeken

Na het inzichtelijk maken van het netwerk aan de hand van de netwerkdiagrammen ben ik zoveel mogelijk informatie over het LAN netwerk gaan verzamelen. De focus die ik heb afgeleid uit de eisen en wensen ligt hierbij met name op de snelheid, beschikbaarheid en beveiliging. Ondanks het feit dat mijn opdrachtgever de logische scheiding van het netwerk als eis heeft geformuleerd heb ik noodzaak ervan, meegenomen in mijn inventarisatie. Op deze manier kan ik, bij het ontwerp van de nieuwe situatie, verifiëren dat de risico's niet meer zullen voorkomen.

Ik heb het LAN netwerk onderzocht aan de hand van de volgende methoden:

- **Bestuderen van subnetten.** Aan de hand van de gecreëerde netwerkdiagram van het LAN en WAN netwerk, heb ik de IP ranges bestudeerd
- **Bestuderen van de netwerkapparatuur.** Door de netwerkapparatuur te bestuderen kan ik aangeven wat de mogelijkheden zijn van deze apparatuur. Tevens heb ik ingelogd, indien mogelijk, op de switches en daaruit heb ik conclusies kunnen trekken over de configuratie van het netwerk en het wel of niet aanwezig zijn van beveiligingsmaatregelen.
- **Monitoren van het netwerk.** Door het monitoren van het netwerk heb ik kunnen vaststellen wat voor soort verkeer zich bevindt op het LAN netwerk en in welke mate een bepaald type verkeer langskomt. Hierbij kan ik opmerken of er overbodig verkeer is dat ten koste gaat van de bandbreedte, of dat er een type verkeer is dat de beveiliging in gevaar brengt. Ik heb dit gedaan met behulp van het programma Wireshark.

Bestuderen van subnetten

Aan de hand van de gecreëerde netwerkdiagram van het LAN en WAN netwerk, heb ik de IP ranges bestudeerd die in tabel 2 staat weergegeven.

De BOAL Group gebruikt 2 subnetten per vestiging. Er is jaren geleden voor een /24 (254 hosts) subnet gekozen is. Dit houdt in dat er 254 adressen per subnet uitgegeven kunnen worden. Met het toevoegen van steeds meer clients is dit niet meer toereikend gebleken. Er is daarom redelijk recent een extra /16 (65534 hosts) subnet bijgeplaatst. Al het verkeer dat van het ene naar het andere subnet gaat, loopt via de router. Dit veroorzaakt onnodige convergentie.

IP Ranges	subnet /24	subnet /16
Colo Rotterdam	10.0.0.0	
DMZ Colo	10.1.2.0	
De Lier	10.0.2.0	10.2.0.0
s-Gravenzande	10.0.1.0	10.1.0.0
Moorsele	10.0.3.0	10.3.0.0
Shephed	10.0.4.0	10.4.0.0

Tabel 2: IP ranges per locatie

Met een subnet van /24 kunnen er maar 254 hosts aangesloten worden op een subnet. Met de geautomatiseerde productie processen, krijgen de PLC's ook een IP adres toegewezen en komen ze IP-adressen tekort. Met een /16 subnet kunnen er 65534 hosts aangesloten worden. Verizon heeft op iedere vestiging, een extra logische interface op de Cisco routers gecreëerd.

Overlappende subnetten

In de vestiging 's-Gravenzande is er een overlappend subnet met de DMZ⁸. Het 10.1.2.0/24 is een subnet van 10.1.0.0/16 en dit houdt in dat momenteel de remote users de hosts, in het 10.1.0.0/16 subnet, niet kunnen bereiken. Ik heb dit getest door een host te bereiken in het 10.1.0.0/16 subnet vanuit de DMZ. Het bleek niet bereikbaar, waardoor remote users dit subnet niet kunnen benaderen.

⁸ Bron: [DMZ](#)

Doornemen de netwerkkaparaatuur

Er zijn Cisco routers van Verizon actief, die als gateway fungeren voor het LAN netwerk. Hierop kan niet worden ingelogd, omdat Verizon dit niet toestaat.

In vestiging De Lier zijn verschillende merken en type switches in gebruik van de volgende fabrikanten:

- 3COM
- Juniper
- Cisco
- A.T. (Allied Texas)
- D-Link

Tijdens het doornemen van de switches ben ik tot de volgende conclusies gekomen:

- **Unmanaged switches.** De A.T. en Cisco switches zijn in gebruik voor het Industriële netwerk. Tussen sommige A.T. switches zijn twee kabels neergelegd zodat de tweede kabel gebruikt kan worden als de eerste kabel defect gaat. Indien beide kabels per ongeluk tegelijk aangesloten worden, wordt er een “loop” gecreëerd die niet wordt afgevangen. De switches zijn unmanaged en hebben daardoor geen enkele mogelijkheid, zoals het RSTP⁹ (Rapid Spanning Tree Protocol), tot het detecteren van de loop. Dit kan een Broadcast Storm¹⁰ veroorzaken. Ik zal deze switches in de nieuwe ontwerpen elimineren om de controle te kunnen blijven behouden.
- **Geen portsecurity.** De 3COM, Cisco, A.T. en D-Link hebben aan de hand van de specificaties geen beveiliging op de meest voorname aanvallen. In het definitierapport staat een uitgebreide beschrijving over deze aanvallen.
Het gaat om de volgende aanvallen:
 - ARP Attack
 - MAC Flooding Attack
 - DHCP Starvation Attack
 - DHCP Rogue Attack
- **VLAN's en QoS.** De Cisco en A.T. switches zijn unmanaged en niet configureerbaar. De 3COM switches kunnen alleen overweg met statische VLAN's. Dit is momenteel niet geconfigureerd. De switches hebben geen mogelijkheid tot QoS (Quality of Service) om bepaald type verkeer voorrang te geven op ander verkeer. Dit beperkt de mogelijkheden die deze apparatuur heeft rondom beveiliging en logische scheiding van netwerkverkeer.
- **Wachtwoorden niet gelijk.** De loginnamen en/of wachtwoorden zijn niet consequent doorgevoerd om een switch te beheren.
- **Geen backup van configuratie.** De configuraties van de switches zijn nergens opgeslagen, wat tijdrovend kan zijn als er een switch uitvalt of een configuratie verkeerd gewijzigd wordt.

⁹ Bron: [RSTP](#)

¹⁰ Bron: [Broadcast Storm](#)

Monitoren van het netwerk

Het monitoren heb ik uitgevoerd om te kunnen onderzoeken wat de “vertraging” veroorzaakt, op het LAN netwerk. Dit heb ik gedaan door op meerdere tijdstippen en plaatsen het netwerk te monitoren, met telkens een sessie van 15 minuten. De voorbeeld uit de uitkomsten heb ik opgenomen in tabel 3. Dit is een resultaat met het meest voorkomende verkeer binnen het LAN netwerk. Voor de totale resultaten verwijst ik naar het definitierapport

Wireshark monitor date 4 june 2012					
ID	location	Cisco HSRP	ARP	EtherNet/IP + CIP	Total
3	MER back office	18,58%	43,45%	12,68%	74,71%
9	DB1 back office	19,21%	42,65%	13,12%	74,98%
14	DB2 front office	19,39%	43,81%	26,24%	89,44%
20	DB5 packing	20,03%	42,58%	11,64%	74,25%
	Average	19,30%	43,12%	15,92%	78,35%

Tabel 3: Broadcast verkeer door verschillende protocollen

Uit tabel 3 blijkt dat 78% procent van de pakketten bestaan uit verkeer dat voortkomt uit verschillende soorten protocollen:

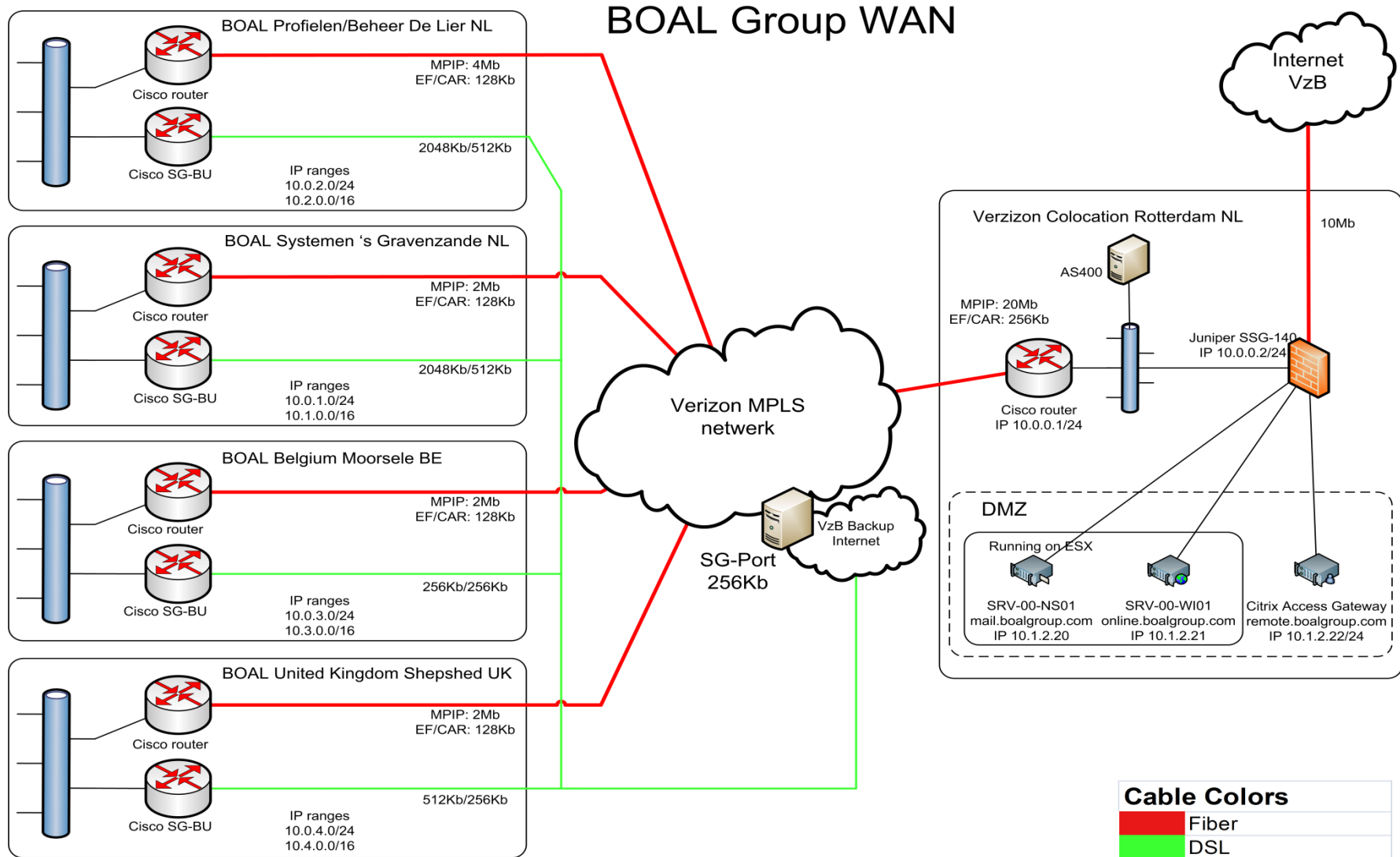
- **Cisco HSRP¹¹, Hot Standby Routing Protocol.** Deze pakketten komen voort uit de communicatie tussen de primaire en backup router. De backup router neemt de taken over, bij uitval van de primaire router. Zoals ik hierboven al heb aangegeven hoort dit verkeer niet over het hele netwerk te gaan. Ook heb ik geconstateerd dat de pakketten op het LAN van de BOAL Group onbeveiligd zijn. Een client kan zich hierdoor via dit protocol op elke plek in het netwerk als primaire router identificeren. Hierdoor kan alle netwerkcommunicatie binnen het LAN worden verstoord.
- **ARP¹², Address Resolution Protocol.** Dit is een protocol binnen TCP/IP dat computers, die allemaal op het LAN netwerk zijn aangesloten, in staat stelt verbinding te maken met andere computers op dat netwerk, zonder hun MAC-adres te kennen. Dit is normaal verkeer alleen door de omvang van het netwerk heeft het impact op het LAN netwerk.
- **CIP¹³, Common Industrial Protocol.** Dit protocol wordt gebruikt door de PLC's om onderling te communiceren. Het genereert een flinke hoeveelheid verkeer op het LAN netwerk, wat veel capaciteit vergt.

Al dit verkeer is in principe nuttig, maar hoort niet over het volledige netwerk verspreid te worden (Broadcasting). Doormiddel van het scheiden van het netwerk zouden enkel de apparaten, die hier daadwerkelijk nut van hebben, het verkeer moeten ontvangen. Voor de rest van het netwerk is dit overbodig verkeer, wat ten koste gaat van de capaciteit van het LAN netwerk. Zo kan de snelheid en betrouwbaarheid, van bijvoorbeeld de Citrix en PLC omgevingen, sterk verbeterd worden.

¹¹ Bron: [HSRP](#)

¹² Bron: [ARP](#)

¹³ Bron: [CIP](#)



Figuur 9: Netwerkdigram WAN

6.4 WAN netwerk onderzoeken

Na het inzichtelijk maken van het netwerk aan de hand van de netwerkdiagrammen ben ik zoveel mogelijk informatie over het WAN gaan verzamelen. De focus die ik heb afgeleid uit de eisen en wensen ligt hierbij met name op:

- Snelheid
- Kosten
- Beheer

Ik heb het WAN onderzocht aan de hand van de volgende methoden:

- **Monitoren van het WAN.** Initieel wilde ik het monitoren van het WAN netwerk uitvoeren op de WAN poort van de router. Hiervoor heb ik geen toestemming gekregen van de infrastructuur specialist. Als alternatief heb ik ingelogd op een server op de colocatie, waarvan ik kon pingen naar de vestigingen. Op het moment dat er klachten kwamen van gebruikers dat het systeem traag werd heb ik de ping metingen uitgevoerd.
- **Doornemen van de specificaties van het WAN netwerk.** Het WAN netwerk van Verizon wordt ingezet voor het WAN van de BOAL Group. Aan de hand van de specificaties, het contract en de Service Level Agreements heb ik conclusies kunnen trekken over de snelheid, mogelijkheden en kosten van het Verizon netwerk. Ook heb ik mijn opdrachtgever geïnterviewd over de algemene ervaringen met Verizon.

Pingen van het netwerk

Op het moment dat de gebruikers klaagden over een trage sessie, ben ik gaan “pingen” van de Colocatie naar de betreffende vestiging en dit leverde de resultaten op, die in tabel 4 staan afbeeld.

Ping	Gemiddeld antwoord
5 juni	351 ms
7 juni	323 ms
20 juni	316 ms
21 juni	456 ms

Tabel 4: Ping resultaten WAN netwerk

Deze waardes zijn te hoog om diensten als VoIP of videoconference te ondersteunen (maximaal 300 ms¹⁴). Bij deze diensten is het cruciaal dat er een constante bitrate tussen de partijen zit. In de huidige situatie is de bitrate variabel, wat bij implementatie van VoIP zeer ongewenst is.

In het huidige ERP systeem is de vertraging al te merken met de verbindingen naar de Colocatie. In de nieuwe situatie waarbij er servers in zowel De Lier als UK worden geplaatst hebben de gebruikers van De Lier weliswaar geen last meer van vertraging, maar de gebruikers van UK hebben hun sessie direct op de server in De Lier. Zonder verbetering zal het probleem dus verplaatst worden. Tevens geeft de synchronisatie tussen de twee servers, extra verkeer op het WAN netwerk

¹⁴Bron: [VoIP](#)

Doornemen van de specificaties van het WAN netwerk

Het WAN netwerk van de BOAL Group is uitbesteed aan de service provider Verizon. Dit bedrijf verzorgt de verbindingen tussen de vestigingen en het beheer daarvan. De verbindingen vormen een MPLS (Multi Protocol Label Switching) netwerk. Het contract met Verizon loopt tot juni 2014, waardoor er pas na die datum overgestapt kan worden naar een andere WAN verbinding. Op basis van mijn bevindingen heb ik een overzicht van voor- en nadelen opgesteld rondom het Verizon WAN.

De voordelen zijn:

- **Betrouwbare lijnen.** Mijn opdrachtgever geeft aan dat de verbindingen betrouwbaar zijn gebleken in de loop der jaren. Ook is er een backup DSL lijn aanwezig die de functies overneemt, mocht de hoofdverbinding uitvallen.
- **Beheer is uitbesteed.** Het beheer van het complete BOAL MPLS netwerk is in handen van Verizon. Daardoor hoeft deze kennis niet binnen de BOAL Group aanwezig te zijn. De verbindingen worden door Verizon 24/7 gemonitord, zodat bij uitval van één van de verbindingen gelijk actie ondernomen wordt.
- **Private IP netwerk.** Het MPLS netwerk is een eigen gegarandeerde verbinding tussen de vestigingen en de Colocatie en is niet onderhevig aan overboeking. Er is maar één firewall nodig, omdat al het verkeer via de Colocatie het internet op gaat.

De nadelen zijn:

- **Zeer kostbare verbindingen.** De Verizon verbindingen, inclusief huur van de colocatie, kosten € 130.000,- per jaar. Hiervoor heeft de BOAL Group de beschikking over de in tabel 4 gespecificeerde verbindingen. Mijn opdrachtgever denkt hier een significante besparing te kunnen realiseren.
- **Relatief slechte support.** Doordat de BOAL Group een te kleine klant is voor Verizon is er geen eigen accountmanager die snel op wensen of klachten reageert. Daarnaast is er, volgens de infrastructuur specialist, 14 dagen reactietijd voordat wijzigingen doorgevoerd worden.
- **Lage snelheid.** De verbindingen van de vestigingen buiten De Lier zijn 2 MB/s (zie tabel 5). Op dit moment zijn er regelmatig klachten over de snelheid van het ERP systeem en het internet. Aangezien er bij de introductie van VoIP per gesprek alleen al 64 Kb nodig zal zijn¹⁵ zullen de 2 MB/s lijnen naar verwachting te traag blijken.

Vestiging	Fiber	Backup DSL
BOAL Profielen	4Mb/4Mb	2Mb/512Kb
BOAL Systemen	2Mb/2Mb	2Mb/512Kb
BOAL België	2Mb/2Mb	256Kb/256Kb
BOAL UK	2Mb/2Mb	512/256Kb
Colocatie	20Mb/20Mb	nvt
Internet vanaf Colocatie	10Mb/10Mb	nvt

Tabel 5: Afgenomen verbindingen bij Verizon

- **Niet geoptimaliseerde verbindingen.** Het verkeer voor de AS400 (van de ERP systemen) heeft een gegarandeerde snelheid van 128 Kb doormiddel van de QoS (zie tabel 6) prioriteit EF/CAR (zie tabel 7). De overige QoS prioriteiten voor ander verkeer staan zouden ook ingesteld moeten staan, maar functioneren niet goed. In de vestiging in België heeft een gebruiker recent een bestand van 200MB gedownload, waarop de TC's, die van de Citrix license server op de colocatie afhankelijk zijn, vastliepen en niet meer te gebruiken waren totdat de lijn weer vrij was. Een gebruiker kan dus onbewust een deel van de fabriek platleggen.

¹⁵ Bron: [G.711 Protocol](#)

Application Name	Source IP	Dest. IP	Port number	TCP/UDP	NBAR Cisco	QoS Level
AS400	any	any	23	TCP	telnet	EF
Citrix Provisioning	any	any	1433	TCP	sqlsever	AF21
Lotus Notes	any	any	1352	TCP	notes	AF31
Internet	any	any	8080	TCP	http	BE
Internet Secure	any	any	443	TCP	secure-http	BE

Tabel 6: QoS applicatievolgorde

Traffic Priority Class	IETF Name
EF	Expedited Forwarding (EF)
AF4	Video/Priority Data (AF41, 42 or 43)
AF3	Mission Critical Data (AF31, 32 or 33)
AF2	Transaction Data (AF21, 22 or 23)
AF1	General Data (AF11 and 12)
BE	Best Effort (Default)

Tabel 7: QoS levels uit documentatie Verizon

- **Internetverkeer wordt via Rotterdam gerouteerd.** Al het internetverkeer gaat via de Colocatie het Internet op. Hierdoor denken websites, die sterk van lokalisering afhankelijk zijn (zoals Google), dat de gebruiker zich in Rotterdam bevindt. De gebruikers krijgen hierdoor standaard Rotterdamse zoekresultaten.

6.5 Remote Access onderzoeken

De BOAL Group geeft voor verschillende werknemers toegang tot het interne netwerk voor het repliceren van bestanden en e-mail. Dit wordt momenteel gedaan via een Citrix Access Gateway d.m.v. een IPSec VPN verbinding. De leveranciers van geautomatiseerde productieprocessen (PLC's) willen ook toegang tot het interne netwerk, om bij storing te kunnen bekijken wat de status van de PLC's is.

Ik ben tot de volgende conclusies gekomen:

- **Clientsoftware.** De ICT-afdeling moet ondersteuning bieden aan een remote user, doordat er cliëntsoftware geïnstalleerd moet worden voor een IPSec VPN verbinding. Met een Tablet of Smartphone kan er geen verbinding gemaakt worden, omdat de client software niet geïnstalleerd kan worden op deze apparaten.
- **Volledige toegang.** Via deze verbinding heeft een remote user volledige toegang tot het interne netwerk. Er is niet bepaald bij delen of specifieke IP-adressen, de remote user mag komen.
- **Geen controle.** Er is geen controle, bij het inloggen, over de status van de client zoals:
 - Besturingssysteem updates
 - Antivirus updates
 - Spyware/Adware checker

Ik zal in de architectuurfase naar een oplossing zoeken voor het inloggen van remote users, omdat de opdrachtgever ook gebruikers via Tablets of Smartphones verbinding wil laten maken. Tevens vormen de externe gebruikers (leveranciers) een risico voor de BOAL Group, doordat de ICT-afdeling geen controle over de client heeft.

6.6 Opstellen van risicoanalyse

Aan de hand van de netwerkdiagrammen, die ik heb opgesteld, ben ik de risico's gaan analyseren van de routers en switches. Zoals bepaald in de scope zal ik mij enkel richten op het LAN netwerk van BOAL Profielen te De Lier. Het LAN netwerk van de overige vestigingen blijft buiten beschouwing, evenals het WAN netwerk.

De risicoanalyse is bedoeld om het risico van het uitvallen van een netwerkapparaat meetbaar te maken en om te bepalen of er verbetering noodzakelijk is. Dit komt voort uit de eis:

- **De risico's van huidige LAN netwerk in kaart brengen**

Het risico heb ik volgens de volgende berekening bepaald:

$$\text{Risiko}(R) = \text{Impact}(I) \times \text{Kans}(K)$$

Deze berekening leidt tot een getal (R) welke het relatieve risico van een apparaat inzichtelijk maakt. Dit risico kan vergeleken worden met andere apparaten in het netwerk. Netwerkapparatuur die in de toekomst wordt aangeschaft, ter vervanging of aanvulling, van de bestaande netwerkapparaten kan volgens dezelfde methodiek van een risico worden voorzien. De toegevoegde waarde van een nieuw ontwerp kan hiermee aangetoond worden. Het risico is relatief omdat er geen standaard is aan de hand waarvan ik het risico kan duiden. Voor de toepassing die het risicocijfer heeft maakt dit geen verschil.

Bepalen van de impact

Voor het bepalen van de impact ben ik op zoek gegaan naar een manier om de netwerkapparatuur te voorzien van een impact score. Mijn eerste idee was de score uit te voeren doormiddel van een classificatie aan de hand van letters, zoals in tabel 8 te zien is.

Critical	A
High	B
Medium	C
Low	D
None	E

Device	Score	Description
Cisco 1921	A	DB1 back office router verizon
Cisco 887	B	DB1 back office backup router verizon
Juniper EX2200	A	MER back office switch
3com 2924-SFP	D	MER back office iS400 UK switch

Tabel 8: Classificeren van impact met letters (voorbeeld)

Tijdens het uitwerken van de impact besloot ik met meerdere wegingsfactoren te werken, zodat ik een transparanter inzicht kon geven in de totstandkoming van de impactscore. Het toevoegen van meerdere wegingsfactoren zou betekenen dat er meerdere letters bij elkaar opgeteld moeten worden, zoals in tabel 9.

Device	1	2	3	Score	Description
Cisco 1921	A	B	A	ABA	DB1 back office router verizon
Cisco 887	B	A	C	BAC	DB1 back office backup router verizon
Juniper EX2200	A	A	A	AAA	MER back office switch
3com 4228G	C	D	B	CDB	SER DB4 Maintenance switch

Tabel 9: Classificeren van impact met meerdere wegingsfactoren en letters (voorbeeld)

Het werd al snel duidelijk dat deze manier van classificatie het onmogelijk zou maken om berekeningen toe te passen op de score. Daarnaast maakt deze methode niet duidelijk waarom een netwerkapparaat een bepaalde score krijgt. Hieruit heb ik de conclusie getrokken dat de scoring aan de hand van cijfers gedaan moet worden. Ik doe dit door een waarde toe te kennen aan de hand van de hieronder beschreven wegingsfactoren. De impact van het uitvallen van een netwerkapparaat is daarnaast volledig afhankelijk van de cliënten en servers die ervan afhankelijk zijn. Hierdoor zal de totaalscore van de impact van een bepaald netwerkapparaat bestaan uit de som van alle wegingsfactoren van de cliënten en servers die aan het respectievelijke netwerkapparaat afhankelijk zijn.

Doormiddel van een brainstormsessie met mijn opdrachtgever heb ik de volgende wegingsfactoren van de cliënten en servers vastgesteld:

- **Network Type (NT).** Hiermee wordt het type netwerkverkeer aangegeven waarmee de client te maken heeft. Hierin onderscheid ik de volgende types:

- **Industrieel.** Voor BOAL Profielen is produceren (persen) het belangrijkste proces binnen het bedrijf. Dit proces moet 24/7 doorgaan. Zonder het industriële verkeer kan er niet geperst worden, wat betekent dat het bedrijf kritisch is. Dit type verkeer krijgt dan ook de hoogste score (3)

N.T.	Score
Industrial	3
Production	2
Office	1

Tabel 10: Network Type

- **Productie.** Het productie verkeer toont de orders van de van de klanten aan het productiepersoneel. In geval van nood kan dit tijdelijk met papier worden opgelost. Hoewel belangrijk is dit verkeer dus niet bedrijf kritisch. Dit type verkeer krijgt de middelste score (2)
- **Office.** Het uitvallen van het kantoorverkeer brengt met name ongemakken met zich mee, maar is niet kritisch. Dit type verkeer krijgt de laagste score (1)

- **Business Impact (BI).** Hiermee wordt de impact aangegeven hoeveel gebruikers last hebben van de uitval. De BI kent het volgende onderscheid:

- **Fabriek.** De productie en alle afdelingen liggen stil, ofwel de gehele fabriek. Dit heeft de hoogste impact (5)

- **Productie proces.** Een gedeelte van productie ligt stil. Dit heeft een impact van (4)

- **Afdeling.** Eén afdeling kan geen gebruik maken van het netwerk. Dit heeft een impact van (3)

- **<5 gebruikers.** Het totale aantal gebruikers dat geen gebruik kan maken van het netwerk is maximaal 5 en heeft geen gevolgen voor het productieproces. Dit heeft een impact van (2)

- **Gebruiker.** Eén gebruiker heeft geen toegang tot het netwerk, maar dit heeft geen gevolgen voor het productieproces. Dit heeft een impact van (1)

B.I.	Score
Fabric	5
Production proces	4
Department	3
<5 Users	2
One User	1

Tabel 11: Business Impact

- **Network Impact (NI).** Met de NI geef ik de invloed van een storing, op de ICT-afdeling, aan in uren. De uren komen uit de SLA die BOAL Profielen met de ICT-afdeling afgesloten heeft. Binnen onderstaande tijd moet er actie ondernomen zijn om het probleem te verhelpen. Ik heb de responstijden voorzien van een score, waarbij ik de laagste responstijd de hoogste score heb gegeven omdat de invloed op de ICT afdeling het hoogste is.

- **1 uur** (5)

- **4 uur** (4)

- **8 uur** (3)

- **24 uur** (2)

- **48 uur** (1)

N.I.	Score
<1	5
<4	4
<8	3
<24	2
<48	1

Tabel 12: Network Impact

- **Business Impact Cost (BIC).** Met de BIC geef ik de financiële impact van uitval van een netwerkkapparaat per dag aan. De BIC is ingeschat door mijn opdrachtgever en is, relatief gezien tot de andere wegingsfactoren, dusdanig belangrijk voor BOAL Profielen dat ik in overleg heb besloten de weging te verdubbelen.

- < €100.000 (10)
- < €50.000 (8)
- < €10.000 (6)
- < €1.000 (4)
- < €100 (2)

B.I.C.	Score
< €100.000	10
< €50.000	8
< €10.000	6
< €1.000	4
< €100	2

Tabel 13: Business Impact

Mijn eerste berekening was het bij elkaar optellen van de wegingsfactoren, maar dit gaf een slecht overzicht met de impact bepaling. Ik heb ervoor gekozen op de NT, als vermenigvuldigingsfactor te gebruiken en daardoor kwamen de impact cijfers beter tot hun recht.

$$\text{Impact} = \text{NT} \times (\text{BI} + \text{NI} + \text{BIC})$$

Bepalen van de kans

Voor het bepalen van de kans ben ik opzoek gegaan naar een eenheid die van toepassing is op zowel de cliënts, servers en netwerkkapparatuur. De enige logisch bruikbare eenheid die hiervoor in aanmerking komt is de Mean Time Between Failure (MTBF), omdat deze door veel fabrikanten wordt opgegeven. De MTBF is de gemiddelde tijd tussen twee defecten die leiden tot het uit bedrijf zijn van een apparaat. Omdat de BOAL Group een economische levensduur van een apparaat van vijf jaar hanteert zal ik de kans die een apparaat heeft om uit te vallen binnen die vijf jaar berekenen. De gehanteerde MTBF heb ik uit de specificaties van de verschillende apparaten gehaald. Waar de fabrikant geen MTBF opgaf, heb ik een MTBF van een vergelijkbaar apparaat gehanteerd.

Voor de kans van uitval, over een periode van vijf jaar, ben ik opzoek gegaan naar een formule¹⁶ om dit te berekenen. De onderstaande formule geeft als resultaat een kans dat het apparaat blijft werken binnen deze periode.

$$\text{Kans} = (\exp(-T/\text{MTBF}))$$

exp = exponentiële functie¹⁷

T = de tijd dat het apparaat actief is gedurende de vijf jaar, berekent in uren.

MTBF = Mean Time Between Failure aangegeven in uren

Ik heb de formule uitgebreid, door als extra informatie (Age & O.T.) de leeftijd van de huidige apparatuur toe te voegen en hoe lang ze aan gestaan hebben. Via deze manier kan ik de kans van de huidige apparatuur berekenen Door de uitkomst van de formule om te draaien, kan ik de kans van uitval aan te geven i.p.v. de kans van het blijven werken.

$$\text{Kans} = (1 - \exp(-T/(\text{MTBF} - (\text{Age} \times \text{OT}))))$$

Age = de leeftijd van het apparaat in jaren

O.T. = Online Time per jaar, berekent in uren. Dit is voor switches en routers 8730 uur (365 dagen).

MTBF (hours)	Age (years)	T.	Chance	R.	Chance2
145000	0,50	43800	26,76%	2	7,16%

Tabel 14: Kans berekening

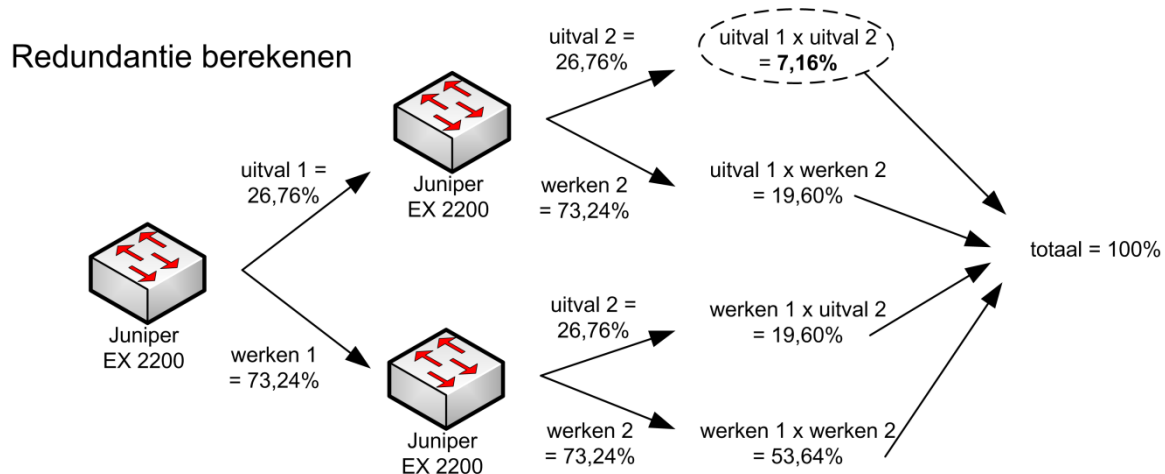
¹⁶ Bron: [MTBF berekenen](#)

¹⁷ Bron: [Exponentiële functie](#)

Nu ik de kans berekent heb op uitval van één apparaat, moet ik de kans berekenen als het apparaat redundant is uitgevoerd. In tabel 14 staat de R. voor een redundante uitvoering:

R = Redundantie, 1 = Nee en 2 = Ja

Ik heb hierbij de hulp van de Business Intelligence (Philip van der Wel) medewerker ingeroepen. Hij is een 3^e jaars student Econometrie aan de Erasmus en werkt voor de BOAL Group. Hij heeft met mij meegedacht hoe zo'n soort berekening uitgevoerd kan worden. In figuur 10 staat de kansberekening, waarbij het percentage altijd op 100% uit moet komen.



Figuur 10: Kans op uitval berekenen met redundantie

De kans op uitval van beide apparaten ligt op **7,16%** in de periode van de komende vijf jaar.

Uitvoeren van de risicoanalyse

Om LAN netwerk goed te kunnen beoordelen heb ik eerst de clients een score gegeven. De clients heb ik gegroepeerd tot afdelingen en productieprocessen (ID's). Tevens heb ik dat op de servers toegepast. Tabel 15 is een voorbeeld uit de totale scoretabel, welke in het definitierapport te vinden is.

Risicoanalyse BOAL Profielen De Lier LAN							Server & Clients
ID	Device	N.T.	N.I.	B.I.	B.I.C.	Impact	Description
C08	Optalex	3	5	4	10	57	Optalex Industrial PC
S08	Dell Power Vault MD1000	3	5	5	10	60	Falconstor Data Store
C23	Security Camera's	3	2	2	4	24	
S02	Dell Power Vault 124T	1	5	2	2	9	Tape Drive

Tabel 15: Voorbeeld risicoanalyse server/clients

Aan de hand van de risicoanalyse van de servers en clients heb ik de switches en routers kunnen scoren. De impact van een netwerkkapparaat wordt bepaald door de totale som van de impact van de cliënts en servers die van het netwerkkapparaat afhankelijk zijn om hun diensten te kunnen leveren. De netwerkdigrammen waarin ik deze servers en clients geteld heb is te vinden in het definitierapport. Tabel 16 is een voorbeeld uit de totale scoretabel, welke in het definitierapport te vinden is.

Risicoanalyse BOAL Profielen De Lier LAN										Switches/Routers
ID	Device	Impact	MTBF (hours)	Age (years)	T.	Chance	R.	R.C.	Risk	Description
3	Juniper EX2200	840	145000	0,50	43800	26,76%	1	26,76%	225	MER back office switch
23	Juniper EX2200	459	145000	0,50	43800	26,76%	1	26,76%	123	SER DB6 Press 1 switch
27	Cisco SF100D-05	61	125000	0,10	43800	29,73%	1	29,73%	18	Packing Industrial Wrapping
5	3com 4200G	774	290000	3,00	43800	15,30%	2	2,34%	18	MER back office ESX switch

Tabel 16: Voorbeeld risicoanalyse switches/routers

In de architectuurfase heb ik de risicoanalyse opnieuw toegepast, op het nieuwe ontwerp. Daaruit blijkt door nieuwe hardware en redundantie toe te passen, de risico's aanzienlijk verkleind worden.

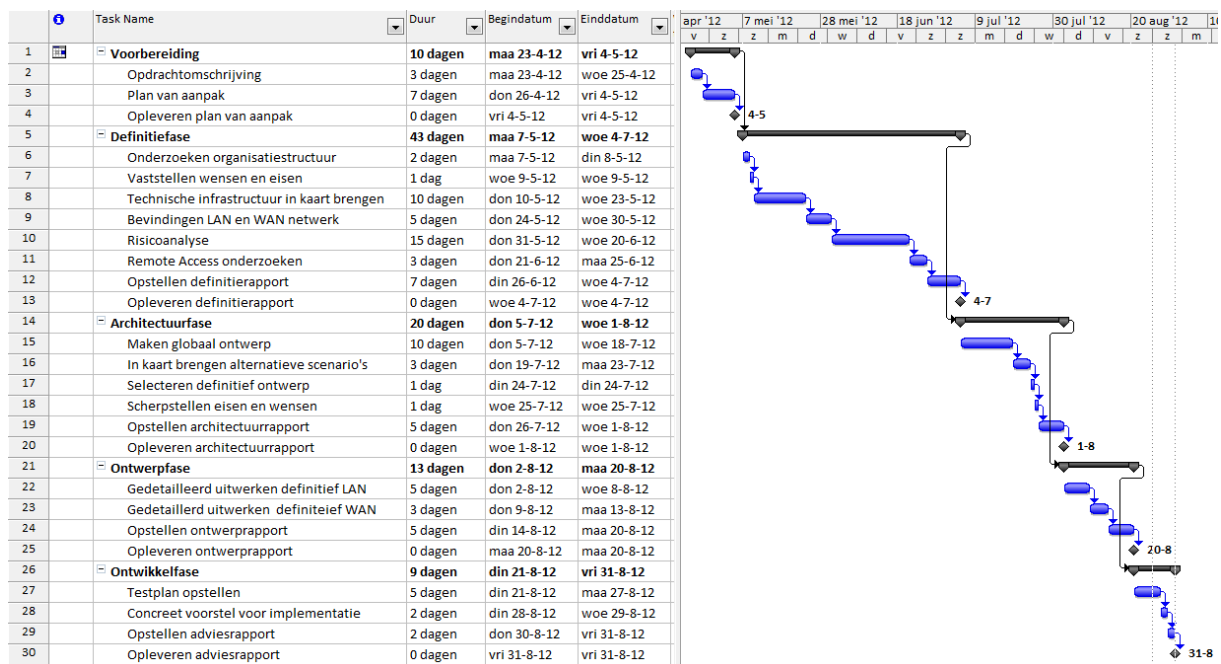
6.7 Opleveren van definitierapport

Het definitierapport bevat een uitwerking van alle onderwerpen die in de definitiefase aan bod zijn gekomen. Ik heb het definitierapport laten goedkeuren door mijn opdrachtgever alvorens de faseovergang naar de architectuurfase te doen. Het definitierapport dient hiermee formeel als input voor de volgende fasen. Tevens vervul ik met het definitierapport twee van de eisen van mijn opdracht:

- Het huidige LAN en WAN netwerk in kaart brengen.
- De risico's van het huidige LAN netwerk in kaart brengen

6.8 Planning bewaken

Tijdens de definitiefase heb ik de planning bewaakt en gekeken of ik op schema lig. Ik heb hier geconcludeerd dat met name de risicoanalyse meer tijd heeft gekost dan ik oorspronkelijk had gebudgetteerd. In plaats van 10 dagen heb ik hier 15 dagen over gedaan. Dit heeft tot gevolg dat het oplevermoment van het totale project 5 dagen naar achteren verschuift. Aangezien de einddatum net binnen de maand augustus blijft, valt het binnen de toleranties van mijn planning. Ik onderneem hier dan ook geen specifieke actie op.



Figuur 11: Bijgewerkte planning n.a.v. definitiefase

7. Fase 2: De architectuurfase

In de architectuurfase wordt een globale opzet van de uiteindelijke technische infrastructuur (gewenste situatie) uitgewerkt. Hiervoor worden enkele alternatieven uitgewerkt en voorzien van een invoeringsscenario en overzicht van kosten.

In de Architectuurfase voer ik de volgende activiteiten uit:

- Maken van een globaal LAN netwerk aan de hand van de eisen en wensen
- Risicoanalyse over geadviseerde LAN netwerk ontwerp
- Maken van een globaal WAN netwerk aan de hand van de eisen en wensen
- Voorstel voor remote access
- Het bespreken van de ontwerpen met de opdrachtgever en het selecteren van een definitief ontwerp
- Het scherpstellen van de eisen en wensen met mijn opdrachtgever
- Het opleveren van een architectuurrapport met de uitwerking van bovenstaande punten

7.1 Maken van een globaal LAN ontwerp

Voor het ontwerpen van het LAN heb ik de wensen en eisen die ik heb geïnterpreteerd omgezet in technische specificaties. Op basis van deze specificaties heb ik twee globale voorstellen voor een LAN ontwerp uitgewerkt. Deze voorstellen zal ik voorleggen aan mijn opdrachtgever, zodat er een keuze gemaakt kan worden.

Omzetten wensen en eisen

Wensen en eisen die toepasbaar zijn op de ontwerpen voor het LAN netwerk heb ik gekoppeld aan concrete specificaties binnen mijn ontwerpen:

Wens/eis

- Hogere beschikbaarheid garanderen

Concrete specificaties

- Redundant maken

Wens/eis

- Het netwerk geschikt maken voor videoconferentie en VoIP

Concrete specificaties

- VLANs prioriteren d.m.v. Quality of Service (QoS)
- Power over Ethernet (PoE) bij toekomstige switches

Wens/eis

- LAN netwerk scheiden

Concrete specificaties

- Het implementeren van VLAN's voor het logisch scheiden van het netwerkverkeer

Wens/eis

- Geen desinvestering.

Concrete specificaties

- Servicecontracten netwerkapparaten selecteren.
- Hardware selecteren.

Wens/eis

- Beheer eenvoudig houden.

Concrete specificaties

- Implementeren dynamische VLAN's i.c.m. Network Access Control (NAC)

Uitwerken concrete specificaties

Na het koppelen van de wensen en eisen aan concrete specificaties heb ik de specificaties verder uitgewerkt:

- **Redundant maken.** Het verbeteren van de beschikbaarheid, heeft te maken met het verkleinen van het risico op uitval. Ik verwerk dit in beide ontwerp door het redundant maken van de belangrijkste netwerkapparatuur.
- **VLAN's prioriteren d.m.v. QoS.** Door het gebruik van VLAN's kan er eenvoudig prioritering doormiddel van QoS worden toegevoegd. Het gebruik van VLAN's neem ik mee in beide ontwerpen. QoS is onderdeel van de configuratie en zal verder worden uitgewerkt in de ontwerpfase.
- **Het implementeren van VLAN's voor het logisch scheiden van netwerkverkeer.** Het implementeren van VLAN's kan op de volgende manieren:
 - **Statische VLAN's.** Met statische VLAN's worden de poorten handmatig op een switch toegewezen door een netwerkbeheerder. Op het moment dat er wijzigingen aan gebracht moeten worden moet er ingelogd worden op de switch om dit aan te passen. Dit maakt het beheer omslachtig en complex. Door de lagere kosten zal ik statische VLAN's toch opnemen in ontwerp 1.

Voordelen	Nadelen
Kosten; Minder investering nodig alleen switches die statische VLAN's ondersteunen.	Flexibiliteit; Beheer is complex, doordat bij iedere wijziging een netwerkbeheerder ingeschakeld moet worden.
	Veiligheid; Door kabels om te wisselen kan er van VLAN's gewisseld worden
	Betrouwbaarheid; geen Host Checker

Tabel 17: Statische VLAN's

- **Dynamische VLAN's.** Met dynamische VLAN's worden VLAN's toegewezen aan de hand van een gebruiker en/of MAC-adres van een apparaat. Dit geeft veel flexibiliteit aan de ICT-afdeling en organisatie, omdat gebruikers makkelijk kunnen verplaatsen binnen het bedrijf. Tevens geeft het de mogelijkheid om een VLAN over meerdere vestigingen te verspreiden. Het voornaamste nadeel is de hogere investering in netwerkapparatuur die dit met zich meeneemt. Dynamische VLAN's worden uitgewerkt in ontwerp 2.

Voordelen	Nadelen
Flexibiliteit; Centraal beheer van VLAN's en flexibel voor de organisatie	Kosten; Switches die dynamische VLAN's ondersteunen en RADIUS-server nodig
Veiligheid; VLAN toewijzen per gebruiker en/of MAC-adres i.p.v. netwerkpoort	Betrouwbaarheid; geen Host Checker

Tabel 18: Dynamische VLAN's

- **Network Access Control (NAC¹⁸)**. Wanneer een computer verbinding maakt met een computer-netwerk, is het niet toegestaan direct toegang te verkrijgen tot het netwerk. Het moet voldoen aan een gedefinieerd beleid van het bedrijf, zoals het anti-virus beschermingsniveau, systeemupdate niveau en configuratie. De computer wordt gecontroleerd door een vooraf geïnstalleerde software-agent en een systeem kan alleen toegang krijgen tot bronnen die kunnen het systeem herstellen op het geëiste niveau. Zodra aan het beleid is voldaan krijgt het systeem toegang tot netwerkbronnen en het Internet afhankelijk van de beleidsgebieden van het NAC-systeem. NAC wordt voornamelijk gebruikt voor endpoint health checks (Host Checker), maar het wordt vaak gekoppeld aan Role Based Access. Toegang tot het netwerk zullen worden gegeven volgens het profiel van de persoon en de resultaten van de health check.

Voordelen	Nadelen
Flexibiliteit ; Centraal beheer van VLAN's en flexibel voor de organisatie	Kosten ; Switches die dynamische VLAN's ondersteunen en NAC/RADIUS-server nodig
Veiligheid ; VLAN toewijzen per gebruiker en/of MAC-adres i.p.v. netwerkpoort	
Betrouwbaarheid ; Host Checker	

Tabel 19: Network Access Control

- **Implementeren dynamische VLANs + NAC**. Ik heb de afwegingen in tabel 20 gezet en daaruit kom ik tot de conclusie dat dynamische VLAN + NAC, de beste mogelijkheid is om te implementeren. Dit is gerelateerd aan de onderstaande eis:
 - **Beheer eenvoudig houden.**

VLAN	Kosten	Flexibiliteit	Veiligheid	Betrouwbaarheid	Totaal
Statisch	+	-	-	-	-2
Dynamisch	+/-	+	+	-	1
Dynamisch + NAC	-	+	+	+	2

Tabel 20: Vergelijking VLAN's

- **Hardware selecteren**. De BOAL Group heeft aangegeven dat de voorkeur uitgaat naar Juniper apparatuur. In de toekomst willen ze dit graag tot standaard verheffen. Ik heb onderzocht of deze voorkeur consequenties heeft voor mijn ontwerp. Aan de onderstaande eisen moeten de switches minimaal voldoen:
 1. **Fiber 24 of 48x PoE+**, Power over Ethernet (PoE) nodig anders moeten er power injectors gebruikt gaan worden bij VoIP telefoons en dat is kosten verhogend.
 2. **802.1x**, een standaard voor het gebruik van NAC
 3. **VoIP VLAN**, het accepteren van tagged Ethernet pakketten. Nodig voor VoIP
 4. **Router On A Stick (ROAS)**, VLAN's kunnen op de switch gerouteerd worden, wat extra verkeer scheelt door de rest van het netwerk.
 5. **QoS**, Quality of Service om verkeer te prioriteren
 6. **Port security**, om de acces poorten op een switch te beveiligen tegen aanvallen, die in het definitierapport zijn beschreven.
 7. **LLDP-MED¹⁹**, Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and PoE power management) etc.

Access switches	1	2	3	4	5	6	7	Prijs
Juniper EX2200-48P	+	+	+	+	+	+	+	€ 2533,-
Cisco 2960S	+	+	+	-	-	+	+	€ 2943,-
HP ProCurve 2910al	+	+	+	+	-	+	+	€ 3060,-

Tabel 21: Vergelijken switches

Uit tabel 22 blijkt dat de Juniper EX2200 switch de beste keuze is, wat inhoudt dat de Juniper switches aan de eisen voldoen en de minste investering is. De volgende eis is hierop van toepassing:

- **Geen desinvestering**, i.c.m. het verplicht gebruik van Juniper producten.

¹⁸ Bron: [NAC](#)

¹⁹ Bron: [LLDP-MED](#)

- **Servicecontracten uitzoeken.** Bij het aanschaffen van apparatuur wordt, binnen de BOAL Group, standaard een servicecontract (SLA) afgesloten. Deze contracten zijn in verschillende varianten af te sluiten (zie tabel 22), gebaseerd op de responsetijd van de leverancier. Het contract met de snelste responsetijd is 4 uur wat voor de BOAL Group een lange tijd is, omdat de productie 24/7 draait. Door geen service contract te nemen en 2 switches te kopen i.p.v. 1 is het over een aantal jaar gezien goedkoper. De PLC's hebben maar één netwerkaansluiting en zijn niet redundant uitvoerbaar. Door de switches naast elkaar te plaatsen, kan een medewerker van de technische dienst de UTP kabels van switch veranderen, bij uitval van de "hoofd" switch en zo kan er direct weer doorgewerkt worden, nagenoeg zonder downtime.

Product	Prijs	4 uur onsite	Next business day onsite	opsturen 10 dagen
Juniper EX2200-24T-4G	€ 899	€ 399	€ 229	€ 49
	5 year	€ 2.894	€ 2.044	€ 1.144

Tabel 22: SLA, jaarlijkse prijzen

Ontwerp 1 (figuur 12)

Voordelen:

- Kostenbesparing door het gebruik van statische VLAN's.

Nadelen:

- Complex beheer en slechte flexibiliteit door statische VLAN's
- Veiligheid, er kan gemakkelijk van VLAN gewisseld worden door kabels te wisselen.
- Afhankelijk van router van Verizon als gateway.

Ontwerp 1	aantal	prijs	totaal
Juniper EX2200-24T-4G	8	€ 899	€ 7.192
Juniper EX2200-48P-4G	8	€ 2.533	€ 20.264
JX-SFP-1GE-SX Modules	18	€ 173	€ 3.114
bestaande apparatuur			
Juniper EX2200-24T-4G	4	-€ 899	-€ 3.596
Juniper EX2200-48P-4G	1	-€ 2.533	-€ 2.533
Juniper SFP modules	8	-€ 173	-€ 1.384
Glasvezel plaatsen	1	€ 9.855	€ 9.855
		Totaal:	€ 32.912

Tabel 23: Kosten ontwerp 1

In ontwerp 2 ik voor andere core switches gekozen met een hogere capaciteit en meer technische functies. Dit is de Juniper EX4200 geworden, omdat deze over volwaardige router functionaliteiten beschikt en door deze redundant uit te voeren, vormen ze samen een Virtual Chassis²⁰. Met Virtual Chassis geactiveerd vormen deze switches één virtuele switch, waarbij de backplane, tussen de switches, een capaciteit heeft van 128Gb/s. Zoals in figuur 12 te zien is kunnen alle servers aan gesloten worden op de core switches, wat extra switches bespaard.

Ontwerp 2 (figuur 12)

Voordelen:

- Eenvoudig beheer en flexibiliteit door dynamische VLAN's
- Capaciteit van Core switches vele malen hoger door Virtual Chassis
- LAN netwerk wordt onafhankelijk van Verizon

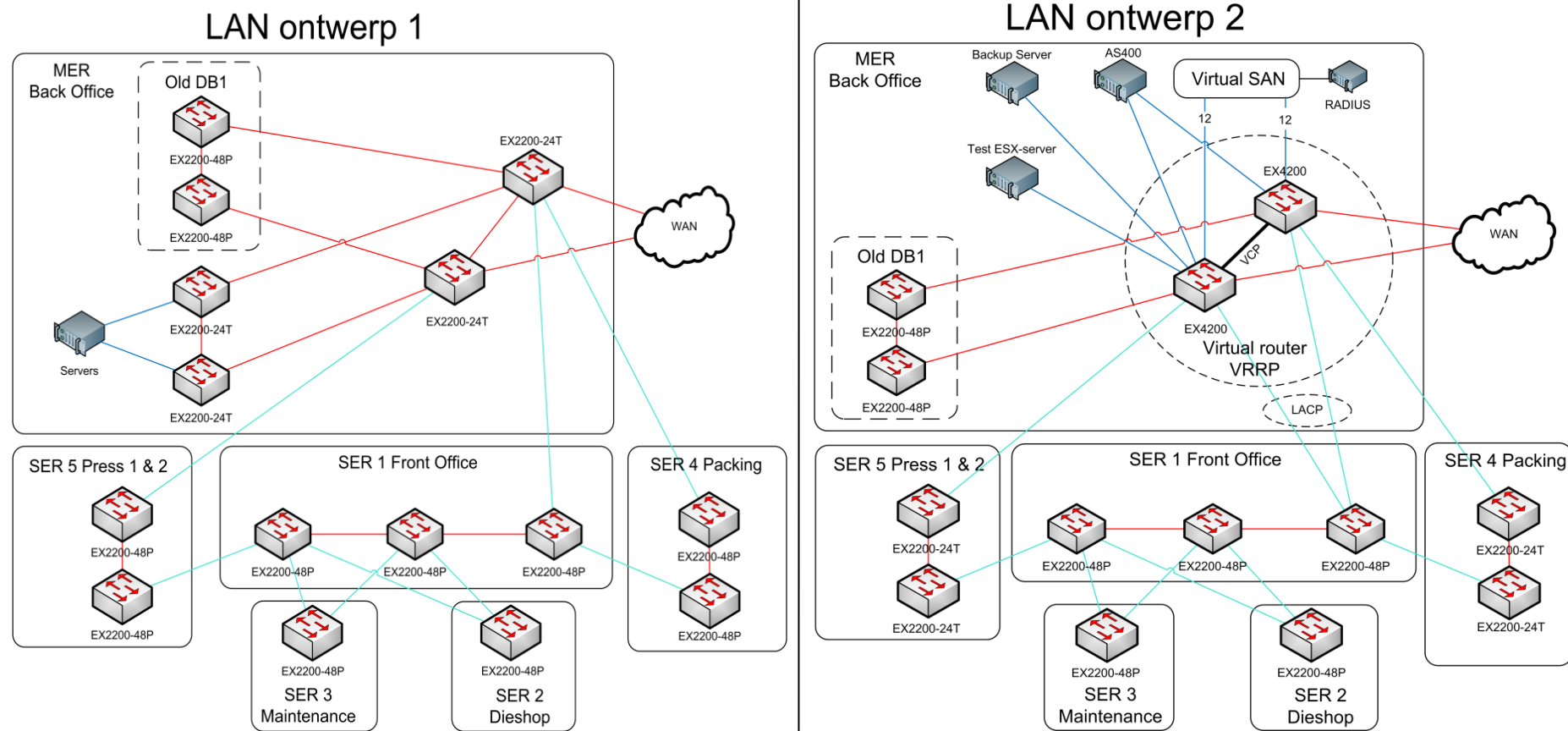
Nadelen:

- Hogere kosten dan ontwerp 1.

Ontwerp 2	aantal	prijs	totaal
Juniper EX4200 VCP	2	€ 3.463	€ 6.926
Uplink module 4x 1GB SFP EX4200	2	€ 1.134	€ 2.268
Juniper EX2200-24T-4G	4	€ 899	€ 3.596
Juniper EX2200-48P-4G	8	€ 2.533	€ 20.264
JX-SFP-1GE-SX Modules	19	€ 173	€ 3.287
bestaande apparatuur			
Juniper EX2200-24T-4G	4	-€ 899	-€ 3.596
Juniper EX2200-48P-4G	1	-€ 2.533	-€ 2.533
Juniper SFP modules	8	-€ 173	-€ 1.384
Glasvezel plaatsen	1	€ 9.855	€ 9.855
		Totaal:	€ 38.683

Tabel 24: Kosten ontwerp 2

²⁰ Bron: [Virtual Chassis](#)



Figuur 12: Ontwerpen LAN netwerk

Risicoanalyse uitvoeren

Aan de hand van onderstaande eis, heb ik de risicoanalyse opnieuw uitgevoerd op ontwerp 2 van het LAN netwerk, omdat dit naar mijn mening het beste ontwerp is voor de BOAL Group.

- **Hogere beschikbaarheid garanderen**

In tabel 25 is de risicoanalyse uitgevoerd op het LAN netwerk. Uit de risicoanalyse blijkt dat door bepaalde apparaten redundant uit te voeren, het risico aanzienlijk verminderd wordt.

Risicoanalyse BOAL Profielen De Lier LAN										Switches/Routers
Id	Device	Impact	MTBF (hou)	Age (year)	T.	Chance	F	Chance	Risk	Description
1	Juniper SRX240H	840	153000	0,20	43800	25,14%	2	6,32%	53	MER back office KPN main
2	Juniper SRX240H	840	153000	0,20	43800	25,14%	2	6,32%	53	MER back office KPN backup
17	Cisco 1921	840	189000	4,20	43800	25,01%	2	6,25%	53	MER back office router verizon
18	Cisco 887	840	189000	4,20	43800	25,01%	2	6,25%	53	DB1 back office backup router verizon
5	Juniper MAG6610	702	707000	0,20	43800	6,02%	1	6,02%	42	MER back office SSLVPN & UAC
3	Juniper EX4200	840	189000	0,20	43800	20,86%	2	4,35%	37	MER back office Core switch
4	Juniper EX4200	840	189000	0,20	43800	20,86%	2	4,35%	37	MER back office Core switch
8	Juniper EX2200-24T	416	145000	0,60	43800	26,91%	2	7,24%	30	SER 5 press 1 & 2 switch
9	Juniper EX2200-24T	416	145000	0,20	43800	26,34%	2	6,94%	29	SER 5 press 1 & 2 backup switch
6	Juniper EX2200-48P	82	145000	0,60	43800	26,91%	1	26,91%	22	MER back office switch for clients
10	Juniper EX2200-48P	51	145000	0,20	43800	26,34%	1	26,34%	13	SER 1 front office switch
11	Juniper EX2200-48P	40	145000	0,20	43800	26,34%	1	26,34%	11	SER 1 front office switch
15	Juniper EX2200-24T	132	145000	0,60	43800	26,91%	2	7,24%	10	SER 4 Packing switch
13	Juniper EX2200-48P	35	145000	0,20	43800	26,34%	1	26,34%	9	SER 3 maintenance switch
14	Juniper EX2200-48P	35	145000	0,20	43800	26,34%	1	26,34%	9	SER 2 dieshop switch
16	Juniper EX2200-24T	132	145000	0,20	43800	26,34%	2	6,94%	9	SER 4 Packing switch
7	Juniper EX2200-48P	32	145000	0,20	43800	26,34%	1	26,34%	8	MER back office switch for clients
12	Juniper EX2200-48P	13	145000	0,20	43800	26,34%	1	26,34%	3	SER 1 front office switch
Average:									27	

Tabel 25: Risicoanalyse LAN ontwerp

7.2 Maken van een globaal WAN ontwerp

Wens/eis

- Het WAN geschikt maken voor videoconferentie en VoIP.
- Het WAN netwerk moet snel genoeg zijn voor het ERP systeem
- Lokaal internetverkeer direct bij een vestiging het internet op

Concrete specificaties

- WAN verkeer scheiden om het huidige netwerk te ontlasten en een verbinding moet gekozen worden met ruimte op expansie. Tevens moet de lokale provider Quality of Service (QoS) accepteren.

Wens/eis

- Geen desinvestering.

Concrete specificaties

- Hardware selecteren met ruimte voor expansie.

Mogelijkheden van WAN

Bij het ontwerp van het WAN ben ik als eerste nagegaan wat de behoefte aan bandbreedte is, aan de hand van de eisen en wensen. Dit heb ik met infrastructuur specialist besproken wat het huidige en toekomstige verkeer zal zijn. Aan de hand van dit gesprek kwam ik erachter dat, vanuit de ICT-afdeling, er behoefte is aan het bestanden uitwisselen tussen vestigingen. Tabel 26 geeft de behoefte aan bandbreedte weer en geeft tevens weer welk verkeer behouden moet blijven, bij uitval van de hoofdlijn.

Bandwidth	kbps	sessies	totaal kbps
Management	56	10	560
VoIP	100	15	1500
Videoconferentie	4096	4	16384
ERP (AS400) verkeer	128	4	512
ERP (AS400) synchronisatie	512	1	512
Citrix provisioning	16	50	800
Lotus Notes replication	128	1	128
Remote users	56	100	5600
File transfers ftp/sftp	4096	1	4096
Internet (http/https)	512	10	5120
E-mail	512	1	512
		Totaal:	35724
Bij uitval hoofdlijn		Totaal:	4012

Tabel 26: Behoeftte aan bandbreedte in De Lier

Mijn eerste onderzoek voor het WAN was het upgraden van de huidige lijnen van Verizon. Dit geeft als voordeel dat de huidige infrastructuur behouden kan blijven. Ik heb een offerte aangevraagd bij Verizon, voor het upgraden van de huidige lijnen.

Verizon upgrade	maanden	kosten	totaal
De Lier 50MB + Backup 6Mb	12	€ 3.947	€ 47.364
Gravenzande 30MB + Backup 6Mb	12	€ 3.368	€ 40.416
Moorsele 30MB + Backup 6Mb	12	€ 3.678	€ 44.136
Shepshed 30MB + Backup 6Mb	12	€ 3.598	€ 43.176
		Totaal jaarlijks:	€ 175.092

Tabel 27: Verizon jaarlijkse kosten na upgrade

De voordelen:

- Huidige infrastructuur kan blijven bestaan
- Colocatie kan geëlimineerd worden

De nadelen:

- Kosten gaan met één derde omhoog

Conclusie

Het is voor BOAL geen optie om de lijnen te upgraden en na juni 2014 zal Verizon niet meer gebruikt worden als provider door de BOAL Group. Tot die tijd loopt het contract en moet er rekening gehouden met deze verbindingen. Ik heb ervoor gekozen om twee ontwerpen voor het WAN te maken, zodat de opdrachtgever vooruit kan plannen. Eén voor de periode tot juni 2014 en een ontwerp voor de periode na juni 2014.

Lokale providers

Verizon is een grote internationale (Internet) service provider, maar maakt gebruik van lokale internet providers. Aangezien de glasvezel aansluitingen via een lokale provider zijn gefaciliteerd is het mogelijk om via hen een andere verbinding te realiseren. Door de glasvezel kabel kunnen 6 aderparen aangesloten worden en momenteel wordt er maar één aderpaar gebruikt door Verizon. Ik heb uitgezocht via Oaktree ICT Services²¹, welke lokale providers gebruikt worden door Verizon.

De volgende providers hebben de glasvezelkabels per vestiging liggen:

- De Lier; **KPN**
- 's Gravenzande; **KPN**
- Moorsele; **Belgacom**
- Shepshed; **Britisch Telecom**

Er hoeft geen geld geïnvesteerd te worden in de aanleg van een nieuwe glasvezelkabel, voor de WAN verbindingen. De onderstaande eis is hier van toepassing:

- **Geen desinvestering**

²¹ Bron: <http://www.oaktree-ict.nl/>

Hardware WAN

In de huidige situatie wordt er één firewall gebruikt, omdat al het internetverkeer via de Colocatie het Internet op gaat. Dit gaat volgens de eisen veranderen, wat betekent dat er per vestiging een firewall geplaatst moet gaan worden. Ik heb onderzocht wat de mogelijkheden van een firewall zijn, door met een externe partij, Oaktree ICT Services, overleg te plegen over de te kiezen hardware.

In het kader van de eis “geen desinvestering” is de keuze voor de Juniper SRX²² series voor de hand liggend. De SRX series zijn routers gecombineerd met een firewall, met de mogelijkheid tot clusteren. De Juniper SRX240H is het instapmodel met mogelijkheid tot clusteren en met voldoende capaciteit

Clusteren:

Voordelen:

- Stateful session failover; geen downtime door uitval van één router of lijn.
- Combinatie van router/firewall

Nadelen:

- Hardware moet identiek zijn, daardoor dubbele kosten

Ontwerp 1 (Figuur 13)

Het is een overgangsfase waar de jaarlijkse kosten voor een periode van 1½ jaar zijn.

Voordelen:

- Verizon netwerk wordt ontlast.
- De lijnen zijn ruim genomen, zodat de Colocatie uitgefaseerd kan worden.
- Quality of Service mogelijk over de lokale verbindingen
- Het Verizon netwerk kan uitgefaseerd worden zonder downtime
- De SLA van de providers is gelijk aan dat van Verizon (99,99%)

Nadelen:

- Kosten extra lijnen
- Kosten van een router en firewall
- Beheer van de lijnen ligt bij BOAL

De kosten van de verbindingen heb ik via lokale providers aangevraagd per land.

Ontwerp 1	aantal	t/m juni 2014	
Verizon	12	€ 10.833	€ 129.996
KPN De Lier 100MB	12	€ 986	€ 11.832
KPN 's Gravenzande 100MB	12	€ 986	€ 11.832
Belgacom Moorsele 50MB	12	€ 823	€ 9.876
BT Shepshed 50MB	12	€ 876	€ 10.512
	Totaal jaarlijks:		€ 174.048
Juniper SRX240H	4	€ 2.559	€ 10.236
	Totaal eenmalig:		€ 10.236

Tabel 28: WAN ontwerp 1

²² Bron: [SRX Series](#)

Ontwerp 2 (Figuur 13)

Het ontwerp kan na juni 2014 in gebruik genomen worden

Voordelen:

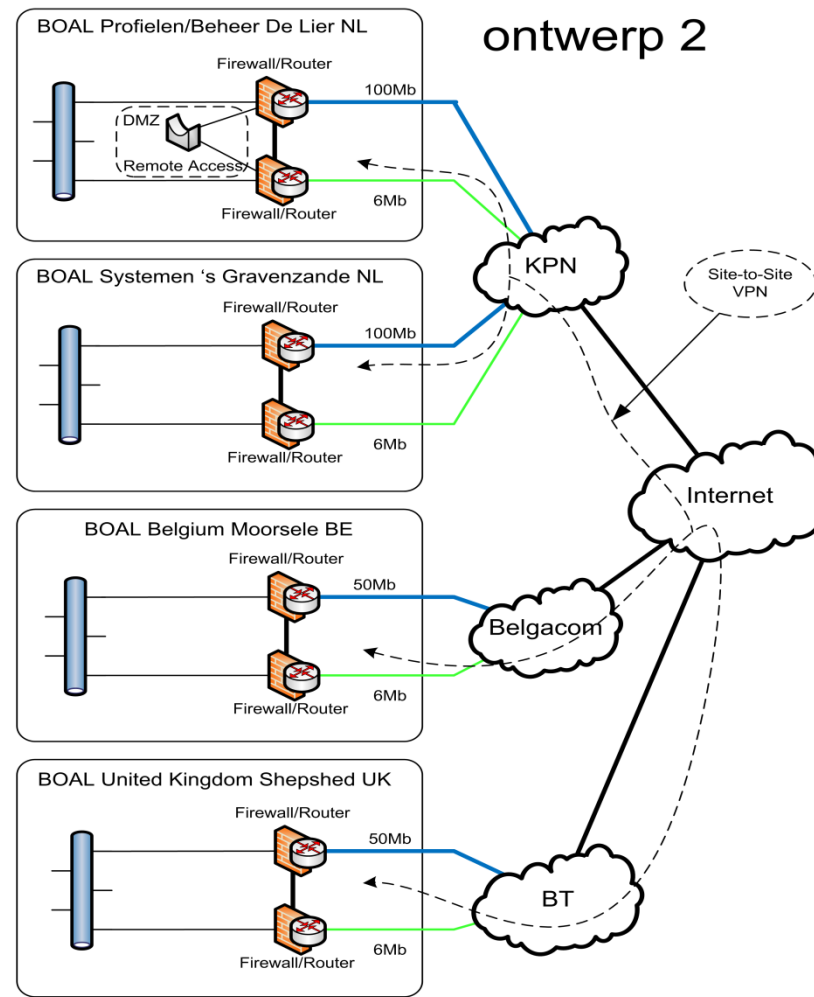
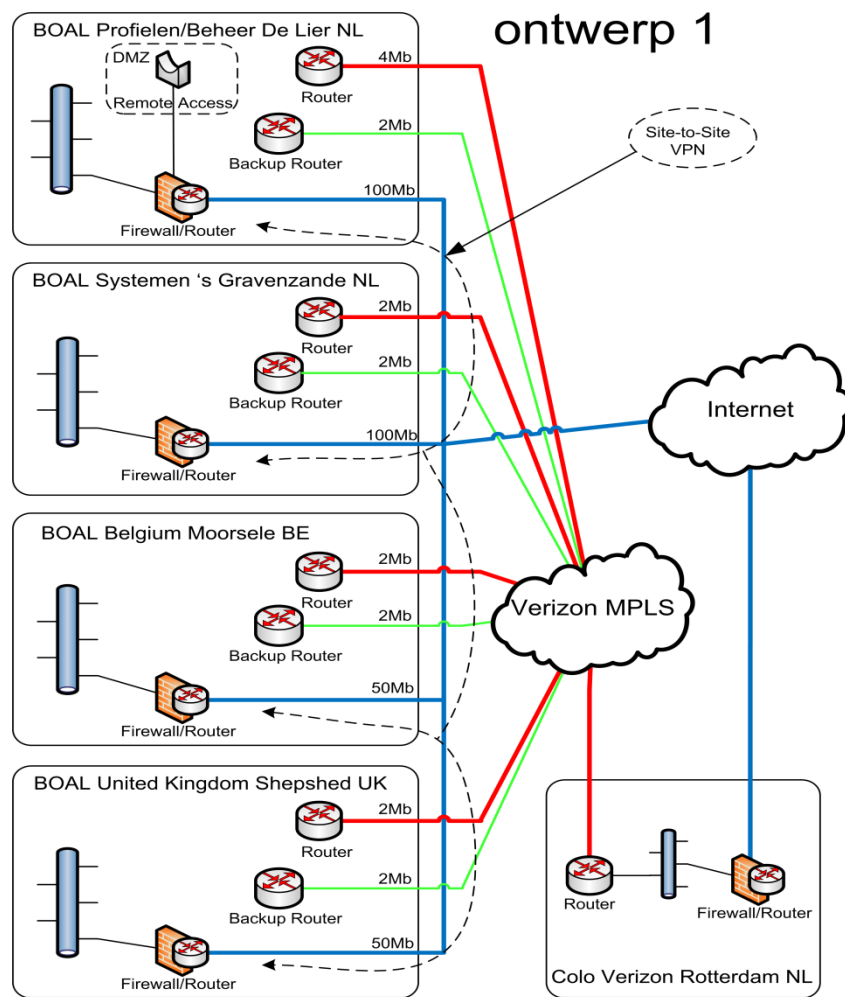
- Kosten zijn gehalveerd t.o.v. de huidige situatie
- Clusteren van de routers, wat de beschikbaarheid ten goede komt.
- De lijnen zijn ruim genomen, zodat de Colocatie uitgefaseerd kan worden.
- Quality of Service mogelijk over de lokale verbindingen
- Het Verizon netwerk kan uitgefaseerd worden zonder downtime
- De SLA van de providers is gelijk aan dat van Verizon (99,99%)
- De verbinding tussen De Lier en 's-Gravenzande heeft genoeg capaciteit, zodat er een mogelijk is om alle servers naar De Lier te verplaatsen, wat een aanzienlijke kostenbesparing kan opleveren.

Nadelen:

- Beheer van het WAN ligt bij BOAL

Ontwerp 2	aantal	vanaf juni 2014	
KPN De Lier 100Mb	12	€ 986	€ 11.832
DSL Backup Line 6Mb	12	€ 193	€ 2.316
KPN 's Gravenzande 100Mb	12	€ 986	€ 11.832
DSL Backup Line 6Mb	12	€ 193	€ 2.316
Belgacom Moorsele 50Mb	12	€ 823	€ 9.876
DSL Backup Line 6Mb	12	€ 234	€ 2.808
BT Shepshed 50MB	12	€ 876	€ 10.512
DSL Backup Line 6Mb	12	€ 223	€ 2.676
		Totaal jaarlijks:	€ 54.168
Juniper SRX240H	4	€ 2.559	€ 10.236
		Totaal eenmalig:	€ 10.236

Tabel 29: WAN ontwerp 2



Figuur 13: WAN ontwerpen

7.3 Voorstel voor remote access

Wens/eis

- Remote Access onderzoeken
- Beheer eenvoudig houden.

Concrete specificaties

- Implementatie van een SSLVPN.

Wens/eis

- Geen desinvestering.

Concrete specificaties

- Implementatie van een SSLVPN gecombineerd met een NAC

Het doel van het onderzoek is om de beheersbaarheid, veiligheid en flexibiliteit te verhogen voor de werknemers, leveranciers en klanten. Die extern inloggen moeten inloggen op het netwerk. Leveranciers eisen ook toegang tot bepaalde delen van het netwerk, om geautomatiseerde productieprocessen te kunnen volgen en storingen kunnen verhelpen. Dit wordt in de huidige situatie gefaciliteerd met een IPSec VPN verbinding via een Citrix Access Gateway.

IPSec VPN

Nadelen:

- Er dient specifieke software op de client te worden geïnstalleerd, wat door ICT-afdeling ondersteund dient te worden.
- Geen Host Checking mogelijk om aan vooraf bepaalde veiligheidseisen te voldoen
- Toegang kan alleen tot een bepaalde IP reeks beperkt worden en niet tot specifieke TCP/UDP poorten.
- NAT problemen met gelijkwaardige subnetten.

SSLVPN

Voordelen:

- Het inloggen wordt via een SSL verbinding tot stand gebracht, wat door alle huidige webbrowsers wordt ondersteund.
- Endpoint health checks mogelijk op de clients om aan vooraf bepaalde veiligheids-eisen van de bedrijfspolicy te voldoen. Software wordt automatisch verspreid op de clients bij login.
- Integratie met LDAP, zoals Active Directory van Microsoft.
- Streamen van applicaties (Web,E-mail etc.) via SSL VPN, zonder directe toegang tot het interne netwerk.

SSLVPN server of een complete oplossing

Ik heb een afweging gemaakt wat voor de ICT-afdeling het beste te implementeren is. De volgende oplossingen zijn mogelijk voor implementatie van een SSLVPN:

- SSLVPN Server
- SSLVPN apparaat, complete oplossing

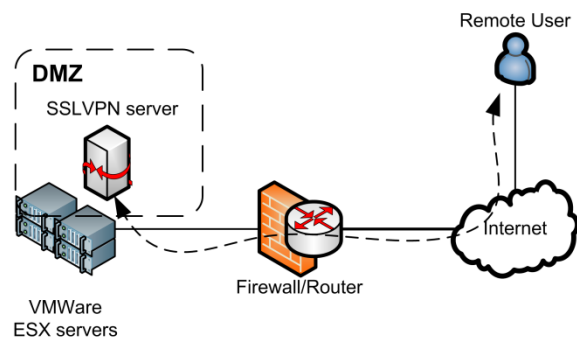
SSLVPN Server (Figuur 14)

Voordelen:

- Geen extra hardware nodig, kan op de ESX servers draaien.

Nadelen:

- Kost meer tijd voor integratie door nieuwe virtuele server installatie.
- DMZ moet direct naar een server wijzen, mogelijk extra risico (zie figuur 14).
- Servers worden extra belast

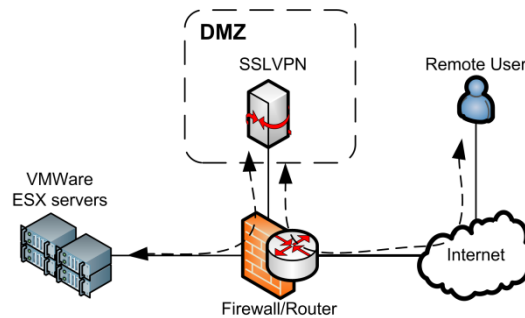


Figuur 14: SSLVPN server

SSLVPN apparaat (complete oplossing figuur 15)

Voordelen:

- DMZ kan buiten de servers blijven, remote user maakt verbinding met SSLVPN niet direct met server (zie figuur 15).
- Snelle implementatie, kan binnen een paar uur operationeel zijn.
- Grote fabrikanten hebben regelmatig updates, zodat de ondersteuning voor een langere periode gegarandeerd blijft. Tevens ondersteuning voor tablets en smartphones d.m.v. Apps.



Figuur 15: SSLVPN

Ik ben hieruit tot de conclusie gekomen dat een complete oplossing ideaal is voor de BOAL Group, omdat de ICT-afdeling niet veel man kracht heeft. Ook met de visie op de toekomst, met de steeds grotere opkomst van tablets en smartphones. Deze conclusie is voortgekomen uit de eis:

- **Beheer eenvoudig houden**

Hardware kiezen

De MAG series²³ van Juniper kunnen voor verschillende functies worden ingezet, zowel als SSLVPN en/of als UAC Unified Access Control (NAC).

Dit komt ten goede aan de volgende aan de volgende eisen:

- **Beheer eenvoudig houden**
- **Geen desinvestering**

SSLVPN / UAC	MAG2600	MAG4610	MAG6610	MAG6611
Functies	SSL VPN or UAC	SSL VPN or UAC	SSLVPN & UAC	SSLVPN & UAC
Maximum gebruikers SSL VPN	100	1000	20000	40000
Maximum gebruikers UAC	250	2500	30000	60000
MTBF in uren	212000	142000	707000	428000
Prijs	€ 759,-	€ 3546,-	€ 5478,-	€ 8569,-

Tabel 30: Juniper MAG series vergelijking

Ik heb gekozen voor de MAG6610, omdat dit apparaat voor alle vestigingen kan dienen en een goede performance kan leveren. Tevens is de MTBF hoog en dat zou een goede beschikbaarheid moeten geven.

De keuze komt voort uit de volgende eisen:

- **Remote Access onderzoeken**
- **Geen desinvestering**
- **Beheer eenvoudig houden**

²³ Bron: [Juniper MAG series](#)

7.4 Bespreken van de ontwerpen

Aan de hand van de voorgestelde opties heb ik met mijn opdrachtgever de opties afgewogen. Hieruit is een selectie gemaakt uit de ontwerpen van het LAN en WAN netwerk, die verder uitgewerkt zullen worden in de volgende fasen, met als uiteindelijk doel de implementatie.

Selectie LAN netwerk ontwerp

Het LAN ontwerp is geselecteerd aan de hand van de opgestelde wensen en eisen. Aangezien LAN ontwerp 2 aan alle eisen voldoet is de keuze op dit ontwerp gevallen. De hogere kosten die dit ontwerp met zich meebrengt zijn van ondergeschikt belang aan het eenvoudige beheer, die de dynamische VLAN's met zich meebrengen.

Selectie WAN netwerk ontwerp

Het WAN ontwerp is geselecteerd aan de hand van de beperking die vanuit het contract met Verizon gelden. Aangezien het contract met Verizon pas in 2014 opgezegd kan worden is er gekozen voor de implementatie van ontwerp 1. Na deze datum zal de BOAL Group overstappen op ontwerp 2.

Selectie SSLVPN

Het voorstel aan de opdrachtgever en infrastructuur specialist, om een gecombineerde vorm van een SSLVPN en UAC te gebruiken, is positief ontvangen. Het zal het beheer, flexibiliteit en veiligheid van het netwerk verhogen. De extra kosten van een SSLVPN en UAC worden terugverdiend, door een tijdsbesparing aan de beheerskant, wat door de opdrachtgever wordt toegejuicht.

7.5 Scherpstellen eisen en wensen

In overleg met mijn opdrachtgever hebben we besloten dat de eisen en wensen dusdanig gedetailleerd en bruikbaar zijn uitgewerkt, dat verder scherpstellen niet nodig is. Op basis van de architectuurfase zijn er geen wensen of eisen bijgekomen waar ik rekening mee moet houden.

7.6 Opleveren van architectuurrapport

Het architectuurrapport bevat een uitwerking van alle onderwerpen die in de architectuurfase aan bod zijn gekomen. Ik heb het architectuurrapport laten goedkeuren door mijn opdrachtgever alvorens de faseovergang naar de ontwerpfase te doen. Het architectuurrapport dient hiermee formeel als input voor de volgende fasen. Tevens vervul ik met het architectuurdokument een aantal eisen van mijn opdracht:

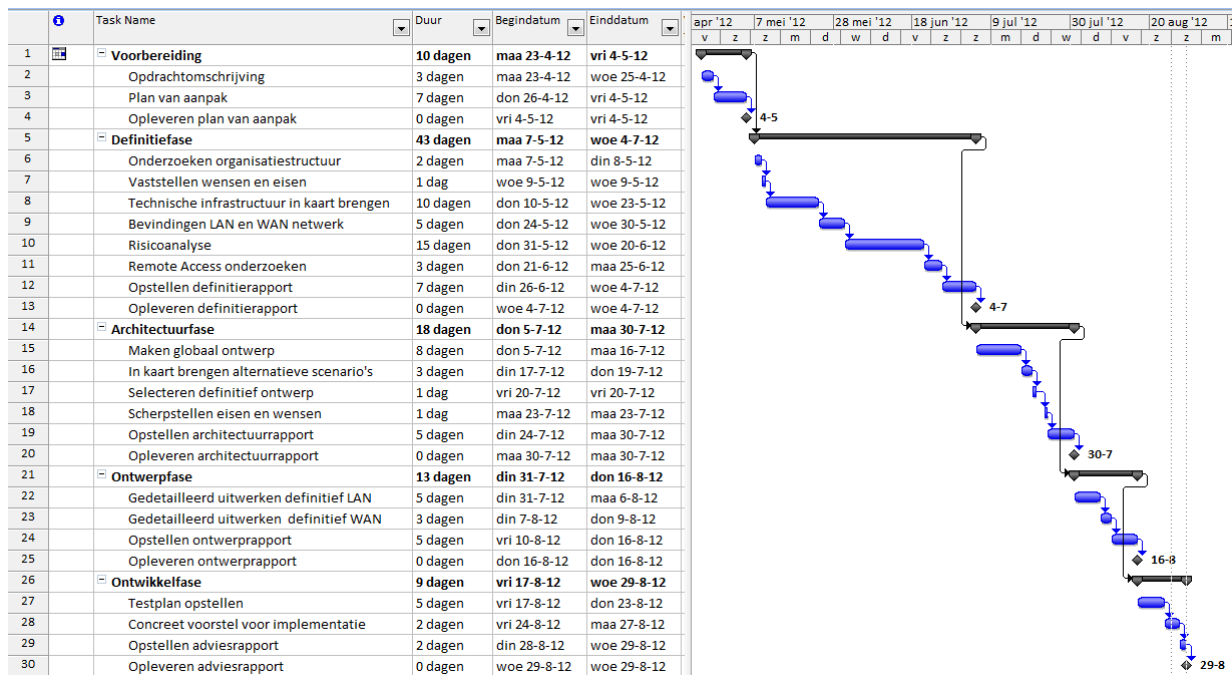
- **Hogere beschikbaarheid garanderen**
- **LAN netwerk scheiden**
- **Het WAN netwerk moet voldoende capaciteit hebben voor de synchronisatie van het ERP systeem**
- **Internetverkeer, bij een vestiging, het internet op via lokale provider**
- **Remote Access onderzoeken**
- **Geen desinvestering**
- **Beheer eenvoudig houden**

De volgende eisen vervul ik gedeeltelijk:

- **Het netwerk geschikt maken voor videoconferentie en VoIP**
- **Het netwerk geschikt maken voor wireless**

7.7 Planning bewaken

Tijdens de architectuurfase heb ik de planning bewaakt en gekeken of ik op schema lig. Ik heb hier geconcludeerd dat ik 2 dagen ben ingelopen op het maken van de globale ontwerpen. Dit geeft me weer wat speling voor de volgende fasen.



Figuur 16: Bijgewerkte planning n.a.v. architectuurfase

8. Fase 3: De ontwerpfase

In de ontwerpfase voer ik de volgende activiteiten uit:

- Het gedetailleerd uitwerken van het definitieve LAN ontwerp.
- Het gedetailleerd uitwerken van het definitieve WAN ontwerp.
- Selectie van toe te passen producten.
- Het opleveren van een ontwerprapport met de uitwerking van bovenstaande punten.

8.1 Het LAN netwerk gedetailleerd uitwerken

De opdrachtgever heeft uit de architectuurfase voor het tweede ontwerp gekozen. De core switches worden de Juniper EX4200 die tezamen een Virtual Chassis vormen.

Het LAN netwerk onafhankelijk maken van Verizon

De core switches hebben een volwaardige router functionaliteit. Ik heb ervoor gekozen om de Virtual Chassis tezamen een virtuele router te laten vormen. Een virtuele router heeft als voordeel dat op het moment van uitval van één van de twee fysieke routers, de andere de taken overneemt. Dit is mogelijk via de protocollen die in tabel 31 vergeleken worden.

- **HSRP**; Hot Standby Router Protocol
- **VRRP**; Virtual Routing Redundancy Protocol
- **GLBP**; Gateway Load Balancing Protocol

	HSRP	VRRP	GLBP
Standard	RFC 2281	RFC 3768	Cisco
Load Balancing	No	No	Yes
IPv6 Support	Yes	No	Yes
Transport	UDP/1985	IP/112	UDP/3222
Default Priority	100	100	100
Default Hello	3 sec	1 sec	3 sec
Multicast Group	224.0.0.2	224.0.0.18	224.0.0.102
Proprietary	Cisco	None	Cisco

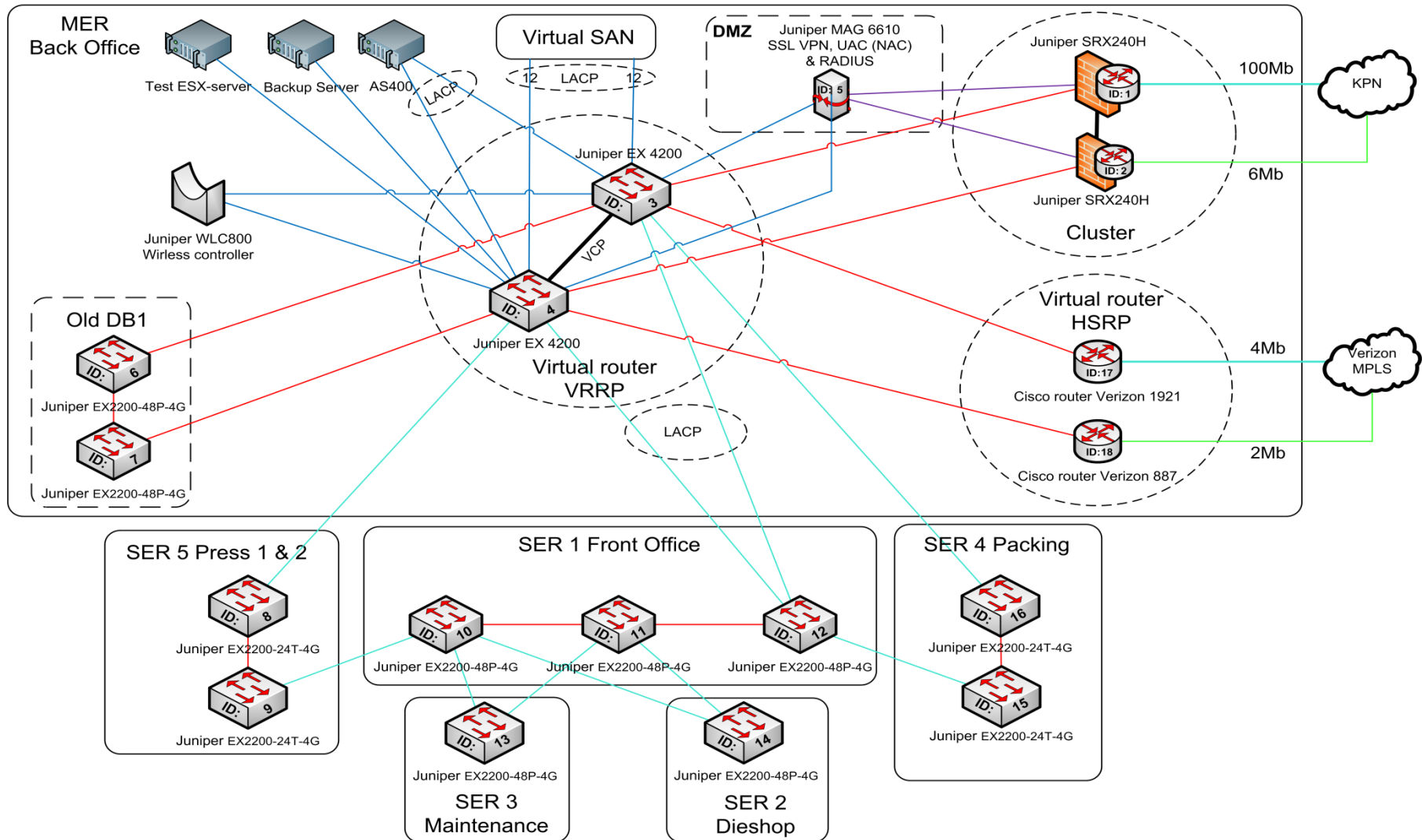
Tabel 31: Virtual router protocollen

Er is op het moment van schrijven geen keuze om een ander protocol te kiezen dan het VRRP protocol. Dit komt doordat de HSRP en GLBP protocollen alleen door de apparatuur van Cisco te gebruiken zijn.

De nadelen van VRRP (het gebrek aan load balancing en IPv6 support) vormen geen probleem, omdat de load balancing wordt opgevangen door de Virtuele Chassis. Er is momenteel geen enkele reden om, binnen 5 jaar, IPv6 te implementeren, wat inhoudt dat de nadelen geen beperkende factor zijn.

Voor alle netwerkapparatuur wordt de gateway de virtuele router, zoals in figuur 17 te zien is. Zo wordt het LAN netwerk onafhankelijk gemaakt van Verizon.

BOAL Profielen De Lier LAN



Figuur 17: Gedetailleerd LAN ontwerp

Verkeer scheiden

Aangezien de Juniper EX4200 switches de gateway vormen voor het LAN netwerk, moeten deze het verkeer gaan scheiden. Firewall Filter Matching²⁴ geeft de mogelijkheid om het verkeer te scheiden op basis van een policy. Ik heb het type netwerk verkeer bepaald en in tabel 32 wordt weergegeven welke route genomen moet worden op basis van de policy.

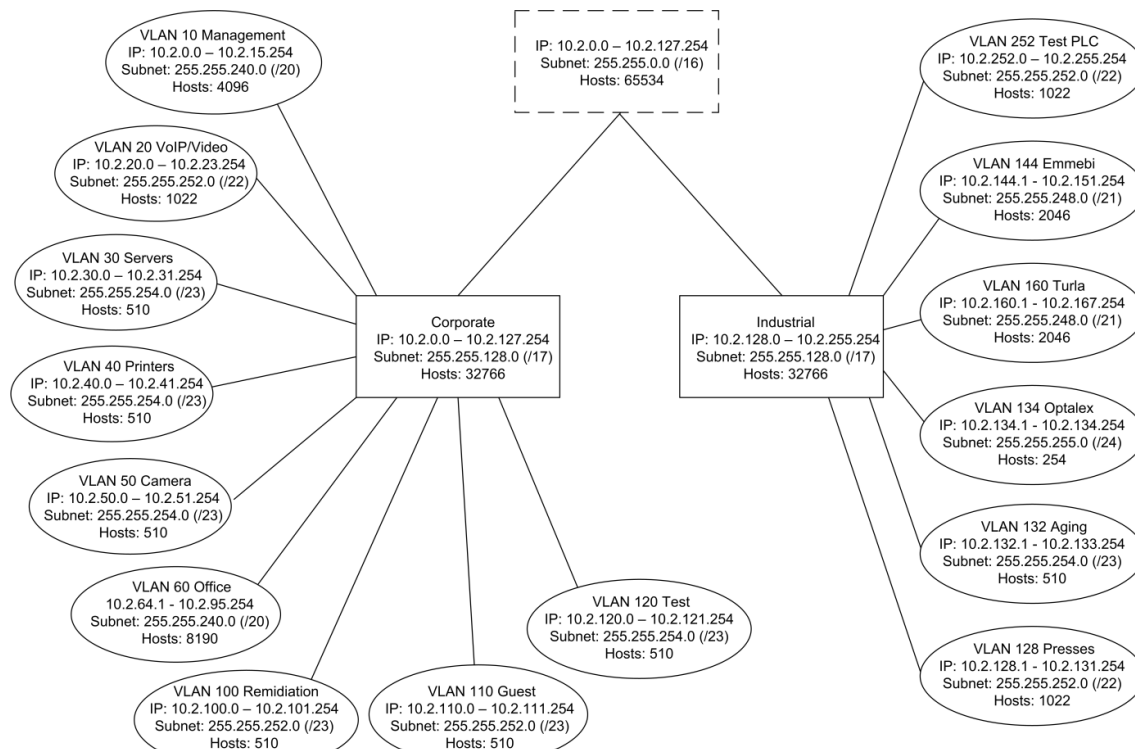
	policy	Verizon	Lokale provider
Management	tcp port rdp		x
VoIP	VLAN		x
Videoconferentie	VLAN		x
ERP (AS400) verkeer	tcp port 23	x	
ERP (AS400) synchronisatie	tcp port 23	x	
Citrix provisioning	tcp port 1433	x	
Lotus Notes replication	tcp port 1352	x	
File transfers ftp/sftp	tcp port 21 & 22		x
Internet (http/https)	tcp port 80/443/8080		x
E-mail	tcp port 25		x

Tabel 32: Policy WAN verkeer

VLAN's ontwerpen

Het definiëren van de VLAN's is een belangrijk onderdeel van het nieuwe ontwerp. Een goede kennis van het netwerk en de verschillende apparaten die op het netwerk zijn aangesloten is hierbij onmisbaar. Hierdoor heb ik besloten een brainstormsessie te organiseren met mijn opdrachtgever, infrastructuur specialist en de PLC-programmeur.

Tijdens deze sessie hebben bedacht wat de verschillende categorieën zijn, waarin het netwerk in te delen is. Vervolgens hebben we het volledige overzicht van de netwerkapparatuur, uit mijn definitierapport erbij gehaald en zijn we de apparaten gaan verdelen onder de verschillende categorieën. Doormiddel van deze methodiek zijn we tot de volgende verdeling gekomen met de daarbij behorende subnetten, zoals in figuur 18 is af te lezen.



Figuur 18: VLAN's met bijbehorende subnetten

²⁴ Bron: [Juniper Firewall Filter Matching](#)

De VLAN's zijn gekozen, door subnetten te gebruiken, met ruime mogelijkheid tot het uitbreiding van cliënts. Tevens heb ik rekening gehouden met de verschillende (toekomstige) segmenten, waar ook de leveranciers een eigen VLAN hebben gekregen, om aan de volgende eis te voldoen:

- **LAN netwerk logisch scheiden**

Ik heb ervoor gekozen om de VLAN nummers overeen te laten komen met de subnetten, om een eenduidige lijn te houden. Tevens is er tijdens de sessie bepaald welke VLAN's met elkaar moeten communiceren.

VLAN	10	20	30	40	50	60	100	110	120	128	132	134	144	160	252
10	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
20		x													
30	x	x	x	x	x	x	x		x	x	x	x	x	x	x
40			x	x		x									
50			x		x										
60			x			x									
100			x				x								
110								x							
120	x		x						x						
128			x							x					
132			x								x				
134			x									x			
144			x										x		
160			x											x	
252															x

Tabel 33: VLAN's onderlinge communicatie

Op basis van tabel 33, kunnen de Access Lists (ACL) bepaald worden voor de VLAN's. Door het implementeren van een UAC kunnen de Access Lists dynamisch worden toegewezen aan alle access switches. Deze keuze heb ik gemaakt aan de hand van de eis:

- **Beheer eenvoudig houden**

Keuze van VLAN protocol

Met de keuze voor dynamische VLAN's is het nodig om een protocol te kiezen die aan alle switches de VLAN's dynamisch distribueert.

Ik heb onderzocht wat voor een protocollen de Juniper EX2200 ondersteunt in combinatie met UAC. Mijn keuze is beperkt gebleven tot één protocol die door beide apparaten ondersteund wordt.

- **Multiple VLAN Registration Protocol (MVRP)²⁵**

Een bijkomend voordeel van het MVRP in combinatie met UAC is de ondersteuning voor het dynamisch distribueren van RVI's (Routed VLAN Interface²⁶). Via een RVI, van de EX switches, kunnen de VLAN's onderling communiceren op IP niveau. Dit geeft als voordeel dat het onderlinge VLAN verkeer op een switch kan blijven en niet naar de core van het netwerk gestuurd hoeft te worden, wat extra verkeer voorkomt.

²⁵ Bron: [Wikipedia MVRP Protocol](#)

²⁶ Bron: [Routed VLAN Interface](#)

Dynamische VLAN's toewijzen

Het toewijzen van een VLAN, op een switchpoort, kan op onderstaande manieren uitgevoerd worden.

- **MAC-adres;** De VLAN wordt toegewezen op basis van het MAC-adres van een host. Dit wordt gebruikt voor printers, PLC's en andere apparaten waar geen inlog gegevens gebruikt worden. Het risico van deze constructie is het "faken" van een MAC-adres, dit kan door UAC afgevangen worden door het MAC-adres te koppelen aan de apparaat gegevens.
- **Login gegevens van gebruiker;** De VLAN wordt toegewezen op basis van de login gegevens van de gebruiker die inlogt op het netwerk.
- **MAC-adres + Login gegevens;** De VLAN wordt toegewezen op basis van een combinatie van bovenstaande punten.

Alle opties kunnen gebruikt worden met de implementatie van een UAC, maar in de praktijk zullen de bovenste twee opties gebruikt gaan worden. Het is voor de ICT-afdeling teveel werk om alle MAC-adressen van de clients bij te houden.

Deze conclusie is voortgekomen uit de eis:

- **Beheer eenvoudig houden**

Trunk poorten

De poorten die de switches met elkaar verbindingen zullen als Trunk²⁷ poorten. Hierover zal het, zoals eerder is beschreven, MVRP protocol gebruikt worden, om de VLAN's te distribueren.

Ik heb tevens de keuze gemaakt om RSTP te implementeren, om "loops" te detecteren. Er is ook een mogelijkheid tot load-balancing van VLAN's d.m.v. het MSTP (Multiple Spanning Tree Protocol). De implementatie hiervan is complex en bij wijziging van topologie, moet de configuratie opnieuw uitgevoerd worden. Dit komt de beheersbaarheid niet ten goede. Tevens worden de core switches root bridge, daardoor heeft het MSTP protocol in de praktijk weinig effect om de capaciteit te verbeteren.

LACP²⁸

De keuze voor LACP (Link Aggregation Control Protocol) geeft de mogelijkheid tot bundelen van fysieke lijnen tot één (virtuele) lijn met dubbele capaciteit.

- **Capaciteit**
- **Redundantie**

Access poorten

De access poorten, van de access switch, moet beveiligd worden tegen de volgende aanvallen:

- **ARP Attack**
- **MAC Flooding Attack**
- **DHCP Starvation Attack**
- **DHCP Rogue Attack**

Voor meer informatie over deze aanvallen verwijs ik naar het definitierapport, waar deze uitgebreid uitgelegd worden.

Ik heb ook rekening moet houden met de factoren:

- **Tagged VLAN,** De access poorten moeten tagged VLAN ondersteunen, omdat VoIP telefoons VLAN's kunnen toewijzen. Dit is nodig omdat er maar één VLAN per fysieke poort toegewezen kan worden. Met een VoIP telefoon wordt de client aan de telefoon gekoppeld, zodat er per werkplek maar één netwerkpoort nodig i.p.v. twee.
- **RSTP,** Dit moet standaard aangezet worden zodat een gebruiker geen "loop" kan creëren.
- **802.1x,** Dit protocol zorgt voor de communicatie tussen de client en de UAC. Met het gebruik van UAC kan met alle EAP types overweg en het is client afhankelijk. Dit zou bij het testen naar voren komen.

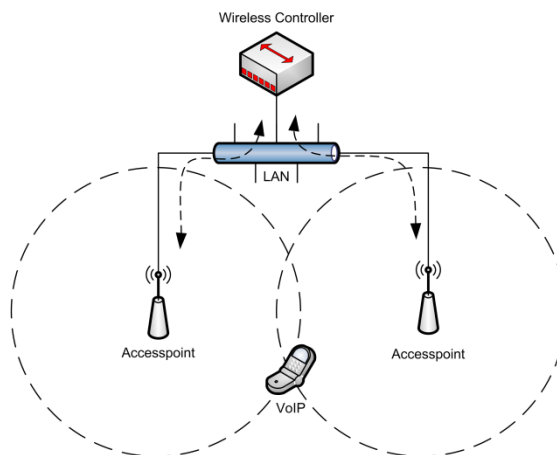
²⁷ Bron: [Trunking](#)

²⁸ Bron: [LACP](#)

Wireless network

Ik ben gebonden aan de keuze van Juniper producten en dit geldt ook voor de wireless apparatuur. Ik heb rekening gehouden met VoIP en WiFi voor draagbare VoIP telefoons en smartphones die via het WiFi verbinding maken. Als er gebruik gemaakt wordt van VoIP i.c.m. WiFi moet er gebruikt worden gemaakt van roaming, zodat de verbinding niet wegvalt als er tussen accesspoints gewisseld wordt (zie figuur 19).

Ik heb de uitgezocht wat de mogelijkheden zijn met Juniper voor het gebruik van accesspoints en wireless controllers.



Figuur 19: Wireless roaming

Tabel 34 geeft de verschillende wireless controllers weer. Mijn keuze is gevallen op de WLC800 controller, omdat deze t/m 128 Access Points aan kan sturen. Dit lijkt een veel te grote raming, maar de wireless controller kan ook op de andere vestigingen Access Points aansturen. De volgende eisen zijn van toepassing op deze conclusie:

- **Geen desinvestering**
- **Beheer eenvoudig houden**

Wireless Controllers	WLC2	WLC8	WLC800	WLC880	WLC2800
Base AP licenses provided	4	12	16	16	64
Maximum AP licenses supported	4	12	128	256	512
Additional license increments	n/a	n/a	16 or 32	16 or 32	64 or 128
Redundant power module standard	-	+	+	+	+
Price	€469,-	€1749,-	€3875,-	€5389,-	€11499,-

Tabel 34: Wireless Controllers

Accesspoints kiezen

Voor het kiezen van een accesspoint heb ik de volgende criteria opgesteld:

- VLAN tagging, Het accesspoint kan Ethernet pakketten aan VLAN's toewijzen.
- Multiple SSID, Er moet een gast en office Wireless komen aangestuurd door UAC
- 2,4GHz & 5GHz, Er moeten verschillende kanalen gebruikt kunnen worden, dit vanwege radio signalen die in de fabriek gebruikt worden, zoals de hijskranen.
- Compatible met WLC880 controller

Door deze eisen ben ik tot één accesspoint gekomen de Juniper AX411. Doordat er gebruik gemaakt wordt van een wireless controller, maakt het niet uit waar in het netwerk de accesspoints geplaatst worden. Ik adviseer ook om een meting te laten uitvoeren i.v.m. de verschillende storingsfactoren die in de fabriek aanwezig kunnen zijn.

Quality of Service op het LAN netwerk

Ik ben voor QoS op het zoek gegaan naar de mogelijkheden waarmee de Juniper apparatuur mee overweg kan. Uit de documentatie van Juniper²⁹ blijkt dat de EX2200 switches momenteel alleen Ethernet pakketten kunnen prioriteren, wat op de Datalink laag (layer 2) wordt uitgevoerd. Het wordt dan geen QoS, maar CoS (Class of Service) waarop de VLAN's prioriteiten krijgen. Ik heb de VLAN's de prioriteiten gegeven die in tabel 35 staan afgebeeld.

Priority	Acronym	Traffic Types	VLAN
0 (lowest)	BK	Background	110
1	BE	Best Effort	40,60,100,120,250
2	EE	Excellent Effort	30,50
3	CA	Critical Applications	128,132,134,160
4	VI	Video, < 100 ms latency and jitter	
5	VO	Voice, < 10 ms latency and jitter	20
6	IC	Internetwork Control	
7 (highest)	NC	Network Control	10

Tabel 35: CoS waarden per VLAN

²⁹ Bron: [Documentatie CoS op EX switches](#)

8.2 Het WAN netwerk gedetailleerd uitwerken

In de architectuurfase is voor ontwerp 1 gekozen, maar in juni 2014 zal ontwerp 2 geïmplementeerd worden. Het LAN en WAN netwerk zijn zo ontworpen dat het Verizon netwerk zonder downtime uitgefaseerd kan worden.

Site to Site VPN

Ik heb voor het opzetten van een Site to Site VPN de handleiding³⁰ van Juniper Networks geraadpleegd, hoe een Site to Site VPN opgezet dient te worden. Op het moment van schrijven is er één manier, om de SRX router/firewall, dit te laten bewerkstelligen en dat is via IPSec VPN.

Dynamische of Statische routing

Ik kies, voor de onderlinge communicatie tussen de vestigingen, voor statische routes, omdat deze routes in de praktijk nooit zullen wijzigen en dit scheelt extra verkeer van een routing protocol³¹ op het WAN netwerk

Quality of Service op het WAN netwerk

Het uitzoeken van QoS via het WAN netwerk is geen gemakkelijke aangelegenheid gebleken. Ik moest achterhalen welke manier KPN, Belgacom en BT onderling kunnen ondersteunen om dit in te voeren. Ik heb contact gehad met KPN International voor de mogelijkheden die er zijn op dit gebied.

Zij kunnen de service tussen de vestigingen leveren, maar alleen met de mogelijkheid van DiffServ³². Tevens moet er voor de verschillende classificaties (zie tabel 36) betaald worden tegelijk met een bepaalde capaciteit aan bandbreedte.

Diffserv is het DS veld in de IP header waarbij prioriteiten aan een IP pakket gegeven kan worden. Het werkt op basis van Per Hop Behaviour (PHB), wat inhoudt dat het pakket per hop (router) opnieuw de prioriteit bekeken wordt en op basis van het DS veld een prioriteit krijgt.

Per Hop Behaviour (PHB)	DiffServ Code Point (DSCP)		
Default	0		
Assured Forwarding	Low Drop Probability	Medium Drop Probability	High Drop Probability
Class 1	AF11	AF12	AF13
	1010	1100	1110
Class 2	AF21	AF22	AF23
	10010	10100	10110
Class 3	AF31	AF32	AF33
	11010	11100	11110
Class 4	AF41	AF42	AF43
	100010	100100	100110
Voice Admit	VA		
	101100		
Expedited Forwarding	EF		
	101110		

Tabel 36: DiffServ classificaties

³⁰ Bron: [handleiding Site to Site](#)

³¹ Bron: [Routing Protocol](#)

³² Bron: [DiffServ](#)

Ik heb ervoor gekozen om aan de hand van de eisen, ten aanzien van de breedte, de toepassingen DiffServ classificaties gegeven (zie tabel 37). De prijzen, per maand per vestiging, staan erbij vermeld. De rest van het verkeer zal de Default classificatie krijgen om over het WAN netwerk te worden getransporteerd.

Toepassing	DSCP	kbps	Prijs p.m.
Management	EF	64	€ 19
VoIP	VA	2048	€ 109
AS400 verkeer	AF41	512	€ 39
AS400 synchronisatie	AF31	512	€ 35
Citrix provisioning	AF21	1024	€ 29
Lotus Notes replication	AF11	256	€ 9

Tabel 37: Gekozen DSCP classificaties

Deze keuze is gebaseerd op de volgende eisen:

- **Het netwerk geschikt maken voor videoconferentie en VoIP**
- **Het WAN netwerk moet voldoende capaciteit hebben voor de synchronisatie van het ERP systeem**

8.3 Selectie van toe te passen producten

Alle kosten heb ik uitgezocht, van zowel de aan te schaffen apparatuur, als de implementatie ervan.

Kosten LAN netwerk

Ik heb de kosten van het LAN netwerk opgevraagd bij de leveranciers van de BOAL Group:

- Connecto networks, voor de bekabeling
- Oaktree ICT services, voor de Juniper apparatuur en implementatie

Kosten LAN netwerk	aantal	prijs	totaal
Juniper EX4200 VCP	2	€ 3.463	€ 6.926
Uplink module 4x 1GB SFP EX4200	2	€ 1.134	€ 2.268
Juniper EX2200-24T-4G	4	€ 899	€ 3.596
Juniper EX2200-48P-4G	8	€ 2.533	€ 20.264
JX-SFP-1GE-SX Modules	19	€ 173	€ 3.287
bestaande apparatuur			
Juniper EX2200-24T-4G	4	-€ 899	-€ 3.596
Juniper EX2200-48P-4G	1	-€ 2.533	-€ 2.533
Juniper SFP modules	8	-€ 173	-€ 1.384
Juniper MAG6610 SSLVPN/UAC	1	€ 5.478	€ 5.478
Licenties SSLVPN & UAC	1	€ 489	€ 489
Juniper WLC800 wireless controller	1	€ 3.875	€ 3.875
Juniper AX Accesspoint	8	€ 399	€ 3.192
Implementeren van het LAN netwerk	1	€ 4.263	€ 4.263
DB1 verplaatsen	1	€ 1.568	€ 1.568
UTP aansluitingen Wifi plaatsen	8	€ 99	€ 792
Glasvezel plaatsen	1	€ 9.855	€ 9.855
Totaal:			€ 58.340

Kosten WAN netwerk

Ik heb de kosten opgevraagd bij de volgende leveranciers

- KPN International, voor de WAN verbindingen
- Oaktree ICT services, voor de Juniper apparatuur en implementatie

De kosten van de periode t/m juni 2014 staan in tabel 38 weergegeven. Er worden er dubbele Juniper SRX240H gekocht, zodat ze geschikt zijn voor het clusteren.

Kosten WAN netwerk	aantal	t/m juni 2014	
Verizon	12	€ 10.833	€ 129.996
KPN De Lier 100MB	12	€ 986	€ 11.832
KPN 's Gravenzande 100MB	12	€ 986	€ 11.832
Belgacom Moorsele 50MB	12	€ 823	€ 9.876
BT Shepshed 50MB	12	€ 876	€ 10.512
SLA Support	12	€ 99	€ 1.188
	Totaal jaarlijks:		€ 175.236
Implementatie WAN	1	€ 3.365	€ 3.365
Juniper SRX240H	8	€ 2.559	€ 20.472
	Totaal eenmalig:		€ 23.837

Tabel 38: Kosten WAN netwerk t/m juni 2014

De kosten van het WAN netwerk na juni 2014 staan in tabel 39 weergegeven.

Kosten WAN netwerk	aantal	vanaf juni 2014	
KPN De Lier 100Mb	12	€ 986	€ 11.832
DSL Backup Line 6Mb	12	€ 193	€ 2.316
DiffServ	12	€ 240	€ 2.880
KPN 's Gravenzande 100Mb	12	€ 986	€ 11.832
DSL Backup Line 6Mb	12	€ 193	€ 2.316
DiffServ	12	€ 240	€ 2.880
Belgacom Moorsele 50Mb	12	€ 823	€ 9.876
DSL Backup Line 6Mb	12	€ 234	€ 2.808
DiffServ	12	€ 240	€ 2.880
BT Shepshed 50MB	12	€ 876	€ 10.512
DSL Backup Line 6Mb	12	€ 223	€ 2.676
DiffServ	12	€ 240	€ 2.880
SLA Support	12	€ 499	€ 5.988
	Totaal jaarlijks:		€ 71.676
Implementatie WAN	1	€ 2.458	€ 2.458
	Totaal eenmalig:		€ 2.458

Tabel 39: Kosten WAN netwerk na juni 2014

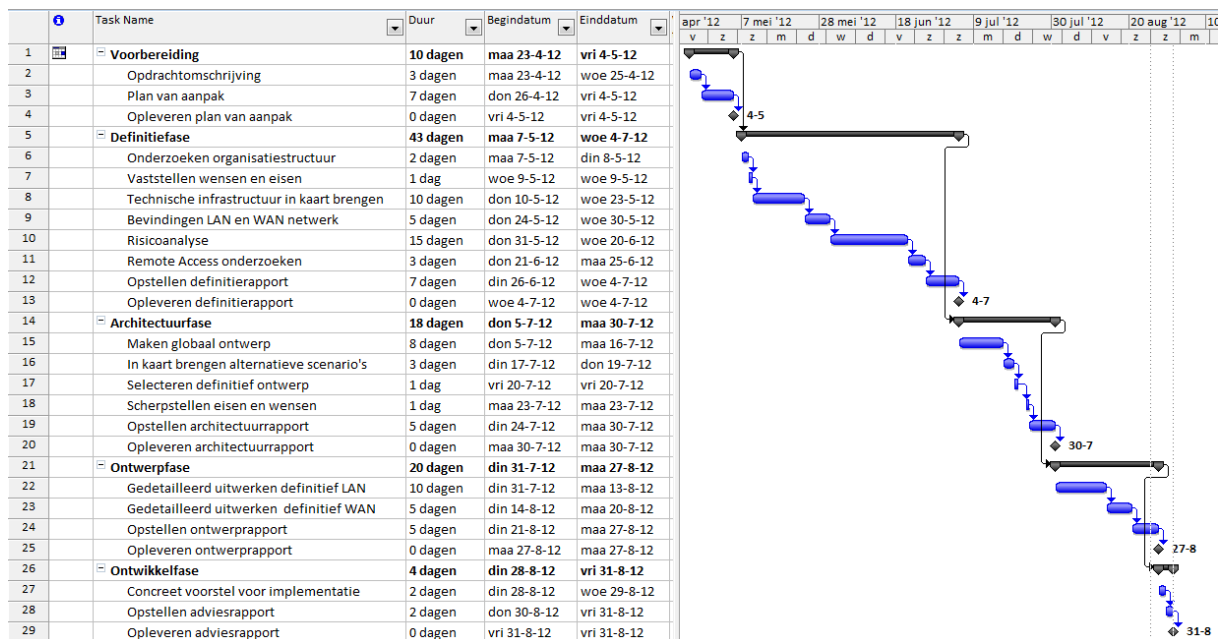
8.4 Opleveren ontwerprapport

Het ontwerprapport bevat een uitwerking van de gedetailleerde ontwerpen die in de architectuurfase aan gekozen zijn. Ik heb het ontwerp rapport laten goedkeuren door mijn opdrachtgever alvorens de faseovergang naar de ontwikkelfase te doen. Het ontwerp rapport dient hiermee formeel als input voor de volgende fasen. Tevens vervul ik met het ontwerp rapport alle eisen van mijn opdracht:

- Hogere beschikbaarheid garanderen
- Het netwerk geschikt maken voor videoconferentie en VoIP
- LAN netwerk scheiden
- Het WAN netwerk moet voldoende capaciteit hebben voor de synchronisatie van het ERP systeem
- Internetverkeer, bij een vestiging, het internet op via lokale provider
- Het netwerk geschikt maken voor wireless
- Geen desinvestering
- Beheer eenvoudig houden

8.5 Planning bewaken

Tijdens de ontwerp fase heb ik de planning bewaakt en gekeken of ik op schema lig. Ik heb hier geconcludeerd dat ik 5 dagen ben uitgelopen op het maken van de gedetailleerde LAN ontwerp en 2 dagen op het maken van het definitieve WAN ontwerp. Dit moet ik compenseren in de ontwikkelfase. Ik heb besloten, dat het maken van een testplan teveel werk is. Volgens het risicolog laat ik het testplan vallen en de opdrachtgever heeft aangegeven dit geen probleem te vinden. De planning heb ik hierop aangepast



Figuur 20: Bijgewerkte planning n.a.v. ontwerpfase

9. Fase 4: De ontwikkelfase

In de Ontwikkelfase voer ik de volgende activiteiten uit:

- Testplan opstellen voor het LAN en WAN netwerk
- Het uitwerken van een concreet voorstel voor de implementatie van het LAN netwerk ontwerp
- Het uitwerken van een concreet voorstel voor de implementatie van het WAN netwerk ontwerp
- Het opleveren van een adviesrapport met de uitwerking van bovenstaande punten

Normaliter wordt het gedetailleerde ontwerp, in de ontwikkelfase, getest. Aangezien er geen apparatuur beschikbaar is om te testen, kan het testen niet uitvoeren. Dit heb ik ook afgebakend in mijn opdracht:

- **De ontwerpen worden niet getest, omdat daar apparatuur voor aangeschaft moet worden. De opdrachtgever geeft mij geen toestemming tot het aanschaffen van de benodigde apparatuur.**

9.1 Testplan opstellen voor het LAN en WAN netwerk

Het is mij niet gelukt om een testrapport te schrijven, die gebruikt kan worden tijdens de implementatie van de ontwerpen. Na de ontwerpfase is gebleken, dat er geen tijd meer was om een testplan op te stellen. Het testplan maken was een wens i.v.m. de kans dat er niet genoeg tijd meer was. Dit is het geval gebleken, wat inhoudt dat het testplan is komen te vervallen, met goedkeuring van de opdrachtgever.

9.2 Advies implementatie ontwerpen

Aangezien er geen testplan gemaakt kan worden, rest mij om het advies te geven, hoe de ontwerpen geïmplementeerd moeten worden. De BOAL Group kan dit advies bij de hand houden, om een planning te realiseren aangaande de implementatie:

- Als eerste advies geef ik aan, dat alle netwerkapparatuur tegelijkertijd aangeschaft moeten worden. Dit i.v.m. de hogere korting die te bedingen is bij de leverancier.

Advies implementatie LAN netwerk ontwerp

Ik heb de keuze gemaakt om het LAN netwerk als volgt te implementeren, omdat dit de logische stappen zijn voor implementatie.

- **De glas- en UTP kabels laten aanleggen binnen de vestiging.** De kabels moeten worden aangelegd om redundantie, onafhankelijkheid en capaciteit te creëren, ten opzichte van de huidige situatie.
- **Testplan LAN opstellen.** Er moet een testplan worden opgesteld, aangezien ik dit niet meer binnen de gestelde tijdsperiode kan voltooien.
- **Alle apparatuur plaatsen en configureren.** De apparatuur voor één maand laten aanstaan, zodat er vanuit gegaan kan worden dat de apparatuur redelijk betrouwbaar is. Dit wordt gedaan om te onderzoeken of de apparatuur blijft werken. Als er uitval van hardware is, wordt dat vaak in de eerste maand duidelijk. Dit advies heb ik van mijn begeleider en infrastructuur specialist gekregen, die in het verleden daar ervaring mee hebben opgedaan. De apparatuur kan naast de bestaande apparatuur geplaatst en geconfigureerd worden. Dit moet door een externe partij gedaan worden, omdat de kennis niet aanwezig is binnen de ICT-afdeling.

- **Testen van de apparatuur en configuraties.** Aan de hand van het testplan kunnen alle functies getest worden. Na het testen moet er een testrapport opgesteld worden om te controleren of het LAN netwerk aan alle eisen voldoet. Indien problemen zich voordoen, moet er naar een oplossing gezocht worden om dit te verhelpen.
- **Implementatie.** Het voordeel, voor de implementatie, is dat er gefaseerd geïmplementeerd kan worden, omdat de huidige apparatuur naast de nieuwe apparatuur actief is. Er kan per segment (VLAN) geïmplementeerd worden, omdat de communicatie op IP niveau beschikbaar blijft.
- **Uitfasen oude apparatuur.** Op het moment dat alles overzet is naar de nieuwe situatie en alles werkt naar behoren, kan de oude apparatuur uitgezet worden en weggehaald worden uit de dataruimtes

Advies implementatie WAN netwerk ontwerp

Ik heb de keuze gemaakt om het WAN netwerk als volgt te implementeren, omdat dit de logische stappen zijn voor implementatie.

- **Verbindingen aanvragen.** Via KPN International de WAN verbindingen aanvragen met een contract voor het gebruik van DiffServ.
- **Testplan WAN opstellen.** . Er moet een testplan worden opgesteld, aangezien ik dit niet meer binnen de gestelde tijdsperiode kan voltooien.
- **Opleveren van de verbinding en configuratie.** Na het opleveren van de verbinden, een extern partij het scheiden van het netwerkverkeer en de IPSec VPN configureren. Dit kan via een de test VLAN getest worden. Tevens moet de firewall geconfigureerd worden.
- **Testen van de apparatuur en configuraties.** Aan de hand van het testplan kunnen alle functies getest worden, zoals de capaciteit van de verbinding en de DiffServ waarden. Na het testen moet er een testrapport opgesteld worden om te controleren of het WAN netwerk aan alle eisen voldoet. Indien problemen zich voordoen, moet er naar een oplossing gezocht worden om dit te verhelpen.
- **Implementatie.** De implementatie kan per segment (VLAN) en service (TCP) geregeld worden zonder downtime.
- **Uitfasen Verizon.** De verbindingen hebben een overlappende periode en er is ruim de tijd om voor te bereiden voor de uitfasering van het Verizon netwerk. De transitie kan zonder downtime verlopen, wat zeer gunstig voor de BOAL Group is.

9.3 Opleveren adviesrapport

Het adviesrapport bevat een uitwerking van de ontwikkelfase. Ik heb het adviesrapport gepresenteerd d.m.v. een informele presentatie, aan de opdrachtgever en infrastructuur specialist. Daarna heeft de opdrachtgever het adviesrapport goedgekeurd. De onderstaande wens kan ik niet vervullen i.v.m. de eerder aangegeven gebrek aan tijd.

- **Testplan opstellen voor het LAN en WAN netwerk**

9.4 Planning bewaken

Ik heb, door het testplan te laten vallen, het adviesrapport binnen de gestelde tijd voltooid. Het is aan de opdrachtgever overhandigd op vrijdag 31 augustus 2012. De opdrachtgever en infrastructuur specialist zijn zeer content met opgeleverde rapporten.

10. Evaluatie

In dit hoofdstuk evalueer ik de producten die aan de opdrachtgever zijn opgeleverd en het proces hoe ik tot deze documentatie ben gekomen. Daarna behandel ik de competenties die ik bij aanvang van de afstudeeropdracht heb gekozen en tot slot evalueer ik de gehele afstudeeropdracht, die ik bij de BOAL Group heb uitgevoerd.

10.1 Product Evaluatie

Ik evalueer in dit hoofdstuk alle producten die ik aan de BOAL Group heb opgeleverd, bestaande uit de volgende producten:

- **Plan van Aanpak**
- **Definitierapport**
- **Architectuurrapport**
- **Ontwerprapport**
- **Adviesrapport**

Plan van Aanpak

Met het maken van het Plan van Aanpak heb ik goed kunnen omschrijven wat de mijn werkzaamheden waren voor mijn afstudeeropdracht en daarop heb ik een planning kunnen maken voor het verloop van de opdracht. De keuze voor de ASI methode hielp mij enorm met het plannen van de op te leveren producten.

Definitierapport

Het definitierapport is zeer uitgebreid geworden en de opdrachtgever is zeer content met dit document, omdat er goed beschreven wordt wat er allemaal “mis” is binnen de huidige situatie. Tevens is er nu inzicht in het netwerk door de oplevering van de LAN en WAN netwerkdiagrammen

Persoonlijk heb ik veel geleerd met het creëren van de risicoanalyse, om de risico's op uitval van de netwerkkaparaatuur weer te geven. Dit gaf mij inzicht dat het niet gemakkelijk is om zo'n analyse te maken, omdat er veel factoren kunnen meespelen om een risico aan een apparaat te geven.

Ik ben van mening dat de kans van uitval een onzekere factor in deze risicoanalyse is. Dit komt doordat de MTBF van een apparaat vaak onrealistisch hoog is, omdat dit getal door de fabrikanten ver boven het afschrijvingstermijn aangegeven. Dit betekent dat er altijd afhankelijkheid is van de kans, terwijl de impact te beïnvloeden is. Voor de opdrachtgever is het “managen” van de impact veel waardevoller, dan de kans van uitval.

De kans had ook met meerdere factoren berekent kunnen worden, maar ik heb een grens moet stellen aan de risicoanalyse. Dit heb ik moeten doen om binnen de gestelde tijd te blijven van mijn opdracht.

Architectuurrapport

Het architectuurrapport is waardevol voor het onderzoeken van mogelijke ontwerpen en de kosten ervan. Hier heb ik veel aan de ASI methode gehad, omdat ik persoonlijk snel geneigd ben naar het maken van een definitief ontwerp om tijd te besparen. Het gaf mij inzicht in het voor een opdrachtgever inzichtelijk wordt gemaakt welke richting het ontwerp heen gaat en of de daarbij behorende kosten, nog in het plaatje van de opdrachtgever passen. Met de risicoanalyse heb ik kunnen aantonen, dat het redundant maken van de netwerkkaparaatuur, het risico op uitval van de complete opstelling drastisch lager ligt

Het onderzoek naar NAC (UAC) en SSLVPN vond ik zeer interessant, doordat ik hiermee nog nooit mee mee in aanraking was geweest.

Ontwerprapport

Met het ontwerprapport heb ik de opdrachtgever een gedetailleerd netwerkdiagram kunnen geven, met de kosten die daarbij gemoeid zijn. Met de implementatie van de nieuwe apparatuur i.c.m. VLAN's en Class of Service, zou het LAN netwerk een flinke "boost" moeten geven. Het WAN netwerk heeft voldoende capaciteit voor de komende jaren en de gebruikers zullen tevreden gesteld worden met de mogelijkheden die dit biedt.

Adviesrapport

Ik heb de ontwerpen niet kunnen testen door het ontbreken van de netwerkapparatuur. Daarin tegen heb ik een wel een advies kunnen geven, hoe de ontwerpen geïmplementeerd moeten worden en wat voor een impact dit heeft op de organisatie. De opdrachtgever was zeer content met het adviesrapport en de ontwerpen zullen aan de hand hiervan geïmplementeerd gaan worden.

10.2 Proces Evaluatie

Projectmethode

Ik heb mijn opdracht ingedeeld aan de hand van de ASI methode. Dit heeft mij in staat gesteld om de opdracht op te delen in een heldere structuur en via een beproefde methodiek naar een eindresultaat toe te werken. Deze structuur sprak mij vooraf dusdanig aan dat ik besloot mijn gehele document op te delen naar de hoofdstukken van de ASI methode.

Gedurende de opdracht heb ik soms moeite gehad het ASI model naar de letter te volgen. Dit kwam doordat de activiteiten in de verschillende fasen enige overlap kennen. Omdat de fasen in mijn opdracht dicht op elkaar zitten heb ik soms het gevoel dat ik dingen dubbel deed. Het beste voorbeeld hiervan zijn de ontwerpen in de architectuurfase. Het detailniveau dat nodig was voor de besluitvorming komt dusdanig overeen met het detailniveau van het uiteindelijke ontwerp, dat ik mij heb afgevraagd waarom ik het uiteindelijke ontwerp niet direct heb gemaakt. Wat echter steeds weer duidelijk werd, is dat de fasering van ASI je dwingt de juiste overwegingen te maken. In grotere projecten zou het gevoel van overlap minder aanwezig zijn, omdat de fasen en de besluitvorming langer zijn.

Al met al ben ik erg tevreden over de structuur die ASI mij geboden heeft en de resultaten die ik daarmee heb kunnen boeken. Mijn opdrachtgever is tevens geholpen met de producten die ik heb afgeleverd en de motivatie die de producten hebben geboden in het maken van het juiste besluit.

Planning

Aan de hand van de ASI methode heb ik ook de planning opgesteld. De grondige voorbereiding waarin ik de opdracht en de uitgewerkte doelstellingen heb opgeknipt in concrete (op ASI gebaseerde) activiteiten, heeft mij in staat gesteld een goede inschatting te maken. Deze inschatting heb ik verwerkt in de initiële planning. Op de planning heb ik gedurende de uitvoer van mijn opdracht gestuurd. Na het einde van iedere fase heb ik een evaluatie gedaan van de planning versus de huidige voortgang.

Over het algemeen kan ik stellen dat ik mijn initiële planning vrij realistisch is geweest. Hier en daar ben ik marginaal uit- of ingelopen maar dit is allemaal binnen de toleranties gebleven. Ook voor mijn opdrachtgever heeft de gestructureerde planning ervoor gezorgd dat mijn voortgang duidelijk inzichtelijk was. De data waarop ik met de rapporten ben bezig geweest waren altijd ruim van te voren bekend, waardoor mijn opdrachtgever nauw betrokken is geweest en de besluitvorming soepel is verlopen. Terugkijkend ben ik erg tevreden over de manier waarop dit is verlopen.

Doelstellingen

De doelstellingen die ik tijdens de voorbereiding heb geformuleerd hebben gediend als uitgangspunt voor mijn opdracht. Dit heb ik gedaan door de doelstellingen te vertalen naar activiteiten, die ik als rode draad in de verschillende hoofdstukken/fasen heb gebruikt. Natuurlijk gaat het uiteindelijk om het behalen van de doelstellingen. De mate waarin ik dit heb behaald heb ik hieronder toegelicht:

- Gezien het niet beschikbaar zijn van de MBO stagiaire zal ik het complete LAN en WAN netwerk in kaart brengen en uitwerken in een topologie tekening.
 - De complete uitwerking hiervan heb ik in de definitiefase uitgevoerd. Dit heeft geresulteerd in een volledige beschrijving van het LAN en WAN in het definitierapport. Deze doelstelling heb ik dan ook volledig behaald.
- Risico's van de opzet van het huidige LAN netwerk van BOAL Profielen in De Lier in kaart brengen.
 - Het uitdiepen van de risico's is één van de meest complexe taken gebleken in de definitiefase. Uiteindelijk heb ik een rekenmodel uitgewerkt dat een goede basis biedt om de vergelijking van de verschillende netwerkapparatuur uit te voeren. Hiermee heb ik de risico's volledig én meetbaar in kaart gebracht. Aan deze doelstelling heb ik dan ook volledig voldaan.
- Onderzoeken in hoeverre de bestaande netwerkverbindingen in staat zijn de gewenste verbindingen te ondersteunen.
 - Doormiddel van het monitoren van de lijnen op het LAN heb ik een goed beeld kunnen vormen van het verkeer dat over de lijnen gaat. Op het WAN ben ik door restricties vanuit mijn opdrachtgever niet in staat geweest het verkeer te monitoren. In plaats daarvan heb ik via ping de responstijden onderzocht. Op het gebied van het WAN heb ik daardoor niet het best mogelijke inzicht kunnen krijgen. Ik vind echter dat de meetresultaten mij voldoende inzicht hebben gegeven, waardoor ik de doelstelling op WAN gebied zo goed als mogelijk heb ingevuld. Op LAN gebied heb ik de doelstelling behaald.
- Onderzoeken naar de mogelijkheden voor het scheiden van het LAN netwerk om de geautomatiseerde productieprocessen niet te verstoren.
 - Het scheiden van het LAN netwerk doe ik doormiddel van VLAN's. De VLAN's heb ik in de architectuur- en ontwerpfase uitgediept en uitgewerkt tot een concreet voorstel. Deze doelstelling heb ik dan ook volledig behaald.
- Verwerken van bovenstaande punten in een advies voor een nieuwe topologie.
 - In de ontwerp- en ontwikkelfase heb ik al mijn bevindingen verwerkt in een voorstel voor een nieuwe topologie. Dit voorstel heeft draagvlak bij mijn opdrachtgever door de nauwe betrokkenheid die hij bij de opdracht heeft gehad. De betrokkenheid heb ik kunnen vergroten door het organiseren van brainstormsessies waarbij mijn opdrachtgever en de betrokken specialist waardevolle input hebben gegeven. Aan deze doelstelling heb ik dan ook volledig voldaan.

10.3 Competenties

De beroepstaken die vanuit mijn opleiding zijn samengesteld geven de competenties aan waaraan ik moet voldoen. In dit hoofdstuk zal ik de mate waarin ik de competenties heb vervuld evalueren. De beroepstaken zijn te vinden in bijlage 6. De competenties waaraan ik moet voldoen zijn:

- A1 - Analyseren van het probleemdomein.
- A3 - Achterhalen van behoeften van belanghebbenden.
- A5 - Opstellen van systeemeisen (requirements).
- C9 - Ontwerpen van een infrastructuur.
- G1 - Praktische aspecten hanteren in (internationale) projecten.

A1 - Analyseren van het probleemdomein

Het analyseren van het probleemdomein heb ik gedaan door in de initiële opdrachtformulering te vertalen naar concrete en meetbare criteria. Dit heb ik gedaan aan de hand van een brainstormsessie met de opdrachtgever en infrastructuur specialist, bij mijn stage bedrijf. Het uitwerken van de probleemstelling heb ik in duidelijke taal gedaan, omdat ik dit het beste vond aansluiten bij de sessie.

Na het uitschrijven van het probleem heb ik de uitwerking getoetst bij mijn opdrachtgever. De probleemstelling is hetgeen waar de hele structuur van mijn document op is gebaseerd. In de definitiefase vertaal ik de probleemstelling naar wensen en eisen. De wensen en eisen vertaal ik in de architectuurfase op hun beurt naar concrete specificaties.

A3 - Achterhalen van behoeften van belanghebbenden

De belanghebbenden binnen de BOAL Group worden vertegenwoordigd door mijn opdrachtgever en de infrastructuur specialist. Ik heb doormiddel van een brainstormsessie de wensen en eisen achterhaald die achter de probleemstelling zaten. Deze wensen en eisen heb ik in verder detail uitgewerkt en laten verifiëren door de twee deelnemers van de sessie.

A5 - Opstellen van systeemeisen (requirements)

Aan de hand van de wensen en eisen heb ik in de architectuurfase een vertaling gemaakt naar concrete specificaties die ik heb verwerkt in de voorgestelde infrastructuur scenario's. Per voorgesteld scenario's heb ik aangegeven op welke manier ik de specificaties verwerkt heb. Waar relevant zijn de specificaties in de ontwerpfase nog verder uitgediept om aan te sluiten op de criteria van competentie *ontwerpen van een infrastructuur*.

C9 - Ontwerpen van een infrastructuur

De infrastructuur is ontworpen aan de hand van de keuze uit twee globale ontwerpen (voor zowel LAN als WAN) in de architectuurfase. De globale ontwerpen heb ik in detail uitgewerkt en voorzien van:

- VLAN's
- IP ranges
- Subnetten
- Network Access Control
- Merk en type netwerkkapparatuur
- QoS
- Remote Access

Aan de hand van het ontwerprapport dat ik heb opgeleverd aan het einde van de ontwerpfase kan de gekozen infrastructuur gerealiseerd worden. In de ontwikkelfase werk ik de verdere voorbereiding uit die nodig is om het ontwerp voor te bereiden voor de implementatie.

G1 - Praktische aspecten hanteren in (internationale) projecten

De opdrachtomschrijving heb ik in zijn geheel uitgewerkt bij het prepareren van de opdracht. Aanleiding, probleemstelling, doelstellingen en resultaten zijn hier uitgeschreven en toegelicht. Aan de hand hiervan heb ik een methodiek gekozen en een plan van aanpak uitgewerkt. De aanpak is gebaseerd op de gekozen methode (ASI) en voorziet in een lijst van concrete activiteiten die ik in de verschillende fasen heb uitgevoerd. Aan de hand van een selectie heb ik de gekozen aanpak geschikt bevonden. Tevens biedt de fasering handvatten om de planning op te baseren, waardoor het voldoende sturingsmogelijkheden biedt.

Aan de hand van de informatie die beschikbaar was aan de start van het project heb ik een risicoanalyse gedaan. De risico's zijn voorzien van een impact, kans en alternatieve maatregel. Aanvullend heb ik de techniek van risicobeheersing per risico toegelicht.

10.4 Tot slot

Tijdens het uitvoeren van mijn opdracht heb ik geleerd ,dat de theorie vaak een ideaal beeld schetst. In de praktijk liggen bepaalde zaken vaak lastiger, dan van te voren geschetst. Dit heeft te maken met financiële middelen en personen waarmee men te maken krijgt.

De opdracht is een bestaand probleem en door het hele traject te doolopen, heb ik een oplossing kunnen bieden aan de BOAL Group. Dit heeft me extra motivatie gegeven om alles zo gedetailleerd mogelijk uit te zoeken en ben zeer content dat de geboden oplossingen tot zijn recht kunnen komen.

Moeilijkheden

In het begin van de opdracht heb ik problemen gehad, met het verkrijgen van informatie, met de infrastructuur specialist. Door te blijven aandringen heeft mij de benodigde informatie gegeven. Bij oplevering van het definitierapport, zag hij in dat het werkt wat ik verrichte wel degelijk nut had en werd de samenwerking sterk verbeterd. Ik heb van dit proces geleerd dat ik me niet zomaar aan de kant moet laten schuiven en door juist te blijven aandringen, de resultaten verbeteren.

Visie

Ik heb veel geleerd van de visie van mijn begeleider, op gebied van risicoanalyse en hoe effectief er met de financiële middelen omgegaan kan worden. Dit is bijvoorbeeld tot uiting gekomen, door niet te kiezen voor een servicecontract, maar een tweede apparaat aan te schaffen. Hiermee worden de kosten verminderd en beschikbaarheid wordt verbeterd.

Ik heb dit als een geheel andere visie ervaren en het heeft mijn kijk op bepaalde aspecten veranderd. Het heeft mijn horizon verbreed in de oplossingen en hoe problemen aangepakt kunnen worden.

Netwerkkaparaatuur

Tijdens de architectuurfase ben ik veel te weten gekomen over de fabrikant Juniper. De Haagse Hogeschool werkt uitsluitend met Cisco apparatuur en Cisco cursussen, terwijl er zich een veel grotere wereld in de netwerkkaparaatuur bevindt. Ik zou aan de opleiding Technische Informatica willen adviseren om ook aandacht aan dit feit te besteden, omdat er vanuit de opleiding een beeld geschetst wordt dat er alleen maar Cisco netwerkkaparaatuur op de wereld bestaat.

Juniper producten hebben over het algemeen dezelfde technische mogelijkheden en zo niet beter. Als extra voordeel is de prijs, die over het algemeen een stuk lager ligt dan vergelijkbare Cisco producten. Ik heb tijdens de opleiding ervaren, dat er nauwelijks aandacht besteed wordt aan de financiële kant van het ontwerpen. Aan de andere kant ben ik me bewust, dat er grens gesteld moet worden, om een opleiding binnen de perken te houden.

Literatuurlijst

Boeken:

- JunOS Enterprise Switching, mei 2009
- JunOS Enterprise Routing, juni 2011

Manuals:

- Verizon
- Juniper:
 - Juniper UAC Admin guide
 - Juniper implementing Virtual Chassis
 - Juniper implementing CoS on EX switches
 - Juniper implementing Firewall Filter Based
 - Juniper implementing Site to Site VPN
 - Juniper implementing VLAN
 - Juniper implementing MSTP
- ASI-rapport

Websites:

www.google.nl
www.youtube.nl
www.wikipedia.com
www.juniper.com
www.cisco.com
www.mitel.com

Bijlagen

Bijlage 1: Plan van Aanpak
Bijlage 2: Definitierapport
Bijlage 3: Architectuurrapport
Bijlage 4: Ontwerprapport
Bijlage 5: Adviesrapport
Bijlage 6: Beroepstaken (competenties)

Figuren

Figuur 1: Extrusie proces.....	7
Figuur 2: Links: aluminium staven bij de oven; Rechts: een matrijs met de vorm van het profiel	7
Figuur 3: Links: De “Puller”; Rechts: de profielen liggen klaar om te worden ingepakt	8
Figuur 4: Bedrijfsstructuur	9
Figuur 5: Organigram BOAL Group.....	10
Figuur 6: Divergeren en convergeren.....	13
Figuur 7: Initiële planning	18
Figuur 8: Netwerkdigram LAN netwerk	25
Figuur 9: Netwerkdigram WAN.....	29
Figuur 10: Kans op uitval berekenen met redundantie	36
Figuur 11: Bijgewerkte planning n.a.v. definitiefase	37
Figuur 12: Ontwerpen LAN netwerk	43
Figuur 13: WAN ontwerpen	49
Figuur 14: SSLVPN server	50
Figuur 15: SSLVPN	51
Figuur 16: Bijgewerkte planning n.a.v. architectuurfase	53
Figuur 17: Gedetailleerd LAN ontwerp	55
Figuur 18: VLAN's met bijbehorende subnetten.....	56
Figuur 19: Wireless roaming.....	59
Figuur 20: Bijgewerkte planning n.a.v. ontwerpfase	64

Tabellen

Tabel 1: Methodieken scoren	16
Tabel 2: IP ranges per locatie.....	26
Tabel 3: Broadcast verkeer door verschillende protocollen	28
Tabel 4: Ping resultaten WAN netwerk	30
Tabel 5: Afgenomen verbindingen bij Verizon.....	31
Tabel 6: QoS applicatievolgorde	32
Tabel 7: QoS levels uit documentatie Verizon	32
Tabel 8: Classificeren van impact met letters (voorbeeld)	33
Tabel 9: Classificeren van impact met meerdere wegingsfactoren en letters (voorbeeld)	33
Tabel 10: Network Type	34
Tabel 11: Business Impact	34
Tabel 12: Network Impact.....	34
Tabel 14: Kans berekening.....	35
Tabel 13: Business Impact	35
Tabel 15: Voorbeeld risicoanalyse server/clients	36
Tabel 16: Voorbeeld risicoanalyse switches/routers	36
Tabel 17: Statische VLAN's	39
Tabel 18: Dynamische VLAN's	39
Tabel 19: Network Access Control	40
Tabel 20: Vergelijking VLAN's	40
Tabel 21: Vergelijken switches	40
Tabel 22: SLA, jaarlijkse prijzen	41
Tabel 23: Kosten ontwerp 1.....	42
Tabel 24: Kosten ontwerp 2.....	42
Tabel 25: Risicoanalyse LAN ontwerp	44
Tabel 26: Behoeftte aan bandbreedte in De Lier	45
Tabel 27: Verizon jaarlijkse kosten na upgrade	45
Tabel 28: WAN ontwerp 1	47
Tabel 29: WAN ontwerp 2	48
Tabel 30: Juniper MAG series vergelijking	51
Tabel 31: Virtual router protocollen	54
Tabel 32: Policy WAN verkeer.....	56
Tabel 33: VLAN's onderlinge communicatie	57
Tabel 34: Wireless Controllers	59
Tabel 35: CoS waarden per VLAN	60
Tabel 36: DiffServ classificaties.....	61
Tabel 37: Gekozen DSCP classificaties	62
Tabel 38: Kosten WAN netwerk t/m juni 2014.....	63
Tabel 39: Kosten WAN netwerk na juni 2014.....	63