Consolidatie en virtualisatie van de core netwerk infrastructuur bij Deloitte

Naam : Chris de Bruin

Titel : Afstudeerscriptie

Versie : 1.0

Datum : 24 mei 2014

Plaats : Amsterdam

Auteur/afstudeerder	:	Chris de Bruin
Studentnummer	:	09000577
E-mail	:	c.debruin@student.hhs.nl
Afstudeerperiode	:	18 november 2013 – 6 juni 2014
Afstudeerbedrijf	:	Deloitte - IT & Workplace Services
Opdrachtgever	:	John Snel
Bedrijfsmentor	:	Jeroen Hassing
Onderwijsinstelling	:	Haagse Hogeschool
Begeleider/examinator	:	John Visser
Expert/examinator	:	Pieter Burghouwt

Voorwoord

Deze scriptie beschrijft de afstudeeropdracht van Chris de Bruin ter afsluiting van de opleiding Technische Informatica aan de Haagse Hogeschool en is geschreven voor de examinatoren, de gecommitteerde en afstudeerbegeleiders zodat zij een eindoordeel kunnen maken over mijn inzet, mijn vorderingen en de resultaten die ik heb geboekt gedurende deze afstudeerperiode.

Dit is het resultaat van een lang, moeilijk, druk, stressvol, maar ook zeker mooi en bevredigend jaar hard werken en lange dagen. Maar laat ik ook de daaraan voorafgaande jaren niet wegvlakken.

Het concept consolidatie en virtualisatie van een netwerk infrastructuur is zonder twijfel verre van uniek. Deze scriptie is echter wel uniek, hij is van mij.

Ik ben mijn studie puur uit interesse voor de behandelde onderwerpen gaan volgen en niet omdat deze mijn carrière zou kunnen helpen. Natuurlijk heb ik daar wel over nagedacht, maar het is nooit de primaire drijfveer geweest.
De inhoud van de studie staat dan ook een heel eind van mijn reguliere, dagelijkse werk als technisch applicatiebeheerder. Hierdoor ben ik langere tijd onzeker geweest of er voor mij wel een mogelijkheid zou zijn om af te kunnen studeren bij Deloitte.
Tijdens een gesprek met Jeroen Hassing – mijn begeleider tijdens het afstuderen – verscheen er toch een lichtpuntje aan de horizon. Ik heb er dan ook alles aan gedaan om van dit lichtpuntje een mooie afstudeeropdracht te kunnen maken. En ik mag zeggen; met succes!

Net als zoveel afstudeerders voor mij wil ook ik een woord van dank uitspreken. Als eerste wil ik Jeroen Hassing bedanken omdat hij mij de mogelijkheid heeft geboden om af te kunnen studeren. Ook wil ik Jelle Boeijinga en Bart van den Heuvel bedanken voor hun motivatie en inspiratie en mijn examinatoren John Visser en Pieter Burghouwt voor het denken in oplossingen.
Maar in het bijzonder wil ik Nathaly en Tim bedanken voor hun steun, begrip en eindeloze geduld.

Bedankt!

Dordrecht, 15 mei 2014

Chris de Bruin

Referaat

Chris de Bruin, afstudeerscriptie consolidatie en virtualisatie van de core netwerk infrastructuur bij Deloitte, Amsterdam 2014.

Deze afstudeerscriptie beschrijft het proces dat is gevolgd tijdens het uitvoeren van deze afstudeeropdracht. De opdracht is gericht op het aantonen dat het mogelijk is om met behulp van bestaande virtualisatie technieken de core netwerk infrastructuur van Deloitte te consolideren. De opdracht is uitgevoerd in de periode van 18 november 2013 tot 6 juni 2014 in opdracht van Deloitte IT & Workplace Services.

Descriptoren

- Afstudeerscriptie
- Deloitte
- Networking
- Netwerkconsolidatie
- Virtualisatie
- Routers
- Switches
- Virtual Routing & Forwarding
- Technische informatica
- Haagse Hogeschool
- Deeltijd

Inhoudsopgave

Deloitte.

1. Inleiding

De doelstelling van deze afstudeeropdracht is om aan te tonen dat het mogelijk is om met behulp van bestaande virtualisatie technieken de core netwerk infrastructuur van Deloitte te consolideren.

Aanleiding

Om beter grip te krijgen op de beheerbaarheid, het onderhoud en ook de kosten van beheer en onderhoud is door Deloitte IT & Workplace Services de wens uitgesproken dat het aantal hardware componenten binnen het Deloitte netwerk wordt geconsolideerd.

In het verleden is vanuit veiligheid perspectief gekozen om bepaalde omgevingen fysiek van elkaar te scheiden. Dit zodat externe en interne omgevingen van het Deloitte netwerk niet direct met elkaar in verbinding staan. De afgelopen jaren is de capaciteit van netwerkapparatuur fors toegenomen en zijn er nieuwe technieken beschikbaar gekomen die kunnen voorzien in de consolidatie van de verschillende omgevingen.

In plaats van de interne en externe omgevingen fysiek te scheiden op verschillende netwerkcomponenten kan deze scheiding nu door middel van virtualisatie softwarematig worden gerealiseerd op dezelfde fysieke hardware. Met behulp van deze virtualisatie blijft de netwerkveiligheid gehandhaafd en wordt er tegelijkertijd bespaard op hardware-, stroom- en koelingskosten. Omdat er minder hardwarecomponenten benodigd zijn, is er minder tijd nodig voor onderhoud en wordt er bespaard op fysieke ruimte.

Leeswijzer

Hoofdstuk 1, een korte inleiding in de afstudeerscriptie.
Hoofdstuk 2, een beschrijving van de Deloitte organisatie.
Hoofdstuk 3, de probleemstelling met de probleemomschrijving, de doelstelling en het resultaat.
Hoofdstuk 4, de keuze van een geschikte methodiek.
Hoofdstuk 5, de eerste fase: de definitiefase.
Hoofdstuk 6, de tweede fase: de architectuurfase.
Hoofdstuk 7, de derde fase: de ontwerpfase.
Hoofdstuk 8, de laatste fase: de ontwikkelfase.
Hoofdstuk 9, een beschrijving van de getrokken conclusies en de aanbeveling.
Hoofdstuk 10, een terugblik op het afstudeerproces en het tot stand komen van het eindproduct.

2. Organisatie

De volgende paragrafen schetsen een algemeen beeld van Deloitte als wereldwijde organisatie [1], maar ook van Deloitte Nederland [2]. Tevens wordt kort beschreven hoe de Nederlandse support organisatie, het Group Support Center, is opgebouwd.

2.1. Deloitte Global

Deloitte is een van de "Big Four". De Big Four zijn de vier grootste internationale, professionele dienstverleners die services bieden voor onder andere audits, belastingen en legal services. De Big Four wordt gevormd door PricewaterhouseCoopers, Ernst & Young, KPMG en Deloitte.

In het boekjaar 2013 had Deloitte wereldwijd ongeveer 200.000 medewerkers en partners en heeft zij een omzet gemaakt van $32,4 miljard [3].

Deloitte is de merknaam waaronder zelfstandige memberfirms wereldwijd samenwerken op het gebied van accountancy, consulting, financiële advisering, risk management en belastingadvies. Al deze memberfirms zijn onderdeel van Deloitte Touche Tohmatsu Limited (DTTL), een naamloze vennootschap in het Verenigd Koninkrijk.

Omdat elke memberfirm in een bepaald (geografisch) gebied actief is, is zij daardoor onderworpen aan de wetgeving en de professionele regelgeving van het land of de landen waarin wordt geopereerd.

De structuur van de afzonderlijke DTTL memberfirms verschilt afhankelijk van de plaatselijke wet- en regelgeving, usance en eventuele andere factoren.

2.2. Deloitte Nederland

Op het moment van schrijven heeft Deloitte Nederland ongeveer 4500 medewerkers en partners verspreid over 19 kantoren.

Deloitte Nederland – zoals we deze nu kennen – kent een rijke geschiedenis en heeft vele rechtsvoorgangers gehad. Het volgende overzicht is een weergave van een aantal van de belangrijkste overnames en fusies;

1955 De belangrijkste rechtsvoorganger Nederlandse Accountants Maatschap (NAM).
1986 Belastingadvies wordt belangrijker en om de samenwerking met Touch Ross International te verduidelijken veranderd de naam in TRN Groep.
1988 TRN Groep fuseert met de Tombe/Melse Groep (TMG).
1992 Touche Ross International gaat samen met Deloitte Haskins &Sells, een nieuwe wereldwijde verbintenis met als nieuwe naam Deloitte Touch Tohmatsu International. De naam verandert in Deloitte & Touche.
1998 De grootste fusie uit de geschiedenis van de Nederlandse organisatie, Deloitte & Touche fuseert met de VB Groep.
2002 Deloitte & Touche fuseert met Andersen Nederland. Hiermee wordt de Big Five gereduceerd tot de Big Four.
2003 De naam wordt ingekort naar Deloitte, maar het blijft een "member of Deloitte Touche Tohmatsu".

In het boekjaar 2013 heeft Deloitte Nederland een omzet gemaakt van €631 miljoen [4].

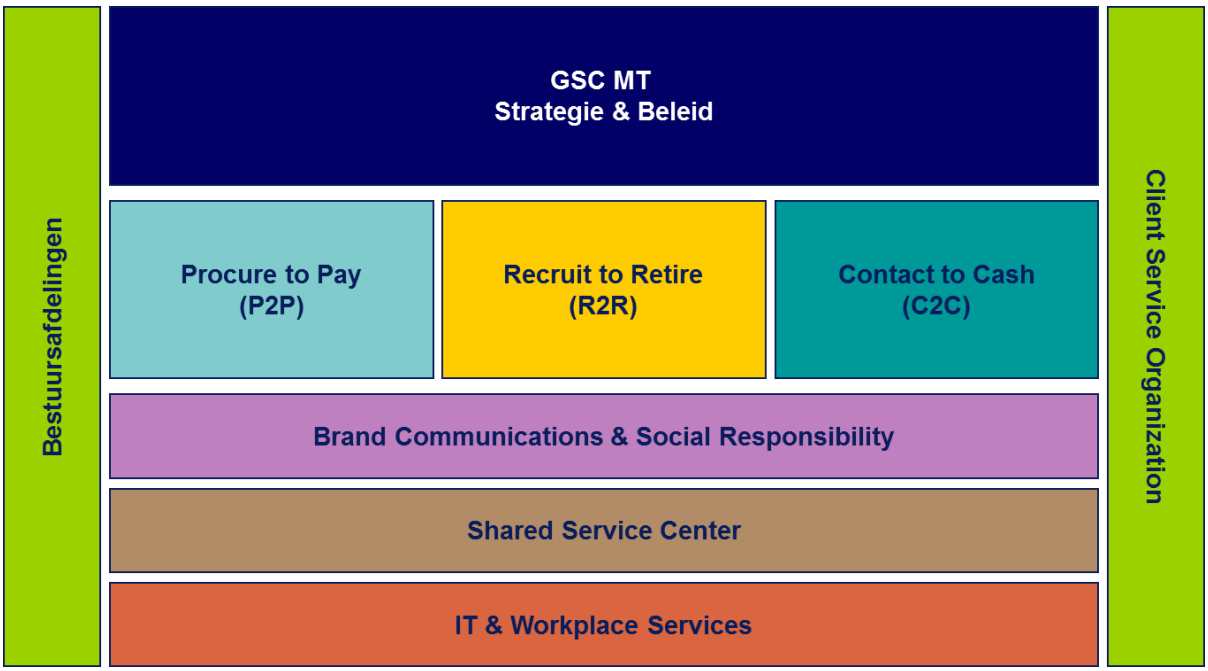
De vier belangrijkste onderdelen van Deloitte Nederland waarmee zij de markt bedient, zijn de diensten (functions); Accountancy (Audit), Belastingen (Tax), Consulting en Financial Advisory Services. Deloitte biedt een branche specifieke aanpak via verschillende industriegroepen in diverse regio's.

Naast haar economische verantwoordelijkheid heeft Deloitte ook een maatschappelijke verantwoordelijkheid. Zo heeft Deloitte onder andere de Fair Chance Foundation opgericht, een stichting met als primair doel het overdragen van financiële kennis (de core business van Deloitte) naar een bijzondere doelgroep; jongeren in achterstandssituaties. [5]

2.3. Group Support Center

De directe medewerkers in de functions worden ondersteund door het Group Support Center (GSC). Het GSC is onderverdeeld in een aantal ketens en kennisgebieden waarbinnen verschillende ondersteunende afdelingen actief zijn;

- Bestuursafdelingen
- Client Service Organization
- Talent
- Shared Service Center
- IT & Workplace Services
- Finance & Control
- Brand Communications & Social Responsibility



Figuur 1 - GSC ketens en kennisgebieden

Figuur 1 laat zien hoe de afdelingen binnen het GSC zich tot elkaar verhouden. Elk van de afdelingen levert een specifiek deel ondersteuning aan de directe medewerkers, maar ook aan de indirecte – ondersteunende – medewerkers. Hieronder worden de afdelingen kort omschreven;

Bestuursafdelingen

Hieronder vallen onder andere de afdelingen Juridische Zaken en Risk & Reputation Leadership. Reputation & Risk Leadership Office houden zich bezig met beheersing van risico's onder ander op het gebied van reputatie, bedrijfsrisico's, compliance met wet & regelgeving en verantwoord ondernemen.

Juridische zaken ondersteunt bij vraagstukken over privacy, de wet ter voorkoming van witwassen en financiering van terrorisme en toezicht.

Client Service Organization

De Client Service Organization levert onder andere secretariële ondersteunende diensten aan directe en indirecte medewerkers. Maar ook het beheer en onderhoud van Insite Support – de online self-service-portal voor Deloitte medewerkers – vallen onder de verantwoordelijkheid van de Client Service Organization.

Een ander bijzonder belangrijk onderdeel van de Client Service Organization is de Deloitte service desk. Hier kunnen directe en indirecte medewerkers terecht met al hun vragen en/of verzoeken met betrekking tot ICT, personele, financiële en/of facilitaire zaken.

Talent

De afdeling Talent - voorheen Human Resources - heeft als belangrijkste taak het begeleiden van de carrière van de medewerkers vanaf het moment dat zij in dienst treden tot aan het moment dat zij weer uit dienst treden.

Shared Service Center

Het Shared Service Center heeft haar verantwoordelijkheden vooral bij de backoffice taken. Het administreren en faciliteren van trainingen, maar ook het administreren van personele zaken, de outsourcing naar India en de salaris administratie.

IT & Workplace Services

Voorheen de afdelingen Facility Management & Services en ICT Services, maar nu een samengevoegd geheel met als belangrijkste verantwoordelijkheid het faciliteren van complete en functionele werkplekken en andere faciliteiten voor medewerkers van Deloitte, maar eventueel ook voor klanten en/of gasten.

Finance & Control

De afdeling Finance & Control is verantwoordelijk voor de interne financiële boekhouding. Denk hierbij aan onder andere het maken van maand- en jaarafsluitingen.

Brand Communications & Social Responsibility

Brand Communications & Social Responsibility is als het ware het gezicht van Deloitte. Zij houdt zich bezig met de merknaam, sponsoring, publicaties en persvoorlichting. Ook het social media beleid valt onder haar verantwoordelijkheden.

Events die worden georganiseerd geassocieerd aan de merknaam Deloitte, worden ook begeleid door de Brand Communications & Social Responsibility.

2.4. IT & Workplace Services

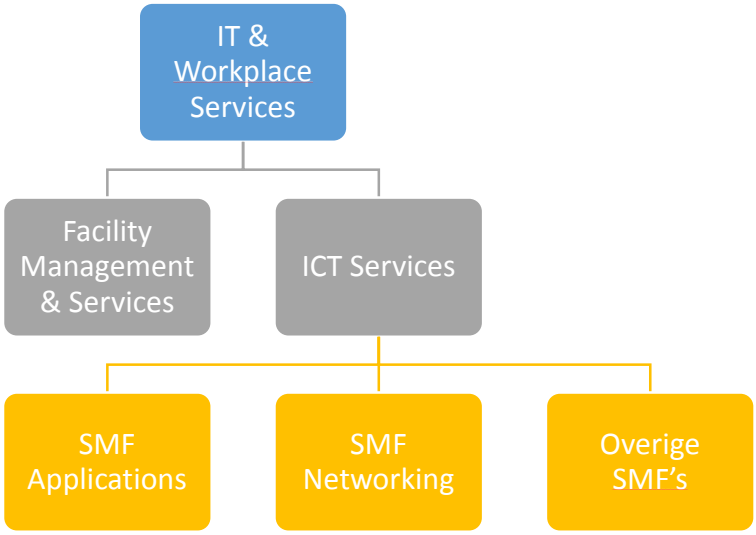
IT & Workplace Services is ontstaan uit een samen gaan van de afdelingen Facility Management & Services en ICT Services. Samen hebben zij als hoofdverantwoordelijkheid het faciliteren van complete en functionele werkplekken, maar ook andere faciliteiten – denk aan bedrijfsrestauraties, koffiecorners en de IT infrastructuur

FM&S zal verder niet worden besproken in dit document, omdat deze verder geen raakvlak heeft met de opdracht.

Service Management Functions

De afdelingen, maar ook de processen van ICT Services zijn ingericht aan de hand van het Microsoft Operations Framework (MOF). [6]
Activiteiten en processen zijn verdeeld onder verschillende Service Management Functions (SMF).

Bovenstaand zijn slechts twee voorbeelden van de SMF's zoals Deloitte IT & Workplace Services deze heeft ingericht. Figuur 2 toont een vereenvoudigd overzicht van IT & Workplace Services en de onderliggende onderdelen. Om het organigram niet te groot te maken, worden maar twee van de SMF's bij naam genoemd.



Figuur 2 – IT & Workplace Services organigram (vereenvoudigd overzicht)

SMF Applications

Ik ben werkzaam bij SMF Applications als technisch beheerder. SMF Applications is verantwoordelijk voor het beheren, ontwerpen en vernieuwen van het applicatie landschap van Deloitte Nederland. Dit betreft het uitvoeren van updates op de verschillende applicatieplatformen en het afhandelen van calamiteiten en klantincidenten, maar ook het onderhouden van contacten met zowel interne als externe leveranciers van software.

SMF Networking

SMF Networking is verantwoordelijk voor het beheren, ontwerpen en vernieuwen van het bedrijfsnetwerk van Deloitte Nederland. Denk hierbij aan netwerkapparatuur (routers en switches), netwerkbekabeling, maar ook het onderhouden van contacten met externe partijen als KPN en AVAYA en het oplossen van calamiteiten.

Deze afstudeeropdracht wordt uitgevoerd in opdracht van SMF Networking.

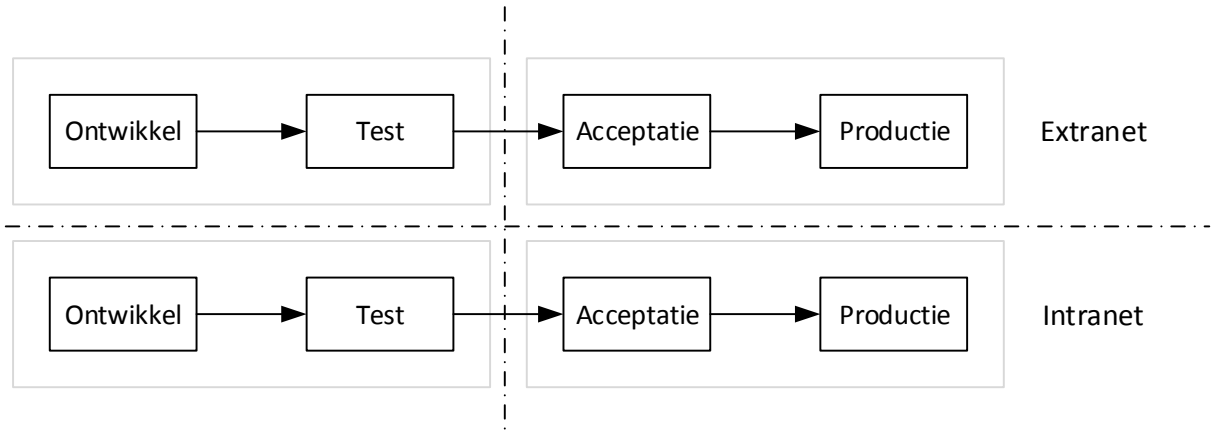
3. Probleemstelling

Het Deloitte netwerk is opgebouwd als een Ontwikkel, Test, Acceptatie en Productie (OTAP) structuur.

De ontwikkel- en testomgevingen en de acceptatie- en productieomgevingen zijn fysiek van elkaar gescheiden. De ontwikkel- en testomgeving wordt gehost op een separate netwerk infrastructuur dan de acceptatie- en productieomgeving.

Beide infrastructuren (ontwikkel-test en acceptatie-productie) hebben een intranet- en een extranet omgeving. Voor beide infrastructuren geldt dat de intranetomgeving en de extranet omgeving wordt gehost op fysiek gescheiden hardware.

Figuur 4 toont een vereenvoudigde weergave van de gescheiden ontwikkel-test en acceptatie-productie infrastructuren en de gescheiden intranet omgevingen en extranet omgevingen.



Figuur 3 - Schematische weergave OTAP infrastructuren

Ontwikkel- en testomgeving

- De ontwikkelomgevingen worden gebruikt voor het (iteratief) ontwikkelen van software oplossingen voor interne en externe klanten van Deloitte.
- De testomgevingen worden gebruikt door de technisch beheerders voor het uitvoeren van technische tests van de ontwikkelde software oplossingen; welk impact heeft de installatie van een oplossing op de infrastructuur?

Omdat niet bekend is wat de impact van een software oplossing is op de infrastructuur en om te voorkomen dat door het uitvoeren van technische tests onderdelen van de infrastructuur niet meer beschikbaar zouden zijn, is ervoor gekozen om de ontwikkel- en testomgevingen fysiek op een andere netwerk infrastructuur te hosten.

Acceptatie- en productieomgeving

- De acceptatieomgeving wordt gebruikt voor het uitvoeren van functionele tests door key users en functioneel beheerders van de ontwikkelde software oplossingen.
- Wanneer vanuit de functionele tests in de acceptatieomgevingen blijkt dat de software oplossing voldoet aan de eisen van de klant, wordt deze in de productieomgeving geïnstalleerd en komt de oplossing beschikbaar voor alle gebruikers.

De productieomgevingen zijn de omgevingen waarin de dagelijkse werkzaamheden door alle gebruikers worden uitgevoerd. Voordat een software oplossing hier geïnstalleerd mag worden, moet deze zowel technische als functioneel uitvoerig getest zijn.

De ontwikkel- en testomgeving is in principe gelijk aan de acceptie- en productieomgeving, alleen kleiner uitgevoerd. De afstudeeropdracht richt zich enkel op de acceptatie- en productieomgeving.

3.1. Probleemomschrijving

Om de beheerbaarheid en het onderhoud van het Deloitte netwerk te vergemakkelijken maar ook vanuit kostenoogpunt, wil Deloitte IT & Workplace Services de intranet omgeving en de extranet omgevingen consolideren naar één core netwerk infrastructuur. De opdrachtgever heeft aangegeven aan welke eisen en wensen (requirements) de nieuwe core netwerk infrastructuur moet voldoen, echter is op dit moment niet bekend op welke manier de nieuwe infrastructuur gerealiseerd moet worden.

3.2. Doelstelling

Het doel van deze afstudeeropdracht is het komen tot een bewezen ontwerp van een geconsolideerde core netwerk infrastructuur, waar de intranet omgeving en de extranet omgeving met behulp van bestaande virtualisatie technieken op dezelfde fysieke apparatuur kunnen bestaan.

3.3. Resultaat

De resultaten van deze afstudeeropdracht zijn een architectuur, een detail ontwerp en een advies ten behoeve van het implementeren van een nieuwe core netwerk infrastructuur.

De architectuur, het detail ontwerp van de vernieuwde core netwerk infrastructuur en het implementatieplan dienen als PoC voor het consolideren en virtualiseren van de huidige core netwerk infrastructuur.

Directe resultaten van de consolidatie en virtualisatie zullen zijn; gemakkelijkere en betere beheerbaarheid van de omgevingen, gemakkelijker onderhoud en verlaging van de kosten.

4. Methodisch werken

Tijdens de studie is een bescheiden aantal verschillende project technieken en methodes behandeld, zoals PRINCE2, Rational Unified Process (RUP) en ASI Rapport. Om deze opdracht gestructureerd tot een goed einde te brengen is het zaak om een geschikte methode te kiezen en te gebruiken.

4.1. Een methode kiezen

Om voor deze opdracht de juiste methode te kunnen kiezen is een aantal eisen en wensen aan de te kiezen methode gesteld;

- De gekozen methode moet passen bij de omvang van de opdracht.
- Voor een gestructureerde en gefaseerde aanpak moet de gekozen methode een geschikte fasering voor de opdracht bieden.
- De (deel)producten die tijdens de opdracht tot stand komen, moeten goed aansluiten op de fasering van de opdracht.
- Omdat er geen product gebouwd wordt, is een iteratieve methode niet nodig.
- Tijd is geen vanzelfsprekendheid tijdens het uitvoeren van de opdracht. Er moet een mate van flexibiliteit in de planning aanwezig zijn.
- De opdracht omvat het bedenken en ontwerpen van een nieuwe netwerk infrastructuur, de methode moet hiervoor geschikt zijn.

Een ander belangrijk aspect voor het maken van de keuze voor de juiste methode is dat het werk niet ingewikkelder moet worden dan nodig is – *keep it simple*.

PRINCE2

PRINCE2 is een flexibele methode en is in principe toepasbaar op alle soorten projecten, niet alleen ICT gerelateerde projecten. De methode is gebaseerd op een reeks best practices [7].

Er is niet voor PRINCE2 gekozen omdat deze methode naar mijn mening te omslachtig is voor de omvang van dit project. Ondanks het feit dat PRINCE2 een flexibele methode is die inzetbaar is voor veel projecten, kost het op maat maken ervan teveel tijd.

RUP

RUP is een raamwerk van industry-tested practices voor het ontwerpen, ontwikkelen en implementeren van software en systeem oplossingen [8].

RUP leent zich uitstekend als methode voor het ontwikkelen van software. Uitermate geschikt voor een iteratieve werkwijze. Omdat er geen iteratieve werkwijze wordt gehanteerd, maar eerder een waterval methode, en er ook geen software wordt ontwikkeld, is deze methode niet geschikt voor deze opdracht.

ASI rapport

Het ASI rapport is een methode die is bedacht als hulpstuk bij het ontwikkelen van technische infrastructuren [9]. Het is meer een gefaseerde aanpak dan een methode. Een ‘handleiding’ die zich uitstekend leent voor deze opdracht.

Tabel 1 toont een keuze matrix met de verschillende eigenschappen van de eerder genoemde methodes. Hieruit blijkt dat ASI rapport het beste geschikt is voor deze opdracht.

	PRINCE2	RUP	ASI
GESCHIKT VOOR OMVANG VAN DE OPDRACHT	--	+	++
GESCHIKTE FASERING	+-	-	+
(DEEL)PRODUCTEN SLUITEN AAN OP DE FASERING	+	+	++
GEEN ITERATIEVE METHODE	+	--	+
MOGELIJKHEDEN VOOR FLEXIBILITEIT IN DE PLANNING	+	++	++

Tabel 1 - Keuze matrix methodes

4.2. De gekozen methode: ASI rapport

Er is gekozen om een delen van het de methode ASI rapport te gebruiken als basis structuur voor het werken aan deze opdracht; de fasering en de op te leveren (deel)producten.

Helaas is over ASI heel weinig – eigenlijk niets – terug te vinden op het internet. De enige documentatie die mij hierover bekend is, is de documentatie die ons tijdens de colleges is toegereikt. Deze documentatie is opgenomen in het afstudeerdossier.

Fasering

ASI deelt een project op in vier verschillende fases [9];

- **Definitiefase**: Vastleggen wat het resultaat van het te doorlopen traject wordt, aan welke eisen het resultaat moet voldoen en welke uitgangspunten er gehanteerd worden.
- **Architectuurfase**: Opstellen van een blauwdruk van de te realiseren infrastructuur.
- **Ontwerpfase**: Detail uitwerking van de architectuur naar de feitelijke geografische, technische en organisatorische context. Selectie van toe te passen producten en externe diensten.
- **Ontwikkelfase**: Toetsing van de goede werking en de schaalbaarheid van het ontwerp. Realisatie van maatwerk aanpassingen en aanvullingen. Opstellen van technische en procedurele richtlijnen.

Elk van deze fases levert een of meerdere (deel)producten op en het einde van een fase wordt geborgd met een te behalen mijlpaal.

Deelproducten en mijlpalen

Tabel 2 laat zien dat de verschillende fasen van deze opdracht verschillende (deel)producten en mijlpalen opleveren;

	DEELPRODUCTEN	MIJLPALEN
DEFINITIEFASE	--	- Plan van aanpak
ARCHITECTUURFASE	--	- Architectuurdocument
ONTWERPFASE	- Fysiek ontwerp - Logisch ontwerp - IP nummerplan	- Detail ontwerp
ONTWIKKELFASE	--	- Implementatieplan

Tabel 2 - Deelproducten en mijlpalen

De ontwikkelfase wordt gebruikt voor het schrijven van een implementatieplan voor de nieuwe core infrastructuur.

Omdat deze opdracht een PoC heeft als eindproduct waarvan de werking en de schaalbaarheid niet kunnen worden getoetst, wordt er gekeken naar de bruikbaarheid van het PoC.

5. Fase 1: Definitiefase

Tijdens de definitiefase van de opdracht wordt vastgesteld wat de aanleiding is voor de opdracht, welk probleem opgelost moet worden, wat de doelstelling van de opdracht is en wat de resultaten zijn die uit de opdracht voortkomen.

Er wordt informatie verzameld om te kunnen bepalen welke eisen en wensen aan het product worden gesteld en om de scope van de opdracht te kunnen bepalen.

Tot slot wordt een risicoanalyse gemaakt om vast te kunnen stellen welke risico's aan de opdracht verbonden zijn en worden afspraken vastgelegd om de kwaliteit van de opdracht te kunnen waarborgen.

Op te leveren (deel)producten in deze fase

- Plan van aanpak

5.1. Eisen en wensen aan het product

Om goed zicht te krijgen op de eisen en wensen die aan het product worden gesteld, is een lijst met functionele en niet-functionele requirements samengesteld.

Deze lijst met eisen en wensen is tot stand gekomen door het voeren van gesprekken met de opdrachtgever. Deloitte IT & Workplace Services had hier al een duidelijk idee over waardoor onderstaande lijsten met requirements snel tot stand kon komen.

Functionele requirements

- De switches in de core laag bevatten de intelligentie van het de core netwerk infrastructuur en hebben als primaire taak het routeren van al het inkomende en uitgaande netwerkverkeer.
- De switches in de distributie laag hebben een minimale intelligentie en hebben als primaire taak het verschaffen van toegang tot de netwerk infrastructuur aan verschillende applicaties en services. Denk hierbij aan bijvoorbeeld Microsoft Exchange servers, Microsoft SQL servers en SAP systemen.
- Het moet mogelijk zijn om via de netwerk infrastructuur narrowcasts (IPTV) te routeren naar alle branch offices.
- Interne Deloitte gebruikers hebben toegang tot zowel de intranet omgeving als de VLAN's in de extranet omgeving waarin de services draaien waartoe zij toegang nodig hebben.
- Externe Deloitte gebruikers hebben door middel van Direct Access toegang tot zowel de intranet omgeving als de VLAN's in de extranet omgeving waarin de services draaien waartoe zij toegang nodig hebben.
- Externe klanten hebben alleen toegang tot de extranet omgeving en dan alleen tot de specifieke VLAN's waarin de services draaien waartoe zij toegang nodig hebben. Zij hebben onder geen beding toegang tot de intranet omgeving.

Niet-functionele requirements

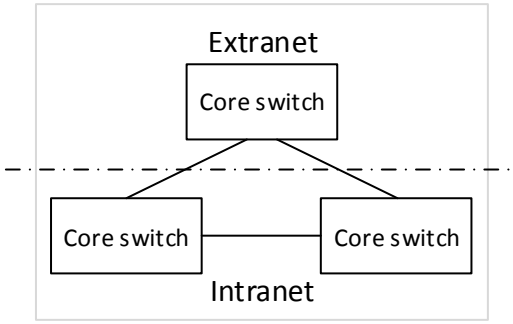
- De intranet omgeving en de extranet omgeving moeten met elkaar op dezelfde hardware kunnen bestaan.
- De nieuwe core netwerk infrastructuur bestaat uit een core laag met aparte (core) switches en een distributie laat met aparte (distributie) switches.
- De switches in de distributie laag worden opgebouwd en geconfigureerd als (distributie) stacks.
- Op zowel de core switches als op de distributie stacks moet load balancing en link aggregatie aanwezig zijn.
- Het hardware platform moet voorbereid zijn op hoge interface snelheden van 10, 40 en 100 Gbps.
- Om een uptime van 99,99% te kunnen garanderen moeten de switches in de core laag en in de distributie laag redundant worden geconfigureerd, moeten componenten hot swappable zijn en moet de configuratie van switches, maar ook het configureren van netwerken en subnets moet on-the-fly gedaan kunnen worden.
- Omdat op de netwerk infrastructuur veel verschillende diensten actief zijn, zoals routing, IPTV narrowcasting en load balancing, moet ondersteuning van verschillende protocollen (bijv. RIP, IGMP, SMLT, IST, etc.).

5.2. Afbakening van de opdracht

Het is belangrijk om op voorhand te weten welke onderdelen wel en welke onderdelen niet binnen de scope van de opdracht vallen.

Wat valt binnen scope?

Voor deze opdracht is gekozen om de focus volledig te richten op consolidatie en virtualisatie van de core netwerk infrastructuur van de intranet omgeving en de extranet omgeving. Figuur 4 toont de te consolideren onderdelen van het core netwerk binnen de scope van de opdracht.



Figuur 4 - Scope van de opdracht

Wat valt niet binnen scope?

De infrastructuur van de branch offices zelf valt niet binnen de scope van deze opdracht. Dit heeft twee redenen;

- Op termijn zal de infrastructuur van de branch offices vernieuwd worden. Nieuwe switches en nieuwe architectuur – dit laatste voornamelijk voor de grotere branch offices. De opdrachtgever heeft aangegeven dit in een later stadium te willen doen.
- Dit betekent dat voor 18 branch offices de infrastructuur apart uitgewerkt moet worden. Hiermee zou de opdracht te uitgebreid worden in opzet.

De configuratie van de intranet firewall en de extranet firewall valt ook buiten de scope van de opdracht;

- De opdrachtgever heeft laten weten dat de firewalls op voorlopig onveranderd blijven functioneren. In een later stadium zal een project gestart worden voor het consolideren van de intranet firewalls en de extranet firewalls.

Aanpassingen aan de Windows domein structuur vallen buiten de scope van deze opdracht alsmede eventuele aanpassingen aan servers in het Windows domein.

- Dit gebeurd naar aanleiding van een ander project, Deloitte Private Cloud.

5.3. Een risicoanalyse maken

Om te kunnen bepalen welke risico's aan deze opdracht verbonden zijn, is er een kwalitatieve risicoanalyse opgesteld. Er is een schatting gemaakt om tot de waardes van Kans en Impact te komen.
Tabel 3 laat zien hoe Kans en Impact tegen elkaar worden weggezet. Hierdoor wordt het mogelijk om de waarde van Risico te berekenen.

Voor het waarderen van de risico's voor deze opdracht is gebruik gemaakt van de formule:
Risico = Kans x Impact.

Omschrijving	Mitigatie	Kans	Impact	Risico
Ontwerp voldoet niet aan de eisen en wensen van de opdrachtgever.	Tussentijdse contactmomenten met de opdrachtgever om de voortgang van het ontwerp te bespreken.	2	5	10
Onderdelen van de opdracht zijn complexer dan verwacht.	Schuiven met tijd in de planning om meer tijd vrij te maken voor complexere onderdelen.	3	4	12
Niet alle benodigde technieken zijn beschikbaar (of volledig uitgekristalliseerd) voor een correcte uitvoering van de opdracht.	In overleg met de opdrachtgever zal naar een alternatief gezocht worden.	2	4	8
Niet voldoende tijd voor werkzaamheden door drukte bij de dagelijkse werkzaamheden.	Tijdig afspraken maken met de opdrachtgever, begeleider en examinatoren voor het verlengen van de afstudeerperiode.	3	5	15
Onzekerheden omtrent de informatiebeveiliging.	Specialisten audits uit laten voeren ten behoeve van de beveiliging in het ontwerp.	4	5	20

Tabel 3 – Risicoanalyse

- **Omschrijving**: beschrijft de risico's die kunnen ontstaan tijdens de uitvoering van de opdracht.
- **Mitigatie**: beschrijft de actie om de impact van het risico te verkleinen.
- **Kans**: de kans dat het risico optreedt tijdens de uitvoering van de opdracht. De waarde ligt tussen 1 (= geen) en 5 (= aanwezig).
- **Impact**: de impact dat het risico heeft op de uitvoering van de opdracht. De waarde ligt tussen 1 (= geen) en 5 (= hoog).
- **Risico**: Kans x Impact = het geschatte risico.

Tabel 4 toont de waardes die in de risicoanalyse zijn toegepast. Deze waardes corresponderen met de waardes van Kans en Impact in Tabel 3.

	KANS	IMPACT
1	Hele kleine kans	Heel laag
2	Kleine kans	Laag
3	Matige kans	Matig
4	Grote kans	Groot
5	Hele grote kans	Heel groot

Tabel 4 - Toegepaste waardes in de risicoanalyse

5.4. De kwaliteit van de opdracht borgen

Voor het borgen van de kwaliteit van de opdracht is een aantal afspraken gemaakt met de opdrachtgever.

Kwaliteit van documenten

Om de kwaliteit van de op te leveren documenten te waarborgen, worden de op te leveren documenten ter review aan de opdrachtgever aangeboden.

- De opdrachtgever geeft hierop feedback die – eventueel na overleg – wordt verwerkt.
- Wanneer informatie niet buiten de organisatie gebracht mag worden, zal gebruik gemaakt worden van fictieve gegevens. Wanneer gebruik gemaakt wordt van fictieve gegevens, zal dit worden benoemd.

Uniformiteit van documenten

Omdat het belangrijk is dat de betrokkenen zonder problemen alle documenten kunnen inzien, is afgesproken een beperkt aantal tools te gebruiken voor het creëren van documenten;

- Microsoft Office 2013
- Microsoft Office Visio 2013
- Microsoft Office Project 2013

Om de documenten ook toegankelijk te maken voor anderen, worden de documenten waar mogelijk ook in PDF formaat aangeboden.

Planning en mijlpalen

Voor het waarborgen van de planning van de opdracht zijn een globale planning en een faseplanning opgenomen in de documentatie.

- De globale planning geeft een overzicht van de gehele opdracht.
- De faseplanning breekt de globale planning op in fases waarin de deelproducten en mijlpalen zijn opgenomen.

Per fase is in de documentatie de faseplanning voor de volgende fase opgenomen.

Dus;

- Het plan van aanpak bevat de faseplanning voor de architectuurfase
- De architectuur bevat de faseplanning voor de ontwerpfase.
- Het detail ontwerp bevat de faseplanning voor de ontwikkelfase.

Communicatie met de opdrachtgever

- Cruciale onderdelen van de infrastructuur zullen in samenwerking met de opdrachtgever tussentijds worden beoordeeld.
- Communicatie per e-mail wordt verstuurd naar alle stakeholders van deze opdracht tenzij specifiek aangegeven in de documentatie.

5.5. De kosten en de baten

Op het moment van schrijven van het plan van aanpak is het nog niet mogelijk om een goede inschatting te maken van de kosten voor de aanschaf van hardware voor deze opdracht. Dit komt omdat vooralsnog niet bekend is welke en hoeveel hardware componenten gebruikt zullen worden in het ontwerp.

Er zal tijdens het verdere verloop van de opdracht geen rekening gehouden worden met kosten, voor aanschaf van hardware.

Tabel 5 toont de baten die voortkomen uit de opdracht.

Baten	**Hoe te bereiken**
Vermindering van de benodigde hardware en ruimte.	Door het consolideren van de omgevingen wordt het mogelijk om meerdere omgevingen te laten landen op dezelfde fysieke hardware. Hierdoor kunnen de benodigde hardware en ruimte aanzienlijk worden verminderd.
Besparing op beheer-, onderhoud- en energiekosten.	Door het verminderen van de benodigde fysieke hardware wordt beheer van de hardware vergemakkelijkt en worden kosten bespaard op het onderhoud van hardware en energieverbruik.
Verlaging van de TCO.	Door vermindering van hardware en ruimte en de besparingen op beheer, onderhoud en energie wordt zal de TCO ook flink lager worden.

Tabel 5 - De baten van de opdracht

6. Fase 2: Architectuurfase

Tijdens de architectuurfase van de opdracht wordt de huidige architectuur in kaart gebracht, waarna de nieuwe architectuur uitgewerkt.

Met deze gegevens wordt een blauwdruk gemaakt van beide architecturen - huidig en nieuw – en wordt een architectuur document geschreven.

Op te leveren (deel)producten in deze fase

- Architectuur document

6.1. De huidige netwerk architectuur

Om een duidelijk beeld te krijgen bij de huidige situatie is het van belang dat de huidige architectuur goed in kaart wordt gebracht.

Het Deloitte CyberCentre is een Twin Datacenter. Hard- en software configuraties evenals data opslag zijn redundant uitgevoerd in twee verschillende datacenters. In het verleden is de keuze gemaakt om de twee datacenters direct naast elkaar te plaatsen.

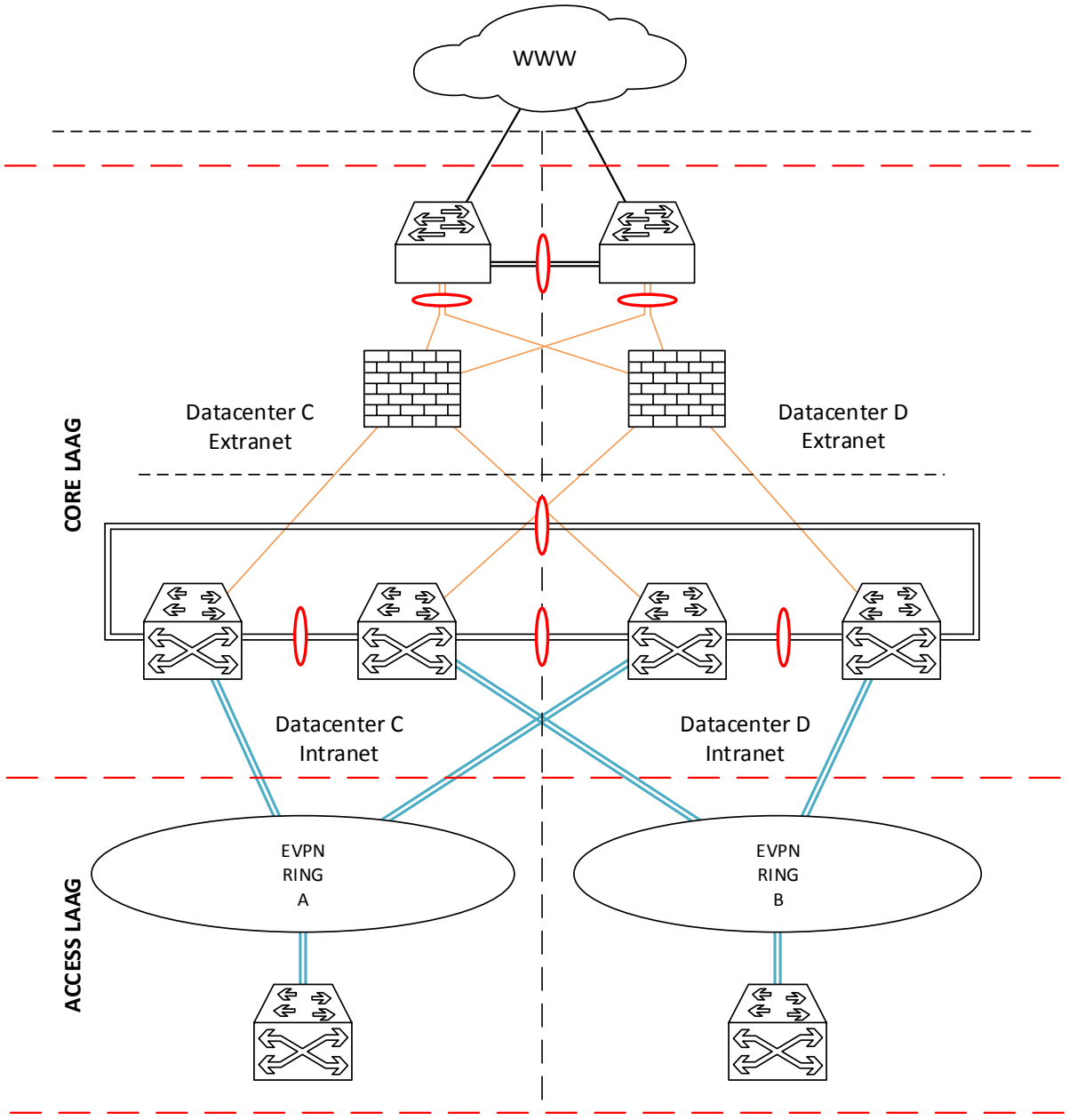
Om de huidige netwerk architectuur goed in kaart te kunnen brengen, is gebruik gemaakt van bestaande documentatie en tekeningen en zijn meerdere gesprekken gevoerd met de opdrachtgever.
Figuur 5 laat de belangrijkste onderdelen van de huidige architectuur zien. Echter zijn niet alle onderdelen relevant voor de opdracht. Alleen de onderdelen die relevant zijn voor de opdracht zijn verder uitgewerkt.

Topologie

De huidige core netwerk infrastructuur (Figuur 5) is een collapsed core design. Het bestaat uit een access laag en een samengevoegde core laag en distributie laag. [10]

De core laag is opgebouwd met twee externe core switches – een in elk van de datacenters – en vier interne core switches – twee in elk van de datacenters. Tussen de interne en externe core switches zijn de firewalls geplaatst, die er voor zorgen dat netwerkverkeer in het extranet blijft of juist naar het intranet wordt gestuurd.

De access laag wordt gebruikt voor het verschaffen van toegang tot de netwerk infrastructuur aan end devices (computers, printers, mobiele devices) vanuit de branch offices.
Tussen de core laag en de access laag bevinden zich Ethernet VPN (EVPN) verbindingen van KPN waarmee de verbindingen tussen de branch offices en het CyberCentre worden gefaciliteerd.

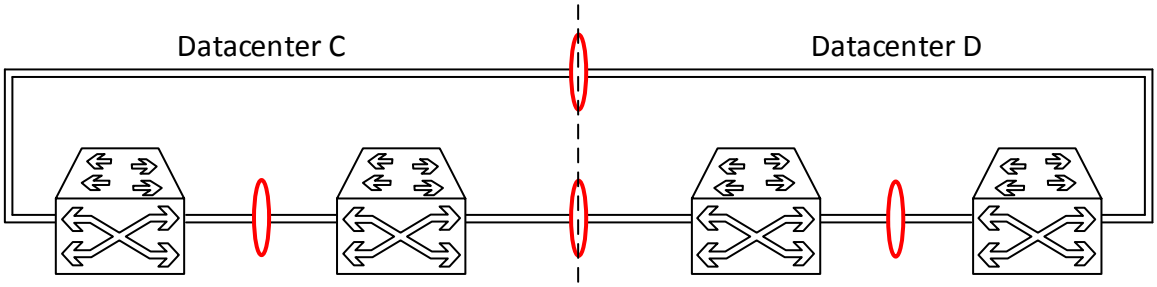


Figuur 5 - Huidige netwerk infrastructuur (vereenvoudigd overzicht)

Interne core switches

De vier interne core switches (Figuur 6) zijn met elkaar verbonden als twee sets van twee switches. De switches in een set staan elk in een van de twee datacenters en zijn door middel van trunk verbindingen geconfigureerd als een redundant switch cluster.
De twee switch clusters zijn door middel van trunk verbindingen met elkaar verbonden voor redundantie en load balancing tussen de clusters.

De interne core switches zijn door middel van aparte trunk verbindingen verbonden met de switches van de branch offices in de access laag.
Door middel van redundante verbindingen zijn de interne core switches verbonden met de firewalls.

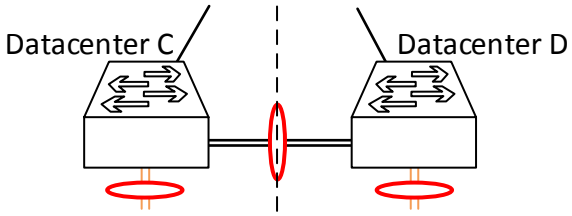


Figuur 6 - Interne core switches in de huidige situatie

De interne core switches worden gebruikt voor het verschaffen van toegang tot het netwerk aan servers.

Externe core switches

De externe core switches (Figuur 7) zijn door middel van trunk verbindingen als redundant cluster uitgevoerd, elke switch in een van de twee datacenters.
Door middel van aparte trunk verbindingen zijn de externe core switches verbonden met de firewalls en door middel van een aparte redundante verbinding zijn de externe core switches verbonden met de Internet Service Provider (ISP).



Figuur 7 - Externe core switches in de huidige situatie

6.2. De nieuwe netwerk architectuur

Nadat de huidige architectuur in kaart is gebracht is het zaak de nieuwe architectuur in kaart te brengen.
Omdat de opdrachtgever al wat ideeën heeft met betrekking tot de nieuwe architectuur en hoe deze er uit zou moeten zien, is er direct een mooi startpunt voor het uitwerken van de nieuwe architectuur aanwezig.

Topologie

De nieuwe core netwerk infrastructuur (Figuur 8) bestaat uit een core laag, een distributie laag en een access laag.

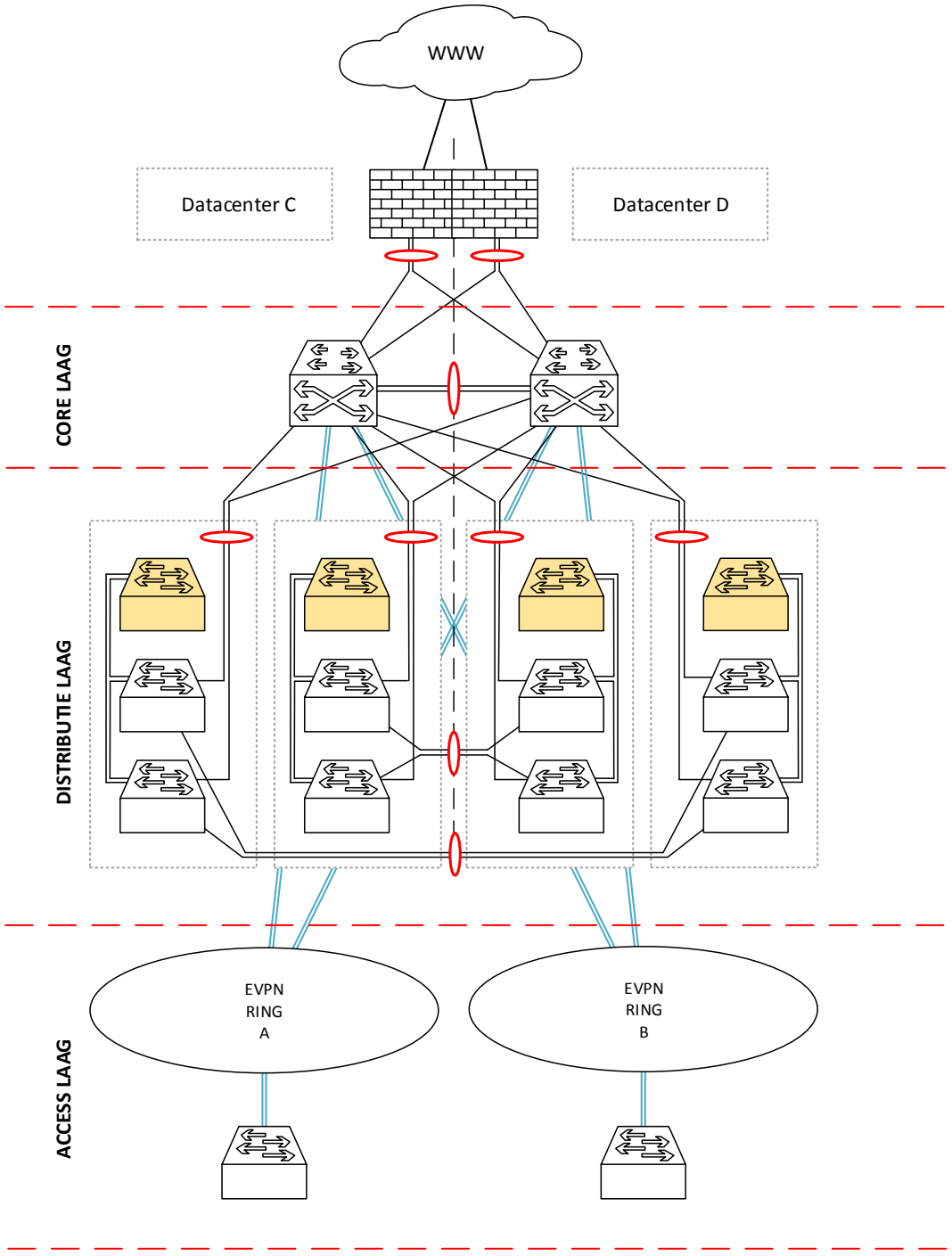
De core laag is opgebouwd met twee core switches – een in elk van de datacenters. De core switches zijn direct verbonden met de firewalls.

De distributie laag is opgebouwd aan de hand van het Avaya Distributed Top of Rack principe – het Data Center reference architecture [11]. Er is gekozen voor vier distributie stacks die elk weer zijn opgebouwd met drie distributie switches. De distributie laag worden gebruikt voor het verschaffen

van toegang aan de servers en andere netwerkdiensten tot de netwerk infrastructuur en zijn verbonden met de switches in de core laag waardoor de core switches voor een groot deel ontlast worden.

De access laag wordt – net als de distributie laag – gebruikt voor het verschaffen van toegang tot de netwerk infrastructuur, maar dan aan end devices (computers, printers, mobiele devices etc.) in de branch offices.

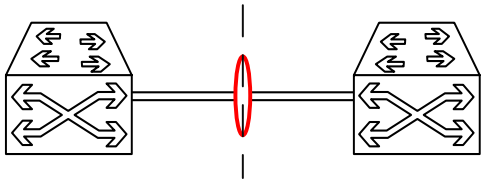
Tussen de core laag en de access laag zitten Ethernet VPN verbindingen (EVPN) van KPN waarmee de verbindingen tussen de branch offices en het CyberCentre worden gefaciliteerd.



Figuur 8 - Nieuwe architectuur van de netwerk infrastructuur (vereenvoudigd overzicht)

Core laag

De core laag is opgebouwd met twee core switches (Figuur 9) – een in elk van de datacenters. De switches in de core laag zijn door middel van trunk verbindingen geconfigureerd als redundant switch cluster.
De core switches zijn door middel van trunk verbindingen verbonden met de switch stacks in de distributie laag, de branch offices in de access laag en ook de firewalls.

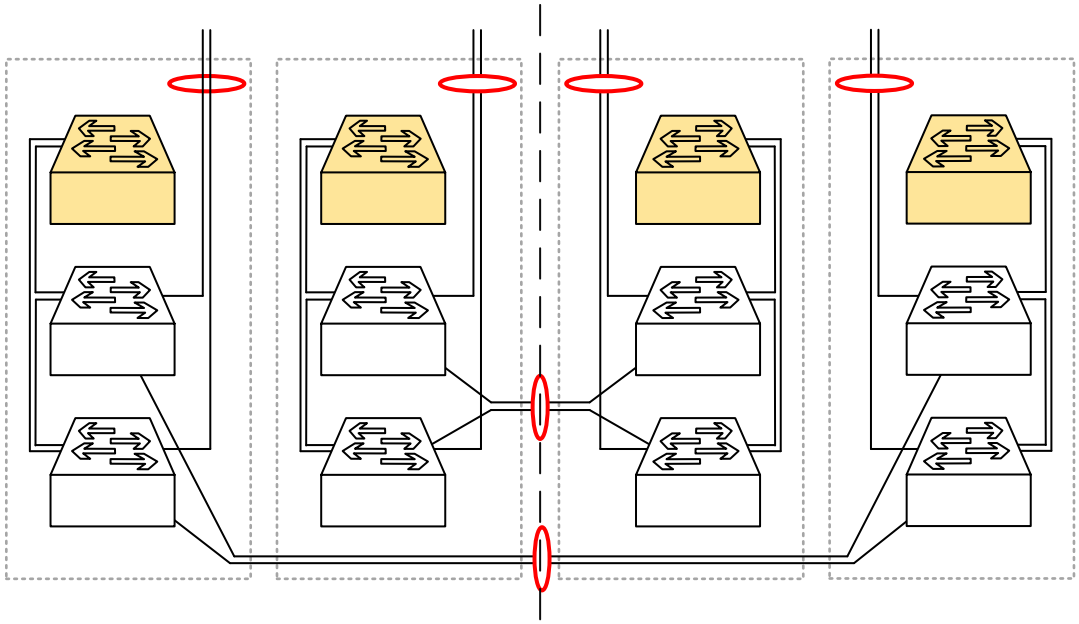


Figuur 9 - Core switches in de nieuwe situatie

Distributie laag

De switches in de distributie laag zijn door middel van redundante verbindingen geconfigureerd als switch stacks, vier in totaal. Elke distributie stack bestaat uit drie distributie switches.

De vier distributie stacks – zoals getoond in Figuur 10- zijn met elkaar verbonden als sets van twee stacks. De stacks in een set staan elk in een van de twee datacenters en zijn door middel van trunk verbindingen geconfigureerd als een redundant cluster.
De distributie stacks zijn door middel van trunk verbindingen verbonden met de core switches.



Figuur 10 - Distributie stacks in de nieuwe situatie (vereenvoudigd overzicht)

Specifieke kenmerken van de nieuwe architectuur

Ten opzichte van de huidige architectuur valt aan de nieuwe architectuur een aantal specifieke kenmerken op;

- Er is geen onderscheid meer tussen interne core switches en externe core switches. De intranet omgeving en de extranet omgeving bestaan op dezelfde fysieke hardware en worden softwarematig gescheiden.
- Het aantal core switches is teruggebracht naar twee.
- De Deloitte infrastructuur bestaat nu uit een aparte core laag, een aparte distributie laag en een aparte access laag. In tegenstelling tot de huidige infrastructuur, deze bestaat uit alleen een (collapsed) core laag en een access laag.
- De switches in de distributie laag en de access laag hebben redundante verbindingen met de switches in de core laag.
- De core switches en de distributie stacks worden als redundante clusters uitgevoerd.
- Redundantie wordt niet alleen gerealiseerd door de onderlinge verbindingen tussen de switches, maar ook door het feit dat de switches zijn verdeeld over twee datacenters.

7. Fase 3: Ontwerpfase

Tijdens de ontwerpfase van de opdracht komt het detail ontwerp van de nieuwe core netwerk infrastructuur tot stand. Er wordt een verdeling gemaakt tussen het fysieke ontwerp, het logisch ontwerp en het beheer ontwerp.

In het fysieke ontwerp worden de fysieke aspecten van het ontwerp beschreven; gebruikte apparatuur, de verschillende toegangslagen en de onderlinge verbindingen tussen de lagen.

Het logische ontwerp beschrijft de logische aspecten van het ontwerp; logische scheiding van netwerken op lagen twee en drie van het OSI model door middel van Vitual LAN's (VLAN) en Virtual Routing & Forwarding (VRF), de gebruikte protocollen en beveiliging.

Op te leveren (deel)producten in deze fase

- Detail ontwerp

7.1. Fysiek ontwerp

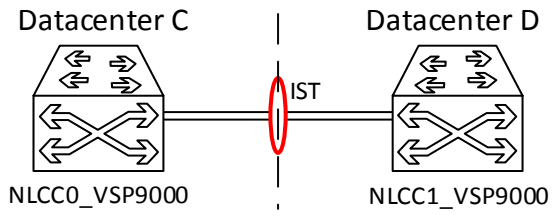
Na onderzoek naar de requirements en in overleg met de leverancier is er gekozen voor het Virtual Services Platform (VSP) van Avaya. In zijn totaliteit zullen twee types switches worden gebruikt in de nieuwe core netwerk infrastructuur;

- Er worden twee Avaya VSP 9000 switches geconfigureerd ten behoeve van de core laag.
- Er worden 12 Avaya VSP 7000 swithes geconfigureerd ten behoeve van de distributie laag.

Alle benodigde bekabeling zal nieuw worden geleverd door CommScope. De huidige bekabeling wordt voor de nieuwe infrastructuur niet opnieuw ingezet.

Hardware keuze van de core laag

Figuur 11 laat zien hoe de core laag is opgebouwd met twee VSP 9000 switches – een core switch per datacenter.



Figuur 11 - VSP 9000 configuratie in de core laag

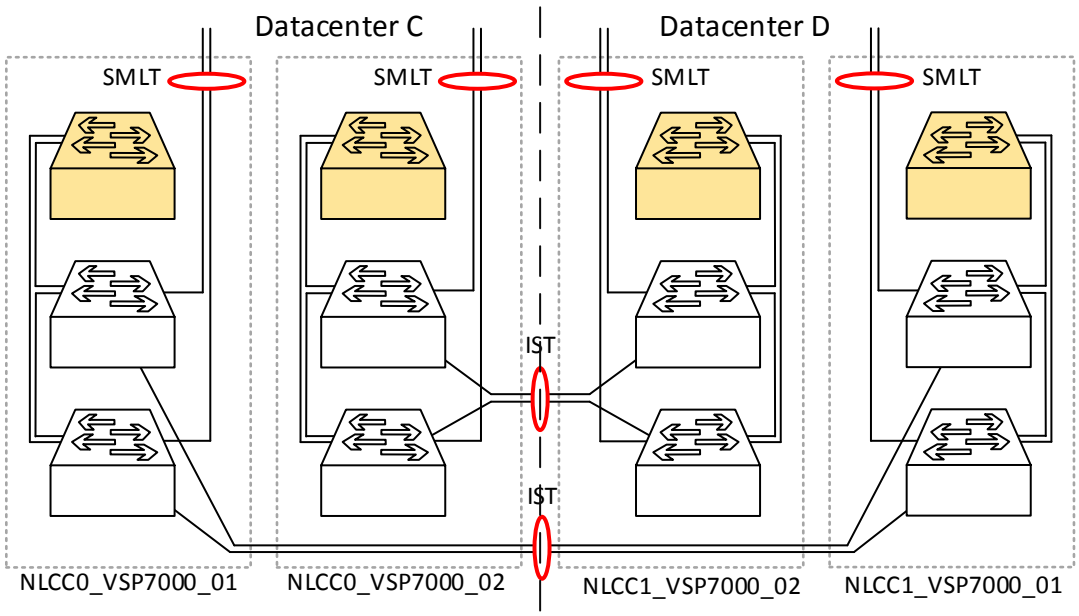
- Beide switches zijn opgebouwd met elk twee 9024XL 24-port 10G Ethernet SFP+ interface modules (10 Gbps) en een 9048GB 48-port 1G Ethernet SFP interface module (1 Gbps).
- De totale switch capaciteit is twee maal 288 Gbps per switch.
- Met oog op de toekomst zijn de VSP 9000 switches voorbereid op netwerk- en switchsnelheden van 40 Gbps en 100 Gbps.
- De core switches zijn elk uitgerust met drie netvoedingen. Deze netvoedingen kunnen worden vervangen terwijl de switches operationeel zijn – hot swappable. De totale belasting van de netvoedingen wordt automatisch evenredig gereguleerd.

- De interface modules, de voedingen en de cooling fans kunnen worden vervangen terwijl de switches operationeel zijn – hot swappable.
- Doordat de interface modules en de netvoedingen hot swappable zijn wordt voorkomen dat er een onderbreking plaats vindt in de te leveren services en diensten, hooguit kan een kort moment van performance verlies worden ervaren.
- Doordat de VSP 9000 switches Virtual Routing and Forwarding (VRF) ondersteunen, is het mogelijk om meerdere laag drie routing domains te configureren op een hardware platform. Hierdoor kunnen zowel de intranet omgeving als de extranet omgeving gescheiden van elkaar bestaan op dezelfde fysieke core switches.

Ten behoeve van redundantie is gekozen voor twee 9024XL modules per core switch. De core switches worden door middel van een trunk verbinding aan elkaar gekoppeld, waarbij de trunk verdeeld is over de beide modules.

Hardware keuze van de distributie laag

De distributie laag van de nieuwe infrastructuur wordt opgebouwd met vier distributie stacks, welke elk weer zijn opgebouwd met drie VSP 7000 switches (ook wel units genoemd) – twee distributie stacks per datacenter.



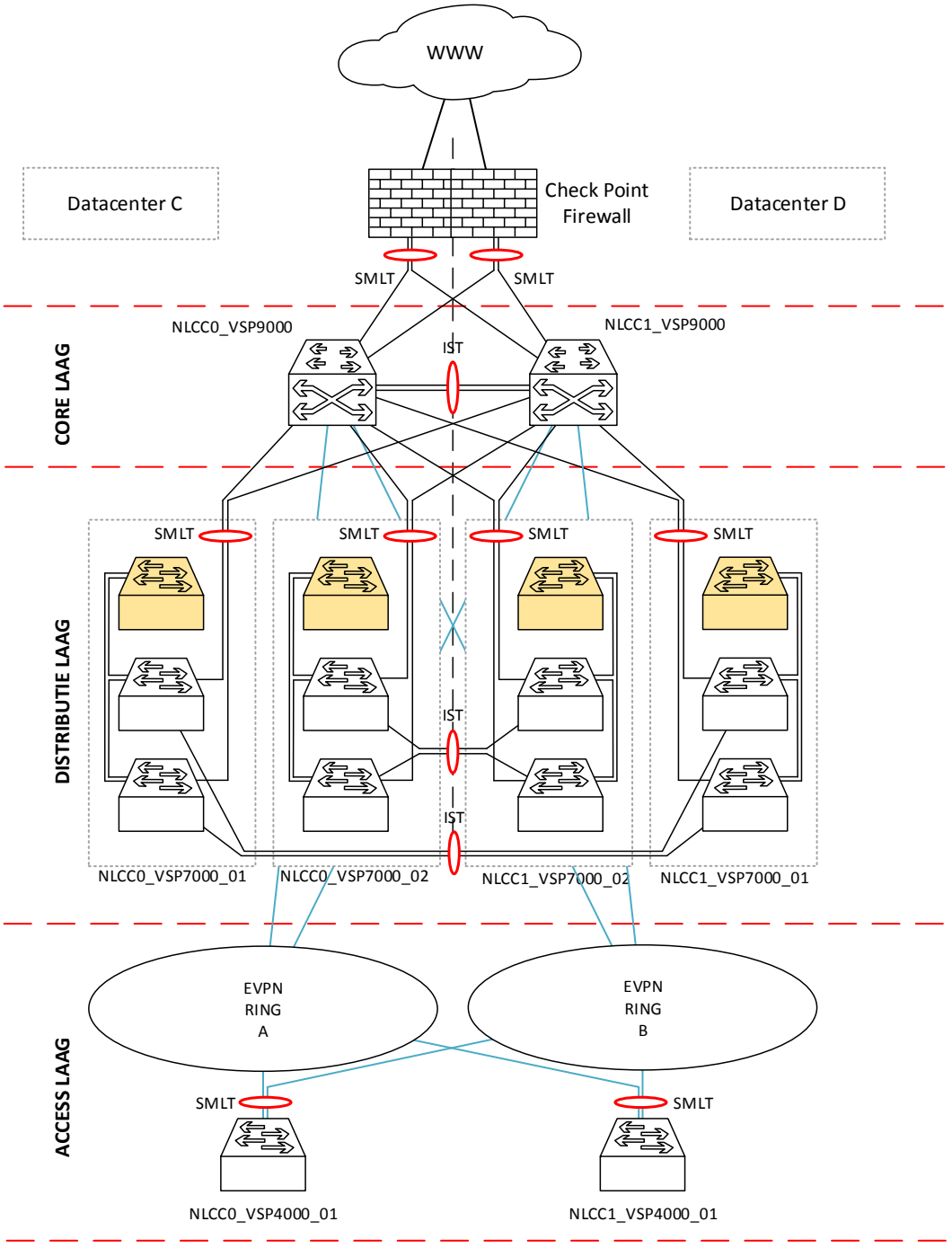
Figuur 12 - VSP 7000 configuratie in de distributie laag (vereenvoudigd overzicht)

- De distributie stacks zijn opgebouwd met twee 7024XLS 24-port 1/10 Gigabit Ethernet SFP+ switches (10 Gbps).
- Een VSP 7000 variant met 24 koper aansluitingen, dit ten behoeve van devices die niet beschikken over een SFP connector.
- De totale switch capaciteit is straks drie maal 240 Gbps per distributie stack.
- Met oog op de toekomst zijn de VSP 7000 switches voorbereid op netwerk- en switchsnelheden van 40 Gbps en 100 Gbps.
- De voedingen en de cooling fans kunnen worden vervangen terwijl de switches operationeel zijn – hot swappable.

Ten behoeve van redundantie is gekozen voor minimaal twee 7024XLS switches per distributie stack. De distributie stacks worden door middel van een trunk verbinding aan elkaar gekoppeld, waarbij de trunk verdeeld is over twee switches.

Tijdelijke distributie switches

Tot de koper variant van de VSP 7000 switch wordt uitgebracht, wordt per distributie stack een oude core switch gebruikt ten behoeve van de benodigde koper aansluitingen.
Deze nieuwe variant is wel getekend in de architectuur en in het detail ontwerp (in het geel), maar wordt verder niet besproken.



Figuur 13 - Nieuw ontwerp van de netwerk infrastructuur (vereenvoudigd overzicht)

Redundancy

De core switches zijn onderling met elkaar verbonden door middel van een Distributed Multi Link Trunk (DMLT) en een InterSwitch Trunk (IST), deze twee protocollen zijn actief op dezelfde fysieke trunk. DMLT maakt het mogelijk om een redundante verbinding tot stand te brengen en door gebruik te maken van IST is het mogelijk om met de twee fysieke switches een logisch device te maken, dat via verschillende routes en netwerkpaden benaderbaar is.

Door middel van Split Multi-Link Trunks (SMLT) zijn de core switches verbonden met de Check Point Firewalls. Door gebruik te maken van SMLTs worden redundante verbindingen gemaakt met de firewalls in beide datacenters.

De distributie stacks zijn door middel van SMLTs verbonden met core switches.

De branch offices zijn door middel van redundante Multi Protocol Label Switching (MPLS) verbindingen via de Ethernet-VPN (EVPN) ringen van KPN verbonden met de core switches.

Trunking

Tabel 6 toont de verbindingen van de interfaces tussen de verschillende devices in de core laag, distributie laag en access laag.

De benamingen die gebruikt zijn voor de devices, de interfaces en de trunks – alsmede de verdelingen van de interfaces en trunks – zijn op verzoek van de opdrachtgever fictief.

Device	Interface	Device	Interface	Trunk
NLCC0_VSP9000	M0_SFP00 M1_SFP00	NLCC1_VSP9000	M0_SFP00 M1_SFP00	T0
NLCC0_Firewall	*BUITEN SCOPE*	NLCC0_VSP9000 NLCC1_VSP9000	M0_SFP01 M0_SFP01	T1
NLCC1_Firewall		NLCC0_VSP9000 NLCC1_VSP9000	M1_SFP01 M1_SFP01	T2
NLCC0_VSP4000_01	*BUITEN SCOPE*	NLCC0_VSP9000 NLCC1_VSP9000	M0_SFP02 M0_SFP02	T3
NLCC1_VSP4000_01		NLCC0_VSP9000 NLCC1_VSP9000	M1_SFP02 M1_SFP02	T4
NLCC0_VSP7000_01	U0_SFP00 U1_SFP00	NLCC1_VSP7000_01	U0_SFP00 U1_SFP00	T5
NLCC0_VSP7000_02	U0_SFP00 U1_SFP00	NLCC1_VSP7000_02	U0_SFP00 U1_SFP00	T6
NLCC0_VSP7000_01	U0_SFP01 U1_SFP01	NLCC0_VSP9000 NLCC1_VSP9000	M0_SFP03 M0_SFP03	T7
NLCC0_VSP7000_02	U0_SFP01 U1_SFP01	NLCC0_VSP9000 NLCC1_VSP9000	M1_SFP03 M1_SFP03	T8
NLCC1_VSP7000_02	U0_SFP01 U1_SFP01	NLCC0_VSP9000 NLCC1_VSP9000	M0_SFP04 M0_SFP04	T9
NLCC1_VSP7000_01	U0_SFP01 U1_SFP01	NLCC0_VSP9000 NLCC1_VSP9000	M1_SFP04 M1_SFP04	T10

Tabel 6 - Getrunkte interfaces in de core en distributie laag

De kolommen “Device” geven aan tussen welke twee devices de verbinding(en) tot stand is gebracht; core switches, distributie stacks, access switches of firewalls.

Bijvoorbeeld:
NLCC0_VSP9000 betreft de VSP 9000 core switch van site 0 (Datacenter C).

De kolommen “Interface” geven aan welke interfaces – maar ook modules en units – gebruikt zijn om de verbinding op tot stand te brengen.

- M = Module nummer in het VSP 9000 chassis.
- U = Unit nummer in de VSP 7000 stack (of VSP 4000 stack).
- SFP = Poort nummer van de betreffende module of unit.

Bijvoorbeeld:
M0_SFP01 betreft poort nummer 1 van module 0 in een van de twee core switches.

Omdat de Check Point firewalls en de access switches (VSP 4000) buiten de scope van de opdracht vallen, zijn deze slechts deels uitgewerkt in de tabel.

De kolom “Trunk” beschrijft de trunk naam die is toegekend aan de getrunkte interfaces.

Flexible Advanced Stacking Technology (FAST)

De distributie stacks zijn geconfigureerd in stack-mode. De distributie switches zijn onderling met elkaar verbonden door een virtual backplane te creëren door middel van het toepassen van Flexible Advanced Stacking Technology (FAST).

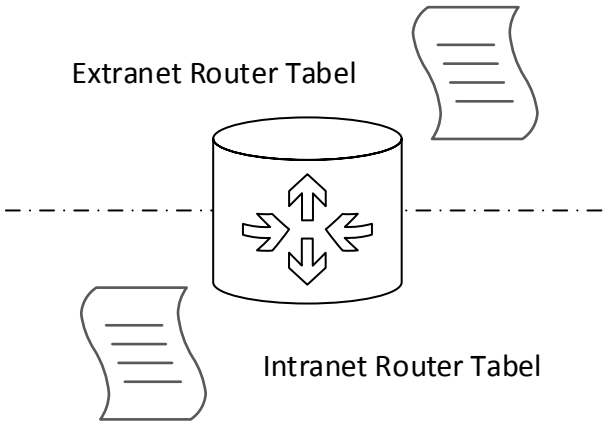
FAST werkt bi directioneel over de stacks en werkt ook full duplex. Door gebruik te maken van FAST is op de distributie stacks een shortest path first protocol actief waardoor data gegarandeerd over het kortste pad door de stack wordt geforward. Ook wanneer een switch of een link wegvalt, forward FAST data over het kortst mogelijke datapad door de stack. [12]

Dankzij Auto Unit Replacement (AUR) en New Unit Quick Config is het mogelijk om switches uit de stack gemakkelijk te vervangen en configureren. [12]

7.2. Logisch ontwerp

Virtual Routing and Forwarding

Netwerkverkeer voor de intranet omgeving en voor de extranet omgeving wordt op laag drie van elkaar gescheiden door middel van Virtual Routing and Forwarding (VRF). Dit maakt het mogelijk om meerder router tabellen op dezelfde fysieke hardware te laten bestaan. Figuur 14 laat dit op een vereenvoudigde manier zien.



Figuur 14 - Het principe van Virtual Routing and Forwarding

Elk van de twee VRF's – de intranet omgeving en de extranet omgeving – krijgt een eigen subnet toebedeeld. Binnen zijn eigen subnet is het VRF verantwoordelijk voor het correct routeren van al het netwerkverkeer. Tabel 7 toont de VRF's en de toebedeelde subnets.

Op verzoek van de opdrachtgever zijn er fictieve IP reeksen gebruikt.

VRF	SUBNET	IP RANGE		SUBNET MASK
VRF1 (INTRANET)	10.1.0.0/16	10.1.0.1	10.1.255.254	255.255.0.0
VRF2 (EXTRANET)	192.168.0.0/16	192.168.0.1	192.168.255.254	255.255.0.0

Tabel 7 - Overzicht van de VRF's op de core switches

Elk VRF is vervolgens weer opgedeeld in kleinere subnets, welke weer zijn ondergebrachte in aparte VLAN's.

Virtual LAN

Netwerkverkeer op laag twee wordt van elkaar gescheiden door elk van de subnets in een eigen Virtual LAN (VLAN) te plaatsen. Door de kleinere subnets in VLAN's te plaatsen, wordt de grootte van de laag twee broadcastdomeinen aanzienlijk gereduceerd en daarmee ook de kans op broadcaststorms.
Door gebruik te maken van VLAN's kunnen hosts (nodes) op verschillende locaties toch tot hetzelfde logische netwerk behoren.

Tabel 8 toont een overzicht van de VLAN's voor het intranet core netwerk.

VLAN	VLAN ID	IP RANGE		SUBNET MASK	VLAN IP
WIRELESS	1000	10.1.0.1	10.1.63.254	255.255.192.0	10.1.63.254
LOAD BALANCER	1064	10.1.64.1	10.1.65.254	255.255.254.0	10.1.65.254
BEHEERSYSTEMEN	1066	10.1.66.1	10.1.67.254	255.255.254.0	10.1.67.254
CORE	1068	10.1.68.1	10.1.68.254	255.255.255.0	10.1.68.254
DISTRIBUTION	1069	10.1.69.1	10.1.69.254	255.255.255.0	10.1.69.254
ACCESS	1070	10.1.70.1	10.1.70.254	255.255.255.0	10.1.70.254
FIREWALL	1071	10.1.71.1	10.1.71.254	255.255.255.0	10.1.71.254
GWAN	1072	10.1.72.1	10.1.72.254	255.255.255.0	10.1.72.254
IPTV	1073	10.1.73.1	10.1.73.254	255.255.255.0	10.1.73.254

Tabel 8 - Overzicht van de VLAN's voor het intranet core netwerk

Tabel 9 toont een overzicht van de VLAN's voor de servers in het intranet.

VLAN	VLAN ID	IP RANGE		SUBNET MASK	VLAN IP
WEB01	2000	10.2.0.1	10.2.3.254	255.255.252.0	10.2.3.254
APP01	2004	10.2.4.1	10.2.7.254	255.255.252.0	10.2.7.254
DB01	2008	10.2.8.1	10.2.11.254	255.255.252.0	10.2.11.254
SAP	2012	10.2.12.1	10.2.13.254	255.255.254.0	10.2.13.254
SAP_BEDK	2014	10.2.14.1	10.2.14.254	255.255.255.0	10.2.14.254
SAP_TR	2015	10.2.15.1	10.2.15.254	255.255.255.0	10.2.15.254

Tabel 9 - Overzicht van de VLAN's voor de intranet servers

Tabel 10 toont een overzicht van de VLAN's voor alle end devices, deze bevinden zich allemaal in het intranet.

VLAN	VLAN ID	IP RANGE		SUBNET MASK	VLAN IP
NOTEBOOKS	3000	10.3.0.1	10.3.31.254	255.255.224.0	10.3.31.254
MOBILE_DEVICES	3032	10.3.32.1	10.3.63.254	255.255.224.0	10.3.63.254
VDI	3064	10.3.64.1	10.3.65.254	255.255.254.0	10.3.65.254
DESKTOPS	3066	10.3.66.1	10.3.66.254	255.255.255.0	10.3.66.254
PRINTERS	3067	10.3.67.1	10.3.67.254	255.255.255.0	10.3.67.254

Tabel 10 - Overzicht van de VLAN's voor de end devices

Tabel 11 toont het VLAN voor het gasten netwerk.

VLAN	VLAN ID	IP RANGE		SUBNET MASK	VLAN IP
GUEST	1600	172.16.0.1	172.16.3.254	255.255.252.0	172.16.3.254

Tabel 11 - VLAN voor het gasten netwerk

Tabel 12 toont een overzicht van de VLAN's voor het extranet core netwerk.

VLAN	VLAN ID	IP RANGE		SUBNET MASK	VLAN IP
CORE	5000	192.168.50.1	192.168.50.254	255.255.255.0	192.168.50.254
DISTRIBUTION	5001	192.168.51.1	192.168.51.254	255.255.255.0	192.168.51.254
FIREWALL	5002	192.168.52.1	192.168.52.254	255.255.255.0	192.168.52.254
LOAD BALANCER	5003	192.168.53.1	192.168.53.254	255.255.255.0	192.168.53.254

Tabel 12 - Overzicht van de VLAN's voor het extranet core netwerk

Tabel 13 toont een overzicht van de VLAN's voor de servers in het extranet.

VLAN	VLAN ID	IP RANGE		SUBNET MASK	VLAN IP
WEB01	6000	192.168.60.1	192.168.60.254	255.255.255.0	192.168.60.254
APP01	6001	192.168.61.1	192.168.61.254	255.255.255.0	192.168.61.254
DB01	6002	192.168.62.1	192.168.62.254	255.255.255.0	192.168.62.254

Tabel 13 - Overzicht van de VLAN's voor de extranet servers

Gebruikte netwerk protocollen

Voor het correct functioneren van de verschillende onderdelen van de Deloitte netwerk infrastructuur is in de core netwerk infrastructuur een combinatie van protocollen actief uit laag twee en laag drie van het OSI model.
De belangrijkste reden waarom is gekozen voor een combinatie van protocollen uit en laag twee en laag drie is dat laag twee protocollen minder tijd nodig hebben om uitval van netwerkpaden te detecteren, waardoor minder tijd nodig is voor een failover tussen netwerkpaden.

- **InterSwitch Trunk (IST)** is geconfigureerd op de core switches en de distributie stacks ten behoeve van link aggregatie tussen de core switches onderling en de distributie stacks (voor de distributie stacks geldt dat deze in sets van twee worden geclusterd) onderling. Door op deze manier link aggregatie toe te passen tussen peer devices in een switch cluster kan van twee fysieke devices een logisch device worden gemaakt.

- **Distributed Multi Link Trunk (DMLT)** is naast IST geconfigureerd op de core switches en distributie stacks. Het zorgt voor een redundante verbinding tussen de core switches onderling en de distributie stacks onderling. Als een module van een van de core switches of een switch van een van de distributie stacks uitvalt, blijft de verbinding tussen de devices en de IST in tact.

- **Split Multi-Link Trunk (SMLT)** is geconfigureerd tussen de core switches en de firewalls en tussen de core switches en de distributie stacks voor het leveren van load balancing en redundante verbindingen tussen core switches en firewalls en core switches en distributie stacks. Wanneer een van de core switches wegvalt, blijven alle diensten en verbindingen beschikbaar op de overgebleven core switch. Op deze manier wordt het Single Point of Failure (SPOF) weggenomen in de core laag van de infrastructuur.

- **Virtual Router Redundancy Protocol (VRRP)** is geconfigureerd op de core switches en zorgt voor een hogere beschikbaarheid van de core switches voor de distributie stacks.

- **Simple Loop Prevention Protocol (SLPP)** wordt op de core switches geconfigureerd om te voorkomen dat dezelfde data over verschillende data paden wordt aangeboden en er netwerk loops ontstaan.

- **Shortest Path Bridging (SPB)** is geconfigureerd op de core switches en de distributie stacks om mogelijk te maken dat de core laag en de distributie laag full mesh geconfigureerd worden en om gebruik te maken van load balancing.
  SPB maakt ook snelle fail overs mogelijk, zou er een data pad wegvallen. Ook kunnen op deze manier alle VLAN’s beschikbaar gemaakt worden op alle locaties – ook op de branch offices.

- **Virtual Link Aggregation Control Protocol (VLACP)** is geconfigureerd op de interfaces tussen de core switches en de branch offices ten behoeve van een snelle fail over in geval dat een van de data paden tussen de core laag en de access laag wegvalt.

- **Protocol Independent Multicast (PIM)** is geconfigureerd op de core switches ten behoeve van het multicasten van IPTV.

- **Internet Group Management Protocol (IGMP)** is geconfigureerd op de access switches in de branch offices en wordt – net als PIM – gebruikt voor het multicasten van IPTV.

- **Border Gateway Protocol (BGP)** is geconfigureerd op het extranet VRF om netwerk paden van en naar het internet te bekend te maken en netwerkverkeer van en naar van en naar het internet te routeren.

- **Routing Information Protocol (RIP)** is geconfigureerd op de core switches en de access switches ten behoeve van het uitwisselen van routing informatie tussen de core laag en de access laag.

IP configuratie van de core switches en de distributie stacks

Aan de hand van het IP nummer plan (Figuur 17 op pagina 58) krijgen de interfaces van de switches IP adressen toegekend.

De tabellen - IP configuratie van het intranet VRF en - IP configuratie van het extranet VRF (Tabel 14 en Tabel 15) laten zien welk IP adres, welk routing protocol en welk trunk type op de switch interfaces is geconfigureerd.

Op verzoek van de opdrachtgever zijn er fictieve benamingen gebruikt voor devices, interfaces en trunks.

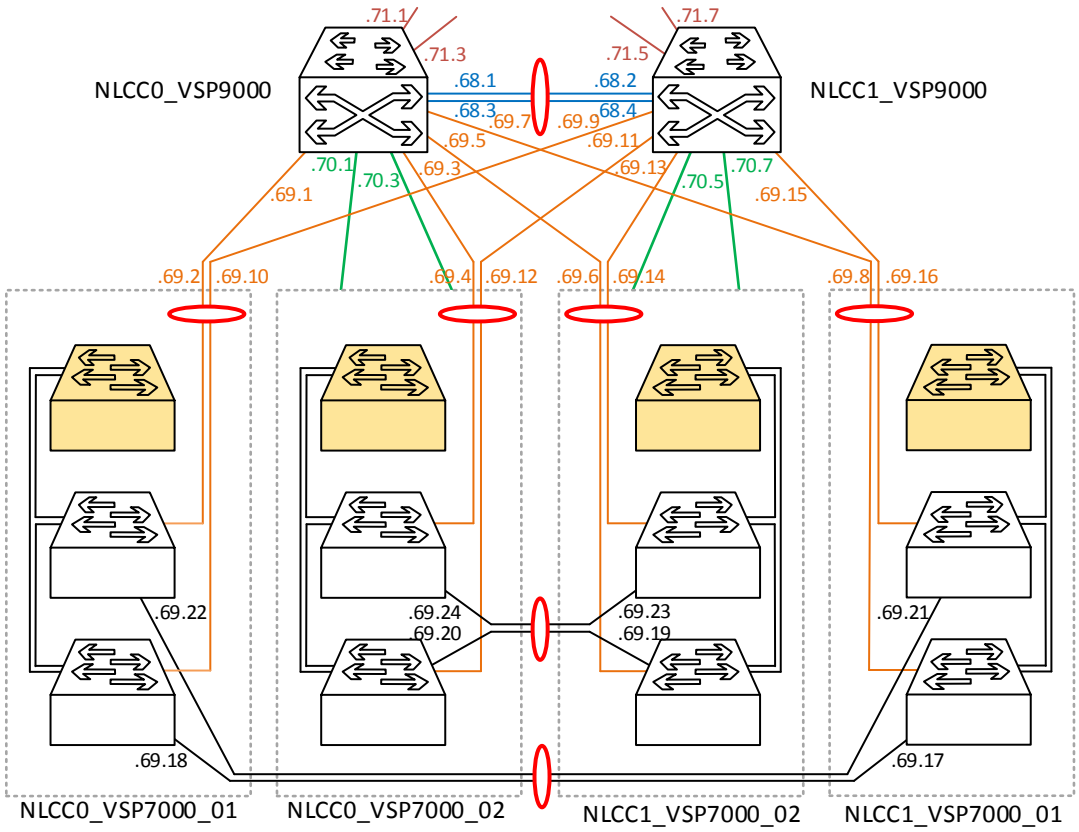
IP CONFIGURATIE INTRANET VRF							
Device	**Interface**	**IP**	**Device**	**Interface**	**IP**	**Protocol**	**Trunk type**
NLCC0_VSP9000	M0_SFP00 M1_SFP00	10.1.68.1 10.1.68.3	NLCC1_VSP9000	M0_SFP00 M1_SFP00	10.1.68.2 10.1.68.4	RIP	IST
NLCC0_Firewall	*BUITEN SCOPE*	10.1.71.2 10.1.71.6	NLCC0_VSP9000 NLCC1_VSP9000	M0_SFP01 M0_SFP01	10.1.71.1 10.1.71.5	RIP	SMLT
NLCC1_Firewall		10.1.71.4 10.1.71.8	NLCC0_VSP9000 NLCC1_VSP9000	M1_SFP01 M1_SFP01	10.1.71.3 10.1.71.7	RIP	SMLT
NLCC0_VSP4000_01	*BUITEN SCOPE*	10.1.70.2 10.1.70.6	NLCC0_VSP9000 NLCC1_VSP9000	M0_SFP02 M0_SFP02	10.1.70.1 10.1.70.5	RIP	SMLT
NLCC1_VSP4000_01		10.1.70.4 10.1.70.8	NLCC0_VSP9000 NLCC1_VSP9000	M1_SFP02 M1_SFP02	10.1.70.3 10.1.70.7	RIP	SMLT
NLCC0_VSP7000_01	U0_SFP00 U1_SFP00	10.1.69.18 10.1.69.22	NLCC1_VSP7000_01	U0_SFP00 U1_SFP00	10.1.69.17 10.1.69.21	RIP	IST
NLCC0_VSP7000_02	U0_SFP00 U1_SFP00	10.1.69.20 10.1.69.24	NLCC1_VSP7000_02	U0_SFP00 U1_SFP00	10.1.69.19 10.1.69.23	RIP	IST
NLCC0_VSP7000_01	U1_SFP01 U2_SFP00	10.1.69.2 10.1.69.10	NLCC0_VSP9000 NLCC1_VSP9000	M0_SFP03 M0_SFP03	10.1.69.1 10.1.69.9	RIP	SMLT
NLCC0_VSP7000_02	U1_SFP01 U2_SFP00	10.1.69.4 10.1.69.12	NLCC0_VSP9000 NLCC1_VSP9000	M1_SFP03 M1_SFP03	10.1.69.3 10.1.69.11	RIP	SMLT
NLCC1_VSP7000_02	U1_SFP01 U2_SFP00	10.1.69.6 10.1.69.14	NLCC0_VSP9000 NLCC1_VSP9000	M0_SFP04 M0_SFP04	10.1.69.5 10.1.69.13	RIP	SMLT
NLCC1_VSP7000_01	U1_SFP01 U2_SFP00	10.1.69.8 10.1.69.16	NLCC0_VSP9000 NLCC1_VSP9000	M1_SFP04 M1_SFP04	10.1.69.7 10.1.69.15	RIP	SMLT

Tabel 14 - IP configuratie van het intranet VRF

IP CONFIGURATIE EXTRANET VRF							
Device	**Interface**	**IP**	**Device**	**Interface**	**IP**	**Protocol**	**Trunk type**
NLCC0_Firewall	*BUITEN SCOPE*	192.168.52.2 192.168.52.4	NLCC0_VSP9000 NLCC1_VSP9000	M0_SFP01 M0_SFP01	192.168.52.1 192.168.52.3	RIP	SMLT
NLCC1_Firewall		192.168.52.6 192.168.52.8	NLCC0_VSP9000 NLCC1_VSP9000	M1_SFP01 M1_SFP01	192.168.52.5 192.168.52.7	RIP	SMLT

Tabel 15 - IP configuratie van het extranet VRF

Ter illustratie laat Figuur 15 - IP configuratie van de core laag en de distributie laag – zien hoe de IP configuratie in de core laag en de distributie laag is.



Figuur 15 - IP configuratie van de core laag en de distributie laag

- Blauw = trunk verbinding (IST) tussen de core switches.
- Oranje = trunk verbinding (SMLT) tussen de distributie laag en de core laag.
- Bruin = trunk verbinding (SMLT) tussen de core laag en de firewalls.
- Groen = trunk verbinding (SMLT) tussen de core laag en de access laag.
- Zwart = trunk verbinding (IST) tussen de distributie stacks.

Toegepaste beveiliging

Authenticatie voor toegang tot de core netwerk infrastructuur gebeurd op basis van het Extensible Authentication Protocol (EAP) door middel van de installatie van certificaten op netwerk clients. Elke netwerk client – computer, smartphone, e.d. – die toegang wil tot de infrastructuur moet een geldig certificaat zijn voorzien.
Voor overige devices – waarvoor het niet mogelijk is om door middel van een certificaat te authentiseren – worden interfaces op de access switches gereserveerd.

Authenticatie gebeurd alleen in de access laag. Devices in de core laag en distributie laag worden als veilig beschouwd en hoeven niet geauthentiseerd te worden.

Authenticatie voor het gasten netwerk gebeurd op basis van een gebruikersnaam en wachtwoord. Deze worden beheerd met behulp van het software pakket SmartPass, dat ook in de huidige situatie wordt gebruikt voor het beheren van gasten accounts. Gasten hebben na authenticatie enkel toegang tot het internet.

8. Fase 4: Ontwikkelfase

De migratie van de oude core infrastructuur naar de nieuwe core infrastructuur wordt uitgevoerd als een “Big Bang”. Alle acties worden binnen een gereserveerd tijdslot uitgevoerd.

Om de overgang van de oude core infrastructuur naar de nieuwe core infrastructuur zo soepel mogelijk te laten verlopen is het van belang dat een goed stappenplan aanwezig is. In de ontwikkelfase komt een implementatieplan tot stand dat de acties en stappen beschrijft die nodig zijn om deze soepele overgang te kunnen realiseren.

De nieuwe core netwerk infrastructuur wordt opgebouwd naast de bestaande en zal in eerste instantie ‘droog’ schaduw draaien. Hierna zullen de verschillende onderdelen stap voor stap worden verhuist van de oude naar de nieuwe core netwerk infrastructuur.

Tijdens het implementeren wordt gebruik gemaakt van tijdelijke distributie switches ten behoeve van de benodigde koperaansluitingen (zoals beschreven op pagina 24).

Op te leveren (deel)producten in deze fase

- Implementatieplan

8.1. Voorbereidingen

De eerste stap voor het daadwerkelijke migreren van de core infrastructuur is controleren of het datacenter voldoende is uitgerust om alle apparatuur te kunnen plaatsen.

- Controleren of de 19” racks voldoende capaciteit hebben om tijdelijk de nieuwe apparatuur naast de oude apparatuur te kunnen inbouwen. Als dit niet het geval is, moeten extra racks worden bijgeplaatst.
- Controleren of er voldoende stroomgroepen en 230V aansluitingen aanwezig zijn om tijdelijk de nieuwe apparatuur naast de oude apparatuur te kunnen voorzien van spanning en redundantie.
- Controleren of er voldoende noodstroomvoorzieningen aanwezig zijn om de core switches en distributie stacks op aan de te sluiten.

Redundante voedingen

- De VSP 9000 switches worden elk uitgevoerd met drie voedingen met een vermogen van 2kW elk. Dit komt neer op 6kW vermogen per switch.
  Elk van de drie voedingen wordt aangesloten op een aparte stroomgroep. Op deze manier is er niet alleen redundantie als een van de voedingen uitvalt, maar ook als een van de stroomgroepen uit zou vallen.
- De VSP 7000 switches worden elk uitgevoerd met twee voedingen met een vermogen van 450W elk. Dit komt neer op 900W vermogen per switch en 1,8kW vermogen per distributie stack.
  De voedingen van de distributie stacks worden per twee aangesloten op een aparte stroom groep. Per groep mag niet meer dan één voeding van eenzelfde switch zijn aangesloten.

Tabel 16 toont het aantal voedingen per core switch en per distributie stack en het totale verbruik ervan.

	Switch(-stack)	Aantal voedingen	Verbruik per voeding	Totaal verbruik
Core laag	NLCC0_VSP9000	3	2kW	6kW
	NLCC1_VSP9000	3	2kW	6kW
Distributie laag	NLCC0_VSP7000_01	4	450W	1,8kW
	NLCC0_VSP7000_02	4	450W	1,8kW
	NLCC1_VSP7000_01	4	450W	1,8kW
	NLCC1_VSP7000_02	4	450W	1,8kW

Tabel 16 - Overzicht stroomverbuik

8.2. GO of NO-GO

Om de migratie gefaseerd uit te kunnen voeren is deze verdeeld in zeven stappen. Per stap wordt bekeken of het nodig is om het implementatieplan bij te sturen. Bijsturing van het implementatieplan kan nodig zijn om een stap succesvol af te kunnen worden, zelfs als zich onvoorziene incidenten voordoen.

Er kan alleen naar een volgende stap worden overgegaan wanneer de voorgaande stap succesvol is afgerond.

8.3. Stap 1: de core laag opbouwen

De eerste stap is het opbouwen van de nieuwe core laag. Het plaatsen van de nieuwe core switches en het realiseren van de trunk verbindingen van en naar de core switches.

De acties die in deze stap worden uitgevoerd, staan beschreven in Tabel 17 - Uit te voeren acties in migratie stap 1.

	Uit te voeren acties
1.	Configuraties plaatsen op de nieuwe core switches.
2.	Nieuwe core switches in de 19” racks plaatsen.
3.	Trunk bekabeling tussen de core switches aanbrengen.
4.	Nieuwe core switches één voor één online brengen.
5.	Tests uitvoeren; - Controleren of de nieuwe core switches online zijn. - Testen of de trunk verbinding tot stand komt. - Controleren of er routing informatie wordt uitgewisseld.
6.	Firewall verbindingen migreren van de oude core switches naar de nieuwe core switches en online brengen.
7.	Tests uitvoeren; - Testen of de trunk verbindingen tot stand komen. - Testen of er dataverkeer van en naar de firewalls gerouteerd kan worden.
8.	Externe verbindingen migreren van de oude core switches naar de nieuwe core switches en online brengen.
9.	Tests uitvoeren; - Testen of de trunk verbindingen tot stand komen. - Testen of er dataverkeer van en naar de ISP gerouteerd kan worden.

Tabel 17 - Uit te voeren acties in migratie stap 1

8.4. Stap 2: de distributie laag opbouwen

Het realiseren van de distributie laag in de nieuwe core infrastructuur gebeurd in twee stappen. De eerste stap is het inbouwen van de distributie switches en de FAST koppelingen maken om de distributie switches te configureren als distributie stacks. Hierna kan de distributie laag worden gekoppeld aan de core laag.

De acties die in deze stap worden uitgevoerd, staan beschreven in Tabel 18 - Uit te voeren acties in migratie stap 2.

	Uit te voeren acties
1.	Configuraties plaatsen op de nieuwe distributie switches.
2.	Distributie switches in de 19” racks plaatsen.
3.	FAST bekabeling ten behoeve van de stack configuratie tussen de distributie switches aanbrengen.
4.	Trunk bekabeling tussen de distributie stacks en de core switches en de distributie stacks onderling aanbrengen.
5.	Distributie stacks één voor één online brengen.
6.	Tests uitvoeren; - Controleren of de distributie stacks online zijn. - Testen of de trunk verbindingen tot stand komen. - Controleren of de datapaden worden gemaakt. - Controleren of de core laag en distributie laag loop-vrij zijn. - Controleren of er routing informatie wordt uitgewisseld tussen de distributie stacks onderling en tussen de distributie stacks en de core switches.
7.	Trunk bekabeling tussen de tijdelijke distributie switches en de core switches aanbrengen.
8.	De tijdelijke distributie switches één voor één online brengen.
9.	Tests uitvoeren; - Controleren of de tijdelijke distributie switches online zijn. - Testen of de trunk verbindingen tot stand komen. - Controleren of de datapaden worden gemaakt. - Controleren of de core laag en de distributie laag loop-vrij zijn. - Controleren of er routing informatie wordt uitgewisseld tussen de tijdelijke distributie switches en de core switches.

Tabel 18 - Uit te voeren acties in migratie stap 2

8.5. Stap 3: de distributie laag migreren

De tweede stap voor het realiseren van den distributie laag is het migreren van de netwerkaansluitingen van de oude core switches naar de nieuwe distributie stacks en de tijdelijke distributie switches.

De acties die in deze stap worden uitgevoerd, staan beschreven in Tabel 19 - Uit te voeren acties in migratie stap 3.

	Uit te voeren acties
1.	Fiber aansluitingen verhuizen van de oude core switches naar de distributie stacks.
2.	Koper aansluitingen verhuizen van de oude core switches naar de tijdelijke distributie switches.
3.	Nieuwe DHCP scope met gereserveerde IP adressen activeren.
4.	Alle devices in de distributie laag voorzien van een nieuw IP adres door middel van bijvoorbeeld een herstart van het device of van de TCP/IP stack van het device.
5.	Tests uitvoeren (steekproefsgewijs vanaf verschillende servers); - Testen of er verbinding is met de distributie stacks en distributie switches. - Testen of er verbinding is met de core switches. - Controleren of er internet connectivity is.

Tabel 19 - Uit te voeren acties in migratie stap 3

8.6. Stap 4: de access laag migreren

Hoewel de access laag zelf buiten scope valt van deze opdracht, is het verhuizen van de access laag van de oude naar de nieuwe infrastructuur wel een onderdeel van deze opdracht. Daarom is ook deze stap opgenomen in het implementatieplan.

De acties die in deze stap worden uitgevoerd, staan beschreven in Tabel 20 - Uit te voeren acties in migratie stap 4.

	Uit te voeren acties
1.	Aangepaste configuraties plaatsen op de bestaande access switches.
2.	Trunkbekabeling tussen de access laag en de core laag verhuizen van de oude core switches naar de nieuwe core switches.
3.	Trunk verbindingen tussen de access switches en de core switches down brengen en opnieuw up brengen ten behoeve van de aangepaste configuraties.
4.	Tests uitvoeren; - Testen of de trunk verbindingen opnieuw tot stand komen. - Controleren of de datapaden opnieuw worden gemaakt. - Controleren of de core laag en de access laag loop-vrij zijn. - Controleren of er routing informatie wordt uitgewisseld tussen de access switches en de core switches. Steekproefsgewijs van verschillende clients testen;. - Testen of er verbinding is met de access switch. - Testen of er verbinding is met de core switch. - Controleren of servers en services beschikbaar zijn. - Controleren of er internet connectivity is.

Tabel 20 - Uit te voeren acties in migratie stap 4

8.7. Stap 5: het network management systeem opnieuw inrichten

Om ook in de nieuwe situatie de core infrastructuur goed te kunnen blijven monitoren is het van belang dat het network management systeem opnieuw wordt ingericht.
Hiervoor is het niet nodig om een nieuwe server te installeren, maar zal de bestaande server worden gebruikt.

Hier voor is het nodig dat;

- Er een complete netwerkscan wordt uitgevoerd om alle aanwezige netwerk apparatuur te kunnen detecteren zodat deze kan worden opgenomen in het network management systeem.
- Het network management systeem opnieuw wordt ingericht voor de nieuwe infrastructuur, gebaseerd op de informatie die wordt verkregen uit de netwerkscan.
- Alle in het network management systeem opgenomen devices wordt verdeeld in logische groepen zodat deze gemakkelijk beheerd kunnen worden.

8.8. Stap 6: monitoring

Gedurende de eerste weken is het van belang dat de netwerklogs dagelijks worden nagelopen en dat de nieuwe core infrastructuur nauwlettend wordt gemonitord op;

- CPU gebruik
- QoS
- Throughput
- Packetloss

8.9. Stap 7: ontmantelen

Wanneer de nieuwe core infrastructuur voor 100% up-and-running is, worden de componenten van de oude core infrastructuur ontmanteld.

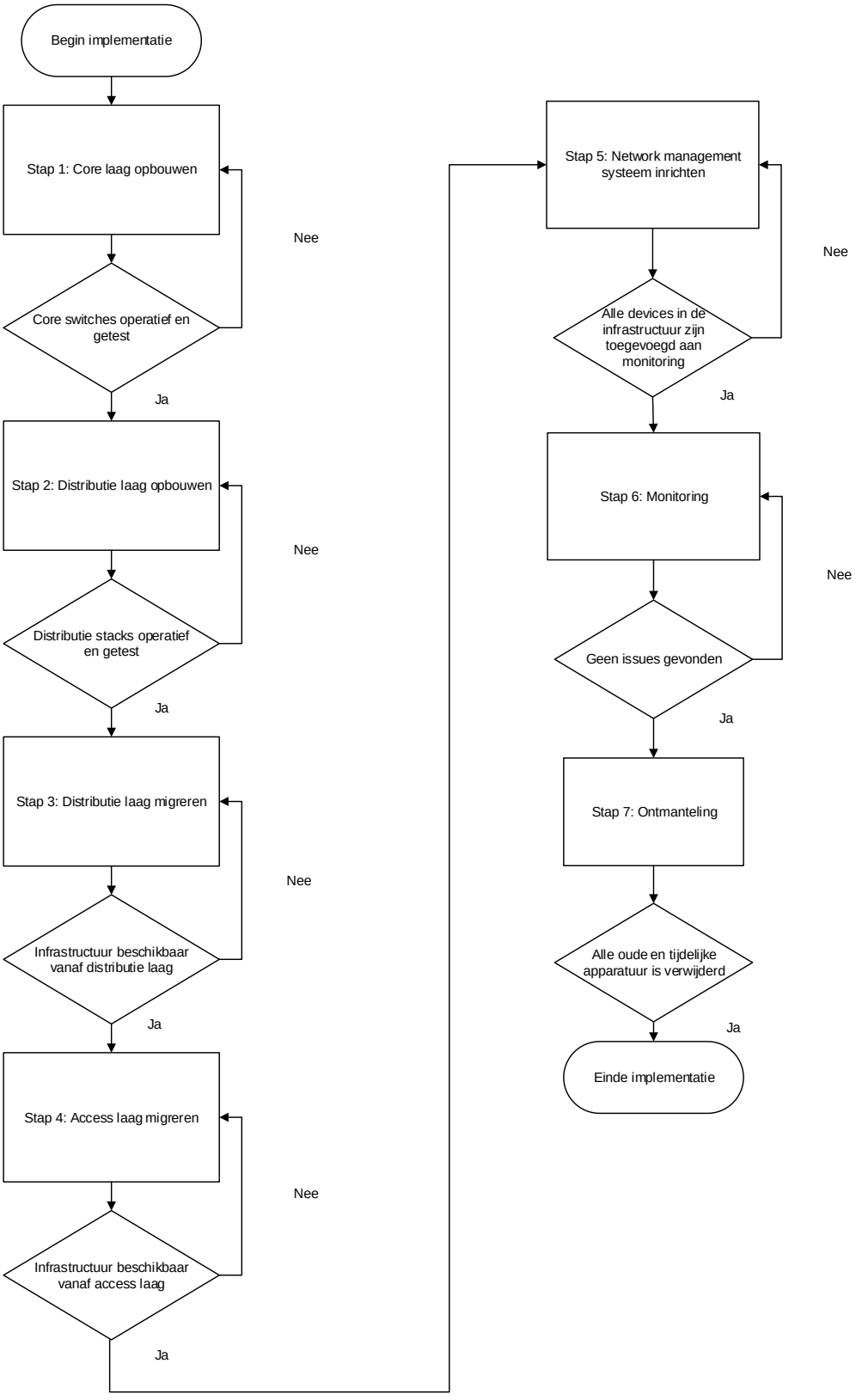
De acties die in deze stap worden uitgevoerd, staan beschreven in Tabel 21 - Uit te voeren acties in migratie stap 7.

	Uit te voeren acties
1.	Oude apparatuur verwijderen uit de 19” racks.
2.	Oude bekabeling verwijderen.
3.	Eventuele tijdelijke 19” racks verwijderen.
4.	Configuratie verwijderen van de oude core switches.
5.	Contact opnemen met mogelijk opkopers.

Tabel 21 - Uit te voeren acties in migratie stap 7

8.10. Flowchart van de stappen

Ter illustratie toont Figuur 16 - Flowchart met de stappen van de migratie – het stappenplan als een flowchart.



Figuur 16 - Flowchart met de stappen van de migratie

9. Conclusies en aanbevelingen

Onderstaande conclusie – en de daarbij horende aanbevelingen – komen direct voort uit het proof of concept. Hieruit zal blijken of het loont om het om proof of concept te accepteren en dit in de praktijk door te voeren.

9.1. Ter conclusie

Door het aantal core switches in de infrastructuur terug te brengen van zes naar twee core switches en een verdeling aan te brengen in een core laag en een distributie laag wordt het beheren en onderhouden van de core infrastructuur gemakkelijker, overzichtelijker, minder intensief en goedkoper.

Schaalbaarheid en flexibiliteit

- Door de infrastructuur op te splitsen in een fysieke core laag – de core switches – en een fysieke distributie laag – de distributie stacks – wordt een grote mate van schaalbaarheid en flexibiliteit gecreëerd.
  Zouden er niet voldoende netwerkaansluitingen beschikbaar zouden zijn in de distributie laag, dan kan de distributie laag gemakkelijk worden uitgebreid door switches bij te plaatsen in de distributie stacks. De andere kant op werkt dit natuurlijk ook, switches kunnen worden verwijderd uit een distributie stack als er een overschot aan netwerkaansluitingen zou ontstaan door bijvoorbeeld (verdere) consolidatie van het server platform.

- Voor de core switches en distributie stacks is minder ruimte nodig in de datacenters. Dit wordt in de nabije toekomst nog minder wanneer meer fysieke servers verdwijnen en het server platform verder gevirtualiseerd wordt.

Waarborgen van veiligheid

- Door gebruik te maken van Virtual Routing and Forwarding voor het scheiden van netwerkverkeer op laag drie en Virtual LAN's voor het scheiden van netwerkverkeer op laag twee, wordt de beveiliging van data (-verkeer) gewaarborgd.
  Verkeer van de intranet omgeving en verkeer van de extranet omgeving worden net als voorheen van elkaar gescheiden van elkaar afgehandeld door de core netwerk infrastructuur.

Meer netwerk performance

- Door de core netwerk infrastructuur opsplitsen in een core laag en een distributie laag is het niet langer nodig dat de core switches connectivity verzorgen en netwerkverkeer routeren en forwarden.
  De core switches routeren en forwarden netwerkverkeer terwijl de distributie stacks alle functionaliteiten ten behoeve van connectivity verzorgen. Dit levert extra netwerk performance op doordat de core switches ontlast worden.

Betere beschikbaarheid

- Door de netwerkaansluitingen op de distributie laag ten behoeve van servers en andere netwerkdiensten redundant uit te voeren, net als de aansluitingen op de core laag ten behoeve van de distributie stacks ontstaat een hoge mate van beschikbaarheid.
  Wanneer een enkele distributie switch, een complete distributie stack of zelfs een core switch down gebracht moet worden voor onderhoudswerkzaamheden of down gaat door een storing, blijven alle servers en netwerkdiensten voor 100% beschikbaar. Zelfs wanneer een distributie stack samen met een core switch down gebracht moet worden.

Besparen op onderhouds- en beheerkosten

- Door de core laag en de distributie laag op te splitsen en stack technologie te gebruiken in de distributie laag wordt onderhoud aan de infrastructuur minder arbeidsintensief. In principe kan onderhoud door een persoon worden uitgevoerd.

- Omdat er minder downtime nodig is voor onderhoudswerkzaamheden, blijven er meer productie uren beschikbaar.

9.2. Aanbevelingen naar aanleiding van de conclusie

Naar aanleiding van de conclusie die getrokken wordt in hoofdstuk 9.1 worden onderstaande aanbevelingen gedaan;

Optimaal gebruik van bandbreedte

- Er kan voor gekozen wordenom gebruik te maken van looppreventie protocollen zodat de infrastructuur full mesh geconfigureerd kan worden en er ook gebruik gemaakt worden van load balancing zodat alle beschikbare bandbreedte optimaal gebruikt wordt.

Onderdelen vervangen zonder downtime

- In de nieuwe situatie kan er voor gekozen worden om onderdelen van een switch die het meest gevoelig zijn voor storingen, zoals cooling fans en voedingen, te vervangen zonder dat het device down gebracht hoeft te worden.

Kosten besparen op verbruik

- In de nieuwe situatie kan het aantal voedingen in de core switches en distributie switches zo afgestemd worden op het benodigde vermogen en de gewenste mate van redundancy dat uiteindelijk minder vermogen nodig.
  Daarbij komt ook dat de nieuwe core switches en distributie stacks minder stroom vragen dan de oude core switches.

10. Evaluatie

In het afstudeerplan is benoemd dat onderstaande competenties en beroepstaken worden getoond tijdens het werken aan de afstudeeropdracht;

- A1 – Analyseren van het probleemdomein.
- A5 – Opstellen van systeemeisen.
- C9 – Ontwerpen van een infrastructuur.
- J12 – Adviesproces uitvoeren.

In hoofdstuk 10.1 wordt teruggeblikt op het afstudeerproces en in hoofdstuk 10.2 op het tot stand komen van het geleverde product; het Proof of Concept. Hier zal ook worden beschreven wanneer en op welke manier aan een competentie of beroepstaak is voldaan.

10.1. Proces evaluatie: een terugblik op het afstudeerproces

Tijdens het oriënterende gedeelte en de zoektocht naar een geschikte afstudeeropdracht heb ik wel een paar benauwde momenten gekend. Telkens weer spookten dezelfde twee vragen door mijn hoofd;

- Lukt het mij om een geschikte afstudeeropdracht te vinden bij Deloitte?
- Als ik geen geschikte afstudeeropdracht vind bij Deloitte, kan school mij voorzien van een geschikte opdracht?

De zoektocht

Omdat mijn eigen werkzaamheden weinig tot geen direct raakvlak hebben met de inhoud van de studie Technische Informatica ben gaan rondvragen bij de twee afdelingen waarvan ik dacht dat ze wel voldoende raakvlak hebben met de inhoud van de studie; Server en Networking.

Server was een gemiste kans. Zij hebben net een ontwerp opgeleverd voor een nieuw op te leveren Cloud infrastructuur, hierin kon ik helaas niets meer betekenen.

Networking had al enige tijd een mooie opdracht op de plank liggen die leek te voldoen aan de eisen van een goede afstudeeropdracht; *Consolidatie van de intranet omgeving en de extranet omgeving naar op dezelfde fysieke apparatuur*.

De opdracht

De strekking van de opdracht was simpel; ten behoeve van kostenbesparing en beheergemak wil men de intranet omgeving en de extranet omgeving consolideren en het aantal gebruikte core switches terugbrengen van zes core switches naar twee core switches.

Het was duidelijk en zeker dat deze consolidatie zou gebeuren, alleen wist men nog niet hoe dit moest gebeuren.

Zo is bij mij het idee ontstaan om hiervoor een Proof of Concept (PoC) te maken; een bewezen ontwerp dat aantoont dat het mogelijk is om met bestaande technologieën de omgevingen samen te brengen op dezelfde fysieke apparatuur.

Ook als gekozen wordt om het ontwerp niet als zodanig aan te nemen en voor een ander ontwerp wordt gekozen, blijft het mogelijk om ideeën uit het PoC te lenen en te implementeren in het uiteindelijke ontwerp – *the best of both worlds*.

Ik heb mijn ideeën uiteengezet en voorgelegd aan het team van Networking. Zij waren eigenlijk direct enthousiast over het idee en een nieuwe samenwerking kwam tot stand.

Beperkende factoren

Helaas heb ik tijdens het afstuderen te maken gehad met een aantal beperkende factoren;

- Wat ik als de grootste beperkende factor heb beschouwd is het feit dat er vanuit Deloitte IT & WS geen tijd beschikbaar is gesteld om aan de opdracht te werken. Ik heb de afstudeeropdracht voor 100% in mijn eigen tijd uitgevoerd. Dit heeft uiteindelijk geresulteerd in een verlenging van de afstudeerperiode.

- Mijn begeleider heeft het vreselijk druk met zijn eigen werkzaamheden en kon daarom niet altijd tijd vrijmaken voor het lezen van documenten of voor het maken van afspraken.

- Door een crash van een van onze datacenters is heel wat afstudeertijd verloren gegaan aan het herstellen van systemen en services.

- Ongeveer halverwege de afstudeeropdracht kwamen de ontwikkelingen bij Deloitte IT & WS in een stroomversnelling en is een aantal beslissingen genomen; de consolidatie van de core netwerk infrastructuur was uitgewerkt en is in april 2014 geïmplementeerd. Het initiële idee achter mijn afstudeeropdracht – het maken van een PoC – werd hiermee abrupt de spreekwoordelijke “mosterd na de maaltijd”.
  Dit was een flinke deuk in mijn motivatie en ik twijfelde eraan of het nog de moeite was om verder te gaan met de opdracht. In overleg met John Visser en Pieter Burghouwt is besloten om toch met de opdracht verder te gaan.

De afsluiting

Nu ben ik klaar met afstuderen en kijk ik – ondanks tegenslagen en telleurstellingen – terug op een vruchtbare en leerzame periode.

10.2. Product evaluatie: een terugblik op het tot stand komen van het product

Als eerste heb ik een methodiek gekozen aan de hand waarvan ik mijn werkzaamheden kon structureren. Hiervoor heb ik een aantal van methodes naast elkaar gelegd, methodes waarmee ik tijdens de studie heb leren werken – Rational Unified Process (RUP) en het ASI Rapport – en een methode waarmee ik ook al bekend was geraakt bij Deloitte – PRINCE2 (Tabel 1 - Keuze matrix methodes).

De keuze voor het ASI Rapport was snel en gemakkelijk gemaakt. Deze methode leent zicht het beste voor het ontwerpen en ontwikkelen van netwerk infrastructuren.

Het ASI Rapport is niet op de letter gevolgd, maar dient als basis structuur voor het werken aan de afstudeeropdracht.

Plan van aanpak

Tijdens de definitiefase van de opdracht heb ik een plan van aanpak geschreven. De basis hiervan is het afstudeerplan. In overleg met John Visser is besloten om de probleemstelling (probleemomschrijving, doelstelling en resultaten) op een andere manier in het plan van aanpak te beschrijven dan deze in het afstudeerplan staan.

Requirements

In het plan van aanpak heb ik de requirements van de nieuwe core infrastructuur opgenomen. Deze lijst met functionele en niet-functionele requirements is tot stand gekomen naar aanleiding van gesprekken die ik heb gevoerd met de expert van de opdrachtgever – mijn begeleider.

De lijst met requirements is terug te lezen in hoofdstuk 5.1 op pagina 11 en is opgesteld conform de beschrijving van beroepstaak A5 – Opstellen van systeemeisen.

Architectuur

Tijdens de architectuurfase van de opdracht heb ik de oude architectuur in kaart gebracht en in samenspraak met de afdeling Networking een nieuwe architectuur gemaakt.

In hoofdstuk 6.1 op pagina 16 is te lezen hoe de huidige architectuur – het probleemdomein – in kaart is gebracht conform de beschrijving van beroepstaak A1 – Analyseren van het probleemdomein.

Detail ontwerp

Tijdens de ontwerpfase van de opdracht heb ik een detail ontwerp gemaakt van de nieuwe core infrastructuur. Hiervoor heb ik de nieuwe architectuur als basis gebruikt en deze verder uitgewerkt.

De keuze van de hardware en de bekabeling was al gemaakt door de opdrachtgever in samenspraak met de leverancier, Avaya. Hiermee hoefde ik mij niet meer bezig te houden.

De uitwerking van het detail ontwerp is te lezen in hoofdstuk 7 op pagina 22 en is waar van toepassing conform de beschrijving van beroepstaak C9 – Ontwerpen van een infrastructuur.

Implementatieplan

In de laatste fase van de opdracht – de ontwikkelfase – wordt normaliter een product gebouwd en opgeleverd. Omdat ik geen product kan bouwen, heb ik ervoor gekozen om een implementatieplan te schrijven dat gebruikt kan worden om de nieuwe infrastructuur te implementeren.

Proof of concept

Ondanks het feit dat er al een nieuwe core infrastructuur is geïmplementeerd, ben ik op eigen inzicht verder gegaan met de opdracht en vormt het resultaat toch een “aardig” proof of concept.

In hoofdstuk 9 op pagina 38 van deze afstudeerscriptie trek ik mijn conclusies met betrekking tot de mogelijkheden om met bestaande technologieën de nodige gemakken en besparingen te realiseren en ik doe dit conform de beschrijving van beroepstaak J12 – Adviesproces uitvoeren.

Literatuurlijst

[1] Deloitte Global, „Deloitte Home Page," Deloitte, 2014. [Online]. Available: http://www2.deloitte.com/global/en.html. [Geopend 23 03 2014].

[2] Deloitte The Netherlands, „Deloitte The Netherlands Home Page," Deloitte The Netherlands, 2014. [Online]. Available: http://www.deloitte.nl. [Geopend 23 03 2014].

[3] Deloitte Global, „About Deloitte," 2014. [Online]. Available: http://www2.deloitte.com/content/www/global/en/pages/about-deloitte/articles/about-deloitte.html.

[4] Deloitte The Netherlands, „Annual & sustainability report," 2013. [Online]. Available: http://2012-2013.deloitteannualreport.nl/fbcontent.ashx/downloads/2012-2013/Annual_report_2012_2013.pdf.

[5] Deloitte The Netherlands, „Fair Chance Foundation," [Online]. Available: http://www.deloitte.com/view/nl_NL/nl/over-deloitte/fair-chance-foundation/index.htm.

[6] Microsoft Corporation, „Microsoft Technet," juli 2012. [Online]. Available: http://technet.microsoft.com/en-us/solutionaccelerators/dd320379.aspx.

[7] B. Hedemans, H. Fredriksz en G. Vis van Heemst, Project Management een introductie, Van Haren Publishing, 2004.

[8] P. Kruchten, The Rational Unified Process an Introduction, Upper Saddle River, NJ: Pearson Education, Inc., 2009.

[9] NGI, „ASI Rapport," KIVI & NGI, 1995.

[10] Cisco Systems Inc., „Cisco Service Ready Architecture for Schools Design Guide," 09 07 2010. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Education/SchoolsSRA_DG/SchoolsSRA-DG/SchoolsSRA_chap3.html. [Geopend 22 05 2014].

[11] Avaya Inc., „Avaya VENA Reference Architectures & Design Blueprints," 2013. [Online]. Available: http://198.152.212.23/css/P8/documents/100176903. [Geopend 18 05 2014].

[12] Avaya Inc., „Understanding Avaya Stackable Chassis Infrastructure," 2012. [Online]. Available: http://www.avaya.com/usa/documents/understand_stackable_architecture_dn7087.pdf. [Geopend 17 05 2014].

[13] Deloitte Nederland, „Onze Organisatie," Deloitte, [Online]. Available: http://www.deloitte.com/view/nl_NL/nl/over-deloitte/onze-organisatie/index.htm. [Geopend februari 2014].

Deloitte.

Gebruikte afkortingen

- ASI – *Niet bekend*
- AUR – Auto Unit Replacement
- BGP – Border Gateway Protocol
- CPU – Central Processing Unit
- EAP – Extensible Authentication Protocol
- EVPN – Ethernet Virtual Private Network
- FAST – Flexible Advanced Stacking Technology
- Gbps – Gigabit per second
- GSC – Group Support Center
- GWAN – Global Wide Area Network
- IGMP – Internet Group Management Protocol
- IP – Internet Protocol
- ISP – Internet Service Provider
- IST – InterSwitch Trunk
- IT&WS – IT & Workplace Services
- MOF – Microsoft Operations Framework
- MPLS – Multi Protocol Label Switching
- OTAP – Ontwikkel Test Acceptatie Productie
- PIM – Protocol Independent Multicast
- PoC – Proof of Concept
- PRINCE – PRojects IN Controlled Enviroments
- QoS – Quality of Service
- RIP – Routing Information Protocol
- R-SMLT – Routed-Split Multi Link Trunk
- RUP – Rational Unified Process
- SFP – Small Form-factor Pluggable
- SLPP – Simple Loop Prevention Protocol
- SMF – Service Management Function
- SMLT – Split Multi Link Trunk
- SPB – Shortest Path Bridging
- SPOF – Single Point Of Failure
- VDI – Virual Desktop Infrastructure
- VLACP – Virtual Link Aggregation Control Protocol
- VLAN – Virtual Local Area Network
- VRF – Virtual Routing and Forwarding
- VRRP – Virtual Router Redundancy Protocol
- VSP – Virtual Service Platform

Deloitte.

Gebruikte tabellen

Deloitte.

Gebruikte figuren

Bijlage 1: Opdrachtgegevens

Student

Studentnummer	09000577
Naam	Chris de Bruin
Adres	Joop den Uylstraat 34 3317 NW Dordrecht
Telefoonnummer	088-288 2605
E-mailadres	c.debruin@student.hhs.nl
Onderwijsinstelling	Haagse Hogeschool
Opleiding	Technische informatica
Periode afstuderen	November 2013 – juni 2014

Begeleider/examinator

Naam	Dhr. J.J. (John) Visser
E-mailadres	j.j.visser@hhs.nl
Telefoonnummer	015-260 6281

Expert/examinator

Naam	Dhr. Ir. P. (Pieter) Burghouwt
E-mailadres	p.burghouwt@hhs.nl
Telefoonnummer	015-260 6288

Bedrijfsgegevens

Naam	Deloitte
Afdeling	Group Support Center, IT & Workplace Services
Adres	Dynamostraat 50 1014 BZ Amsterdam
Telefoonnummer	088-288 2888

Opdrachtgever

Naam	Dhr. J. (John) Snel
Functie	Fase manager
E-mailadres	jsnel@deloitte.nl
Telefoonnummer	088-288 8116

Begeleider

Naam	Dhr. J. (Jeroen) Hassing
Functie	Network Engineer
E-mailadres	jhassing@deloitte.nl
Telefoonnummer	088-288 8182

Bijlage 2: Afstudeerplan

Informatie afstudeerder en gastbedrijf

Afstudeerblok: 2013-2.2 (start uiterlijk 18 november 2013)
Startdatum uitvoering afstudeeropdracht: 18 november 2013
Inleverdatum afstudeerdossier volgens jaarrooster: 31 maart 2014

Studentnummer: 09000577
Achternaam: dhr. De Bruin
Voorletters: C.
Roepnaam: Chris
Adres: Joop den Uylstraat 34
Postcode: 3317 NW
Woonplaats: Dordrecht
Telefoonnummer: 078-7079989
Mobiel nummer: 06-13127270
Privé emailadres: cdebruin@outlook.com

Opleiding: Technische Informatica
Locatie: Den Haag
Variant: deeltijd c.q. avond

Naam studieloopbaanbegeleider: Tony Andrioli
Naam begeleidend examinator: John Visser
Naam tweede examinator: Pieter Burghouwt

Naam bedrijf: Deloitte
Afdeling bedrijf: IT & Workplace Services
Bezoekadres bedrijf: Dynamostraat 50
Postcode bezoekadres: 1014 BZ
Postbusnummer:
Postcode postbusnummer:
Plaats: Amsterdam
Telefoon bedrijf: 088-2882888
Telefax bedrijf: 088-2889806
Internetsite bedrijf: http://www.deloitte.nl

Achternaam opdrachtgever: dhr. Snel
Voorletters opdrachtgever: J.
Titulatuur opdrachtgever: Senior Manager
Functie opdrachtgever: Fase Manager
Doorkiesnummer opdrachtgever: 088-2888116
Email opdrachtgever: jsnel@deloitte.nl

Achternaam bedrijfsmentor: dhr. Hassing
Voorletters bedrijfsmentor: J.
Titulatuur bedrijfsmentor: Senior Consultant
Functie bedrijfsmentor: Networking Engineer
Doorkiesnummer bedrijfsmentor: 088-2888182
Email bedrijfsmentor: jhassing@deloitte.nl

Doorkiesnummer afstudeerder: 088-2882605
Functie afstudeerder (deeltijd/duaal): Application Engineer

Titel afstudeeropdracht:

Consolidatie en virtualisatie van de core netwerk infrastructuur bij Deloitte.

Opdrachtomschrijving

1. Bedrijf

Deloitte is een van de “Big Four”. De Big Four zijn de vier grootste internationale, professionele dienstverleners die services bieden voor o.a. audits, belastingen en legal services. De Big Four wordt gevormd door PricewaterhouseCoopers, Deloitte, Ernst & Young en KPMG.

“Deloitte” is de merknaam waaronder zelfstandige memberfirms wereldwijd samenwerken op het gebied van accountancy, consulting, financiële advisering, risk management en belastingadvies. Al deze memberfirms zijn onderdeel van Deloitte Touche Tohmatsu Limited (DTTL), een naamloze vennootschap in het Verenigd Koninkrijk.

Elke memberfirm is actief in een bepaald (geografisch) gebied en daardoor onderworpen aan de wetgeving en de professionele regelgeving van het land of de landen waarin zij opereert.

De structuur van de afzonderlijke DTTL memberfirms verschilt afhankelijk van de plaatselijke wet- en regelgeving, usance en eventuele andere factoren.

Deloitte Nederland gaat uit van een multidisciplinaire aanpak. Vanuit de diensten Accountancy, Belastingen, (ICT) Consulting en Financial Advisory Services bedienen wij de markt. Vanuit de markt bieden wij een branche specifieke aanpak via verschillende 'industriegroepen'.

Deloitte Nederland kent een geschiedenis van vele fusies en overnames;

1955 De belangrijkste rechtsvoorganger **Nederlandse Accountants Maatschap (NAM)**.
1986 Belastingadvies wordt belangrijker en om de samenwerking met **Touch Ross International** te verduidelijken veranderd de naam in **TRN Groep**.
1988 **TRN Groep** fuseert met de **Tombe/Melse Groep (TMG)**.
1992 **Touche Ross International** gaat samen met **Deloitte Haskins &Sells**, een nieuwe wereldwijde verbintenis met als nieuwe naam **Deloitte Touch Tohmatsu International**. De naam verandert in **Deloitte & Touche**.
1998 De grootste fusie uit de geschiedenis van de Nederlandse organisatie, **Deloitte & Touche** fuseert met de **VB Groep**.
2002 **Deloitte & Touche** fuseert met **Andersen Nederland**. Hiermee wordt de Big Five gereduceerd tot de Big Four.
2003 De naam wordt ingekort naar **Deloitte**, maar het blijft een “member of Deloitte Touche Tohmatsu”.

Deloitte Nederland telt ongeveer 4500 medewerkers verdeelt over 16 kantoren in o.a. Amsterdam, Rotterdam, Utrecht en Maastricht. De ICT afdeling van Deloitte (IT&WS) opereert vanuit één van de Amsterdamse kantoren, het *CyberCentre*.

In het Deloitte CyberCentre werken ongeveer 70 ICT medewerkers volgens het Microsoft Operations Framework in verschillende Service Management Functions (SMF’s); SMF Server, SMF Storage, SMF Networking, SMF Applications etc. Elke SMF is verantwoordelijk voor het beheren en onderhouden van zijn onderdeel van de infrastructuur.

Figuur: Organisatiestructuur en expertisegebieden

SMF Networking is verantwoordelijk voor het beheren, ontwerpen en vernieuwen van het bedrijfsnetwerk van Deloitte Nederland. Denk hierbij aan netwerkapparatuur (routers en switches), netwerkbekabeling, maar ook het onderhouden van contacten met externe partijen als KPN en AVAYA en het oplossen van calamiteiten.

<u>Aanleiding</u>

Om beter grip te krijgen op de beheerbaarheid, het onderhoud en ook de kosten is het gewenst dat het aantal hardwarecomponenten binnen de Deloitte IT omgeving wordt geconsolideerd.

In het verleden is vanuit veiligheid perspectief gekozen om bepaalde omgevingen fysiek van elkaar te scheiden. Dit zodat externe en interne(domeinen) binnen de bedrijfsomgeving niet direct met elkaar in verbinding staan. De afgelopen jaren is de capaciteit van netwerk apparatuur fors toegenomen, en zijn er nieuwe technieken beschikbaar gekomen die kunnen voorzien in o.a. consolidatie van verschillende omgevingen.

In plaats van deze omgeving fysiek te scheiden op verschillende netwerkcomponenten kan deze scheiding nu softwarematig worden gemaakt op dezelfde fysieke hardware. Met behulp van deze virtualisatie blijft de netwerkveiligheid gehandhaafd, en wordt er tegelijkertijd bespaard op hardware-, stroom- en koelingskosten. Omdat er minder hardware componenten benodigd zijn, is er minder tijd nodig aan onderhoud, en bespaart dit fysieke ruimte.

2. Probleemstelling

Het Deloitte netwerk is opgebouwd als een OTAP (Ontwikkel Test Acceptatie Productie) structuur. De verschillende omgevingen landen op zowel het intranet als het extranet.

De ontwikkel- en testomgevingen (OT) worden gehost op een OT netwerk infrastructuur. De acceptatie- en productieomgevingen (AP) zijn gescheiden van de OT omgeving en worden op separate AP netwerk infrastructuur gehost. Daarbij wordt in beide omgevingen ook onderscheid gemaakt tussen de interne en externe omgeving. De interne OT omgeving wordt gehost op fysiek andere hardware dan de externe OT omgeving. Hetzelfde is het geval voor de AP omgeving.

Om de beheerbaarheid en het onderhoud van de netwerken te vergemakkelijken, maar ook vanuit kostenoogpunt heeft Deloitte IT&WS besloten om de interne en externe omgeving te consolideren. Alle verschillende netwerk core en access componenten in de OT omgeving moeten worden samengevoegd op één core en access infrastructuur. Hetzelfde concept moet worden toegepast binnen de AP omgeving. Door middel van virtualisatie moeten deze omgevingen gescheiden van elkaar blijven, ondanks dat ze fysiek op dezelfde netwerkhardware actief zijn. Dit gebeurd op laag 3 van het OSI model.

Omdat meerdere omgevingen op dezelfde netwerk hardware actief zal zijn, is het noodzakelijk dat, in het bijzonder, de netwerk core omgeving voldoende capaciteit heeft om al het netwerkverkeer binnen de gewenste normen af te kunnen handelen. Het consolideren vergt dan ook het nodige meet- en uitzoekwerk, alvorens dit kan gaan worden uitgevoerd.

Op dit moment is een start gemaakt met het uitwerken van de benodigdheden voor de nieuwe core infrastructuur. We zijn de mogelijkheden aan het bekijken om deze consolidatieslag te kunnen realiseren. Informatie hieromtrent zal worden bekeken om tot een gedegen besluit te komen. Hierin zal het PoC tevens een doorslaggevende rol in kunnen hebben.

3. Doelstelling van de afstudeeropdracht

Het doel van deze afstudeeropdracht is het komen tot een PoC voor het consolideren en virtualiseren van de interne en externe omgevingen van de OT omgeving en van de AP omgeving op het Deloitte netwerk.

Het ontwerp van de nieuwe netwerkarchitectuur zal voldoen aan alle veiligheidseisen die hieraan door Deloitte IT&WS worden gesteld met betrekking tot het scheiden van het netwerkverkeer van en naar de interne en externe omgevingen.

De nieuwe netwerkomgeving zal zo worden ontworpen dat wordt voldaan aan alle performance eisen die hieraan door Deloitte IT&WS worden gesteld.

4. Resultaat

Het resultaat van deze afstudeeropdracht is het opleveren van een architectuur, een ontwerp en een advies ten behoeve van de implementatie van de nieuwe core netwerk architectuur.

De architectuur en het ontwerp van de vernieuwde core netwerk architectuur zullen dienen als PoC voor het consolideren en virtualiseren van de huidige core netwerk architectuur.

Directe resultaten van de consolidatie en virtualisatie zullen zijn; gemakkelijkere en betere beheerbaarheid van de omgevingen, gemakkelijker onderhoud en verlaging van de kosten.

5. Uit te voeren werkzaamheden, inclusief een globale fasering, mijlpalen en bijbehorende activiteiten

Onderstaande tabel geeft een overzicht van de uit te voeren werkzaamheden en een schatting van de tijd die daarvoor nodig is. Dit overzicht is niet definitief en zal tijdens gedurende de afstudeeropdracht worden bijgestuurd waar nodig.

Task Name	Duration	Start	Finish
Definitiefase	**10 days**	**Mon 18-11-13**	**Fri 29-11-13**
Schrijven plan van aanpak	10 days	Mon 18-11-13	Fri 29-11-13
Plan van aanpak	0 days	Fri 29-11-13	Fri 29-11-13
Architectuurfase	**20 days**	**Mon 2-12-13**	**Fri 27-12-13**
Onderzoeken virtualisatie technieken	5 days	Mon 2-12-13	Fri 6-12-13
Schrijven architectuurdocument	15 days	Mon 9-12-13	Fri 27-12-13
Architectuur	0 days	Fri 27-12-13	Fri 27-12-13
Ontwerpfase	**30 days**	**Fri 27-12-13**	**Fri 7-2-14**
Samenstellen ontwerpdocument	**30 days**	**Mon 30-12-13**	**Fri 7-2-14**
Maken logisch ontwerp	15 days	Mon 30-12-13	Fri 17-1-14
IP nummerplan	0 days	Fri 17-1-14	Fri 17-1-14
Logisch ontwerp	0 days	Fri 17-1-14	Fri 17-1-14
Maken fysiek ontwerp	10 days	Mon 20-1-14	Fri 31-1-14
Fysiek ontwerp	0 days	Fri 31-1-14	Fri 31-1-14
Maken beheer ontwerp	5 days	Mon 3-2-14	Fri 7-2-14
Beheer ontwerp	0 days	Fri 7-2-14	Fri 7-2-14
Ontwerp	0 days	Fri 7-2-14	Fri 7-2-14
Ontwikkelfase	**10 days**	**Mon 10-2-14**	**Fri 21-2-14**
Samenstellen adviesrapport	**10 days**	**Mon 10-2-14**	**Fri 21-2-14**
Schrijven advies beheertools	3 days	Mon 10-2-14	Wed 12-2-14
Advies beheertools	0 days	Wed 12-2-14	Wed 12-2-14
Schrijven implementatieplan	7 days	Thu 13-2-14	Fri 21-2-14
Implementatieplan	0 days	Fri 21-2-14	Fri 21-2-14
Adviesrapport	0 days	Fri 21-2-14	Fri 21-2-14
Afstudeerdossier	**15 days**	**Mon 24-2-14**	**Fri 14-3-14**
Schrijven procesverslag	10 days	Mon 24-2-14	Fri 7-3-14
Procesverslag	0 days	Fri 7-3-14	Fri 7-3-14
Samenstellen afstudeerdossier	5 days	Mon 10-3-14	Fri 14-3-14
Afstudeerdossier	0 days	Fri 14-3-14	Fri 14-3-14

Tabel: Overzicht werkzaamheden

6. Op te leveren (tussen)producten

In de planning van punt 5 zijn de tussenproducten ook terug te vinden. Onderstaand een opsomming;

- Plan van aanpak
- Architectuur
- Ontwerp (samengesteld uit; IP nummerplan, logisch ontwerp, fysiek ontwerp, beheer ontwerp)
- Adviesrapport (samengesteld uit; advies beheertools en het implementatieplan)

7. Te demonstreren competenties en wijze waarop

Definitiefase
A5 – Opstellen van systeemeisen.

Architectuurfase
A1 – Analyseren van het probleemdomein.

Ontwerpfase
C9 – Ontwerpen van een infrastructuur.

Ontwikkelfase
J12 – Adviesproces uitvoeren.

Bijlage 3: Competenties en beroepstaken

A1	ANALYSEREN VAN HET PROBLEEMDOMEIN
ACTIVITEITEN	Het onderzoeken en beschrijven van het gegeven probleemdomein (van de opdrachtgever) in termen van het TI domein, en het vaststellen van de gewenste veranderingen. Het inwerken in het domein van de opdrachtgever, maakt onderdeel van deze taak uit.
PRODUCT	Een, waar mogelijk formele, beschrijving van het probleemdomein van de opdrachtgever, beschreven in termen van het TI domein.
TOELICHTING	Voor het onderzoeken van het domein kunnen diverse methoden en technieken gebruikt worden, zoals interviewen en analyse van documenten en bestaande software. Voorbeelden van type beschrijvingen die gebruikt kunnen worden om het resultaat van dat onderzoek vast te leggen zijn: procesbeschrijvingen, S88 modellen, UML modellen, netwerk schema's (of in gewoon natuurlijke taal, bijvoorbeeld Nederlands of Engels). Feitelijk gaat het in deze taak om het 'vertalen' van een probleem van de opdrachtgever naar een 'TI probleem'. Dat wil zeggen dat je het probleem moet omschrijven voor andere TI-ers, gebruik makend van relevante kennis en theorieën die horen bij het TI domein.
TOETSCRITERIA	1. Beschrijvingen zijn zoveel als mogelijk in formele talen gemaakt. 2. De formele talen zijn correct toegepast. 3. Een aantal relevante mogelijkheden zijn verkend. De keuze voor de gebruikte techniek (de gekozen taal) is verantwoord, en correct. 4. Alle aspecten van het probleem zijn benoemd en afdoende beschreven. De probleembeschrijving doet dienst als leidraad bij het ontwerpen. Uit de analyse kunnen de volgende stappen worden afgeleid. 5. De beschrijving van het probleem is afgestemd met de opdrachtgever.

Tabel 22 - Beroepstaak A1: analyseren van het probleemdomein

A5	OPSTELLEN VAN SYSTEEMEISEN (REQUIREMENTS)
ACTIVITEITEN	Analyseren, selecteren, opstellen en beschrijven van specificaties van het te realiseren systeem. Toetsen van het geheel op duidelijkheid, volledigheid en consistentie. Categoriseren van eisen.
PRODUCT	Overzicht van specificaties
TOELICHTING	Analyseren behoeften van belanghebbende met als doel de specificaties vast te stellen. De systeemeisen kunnen ook in verschillende scenario's beschreven zijn. Specificaties staan bij voorkeur vermeld in een apart document of zijn onderdeel van de definitiestudie o.i.d.
TOETSCRITERIA	1. De eisen zijn afgeleid uit de behoeften (output van A3). 2. Bij tegenstrijdige behoeften is een gemotiveerde keuze gemaakt. 3. De eisen zijn geformuleerd als stellende zinnen (een logische bewering) die eenduidig en verifieerbaar zijn 4. Er is gecontroleerd dat de eisen realiseerbaar zijn 5. De eisen zijn gecategoriseerd in minimaal functionele en niet-functionele eisen. 6. De eisen dekken het systeem volledig af. 7. De gemaakte keuzen zijn in overeenstemming met de opdrachtgever (of gemandateerde).

Tabel 23 - Beroepstaak A5: opstellen van systeemeisen (requirements)

C9	ONTWERPEN VAN EEN INFRASTRUCTUUR
ACTIVITEITEN	Het opstellen van een ontwerp naar met name operationele eisen zoals: performance, availability, capacity, managebility, continuity, security, remote access, adaptivity. - Het vaststellen en verantwoorden van een architectuur, die leidt tot een oplossing bij de gegeven eisen. - Het opzetten en in detail uitwerken van de infrastructuur. - Het aantonen dat het ontwerp van de infrastructuur voldoet aan de gestelde eisen (bijvoorbeeld door kritische delen in labopstellingen te testen).
PRODUCT	Architectuurbeschrijving in de vorm van een eenvoudige topologie verantwoording van het concept Uitgebreide topologie + gedetailleerde uitwerking Verantwoording geldigheid ontwerp in de vorm van rapportage (eventueel aangevuld met test van labmodellen)
TOELICHTING	Voorbeelden van details zijn: - configuraties van apparatuur - toepassing van QoS - gebruikte protocollen - gebruikte media en capaciteiten - ip adresplan. Ontwerpen is de schakel tussen het opstellen van de eisen (zie A5) en het implementeren van de infrastructuur. Het testen van een geïmplementeerd netwerk is geen ontwerpactiviteit, het testen van een labopstelling wordt wel bij ontwerpen gedaan. (zie D18)
TOETSCRITERIA	Het product is een ontwerprapport met minimaal de volgende elementen: 1. Verantwoording van de gebruikte ontwerpmethode 2. Beschrijving en verantwoording van de architectuur met mogelijke alternatieven 3. Uitwerking van het ontwerp met zodanige detaillering dat de infrastructuur daarna gerealiseerd kan worden (bijv. topologie, met eindsystemen en netwerkapparatuur, ip adresplan, uitgewerkte beveiligingsmaatregelen, configuraties, media, applicaties, besturingssystemen, gebruikte diensten van providers, kosten-batenanalyse)

Tabel 24 - Beroepstaak C9: ontwerpen van een infrastructuur

J12	ADVIESPROCES UITVOEREN
ACTIVITEITEN	In een concrete situatie in samenspraak met de opdrachtgever en andere betrokkenen op basis van een analyse een adviesstrategie kiezen en uitvoeren. Voorbeelden van gebieden waarop advies gegeven kan worden zijn: technische informatiesystemen en ict-infrastructuren. De adviezen hebben betrekking op: wensen en behoeften, systeemeisen, ontwerpen, bouwen, testen, storingen en problemen. Bij de uitwerking van een adviesstrategie wordt gestreefd naar draagvlak voor acceptatie, uitvoering en invoering.
PRODUCT	- Een probleemanalyse (A1, E23). - Een opsomming van behoeften, systeemeisen (A3, A5) - Een advies voor een platform en besturingssysteem (B6) - Een advies voor de inrichting van een beheerproces (B7) - Een ontwerp met toelichting (C8, C9, C10, C11, C12)
TOELICHTING	Deze beroepstaak wordt uitgevoerd als aspect van bovengenoemde beroepstaken.
TOETSCRITERIA	1. Advies sluit aantoonbaar aan op de aanleiding en analyse van de concrete situatie. 2. Advies past bij de organisatorische, financiële en technische eisen die de opdracht gevende organisatie stelt.

Tabel 25 - Beroepstaak J12: Adviesproces uitvoeren

Bijlage 4: IP nummerplan

Figuur 17 toont een afbeelding van het IP nummerplan voor de nieuwe core netwerk infrastructuur. Het IP nummerplan zal ook als apart document worden toegevoegd aan het afstudeerdossier.
Met de opdrachtgever is de afspraak gemaakt dat voor de afstudeeropdracht geen gebruik gemaakt wordt van de werkelijke Deloitte IP reeksen.

	Connecties	VLAN	Netwerk	Broadcast	Range		Subnet bits	Subnet mask	Hosts in subnet	VLAN IP
Core netwerk intranet										
WIRELESS	10000	1000	10.1.0.0	10.1.63.255	10.1.0.1	10.1.63.254	18	255.255.192.0	16382	10.1.63.254
F5	300	1064	10.1.64.0	10.1.65.255	10.1.64.1	10.1.65.254	23	255.255.254.0	510	10.1.65.254
GBS	400	1066	10.1.66.0	10.1.67.255	10.1.66.1	10.1.67.254	23	255.255.254.0	510	10.1.67.254
CORE	n.v.t.	1068	10.1.68.0	10.1.68.255	10.1.68.1	10.1.68.254	24	255.255.255.0	254	10.1.68.254
DISTRIBUTION	n.v.t.	1069	10.1.69.0	10.1.69.255	10.1.69.1	10.1.69.254	24	255.255.255.0	254	10.1.69.254
ACCESS	n.v.t.	1070	10.1.70.0	10.1.70.255	10.1.70.1	10.1.70.254	24	255.255.255.0	254	10.1.70.254
FIREWALL	n.v.t.	1071	10.1.71.0	10.1.71.255	10.1.71.1	10.1.71.254	24	255.255.255.0	254	10.1.71.254
GWAN	n.v.t.	1072	10.1.72.0	10.1.72.255	10.1.72.1	10.1.72.254	24	255.255.255.0	254	10.1.72.254
IPTV	200	1073	10.1.73.0	10.1.73.255	10.1.73.1	10.1.73.254	24	255.255.255.0	254	10.1.73.254
Core netwerk extranet										
CORE	n.v.t.	5000	192.168.50.0	192.168.50.255	192.168.50.1	192.168.50.254	24	255.255.255.0	254	192.168.50.254
DISTRIBUTION	n.v.t.	5001	192.168.51.0	192.168.51.255	192.168.51.1	192.168.51.254	24	255.255.255.0	254	192.168.51.254
FIREWALL	n.v.t.	5002	192.168.52.0	192.168.52.255	192.168.52.1	192.168.52.254	24	255.255.255.0	254	192.168.52.254
F5	100	5003	192.168.53.0	192.168.53.255	192.168.53.1	192.168.53.254	24	255.255.255.0	254	192.168.53.254
Servers intranet										
WEB01	n.v.t.	2000	10.2.0.0	10.2.3.255	10.2.0.1	10.2.3.254	22	255.255.252.0	1022	10.2.3.254
APP01	n.v.t.	2004	10.2.4.0	10.2.7.255	10.2.4.1	10.2.7.254	22	255.255.252.0	1022	10.2.7.254
DB01	n.v.t.	2008	10.2.8.0	10.2.11.255	10.2.8.1	10.2.11.254	22	255.255.252.0	1022	10.2.11.254
SAP	n.v.t.	2012	10.2.12.0	10.2.13.255	10.2.12.1	10.2.13.254	23	255.255.254.0	510	10.2.13.254
SAP_BEDK	n.v.t.	2014	10.2.14.0	10.2.14.255	10.2.14.1	10.2.14.254	24	255.255.255.0	254	10.2.14.254
SAP_TR	n.v.t.	2015	10.2.15.0	10.2.15.255	10.2.15.1	10.2.15.254	24	255.255.255.0	254	10.2.15.254
Servers extranet										
WEB02	n.v.t.	6000	192.168.60.0	192.168.60.255	192.168.60.1	192.168.60.254	24	255.255.255.0	254	192.168.60.254
APP02	n.v.t.	6001	192.168.61.0	192.168.61.255	192.168.61.1	192.168.61.254	24	255.255.255.0	254	192.168.61.254
DB02	n.v.t.	6002	192.168.62.0	192.168.62.255	192.168.62.1	192.168.62.254	24	255.255.255.0	254	192.168.62.254
End devices										
NOTEBOOKS	5300	3000	10.3.0.0	10.3.31.255	10.3.0.1	10.3.31.254	19	255.255.224.0	8190	10.3.31.254
MOBILE_DEVICES	4500	3032	10.3.32.0	10.3.63.255	10.3.32.1	10.3.63.254	19	255.255.224.0	8190	10.3.63.254
VDI	500	3064	10.3.64.0	10.3.65.255	10.3.64.1	10.3.65.254	23	255.255.254.0	510	10.3.65.254
DESKTOPS	200	3066	10.3.66.0	10.3.66.255	10.3.66.1	10.3.66.254	24	255.255.255.0	254	10.3.66.254
PRINTERS	250	3067	10.3.67.0	10.3.67.255	10.3.67.1	10.3.67.254	24	255.255.255.0	254	10.3.67.254
Guests										
GUEST	1000	1600	172.16.0.0	172.16.3.255	172.16.0.1	172.16.3.254	22	255.255.252.0	1022	172.16.3.254

Figuur 17 - IP nummerplan

Bijlage 5: Opbouw van het afstudeerdossier

Tabel 26 toont de naam, de omschrijving en het type van de documenten waarmee het afstudeerdossier is opgebouwd. Documenten met een [*] worden enkel als softcopy beschikbaar gesteld op cd-rom tijdens de examenzitting.

DOCUMENT	OMSCHRIJVING	TYPE DOCUMENT
AFSTUDEERSCRIPTIE.DOCX	Afstudeerscriptie	Microsoft Word 2013
ARCHITECTUUR.DOCX	Architectuur van de nieuwe infrastructuur.	Microsoft Word 2013
ASI RAPPORT.PDF *	Ontwerp en ontwikkeling van systeem- en netwerk infrastructuren.	Adobe Reader
ONTWERP.DOCX	Detail ontwerp van de nieuwe infrastructuur.	Microsoft Word 2013
DETAIL ONTWERP.VSDX *	Tekening van het nieuwe ontwerp.	Microsoft Visio 2013
FASEPLANNING.XLSX *	Planning van de verschillende fases van het project.	Microsoft Excel 2013
IMPLEMENTATIEPLAN.DOCX	Stappenplan ten behoeve van het implementeren van de nieuwe infrastructuur.	Microsoft Word 2013
IP NUMMERPLAN.XLSX *	IP nummerplan.	Microsoft Excel 2013
NIEUWE ARCHITECTUUR.VSDX *	Tekening van de nieuwe architectuur.	Microsoft Visio 2013
OUDE ARCHITECTUUR.VSDX *	Tekening van de oude architectuur.	Microsoft Visio 2013
PLAN VAN AANPAK.DOCX	Plan van aanpak	Microsoft Word 2013
PLANNING.MPP *	Planning van het complete afstudeertraject.	Microsoft Project 2013
SWITCH CONFIGURATIES.XLSX *	Configuratie fysieke verbindingen tussen de core switches en distributie stacks.	Microsoft Excel 2013

Tabel 26 - Opbouw van het afstudeerdossier