Consolidatie en virtualisatie van de core netwerk infrastructuur bij Deloitte

Naam : Chris de Bruin

Titel : Projectdocumentatie

Versie : 1.0

Datum : 29 mei 2014

Plaats : Amsterdam

Deloitte.

Projectdocumentatie

In dit document zijn de projectdocumenten samengevoegd die samen met de afstudeerscriptie zijn ingeleverd.

Het bevat de volgende documenten;

- Plan van aanpak
- Architectuur
- Detail ontwerp
- Implementatieplan

Deze documenten moeten worden beschouwd als officieuze bijlage en zijn geen onderdeel van afstudeerscriptie zelf.

Deloitte.

Inhoudsopgave

Plan van aanpak

Architectuur

Deloitte.

Detail ontwerp

Implementatieplan

Deloitte.

Consolidatie en virtualisatie van de core netwerk infrastructuur bij Deloitte

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

Titel	:	Plan van aanpak
Versie	:	1.2
Datum	:	24 mei 2014
Plaats	:	Amsterdam

Deloitte.

1. 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 aantal hardware componenten binnen het Deloitte netwerk worden 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 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.

Deloitte.

2. 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.

Deloitte.

3. 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.

4. 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.

5. Eisen en wensen

Deloitte IT&WS heeft een aantal eisen en wensen gesteld aan het op te leveren PoC. De eisen en wensen zijn onderstaand uit een gezet als functionele en niet functionele eisen;

5.1. 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.

5.2. 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.).

6. Afbakening

Niet alle componenten binnen het Deloitte netwerk worden aan de hand van deze opdracht geconsolideerd en/of gevirtualiseerd. Onderstaand staat beschreven welke onderdelen ‘in scope’ en welke onderdelen ‘out of scope’ zijn.

6.1. In 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.

Correcte routering naar VLANs van de branch offices valt ook nog binnen de scope van deze opdracht.

6.2. Out of 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 office 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.

Deloitte.

7. Risicoanalyse

Elke opdracht brengt risico's met zich mee die de uitvoering de opdracht kunnen vertragen en/of bemoeilijken.

Tabel 1 beschrijft de risico's die op deze opdracht van toepassing zijn. Persoonlijke zaken worden hier niet beschreven, deze zouden geen risico mogen vormen voor de uitvoer van de opdracht.

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 1 - Mogelijke risico's

- **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 (= heel klein) en 5 (= heel groot).
- **Impact**: de impact dat het risico heeft op de uitvoering van de opdracht. De waarde ligt tussen 1 (= heel laag) en 5 (= heel hoog).
- **Risico**: Kans x Impact = het geschatte risico.

8. Kwaliteit

Om de kwaliteit van de opdracht en het op te leveren product te kunnen borgen zal een aantal afspraken worden gemaakt;

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

9. Planning en mijlpalen

De planning is een dynamisch geheel en zal tijdens de opdracht worden bijgesteld als dit nodig is. De volledige planning wordt als apart Microsoft Project bestand beschikbaar gemaakt en zal als apart document mee worden ingeleverd.

9.1. Globale planning

Tabel 2 is een vereenvoudigde weergave van de globale planning.

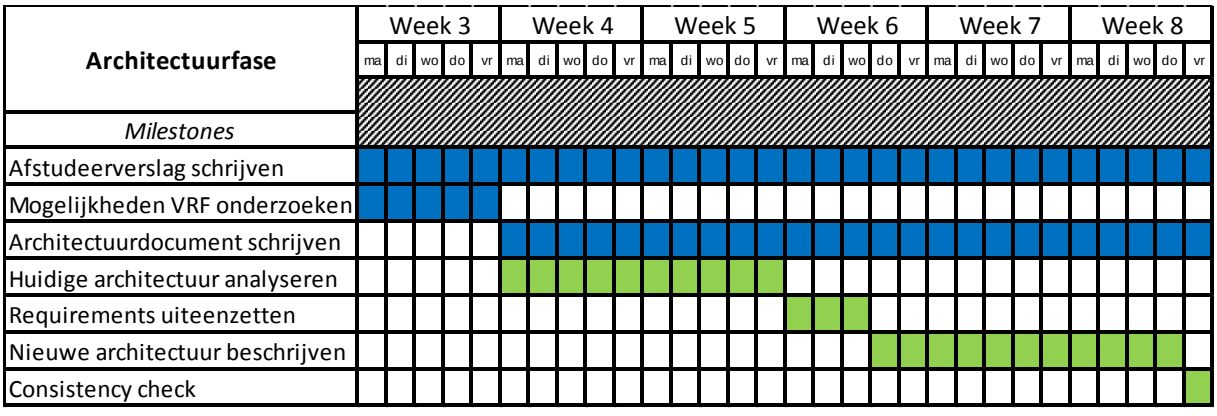
Mijlpaal	**Datum**
Plan van aanpak	29 november 2013
Architectuur	27 december 2013
Ontwerp	7 februari 2014
IP nummerplan	*17 januari 2014*
Logisch ontwerp	*17 januari 2014*
Fysiek ontwerp	*31 januari 2014*
Beheer ontwerp	*7 februari 2014*
Adviesrapport	21 februari 2014
Advies beheertools	*12 februari 2014*
Implementatieplan	*21 februari 2014*
Afstudeerdossier	14 maart 2014
Procesverslag	*7 maart 2014*

Tabel 2 - Globale planning (vereenvoudigde weergave)

Sommige producten bestaan uit meerdere deelproducten. Deze deelproducten zijn (cursief) als mijlpaal opgenomen in de planning.

9.2. Faseplanning

Tabel 3 toont de faseplanning voor de volgende fase – de architectuurfase.



Tabel 3 - Faseplanning architectuurfase

10. Kosten en baten

Kosten en baten zijn voor elke opdracht weer anders. Onderstaand worden de kosten en de baten voor deze opdracht benoemd.

10.1. Kosten

Het is op dit moment (nog) niet mogelijk om een goede inschatting te maken van de kosten voor deze opdracht. Oorzaak hiervan is dat vooralsnog niet bekend is welke en hoeveel hardware componenten gebruikt zullen worden in het ontwerp.

10.2. Baten

Tabel 4 toont de baten die voortkomen uit deze 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 4 - Baten

11. Stakeholders

Tabel 5 geeft een overzicht van de stakeholder en hun rol bij deze opdracht.

Naam	Rol	E-mail	Telefoon
Chris de Bruin	Afstudeerder	c.debruin@student.hhs.nl	+31 (88) 2882605
John Snel	Opdrachtgever	jsnel@deloitte.nl	+31 (88) 2888116
Jeroen Hassing	Begeleider	jhassing@deloitte.nl	+31 (88) 2888182
John Visser	Begeleidend examinator	j.j.visser@hhs.nl	+31 (15) 2606281
Pieter Burghouwt	Tweede examinator	p.burghouwt@hhs.nl	+31 (15) 2606288

Tabel 5 - Stakeholders

Deloitte.

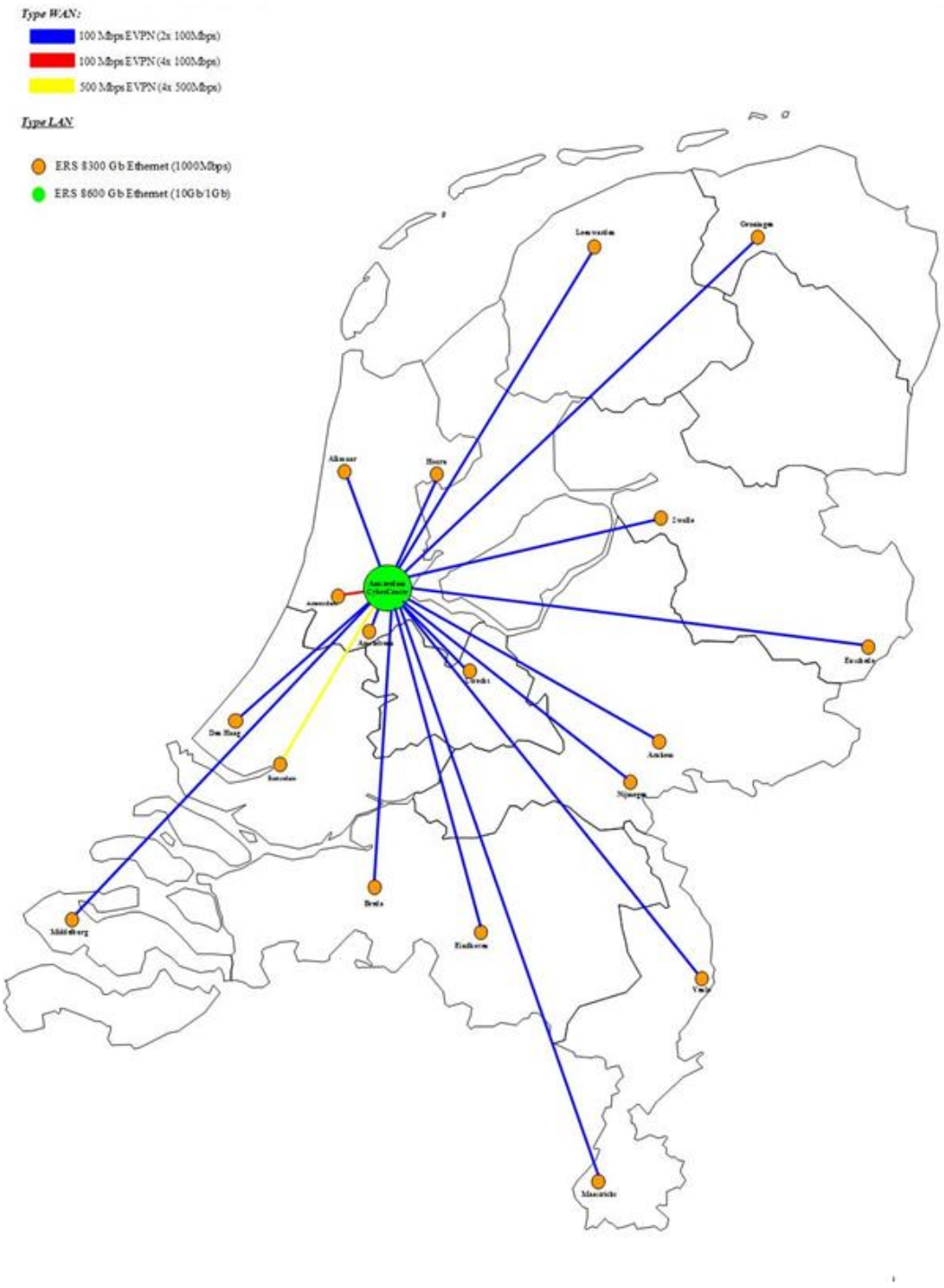
Consolidatie en virtualisatie van de core netwerk infrastructuur bij Deloitte

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

Titel	:	Architectuur
Versie	:	1.2
Datum	:	24 mei 2014
Plaats	:	Amsterdam

1. Inleiding

Al het netwerkverkeer dat over het Deloitte netwerk van en naar de verschillende Deloitte kantoren wordt verstuurd, wordt gerouteerd vanuit het Deloitte CyberCentre. Alle netwerk intelligentie bevindt zich in de core infrastructuur van het Deloitte netwerk.



Figuur 1 - Netwerk topologie Nederland

2. Huidige 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.

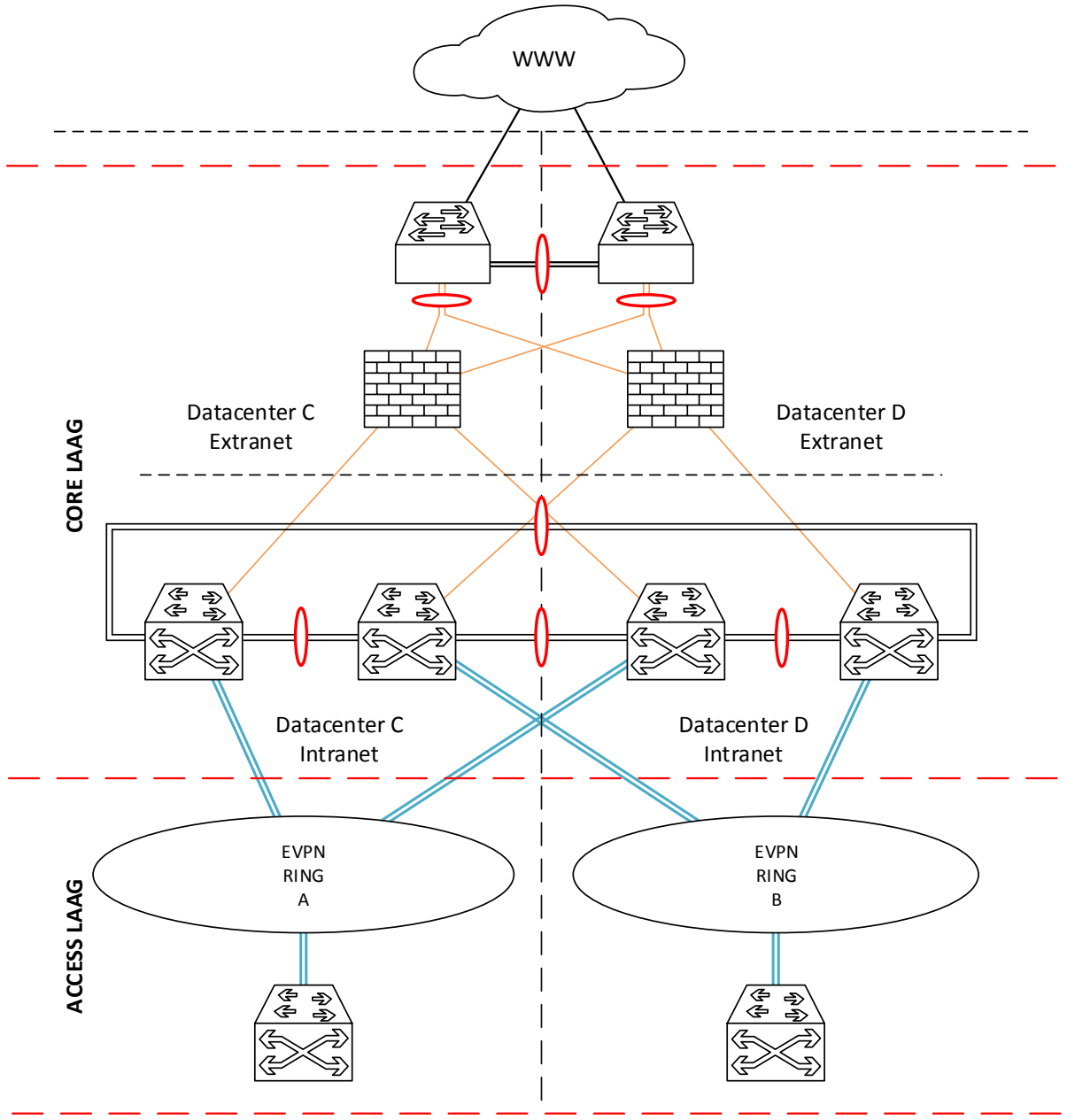
Om de huidige netwerk architectuur goed in kaart te kunnen brengen, is gebruik gemaakt van bestaande documentatie en tekeningen en zijn meerdere gesprekken gevoerd met de opdrachtgever.
Figuur 2 laat de belangrijkste onderdelen van de huidige architectuur zien. Echter zijn niet alle onderdelen relevant voor de opdracht. Alleen de onderdelen die relevant zijn voor de opdracht zijn verder uitgewerkt.

2.1. Topologie

De huidige core netwerk infrastructuur (Figuur 2) is een collapsed core design. Het bestaat uit een access laag en een samengevoegde core laag en distributie laag.

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.



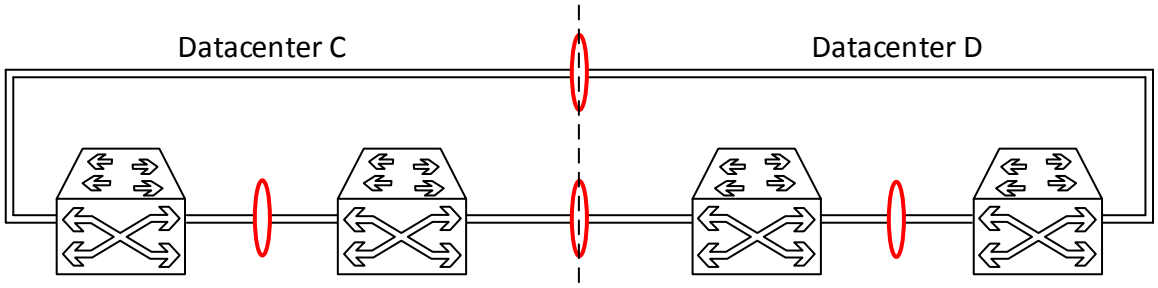
Figuur 2 – Huidige netwerk infrastructuur (vereenvoudigd overzicht)

2.2. Hardware platform

Interne core switches

De vier interne core switches (Figuur 3) 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.

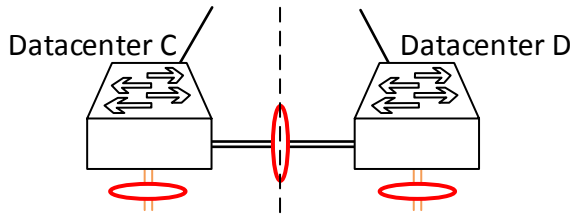


Figuur 3 – Interne core switches in huidige situatie

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

Externe core switches

De externe core switches (Figuur 4) 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 4 - Externe core switches in de huidige situatie

3. Nieuwe architectuur

Nadat de huidige architectuur in kaart is gebracht is het zaak de nieuwe architectuur in kaart te brengen.

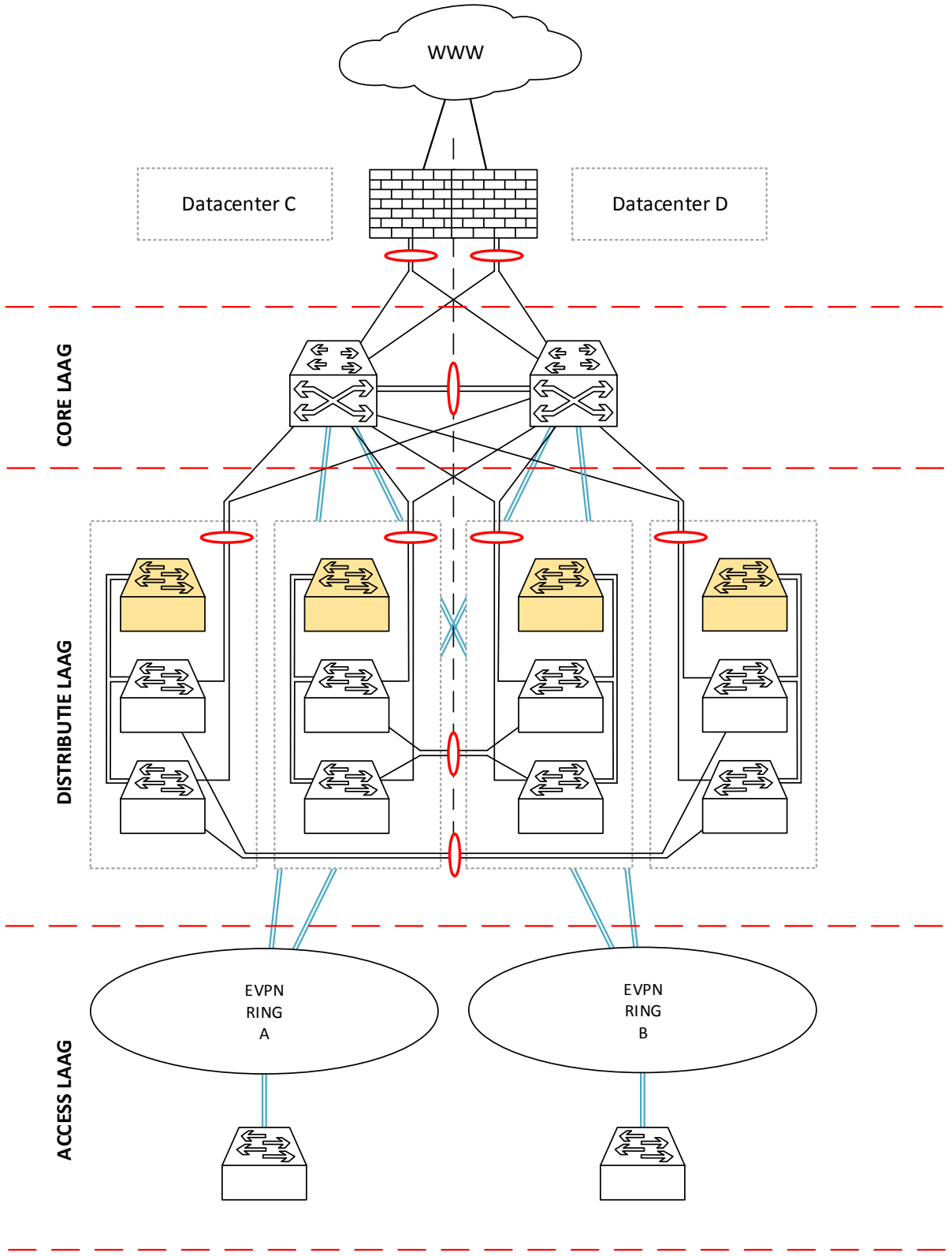
3.1. Topologie

De nieuwe core netwerk infrastructuur (Figuur 5) 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 met vier distributie stacks die elk weer zijn opgebouwd met twee distributie switches. De distributie laag worden gebruikt voor het verschaffen van toegang aan servers en andere netwerkdiensten tot de netwerk infrastructuur en zijn verbonden met de switches in de core laag.

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 zittenEthernet VPN verbindingen (EVPN) van KPN waarmee de verbindingen tussen de branch offices en het CyberCentre worden gefaciliteerd.

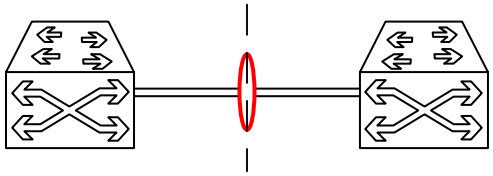


Figuur 5 - Nieuwe netwerk infrastructuur (vereenvoudigd overzicht)

3.2. Hardware platform

Core laag

De core laag is opgebouwd met twee core switches (Figuur 6) – 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.

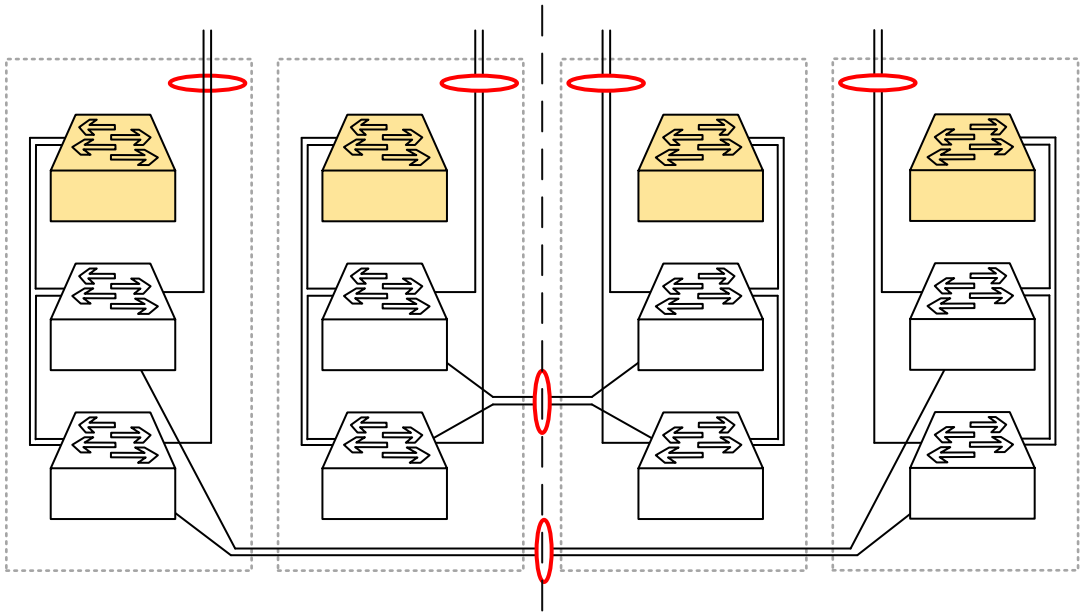


Figuur 6 - Core switches in de nieuwe situatie (vereenvoudigd overzicht)

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 7 - 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 7 - Distributie switches in de nieuwe situatie (vereenvoudigd overzicht)

3.3. Kenmerken

Ten opzichte van de huidige architectuur vallen onderstaande kenmerken op aan de nieuwe architectuur;

- 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.

4. Planning

Onderstaande tabel toont de uit te voeren activiteiten van de volgende (ontwerp)fase zoals deze op dit moment zijn ingepland. Omdat de planning een dynamisch geheel is, kan deze gedurende de betreffende fase worden bijgesteld.

Ontwerpfase	Week 9					Week 10					Week 11					Week 12					Week 13					Week 14					Week 15					Week 16					Week 17					Week 18					Week 19					Week 20				
	ma	di	wo	do	vr	ma	di	wo	do	vr	ma	di	wo	do	vr	ma	di	wo	do	vr	ma	di	wo	do	vr	ma	di	wo	do	vr	ma	di	wo	do	vr	ma	di	wo	do	vr	ma	di	wo	do	vr	ma	di	wo	do	vr	ma	di	wo	do	vr
Milestones																																																								
Afstudeerverslag schrijven																																																								
Ontwerpdocument schrijven																																																							
Fysiek ontwerp maken																																																							
IP nummerplan maken																																																							
Logisch ontwerp maken																																																							
Consistency check																																																							

Tabel 6 - Faseplanning ontwerpfase

Deloitte.

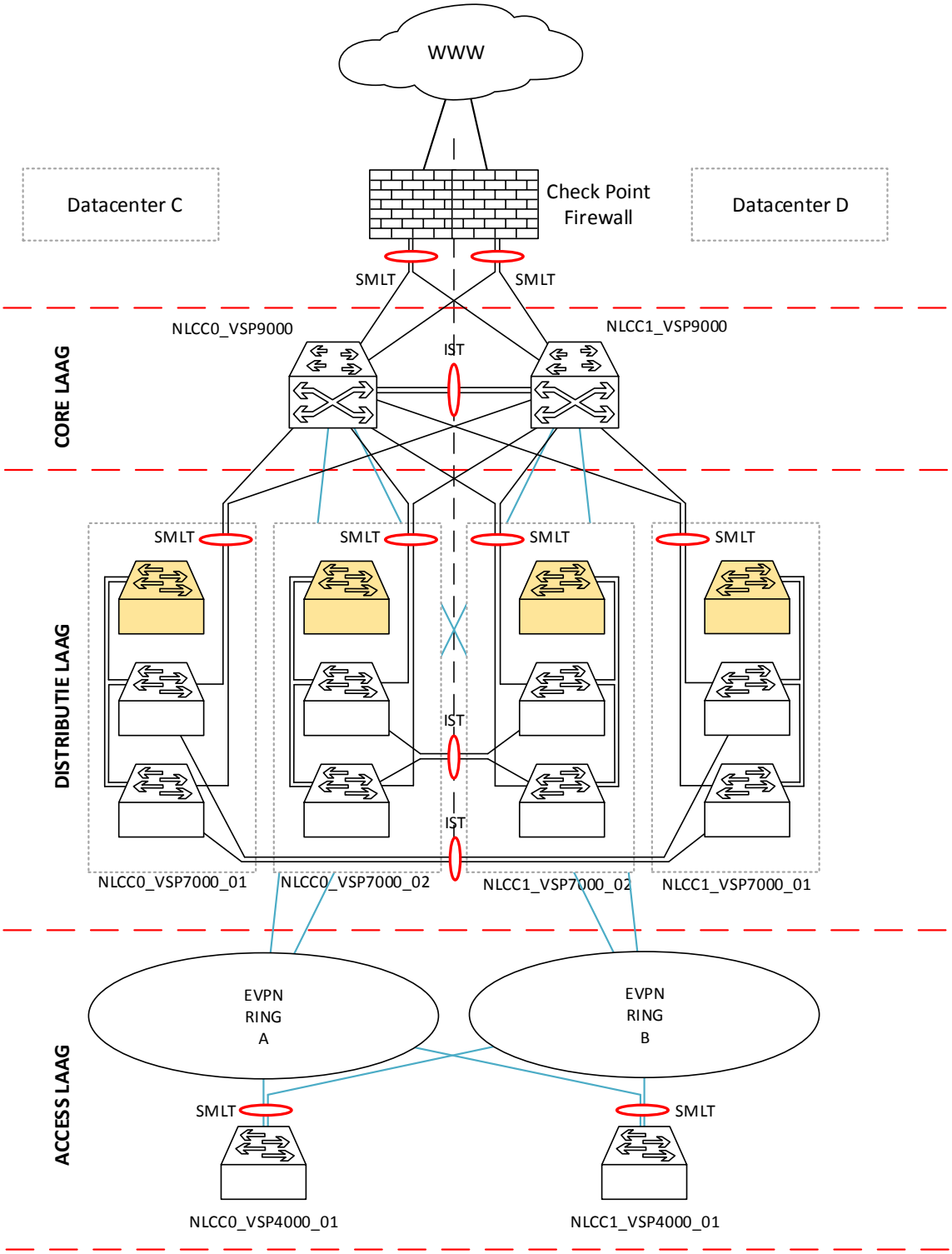
Consolidatie en virtualisatie van de core netwerk infrastructuur bij Deloitte

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

Titel	:	Ontwerp
Versie	:	1.0
Datum	:	24 mei 2014
Plaats	:	Amsterdam

1. Inleiding

Dit hoofdstuk beschrijft het detail ontwerp van de nieuwe infrastructuur. Het beschrijft de gebruikte devices en componenten, maar ook de verbindingen en protocollen die aanwezig zijn en de services die op de infrastructuur actief zijn.



Figuur 8 - Nieuwe architectuur (vereenvoudigd overzicht)

In dit hoofdstuk 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.

Verder is ook opgenomen de planning voor de volgende fase, de ontwikkelfase.

2. 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 drie types switches worden afgenomen; VSP 9000, VSP 7000 en VSP 4000.

Er worden twee VSP 9000 switches geconfigureerd ten behoeve van de core laag en er worden 16 VSP 7000 switches geconfigureerd ten behoeve van de distributie laag.

In dit document worden alleen de configuraties van de VSP 9000 en VSP 7000 switches verder uitgewerkt. De VSP 4000 switches zullen slechts globaal beschreven worden. Deze worden ingezet ten behoeve van de access laag in de branch offices en vallen dus buiten de scope van dit project.

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

2.1. Core laag

De core laag van de nieuwe infrastructuur is opgebouwd met twee VSP 9000 switches – een core switch per data center.

Hardware

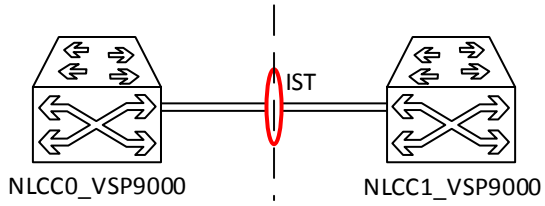
Beide switches zijn opgebouwd met elk twee 9024XL 24-port 10G Ethernet SFP+ interface modules (10 Gbps) en een 9048GB 48-port 1G Ethernet SFP interface module (1 Gbps). Dit levert een switch capaciteit op van twee maal 288 Gbps per switch.

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.



Figuur 9 - VSP 9000 configuratie in de core laag

De op de VSP 9000 aanwezige ondersteuning van Virtual Routing and Forwarding (VRF) maakt het mogelijk dat er meerdere laag drie routing domains bestaan op een hardware platform. Hierdoor

kunnen zowel de intranet omgeving als de extranet omgeving gescheiden van elkaar bestaan op dezelfde fysieke core switches.

Redundancy

De verbindingen tussen de core switches onderling, maar ook alle andere verbindingen tussen de core switches en andere lagen van de infrastructuur komen tot stand door middel van trunk verbindingen.

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

Tabel 7 - Core switch configuratie

Tabel 7 toont de trunk verbindingen die op de core switches gebruikt worden voor de onderlinge verbindingen, maar ook voor de verbindingen met de distributie stacks, de access switches en de Check Point firewalls.

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

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.
- SFP = Poort nummer van de betreffende module of unit.

Omdat de Check Point firewalls en de access switches (VSP 4000) buiten de scope van de opdracht vallen, zijn deze slechts deels uitgewerkt in Tabel 7.

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

2.2. 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 (units) – twee distributie stacks per data center.

Hardware

De distributie stacks zijn opgebouwd met twee 7024XLS 24-port 1/10 Gigabit Ethernet SFP+ switches (10 Gbps) voor fiber aansluitingen.
Later wordt een derde – nog uit te komen – VSP 7000 variant bijgeplaatst met 24 koper

aansluitingen, dit ten behoeve van devices die niet beschikken over een SFP connector. Dit levert een totale switch capaciteit op van drie maal 240 Gbps (fiber en koper) per distributie stack.
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.
In Figuur 10 wordt deze afwijkende switch in het geel afgebeeld.

Met oog op de toekomst zijn de VSP 7000 switches voorbereid op netwerk- en switchsnelheden van 40 Gbps en 100 Gbps.

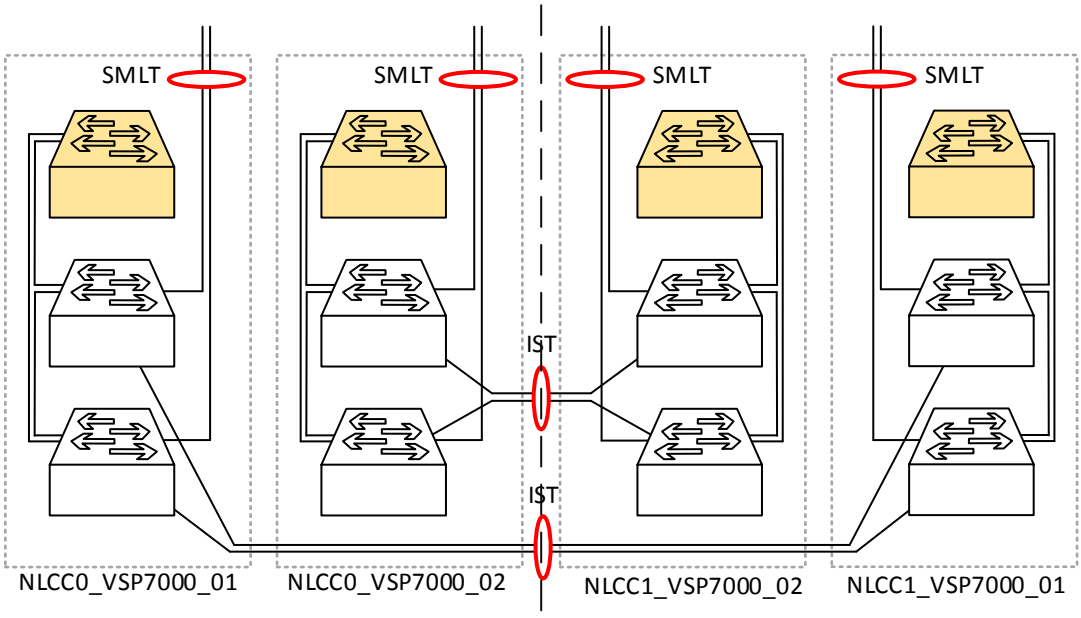
De voedingen en de cooling fans kunnen worden vervangen terwijl de switches operationeel zijn – hot swappable.

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.

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



Figuur 10 - VSP 7000 configuratie in de distributie laag (vereenvoudigd overzicht)

Redundancy

De verbindingen tussen de distributie stacks onderling, maar ook de verbindingen tussen de distributie stacks en de core switches komen tot stand door middel van trunk verbindingen.

Device	Interface	Device	Interface	Trunk
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 8 - Distributie stack configuratie

Tabel 8 toont de aansluitingen die op de distributie stacks gebruikt worden voor de onderlinge verbindingen, maar ook voor de verbindingen met de core switches.

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

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.
- SFP = Poort nummer van de betreffende module of unit.

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

2.3. Access laag

De access laag van de nieuwe infrastructuur valt niet binnen de scope van het project en wordt daarom slechts benoemd en niet in detail uitgewerkt of beschreven.

3. Logisch ontwerp

Ten behoeve van een correcte scheiding van netwerkverkeer op zowel laag twee als laag drie van het OSI model worden verschillende virtualisatie technieken geïmplementeerd in de nieuwe core netwerk infrastructuur; Virtual Routing and Forwarding voor het scheiden van netwerkverkeer op laag drie en Virtual LAN's voor het scheiden van netwerkverkeer op laag twee.

Naast bovengenoemde technieken worden verschillende laag twee en laag drie netwerk protocollen geïmplementeerd zodat alle gewenste services en diensten door de core netwerk infrastructuur gefaciliteerd kunnen worden.

3.1. 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).

VRF maakt het mogelijk om meerdere router tabellen op dezelfde fysieke hardware te laten bestaan. Tabel 9 toont de VRF's en netwerken die op de core switches aanwezig zijn.

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 9 - Overzicht VRF's

3.2. VLAN

Netwerkverkeer op laag twee wordt van elkaar gescheiden door Virtual LAN's (VLAN) te gebruiken. Voor zowel intranet als voor extranet worden VLAN's gebruikt.

Intranet VLAN's

Tabel 10 toont de VLAN's die worden gebruikt voor het intranet gedeelte van het 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 10 - Overzicht VLAN's core netwerk intranet

Tabel 11 toont de VLAN's die worden gebruikt voor de intranet servers.

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 11 - Overzicht VLAN's servers intranet

Tabel 12 toont de VLAN's die worden gebruikt voor de 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 12 - Overzicht VLAN's servers intranet

Tabel 13 toont het VLAN dat gebruikt wordt voor het guest 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 13 - VLAN gasten netwerk

Extranet VLAN's

Tabel 14 toont de VLAN's die worden gebruikt voor het extranet gedeelte van het 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 14 - Overzicht VLAN's core netwerk extranet

Tabel 15 toont de VLAN's die worden gebruikt voor de extranet servers.

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 15 - Overzicht VLAN's servers extranet

3.3. Protocollen

Om alle gewenste diensten beschikbaar te maken via de core netwerk infrastructuur en om redundancy van de infrastructuur te kunnen waarborgen is een aantal protocollen in de core infrastructuur geconfigureerd.
Er wordt gebruik gemaakt van protocollen uit zowel laag twee als laag drie uit het OSI model;

- **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.

3.4. Interfaces

Aan de hand van het IP nummer plan (Figuur 11) krijgen de interfaces van de switches IP adressen toegekend.

De tabellen - IP configuratie intranet VRF en - IP configuratie extranet VRF (Tabel 16 en Tabel 17) laten zien welk IP adres, welk routing protocol en welk trunk type op de switch interfaces is geconfigureerd.

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 16 - IP configuratie intranet VRF

IP CONFIGURATIE EXTRANET VRF							
Host	**Interface**	**IP**	**Host**	**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 17 - IP configuratie extranet VRF

3.5. 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 van 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.

4. Planning

Onderstaande tabel toont de uit te voeren activiteiten van de volgende (ontwikkel)fase zoals deze op dit moment zijn ingepland. Omdat de planning een dynamisch geheel is, kan deze gedurende de betreffende fase worden bijgesteld.

Ontwikkelfase	Week 21					Week 22				
	ma	di	wo	do	vr	ma	di	wo	do	vr
Milestones										
Afstudeerverslag schrijven										
Implementatieplan schrijven										

Tabel 18 - Planning ontwikkelfase

Deloitte.

Bijlage 1: IP nummerplan

	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 11 - IP-nummerplan

Deloitte.

Consolidatie en virtualisatie van de core netwerk infrastructuur bij Deloitte

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

Titel	:	Implementatieplan
Versie	:	1.0
Datum	:	24 mei 2014
Plaats	:	Amsterdam

1. Inleiding

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.

2. Voorbereidingen

- 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 19 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 19 - Overzicht stroomverbuik

3. 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.

4. Stap 1: De core laag vervangen

Tabel 20 - Uit te voeren acties in migratie stap 1 – toont de uit te voeren acties voor 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 20 - Uit te voeren acties in migratie stap 1

5. Stap 2: De distributie laag plaatsen

Tabel 21 - Uit te voeren acties in migratie stap 2 – toont de uit te voeren acties voor 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 21 - Uit te voeren acties in migratie stap 2

6. Stap 3: De distributie laag migreren

Tabel 22 - Uit te voeren acties in migratie stap 3 – toont de uit te voeren acties voor 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 22 - Uit te voeren acties in migratie stap 3

7. Stap 4: De access laag migreren

Tabel 23 - Uit te voeren acties in migratie stap 4 – toont de uit te voeren acties voor 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 23 - Uit te voeren acties in migratie stap 4

8. Stap 5: Het network management systeem inrichten

Om in de nieuwe situatie de core infrastructuur goed te kunnen 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.

9. Stap 6: Monitoring en afkoppeling

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

10. Stap 7: Ontmanteling

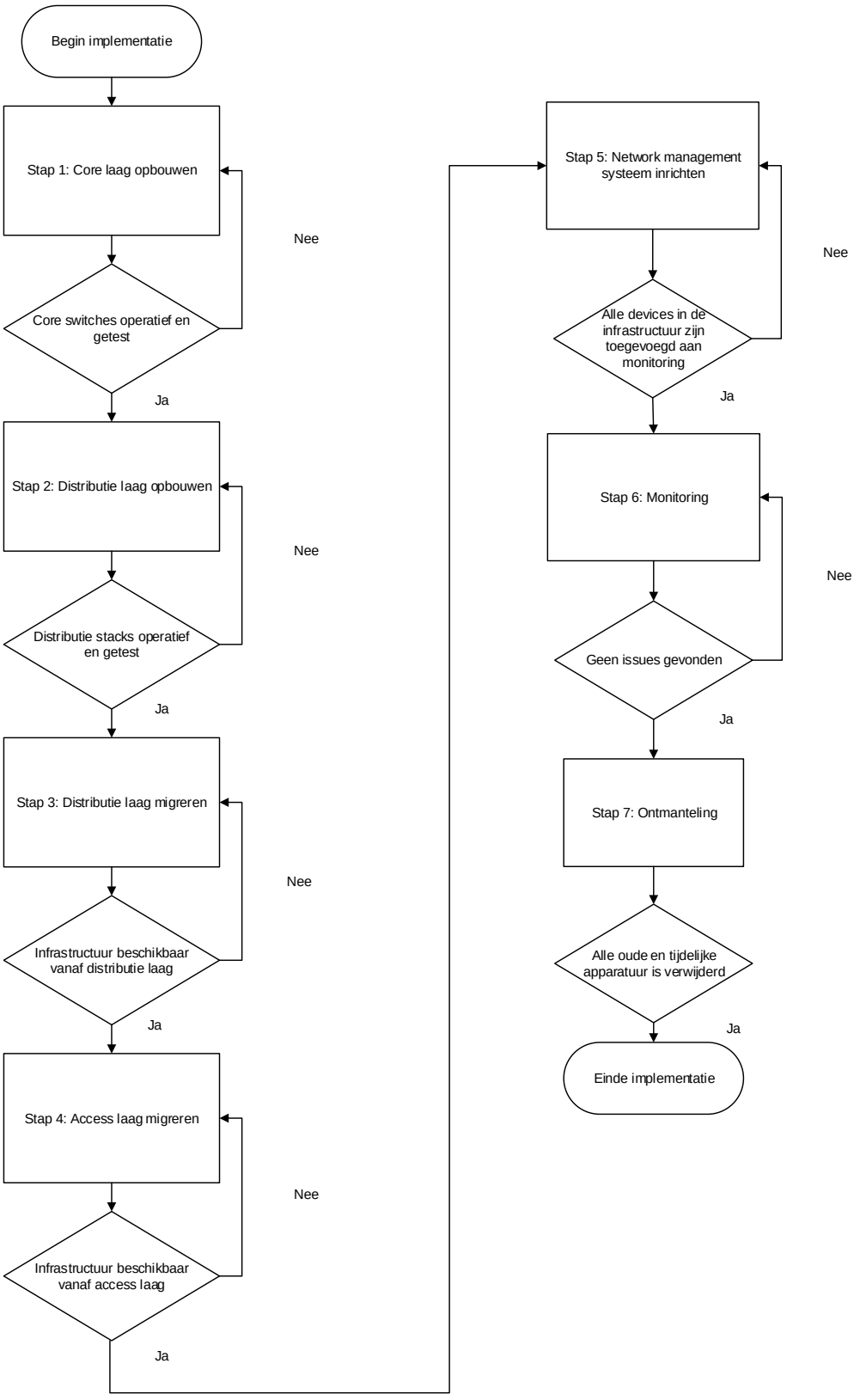
Tabel 24 - Uit te voeren acties in migratie stap 7 – toont de uit te voeren acties voor migratie stap 7.

	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 24 - Uit te voeren acties in migratie stap 7

11. Flowchart implementatie

Figuur 12 - Flowchart met de stappen van de migratie – toont het stappenplan als een flowchart.



Figuur 12 - Flowchart met de stappen van de migratie

Tabellen en figuren

Tabellen

Figuren