LIVING UPTIME

“Onder welke voorwaarden is het met TRILL mogelijk om STP uit een door Qi ict bv. gebruikt switched core netwerk te migreren?”

Student: Frank van Eijk
Studentnummer: 11079045
Onderwijsinstelling: Haagse Hogeschool Delft
Opleiding: Technische Informatica
Afstudeerperiode: 11-04-2016 t/m 30-09-2016
Begeleider: Dhr. F. Wieringa
Tweede examinator: Dhr. M. Rambhadjan

Bedrijf: Qi ict bv.
Afdeling: Field Services (Networks & Storage)
Bedrijfsbegeleider: Hans Suttorp
Opdrachtgever: Jan de Vries

Datum: 03-10-2016
Versie: 1.0

Inhoudsopgave

Bijlage A

Afstudeerplan

Afstudeerplan

Informatie afstudeerder en gastbedrijf (*structuur niet wijzigen*)

Afstudeerblok: 2016-1.2 (start uiterlijk 9 mei 2016)
Startdatum uitvoering afstudeeropdracht: 11 april 2016
Inleverdatum afstudeerdossier volgens jaarrooster: 3 oktober 2016

Studentnummer: 11079045
Achternaam: dhr. van Eijk
Voorletters: F.C.M.
Roepnaam: Frank
Adres: Platanendreef 11
Postcode: 2631JD
Woonplaats: Nootdorp
Telefoonnummer: 015-3107513
Mobiel nummer: +316 12 22 92 02
Privé emailadres: frankvaneijk94@gmail.com

Opleiding: Technische Informatica
Locatie: Delft
Variant: voltijd

Naam studieloopbaanbegeleider: J. van Peski
Naam begeleidend examinator: F. Wieringa
Naam tweede examinator: M. Rambhadjan

Naam bedrijf: Qi ict B.V.
Afdeling bedrijf: Field Services
Bezoekadres bedrijf: Delftechpark 35-37
Postcode bezoekadres: 2628 XJ
Postbusnummer: 402
Postcode postbusnummer: 2600 AK Delft
Plaats: Delft
Telefoon bedrijf: 015 888 04 44
Telefax bedrijf: 015 888 04 45
Internetsite bedrijf: https://www.qi.nl

Achternaam opdrachtgever: dhr. De Vries
Voorletters opdrachtgever: J.
Titulatuur opdrachtgever: ing.
Functie opdrachtgever: Network Engineer
Doorkiesnummer opdrachtgever: 015 888 04 44
Email opdrachtgever: Jan.de.Vries@qi.nl

Achternaam bedrijfsmentor: dhr. Suttorp
Voorletters bedrijfsmentor: H.
Titulatuur bedrijfsmentor: ing.
Functie bedrijfsmentor: Network Engineer
Doorkiesnummer bedrijfsmentor: 015-8880444
Email bedrijfsmentor: hans.suttorp@qi.nl

NB: bedrijfsmentor mag dezelfde zijn als de opdrachtgever

Doorkiesnummer afstudeerder: 015-8880444
Functie afstudeerder (deeltijd/duaal):

Titel afstudeeropdracht:
Spanning Tree Protocol vs. TRILL; wordt Spanning Tree Protocol uit de door QI ict gebruikte switched netwerken gefaseerd?

Opdrachtomschrijving

1. Bedrijf

Qi ict is een gespecialiseerde leverancier van hoogwaardige ict infrastructuurproducten en diensten. Onze missie kan worden omschreven met de woorden “living uptime”. We streven ernaar om voor de ict infrastructuur van onze klanten een zo hoog mogelijk uptime te realiseren.

We doen dat met producten van technology leaders, met de professionaliteit van onze hoog opgeleide engineers en met onze eigen sparevoorraad.

Qi ict is een goed georganiseerd, winstgevend en financieel gezond bedrijf. Binnen Qi ict heerst een informele open sfeer. Collegialiteit, teamspirit, flexibiliteit en eigen initiatief zijn verankerd in onze organisatie.

De afdeling waar de stagiair terecht komt is Field Services. Deze afdeling verricht met name de installaties bij de klanten en zorgt hierbij ook voor het onderhoud van de apparatuur en de diensten die hierbij horen. De stagiair wordt hier geplaatst omdat het onderzoek voornamelijk te maken heeft met de installaties die deze afdeling verzorgt.

2. Probleemstelling

Qi ict gebruikt op dit moment het spanning tree protocol(STP) voor het gebruik van redundantie in hun switched netwerken, deze keuze is gemaakt toen STP de meest voordehand liggende keuze was, maar is dit tegenwoordig nog steeds de meest logische keuze. De hoofdreden voor dit onderzoek is dat Qi ict over weinig kennis beschikt wat betreft de mogelijkheden van alternatieven zoals TRILL.

Doordat er nog geen uitgebreid onderzoek is gedaan, kan Qi ict niet zeggen of zij op de meest efficiënte manier redundantie uitvoeren. Daarmee komt dus de opdracht tot stand. Onderzoek verschillende protocollen om redundantie uit te voeren in een switched netwerk en adviseer welk protocol het efficiëntst is. Hierbij kan de vraag worden gesteld; “wordt Spanning Tree Protocol uit de door QI ict gebruikte switched netwerken gefaseerd?”

Deelvragen die kunnen worden opgesteld bij deze hoofdvraag zijn:
- Bij welk soort netwerk is welk redundantie protocol het efficiëntst.
- Hoe is er compatibility mogelijk tussen TRILL en niet-TRILL netwerken.
- Welke migratie strategieën zijn er die TRILL en de andere alternatieven ondersteunen.

De huidige opdracht is voor Qi ict niet echt een probleem, maar omdat Qi ict uiteraard de beste wil zijn in wat zij doen, zal deze opdracht wel degelijk toegevoegde waarde hebben voor het bedrijf , maar ook voor de klanten van Qi ict. En dat de beste zijn houdt onder andere in; het netwerk zo efficiënt mogelijk inrichten en onderhouden.

3. Doelstelling van de afstudeeropdracht

Het doel van de opdracht is het onderzoeken van de verschillende redundantie protocollen in switched netwerksystemen. Hierin worden de voor- en nadelen van de alternatieven zoals, de mogelijkheden van TRILL, onderzocht ten opzichte van het huidige protocol (STP). Dit onderzoek wordt ondersteund door een lab-opstelling waarin het onderzoek in de praktijk kan worden getest en gedemonstreerd. De resultaten zullen een bijdrage leveren aan de adviezen die Qi ict haar klanten geeft omtrent de keuze voor redundantie oplossingen en de engineers helpen om deze oplossing goed te kunnen implementeren.

4. Resultaat

De resultaten van de opdracht worden verwerkt in een rapport waarin het onderzoek wordt beschreven. Naast het rapport zullen de resultaten worden gepresenteerd aan de stagebegeleider en enkele andere (technische) collega's binnen Qi ict. De resultaten zullen een bijdrage leveren aan de adviezen die Qi ict haar klanten geeft omtrent de keuze voor redundantie oplossingen en de engineers helpen om deze oplossing goed te kunnen implementeren.

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

Fase	Werkzaamheden	Ingeplande dagen
Oriëntatiefase	- Plan van aanpak schrijven - Gesprekken met de engineers die gebruik maken van de huidige redundantie protocollen. - Vast stellen requirements	15 dagen
Onderzoeksfase	Onderzoeken naar alternatieve protocollen voor redundantie.	20 dagen
Ontwerpfase	Ontwerpen en bouwen van de testopstellingen per redundantie protocol.	10 dagen
Testfase	Het testen van de testopstellingen.	15 dagen
Adviseerfase	Het schrijven van het adviesrapport.	10 dagen
Documentatiefase	Opbouwen afstudeerdossier.	15 dagen

6. Op te leveren (tussen)producten

- Plan van Aanpak
- Literatuuronderzoek
- Testopstelling + Testrapport
- Adviesrapport met de resultaten
- Presentatie met de resultaten
- Scriptie (procesverslag)

7. Te demonstreren competenties en wijze waarop

A1 Analyseren van het probleemdomein

Voor het onderzoeken van het (probleem)domein kunnen diverse methoden en technieken gebruikt worden, zoals interviewen en analyse van documenten en de huidig gebruikte protocollen. 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.

A3 Achterhalen van behoeften van belanghebbenden

Om de behoeften en wensen van de belanghebbende te achterhalen zullen er meerdere gesprekken worden gevoerd. Als deze behoeften en wensen conflicteren dan zal er gekozen moeten worden welke behoeften er wel en niet worden uitgevoerd.

J12 Adviesproces uitvoeren

Het adviesproces zal worden uitgevoerd door middel van: het vergaren van de requirements, het onderzoeken naar de verschillende oplossingen voor redundantie, het ontwerpen van een testopstelling, het gebruiken van de testopstelling om waardes aan de verschillende oplossingen te geven, het vergelijken van de waardes en het adviseren welke oplossing het beste is volgens het onderzoek door middel van een adviesrapport.

Bijlage B

Plan van Aanpak

Plan van aanpak

Opdrachtgever: Qi ict bv.
Begeleider: Hans Suttorp
Afstudeerder: Frank van Eijk
Opleiding: Technische Informatica, HHS Delft
Datum: 03-10-2016
Versie: 1.0

Versiebeheer

Versie	Datum	Opmerking
0.1	29-4-2016	Eerste versie
0.2	13-5-2016	Aanpassingen doorgevoerd na feedback van dhr. Hans Suttorp
0.3	23-5-2016	Laatste aanpassingen doorgevoerd na feedback van dhr. Hans Suttorp
1.0	30-9-2016	Opmaak consistent gemaakt

Inhoudsopgave

1. Achtergrond

1.1 Bedrijfsomschrijving

Qi ict bv. is een gespecialiseerde leverancier van hoogwaardige ICT infrastructuurproducten en diensten. De missie van Qi ict bv. kan worden omschreven met de woorden “living uptime”. Er wordt ernaar gestreefd om voor de ICT infrastructuur van onze klanten een zo hoog mogelijk uptime te realiseren.

Qi ict bv. doet dat met producten van technology leaders, met de professionaliteit van haar hoog opgeleide engineers en met de eigen sparevoorraad.

Qi ict bv. is een goed georganiseerd, winstgevend en financieel gezond bedrijf. Binnen Qi heerst een informele open sfeer. Collegialiteit, teamspirit, flexibiliteit en eigen initiatief zijn verankerd in de organisatie.

De afdeling waarvoor de opdracht gedaan wordt is de afdeling Field Services. Deze afdeling verricht voornamelijk de installaties bij de klanten en zorgt hierbij ook voor het onderhoud van de apparatuur en de diensten die hierbij horen. De opdracht wordt uitgevoerd voor deze afdeling omdat het onderzoek voornamelijk te maken heeft met de installaties die Field Services verzorgt.

De begeleider, Hans Suttorp, werkt zelf ook op de afdeling Field Services. Hij is één van de vele network engineers die op deze afdeling werken. Dhr. Suttorp heeft zelf zijn opleiding gevolgd aan de Haagse Hogeschool en heeft zijn afstudeerstage volbracht bij Qi ict bv. Hierbij heeft hij onderzoek gedaan naar carrier ethernet.

1.2 Probleemstelling

Qi ict bv. maakt op dit moment veelal gebruik van het spanning tree protocol(STP) voor het gebruik van redundantie in hun switched core netwerken, deze keuze is gemaakt toen STP de meest voordehand liggende keuze was, maar is dit tegenwoordig nog steeds de beste keuze? De hoofdreden voor dit onderzoek is dat Qi over weinig kennis beschikt wat betreft de mogelijkheden van alternatieven zoals TRILL.

Hierbij kan de vraag worden gesteld; *“Onder welke voorwaarden Is het met TRILL mogelijk om STP uit een door Qi ict bv. gebruikt switched core netwerk te faseren?”*

Aan de hand van bovenstaande hoofdvraag kunnen deelvragen worden opgesteld. Hieronder zijn de verschillende deelvragen beschreven met een globale inhoud per deelvraag:

- Wat is het Spanning Tree Protocol (STP)
  - Hoe werkt het Spanning Tree Protocol in een switched core netwerk
  - Zitten er nadelen aan het Spanning Tree Protocol

- Wat is Transparent Interconnection of Lots of Links (TRILL)
  - Hoe werkt TRILL in een switched core netwerk
  - Wat zijn relevante varianten van TRILL
  - Wat zijn de verschillen tussen TRILL en de varianten
  - Welke randvoorwaarden zijn er om TRILL of de varianten te implementeren

- Verschillen tussen STP en TRILL + de varianten
  - Wat zijn de voor- en nadelen van STP ten opzichte van TRILL en de varianten

- Waar kunnen TRILL en de varianten het beste worden toegepast in een netwerk?

- Kan er naar TRILL gemigreerd worden in de reeds bestaande infrastructuren?
    - Hoe ziet de gekozen netwerk infrastructuur eruit
    - Wat zijn de huidige protocollen die worden gebruikt
    - Is er compatibiliteit mogelijk met de huidig gebruikte protocollen

- Experimenteel onderzoek naar de migratie en werking van TRILL (Proof of Concept)

De huidige opdracht is voor Qi niet echt een probleem, maar omdat Qi ict bv. uiteraard de beste kwaliteit wil leveren, zal deze opdracht wel degelijk toegevoegde waarde hebben voor het bedrijf. Maar niet alleen Qi ict bv. zal hier profijt van hebben, ook de klanten zullen hier van mee profiteren. En dat de beste kwaliteit leveren houdt onder andere in; het netwerk zo efficiënt mogelijk inrichten en onderhouden.

1.3 Doelstelling

Het doel van de opdracht is het onderzoeken onder welke voorwaarden het mogelijk is om met TRILL, STP uit de huidig gebruikte switched core netwerken te kunnen faseren. Hierbij wordt de mogelijkheid bedoeld of TRILL zonder grote veranderingen kan worden doorgevoerd in een bestaand netwerk. Door middel van een literatuuronderzoek en een experimenteel onderzoek zal deze doelstelling behaald moeten worden. Beide onderzoeken zullen een resultaat geven over de mogelijkheid of TRILL daadwerkelijk STP uit een switched core netwerk kan faseren dan wel migreren. Deze resultaten zullen een bijdrage leveren aan de adviezen die Qi ict bv. haar klanten geeft omtrent de keuze voor redundantie oplossingen en de engineers helpen om deze oplossing goed te kunnen implementeren.

2. Project

In dit hoofdstuk worden de verschillende aspecten van de opdracht behandeld. Hierbij wordt de opdracht verder toegelicht.

2.1 De opdracht

Qi ict bv. heeft in de afgelopen jaren in de markt een goede reputatie opgebouwd en deze willen ze ook graag behouden. Dit hebben zij bereikt door het leveren van hoogwaardige producten en diensten, een hoge klantvriendelijkheid en het áltijd nakomen van afgesproken overeenkomsten (contracten). Qi ict bv. wordt in het kopje 2.3 Opdrachtgever verder besproken.

De opdracht heeft in dit geval te maken met het leveren van de diensten, hierin wordt er onderzoek gedaan naar onder andere het huidige protocol (Spanning Tree Protocol) dat gebruikt wordt in switched core netwerken. STP is een, in het OSI Model, Layer 2 switching protocol dat gebruikt wordt om redundantie in te bouwen in switched core netwerken en is geschikt voor het detecteren van loops. Hoewel STP nog veelal gebruikt wordt, zijn er tegenwoordig al meerdere alternatieven op de markt wat betreft het inbouwen van redundantie in switched core netwerken en het detecteren van loops. Een voorbeeld hiervan is Transparent Interconnection of Lots of Links (TRILL). TRILL is ook een Layer 2 switching protocol die gebruikt wordt om redundantie in een (switched)core netwerk te bouwen en ook beschikt TRILL over het detecteren van loops. Verder hebben meeste switch leveranciers een eigen versie van TRILL, een voorbeeld hiervan zijn FabricPath van Cisco, VCS van Brocade en SPB van Alcatel.

Naast het onderzoeken van de protocollen zal ook een switched core netwerk van Qi ict bv. gebruikt worden om uit te zoeken of het mogelijk is om naar een TRILL of naar een variant van TRILL te kunnen migreren. In dit netwerk wordt op dit moment gebruik gemaakt van STP; echter is het niet zeker of dit protocol nog het efficiëntst is om te gebruiken.

Door bovenstaande redenen zal het onderzoek gedaan worden of het mogelijk is om STP uit de huidig gebruikte switched-core netwerken van Qi ict bv. te kunnen te faseren. Dit zal getest worden door het ontwerpen van een simulatie en het maken van een testplan. Uit deze resultaten zal een adviesrapport geschreven worden of het inderdaad mogelijk is om het netwerk te kunnen migreren naar een TRILL netwerk.

2.2 Resultaat

De resultaten van de opdracht worden verwerkt in een rapport waarin het onderzoek wordt beschreven. Naast het rapport zullen de resultaten worden gepresenteerd aan de begeleider en enkele andere (technische) collega's binnen Qi ict bv. De resultaten zullen een bijdrage leveren aan de adviezen die Qi ict bv. haar klanten geeft omtrent de keuze voor redundantie oplossingen en de engineers helpen om deze oplossing goed te kunnen implementeren.

2.3 Scope

Tijdens het werken aan de opdracht zal er voornamelijk bezig gehouden worden met:

- Het onderzoeken van het Spanning Tree Protocol;
- Het onderzoeken van het TRILL protocol;
- Het onderzoeken van TRILL variant, FabricPath van Cisco, VCS van Brocade en SPB van Alcatel
- Onderzoek doen of TRILL te migreren is op een bestaand Qi ict bv. netwerk.

2.4 Randvoorwaarden

De opdracht wordt uitgevoerd onder de volgende randvoorwaarden:

- Begindatum: maandag 11 april 2016.
- Einddatum: vrijdag 30 september 2016.
- Toegang tot Internet of tot benodigde literatuur;
- Qi ict stelt de afstudeerder in de gelegenheid om gebruik te maken van de faciliteiten en tijd welke nodig zal zijn om op de juiste manier de afstudeeropdracht te kunnen afronden.
- Benodigde hardware:
    - TRILL 'ready' apparatuur
    - Drietal werkstations
- Om de kwaliteit te waarborgen wordt er eens per twee weken een gesprek gehouden tussen de afstudeerder en de bedrijfsmentor om de voortgang en documenten te bespreken, en indien nodig het project bij te sturen.

2.5 Project organisatie

In dit hoofdstuk vindt u de contactgegevens en de rollen van de betrokken personen in dit project. Daarnaast kunt u de adresgegevens vinden van de onderwijsinstelling en het bedrijf waar de afstudeeropdracht wordt uitgevoerd.

Naam	Rol	E-mail	Telefoonnummer
Frank van Eijk	Afstudeerder	frankvaneijk94@gmail.com	+31 (0)6 12 22 92 02
Fred Wieringa	Begeleidend examinator	W.F.C.Wieringa@hhs.nl	+31 (0)70 445 85 20
Marvin Rambhadjan	Tweede examinator	marvinr1986@gmail.com	+31 (0)6 12 11 97 75
Hans Suttorp	Bedrijfsmentor	Hans.Suttorp@qi.nl	+31 (0)15 888 04 44
Jan de Vries	Opdrachtgever	Jan.de.Vries@qi.nl	+31 (0)15 888 04 44

Naam	Bezoekadres
De Haagse Hogeschool	Rotterdamseweg 137, 2628 AL Delft
Qi ict	Delftechpark 35-37 2628XJ Delft

2.6 Op te leveren producten

Tijdens en aan het einde van de afstudeerperiode worden verschillende producten opgeleverd. Deze op te leveren producten zijn tot stand gekomen in samenspraak met de afstudeerbegeleider.

Plan van aanpak
Voordat er met de opdracht wordt begonnen moet er wel duidelijk worden gemaakt wat het plan is voor het project en hoe de opdracht tot het gewenste resultaat kan komen.

Rapport literatuuronderzoek
Het onderzoeksrapport wordt gebruikt om bestaande kennis over de probleemstelling te verzamelen. Deze kennis kan in verschillende bronnen gevonden worden, zoals wetenschappelijke tijdschriftartikelen, boeken, papers, scripties en archiefmateriaal.

Ontwerprapport
Het ontwerprapport laat zien hoe de gebruikte simulatie is opgebouwd. Dit document wordt al deels aangeleverd door Qi ict bv. omdat, het ontwerp is gebaseerd op een netwerk die door Qi ict bv. bij een klant is aangelegd. Hierin worden ook de eisen gesteld waaraan het TRILL netwerk moeten voldoen.

Migratieplan
Als het ontwerp klaar is en is gebouwd, dan moet er een plan worden opgesteld om ervoor te zorgen dat het huidige netwerk gemigreerd wordt naar een TRILL netwerk. Hierin wordt stap voor stap uitgelegd hoe deze migratie gaat verlopen.

Testrapport
In het testrapport worden de resultaten van de uitgevoerde testen weergegeven. Met behulp van deze resultaten zal uiteindelijk een advies worden geschreven.

Rapport experimenteel onderzoek
Nadat de resultaten van de test zijn voortgekomen uit het testrapport, kan er begonnen worden aan het schrijven van het experimenteel onderzoek. Hierin komen alle bevindingen van het experiment en de behaalde resultaten van het testrapport verwerkt. Aan de hand van beide onderzoeken wordt er een advies gegeven over wat het beste is voor Qi ict bv. om uit te voeren of juist niet.

Presentatie
De gevonden resultaten die uit het onderzoek komen worden naast het schrijven van het adviesrapport, bekend gemaakt aan de network engineers in de vorm van een presentatie. Hierbij worden de bevindingen gepresenteerd, hoe is deze bevinding tot stand gekomen en waarom is dit resultaat beter dan de huidige situatie.

Scriptie
Aan het eind van de afstudeerperiode moet er een eindverslag worden ingeleverd. Hierin wordt uitgelegd wat er bereikt is en wat onderweg de grootste problemen waren. De opdracht wordt beschreven. Er wordt verantwoordt wat er per fase is gedaan. En hoe is de conclusie tot stand is gekomen.

3. Aanpak

In dit hoofdstuk wordt de aanpak van de opdracht behandeld. Hierin worden de keuzes voor de gekozen methodiek verantwoordt en worden de gebruikte standaarden toegelicht.

3.1 Methodiek

Voor deze opdracht moeten er twee soorten methodiek worden gekozen, één voor het project op zichzelf en één voor het onderzoek.

3.1.1 Projectmethode

Er zijn verschillende methodieken die als projectmethode gebruikt kunnen worden bijvoorbeeld: Waterval, RUP, Scrum of een eigen methodiek. Elke methodiek is in meerdere of mindere mate geschikt voor dit project. Het is daarom belangrijk om de kenmerken van het project te beschrijven:

- Tijdens dit project moeten er verschillende protocollen worden onderzocht.
- Tijdens het project moet er een netwerk worden geanalyseerd.
- Tijdens het project moet er apparatuur worden geconfigureerd.
- De requirements van het project staan vast.
- Tijdens het project zal documentatie worden opgeleverd.
- De hardware wordt door Qi ict bv. geleverd.
- Ervaring met de methodiek wordt gezien als een must.

De methodieken die met elkaar vergeleken worden zijn: Waterval, RUP, SCRUM en een eigen methode.

De watervalmethodiek is relatief eenvoudig te plannen en te beheren, aangezien er een recht pad wordt bewandeld zonder iteraties. Deze methodiek voldoet aan de eis dat de systeemeisen van te voren al vast staan en niet meer veranderen. Ook biedt deze methodiek ruimte voor onderzoek en is er ruimte voor het schrijven van Documentatie. De ervaring met deze methodiek is ook een positief punt[1].

RUP is een iteratieve ontwikkelmethodiek, waarbij een grote ruimte is voor het doen van analyse en onderzoek. Deelsystemen kunnen in verschillende iteraties worden doorlopen, waarbij opnieuw een analyse kan worden uitgevoerd. Doordat er meerdere malen een analyse wordt uitgevoerd is deze methodiek minder bruikbaar voor dit project. RUP is in beginsel ook vooral gericht op grote ontwikkelteams en op het bijhouden van veel documentatie rondom het projectmanagement, wat het complex maakt om het te beheersen. Door deze kenmerken valt deze methodiek af[2].

SCRUM is een iteratieve en incrementele agile-methodiek, wat het erg geschikt maakt voor sterk wisselende of nog onbekende systeemeisen. Echter staan de eisen bij dit project al vast. Ook is SCRUM minder geschikt voor het uitvoeren van veel onderzoek, maar richt zich meer op het opleveren van deelproducten. Hierbij wordt er weinig documentatie geschreven en ligt de nadruk erg op het opereren in kleinere maar nauw samenwerkende teams. Dit project wordt echter solo uitgevoerd. Ook is er weinig ervaring met deze methodiek. Door deze kenmerken is SCRUM minder geschikt als methodiek voor dit project[3].

De eigen methodiek is gebaseerd op de Watervalmethode, hierbij zijn de kenmerken bijna identiek aan die van de Watervalmethode, echter zal de fasering anders verlopen. Zo wordt er een onderzoeksfase en een adviseerfase toegevoegd. Ook worden de implementatiefase en testfase weggelaten en vervangen door een experimentele fase. Doordat er ervaring is met de Watervalmethode zal deze methodiek ook goed aansluiten bij dit project.

Uit de eerder genoemde kenmerken kunnen eisen worden gesteld, deze eisen zijn in de onderstaande tabel weergegeven. In deze tabel worden ook de verschillende methodieken met elkaar vergeleken om te kijken welke het beste past bij dit project

Nr.	Eis	Waterval	RUP	Scrum	Eigen methode
E1	Ervaring van de afstudeerder met deze methodiek.	+	~	~	+
E2	Biedt ruimte voor het uitvoeren van onderzoek	~	+	+	+
E3	Heeft ruimte voor documentatie	+	+	~	+
E4	Kan solo worden uitgevoerd.	+	~	~	+
E5	De systeemeisen staan vast	+	-	-	+

Tabel 1 Vergelijking methodieken

Legenda van Tabel 1	
+	De methodiek voldoet aan de eis
~	De methodiek voldoet deels aan de eis
-	De methodiek voldoet niet aan de eis.

Tabel 2 Legenda tabel 1

Door de kenmerken van de methodieken zal de keuze voor de methodiek van dit project gemaakt worden tussen de waterval aanpak of een eigen aanpak. Hierbij is gekozen voor een eigen methode. De eigen methode is gebaseerd op de waterval methode. Maar heeft biedt meer ruimte voor het onderzoek als dat de standaard Watervalmethode doet. Deze keuze is onder andere gemaakt omdat, de requirements vast staan. Dit houdt in dat er niet terug hoeft te worden gekeerd naar een vorige fase. Hiervoor zijn RUP en Scrum meer geschikt. Ook de ervaring met de methodiek heeft een grote impact gehad op de keuze van de methodiek.

3.1.2 Fasering

De eigen methode wordt doorlopen in fases. Bij deze methode horen de volgende fasen. Tijdens en aan het einde van deze fases worden verschillende producten opgeleverd. Deze op te leveren producten zijn tot stand gekomen in samenspraak met de afstudeerbegeleider.

Fase	Op te leveren product
Oriëntatiefase	Plan van Aanpak Onderzoeksplan
Onderzoeksfase	Literatuur onderzoeksrapport
Ontwerpfase	Ontwerprapport
Experimentele fase	Testdocument Migratieplan Experimenteel onderzoeksrapport
Adviseerfase	Adviesrapport
Afrondingsfase	Scriptie Afstudeerdossier

Oriëntatiefase
Tijdens deze fase zal het voorbereidend werk worden verricht. Zo zal er een plan van aanpak worden gemaakt. Door gebruik te maken van dit plan van aanpak kan er goed voorbereid aan het onderzoek begonnen worden. Ook zal er in deze fase een oriënterend onderzoek uitgevoerd worden naar STP, TRILL en de varianten van TRILL.

Verder zal er aan de hand van het oriënterend onderzoek een onderzoeksplan opgesteld worden welke als basis zal dienen voor de onderzoeksfase. In het onderzoeksplan zullen de hoofdvraag en de deelvragen gedefinieerd worden.

Onderzoeksfase
In de onderzoeksfase wordt er gezocht naar de beschikbare literatuur van Spanning Tree Protocol, TRILL en de varianten VCS en FabricPath. Hiernaast zal ook het gebruikte netwerk onderzocht worden en gekeken worden welke kennis hierbij nog extra nodig is om dit netwerk zo goed mogelijk te kunnen begrijpen.

Ontwerpfase
Tijdens de ontwerpfase wordt er nagedacht over hoe de testopstellingen opgebouwd gaan worden. Hierbij wordt nagedacht over welke apparatuur en welke configuratie er nodig is. Hierin wordt de netwerk topologie gebruikt worden die door Qi ict bv. wordt geleverd.

Experimentele fase
Bij de experimentele fase hoort het realiseren van de simulatie, dit houdt onder ander in dat de switches moeten worden geconfigureerd en de pc's naar de gewenste instellingen moeten worden gezet. Hierbij kan worden gedacht aan de protocollen die onderzocht gaan worden dat die op de juiste manier geconfigureerd worden en op de juiste apparatuur staan.

Als het ontwerp en de simulatie zijn gerealiseerd dan zal het migreren van de simulatie beginnen, hierin wordt de ontworpen simulatie gemigreerd naar een TRILL netwerk. Dit netwerk moet nog steeds voldoen aan de vooraf vastgestelde eisen. Deze migratie zal verlopen volgens een opgesteld migratieplan.

In deze testfase binnen de experimentele fase wordt er gebruik gemaakt van een testplan waar alle voorwaarden staan waaraan het netwerk moet voldoen. Ook staan hierin de tests die uitgevoerd gaan worden tijdens deze fase. Uit deze testen komen uiteindelijk resultaten en deze resultaten zullen worden verwerkt in het testrapport.

Adviseerfase
Tijdens de adviseerfase zal er voornamelijk bezig gehouden worden met het schrijven van het advies naar aanleiding van de gevonden resultaten die zijn verkregen uit de onderzoeksfase en de experimentele fase.

Afrondingsfase
In de afrondingsfase zal zich voornamelijk bezig worden gehouden met het aanpassen van het afstudeerverslag en het opbouwen van het afstudeerdossier. Deze fase zal de laatste ± drie weken van de afstudeerperiode overlappen.

3.1.3 Onderzoeksmethode

Naast de projectmethode moeten er ook onderzoeksmethoden worden vastgesteld, zodat bij het schrijven van het adviesrapport beter begrepen kan worden wat voor type onderzoeken er zijn verricht en wat hier de gevolgen voor zijn[4].

Literatuuronderzoek
Het schrijven van een onderzoek of advies begint vaak met een literatuuronderzoek. Literatuuronderzoek is een methode om bestaande kennis over een onderwerp of probleemstelling te verzamelen. Deze kennis kan gevonden worden in verschillende bronnen, zoals wetenschappelijke tijdschriftartikelen, boeken, papers, scripties en archiefmateriaal. Dit onderzoek wordt uitgevoerd tijdens de Onderzoeksfase. Dit wordt gedaan om ervoor te zorgen dat er geen onduidelijkheden zijn tijdens de experimentele fase. Ook wordt hier een verwachting gesteld over hoe de protocollen reageren op een bepaalde situatie.

Experimenteel onderzoek
Bij een experimenteel onderzoek wordt een bepaalde omstandigheid gemanipuleerd om hiervan het effect te zien. Hierbij gaat het om het bouwen van een bepaalde testopstelling met een gewenst resultaat. Dit onderzoek wordt uitgevoerd in de Experimentele fase. Het experimenteel onderzoek is vooral gebruikt voor het testen van de protocollen en het uitvoeren van de metingen.

Vergelijkend onderzoek
Het testen van de vooraf gestelde testopstellingen en de vooraf bepaalde protocollen zijn een voorbeeld van zowel een vergelijkend onderzoek als een experimenteel onderzoek. Bij een vergelijkend onderzoek wordt het effect van verschillende omstandigheden op bepaalde variabelen gemeten. Ook dit onderzoek wordt uitgevoerd in de Experimentele fase. Dit onderzoek is gedaan om te kunnen adviseren of het migreren naar het Proof of Concept naast mogelijk ook daadwerkelijk wenselijk is.

Toegepast onderzoek
De resultaten van bovenstaande onderzoeken leiden uiteindelijk tot conclusies en aanbevelingen die direct toepasbaar zijn voor in de praktijk. Deze onderzoekmethode wordt veelal gebruikt bij onderzoeken die worden gedaan bij het schrijven van een scriptie bij een bedrijf. Dit onderzoek zal gebruikt worden in de adviseerfase.

3.2 Standaarden

Binnen de opdracht worden er enkele standaarden gebruikt die dienen als hulpmiddel bij het bereiken van het beoogde resultaat. Dit zijn tools van externe partijen, waar de student mee dient te werken.

- Microsoft Visio: De netwerkontwerpen worden opgeleverd in Microsoft Visio, dit is een applicatie voor het maken van technische en logische schema's.
- Microsoft Office: Documenten worden geschreven in Microsoft Word, met extensie .docx alle andere tabellen en grafieken worden gemaakt met applicaties uit de Microsoft Office familie.
- Wireshark: hiermee wordt er gecontroleerd of de frames in het netwerk ook daadwerkelijk gebruik maken van het juiste protocol.
- PuTTY; De switches worden geconfigureerd met behulp van PuTTY, dit is een applicatie om switches via de COM-poort te configureren.

4. Planning

In dit hoofdstuk wordt de planning en de werkgelegenheden beschreven.

4.1 Fasering- en tijdsschema

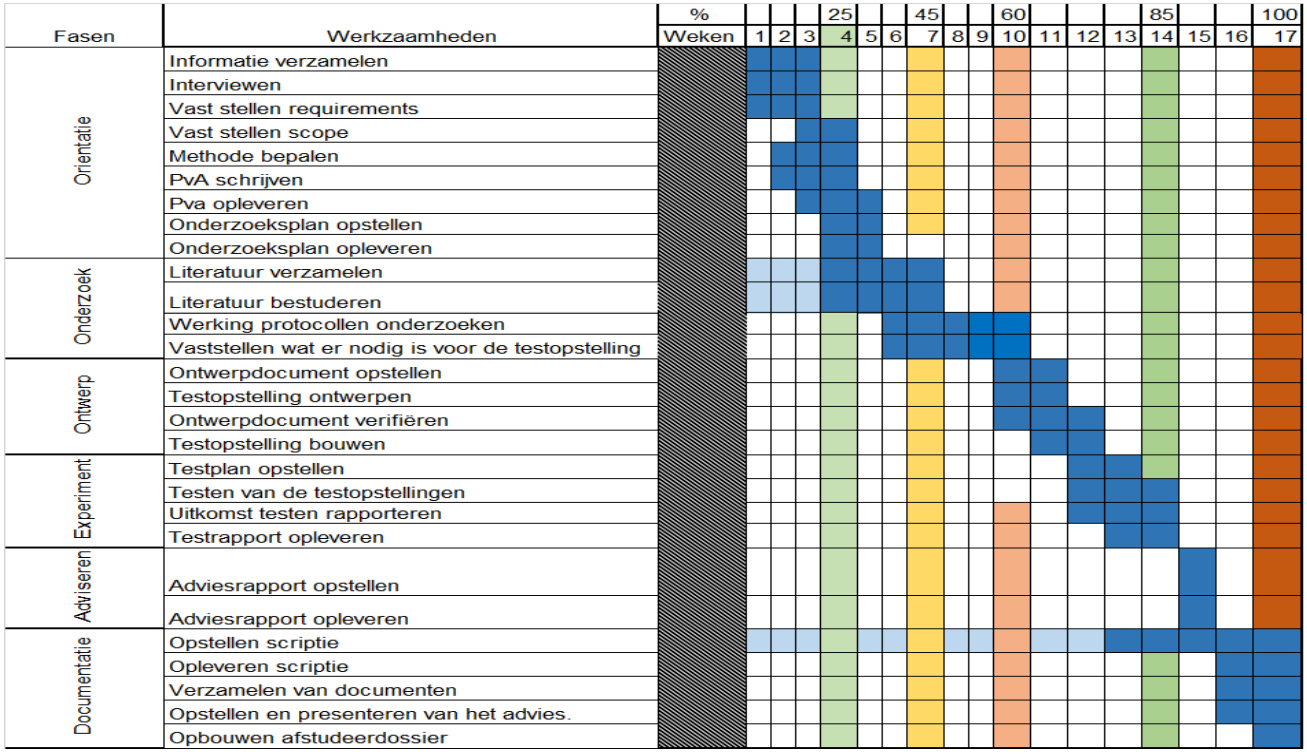
Onderstaande planning geeft een globale planning aan van welke werkzaamheden er per fase worden uitgevoerd en hoeveel dagen er voor elke fase worden ingepland.

Beide planningen zijn gebaseerd op een afstudeerperiode van 17 weken. Nu is er echter eerder begonnen met de opdracht, dit omdat hierdoor er meer speling is in de planning. Ook zal de afstudeerder hier meer ruimte hebben om kennis te maken met de werkomgeving waarin Qi ict bv. werkzaam is. Deze keuze is gemaakt in overleg met de begeleider vanuit de opleiding en met de begeleider van Qi ict bv.

Fase	Werkzaamheden	Ingeplande dagen
Oriëntatiefase	Plan van aanpak schrijven Gesprekken met de engineers die gebruik maken van de huidige redundantie protocollen. Vast stellen requirements + Onderzoeksplan opstellen	15 dagen
Onderzoeksfase	Onderzoeken naar STP en TRILL varianten	25 dagen
Ontwerpfase	Ontwerpen en bouwen van de simulaties	10 dagen
Experiment fase	Het testen van de simulaties.	15 dagen
Adviseerfase	Het schrijven van het adviesrapport.	5 dagen
Afrondingsfase	Opbouwen afstudeerdossier. Presenteren voorbereiden	15 dagen

Figuur 1 Fase planning

Figuur 2 geeft de planning per week aan wat er per week gedaan gaat worden aan welke werkzaamheden.



Figuur 2 Week planning

: Traject

: Uitvoeren

Op ongeveer 25% komt de begeleider van de Haagse Hogeschool langs bij Qi ict bv. Hierbij zal er een kort gesprek zijn tussen de begeleider van de Haagse Hogeschool, de begeleider van uit Qi ict bv. en de afstudeerder. Tijdens dit gesprek zal het voornamelijk gaan over wat de verwachting is vanuit de opleiding. Ook zullen hier een aantal data voor nieuwe afspraken besproken.

Op ongeveer 45% voortgang bespreken met de begeleider van de Haagse Hogeschool. Dit gesprek is optioneel en zal in overleg met de begeleider van uit de opleiding worden gepland of niet.

Op ongeveer 60% bespreken concept afstudeerdossier met de begeleider van de Haagse Hogeschool. De afstudeerder zal een afspraak plannen met de begeleider en tijdens deze afspraak zullen de gemaakt documentatie van de afstudeerder besproken worden. Hierbij kan al een eerste indicatie gegeven worden of de afstudeerder op de goede weg is.

Op ongeveer 85% (3 weken voor de inleverdatum) wordt er een Tussentijdse Assessment (TTA) ingepland met de examinatoren. Bij dit TTA zullen de verslagen van de afstudeerder nogmaals besproken worden en zal er een advies worden geven over het inleveren: Inleveren, Verlengen of Stoppen

4.2 Werkgelegenheid

Er wordt verondersteld dat de student zich minstens 40 uur per week inzet voor de opdracht. In principe zal de student van maandag tot en met vrijdag van 8:30 tot 17:00 bij het Qi ict aanwezig zijn, onder voorbehoud van afgesproken uitzonderingen. De student heeft een eigen werkplek, krijgt de werkapparatuur van Qi ict bv. (laptop, testapparatuur, etc.) en kan ook gebruik maken van het test lab. Naast de vaste werktijden kan de afstudeerder ook in zijn eigen tijd aan de opdracht werken, maar dit zal per week kunnen verschillen.

Ondanks dat de afstudeer periodes door de zomervakantie vallen, heeft de student geen recht op vier weken (school)vakantie, wel heeft is er het recht op een aantal vakantiedagen hoe deze dagen worden ingedeeld is aan de student om dit zelf te plannen. Dit wordt in overleg gedaan met de opdrachtgever en door middel van een verzoek voor verlof.

5. Risicoanalyse

Voor het uitvoeren van de opdracht is het van belang om te weten waar de mogelijke risico's liggen, zodat deze vermeden kunnen worden of kunnen worden opgelost als ze zich toch voordoen. Onderstaande tabel toont de erkende risico's, met bijbehorende maatregelen.

Risico's	Impact			Kans			Kans vermindering	Maatregel
	1	2	3	1	2	3		
Te kort aan tijd							De planning dusdanig maken dat er eventuele uitloop ingecalculeerd wordt.	Uitstel vragen aan de opdrachtgever en/of overwerken in eigen tijd.
Geen beschikbare hardware voor het bouwen van de testopstellingen							Op tijd met de begeleider bespreken over de benodigde apparatuur; Tijdig reserveren van apparatuur.	Test opstelling via remote lab van Brocade of Cisco realiseren
Langdurig afwezigheid van de begeleider (langer dan 1 week)							Contact houden via mail. Afspraken maken met bedrijf voor vervanging	Bedrijf inlichten, en vervanger inlichten van voortgang en huidige situatie.
Langdurig afwezigheid van de afstudeerder (langer dan 1 week)							Contact houden via mail. Afspraken maken met bedrijf voor oplossingen	Uitstel vragen aan de opdrachtgever en/of overwerken in eigen tijd.

De impact en kans worden bepaald aan de hand van de gevolgen die hangen aan het risico.

Bij het risico: "Te kort aan tijd", is dit de verantwoordelijkheid van de afstudeerder zelf om dit op tijd te concluderen. Als de tijdsnood hoog is kan dit ervoor zorgen dat er geen compleet product opgeleverd kan worden. Deze conclusie is de impact. De kans dat dit gebeurt is echter middel; doordat er vooraf een planning wordt gemaakt. Ook wordt tussentijds gecontroleerd of het project nog op schema ligt. Mocht er toch nog tijdsnood zijn, dan is de maatregel dat er in de eigen tijd nog gewerkt kan worden aan het project.

Bij het risico: "Geen beschikbare hardware voor het bouwen van testopstellingen", ligt de verantwoordelijkheid om dit op tijd op te lossen bij de afstudeerder zelf. Als hij de apparatuur niet op tijd aanvraagt kan hij niet verder in de testfase. Deze conclusie is de impact van het risico. De kans is gebaseerd op de beschikbaarheid van de apparatuur. Nu is het zo dat Qi ict bv. beschikt over een eigen spare voorraad. Deze spare voorraad wordt bijgehouden van wat er aanwezig is. Nu zal er gekeken worden hoe deze kans verminderd kan worden of als deze kans niet te verminderen is wat een maatregel zou zijn.

Bij het risico's: "Langdurige afwezigheid begeleider/afstudeerder", geldt voor beide dat de impact groot zal zijn. Als de afstudeerder lang afwezig is kan hij niet verder met de experimentele fase aangezien hij niet op kantoor kan zijn. Bij afwezigheid begeleider kunnen de verslagen hooguit over de mail besproken worden. Echter is de kans op beide klein. Dit zal echter voorkomen met vakantie of ziekte; maar zal naar alle waarschijnlijkheid niet langer als 2 à 3 weken zijn. Hier kan omheen

gepland worden wanneer er wel afgesproken wordt. In het geval van de afwezigheid van de begeleider zal er in overleg met het bedrijf gekeken worden of er een vervanger kan worden aangewezen. Deze zal dan worden ingelicht over de gang van zaken. Bij langdurige afwezigheid van de afstudeerder zal er in de eigen tijd gewerkt moeten worden om de verloren tijd in te halen.

6. Kosten en baten

De opdracht wordt gedaan door de afstudeerder, die onder begeleiding van een network engineer vanuit het bedrijf staat. De engineer en tevens de begeleider zal de opdracht in de gaten houden en zal de afstudeerder begeleiden waar nodig. De uren die de student maakt worden uitbetaald naar contract.

Voor de realisatie van de opdracht is er verschillende apparatuur nodig. Door de student zal de juiste apparatuur geanalyseerd worden, gekozen en wordt dan in overleg met de opdrachtgever gebruikt.

Betrokken personen	Wekelijkse uren	Eenmalige uren	Totale uren
Afstudeerder	20 weken x 40 uren		800 uren
Opdrachtgever	10 weken x 1 uur	1 uur presentatie 2 uren eventuele extra bijeenkomst	13 uren
Referentiegroep		10 engineers x 1 uur presentatie/demonstratie	10 uren
Totaal	810 uren	13 uren	823 uren

Kosten

- De opdracht kost voornamelijk mensuren, hieronder een schema met de geschatte uren.
- Aanschaf en/of huurkosten van TRILL apparatuur, overige apparatuur is aanwezig en breng geen extra kosten met zich mee.

Baten

- Kennis verkrijgen over TRILL, FabricPath en VCS
- Kennis verkrijgen over de mogelijkheden van TRILL, FabricPath en VCS
- Kennis betreft de migratiemogelijkheden van TRILL, FabricPath en VCS
- Door de verkregen kennis kan het migreren naar een TRILL omgeving later als dienst worden aangeboden.

Literatuurlijst

[1] Istqbexamcertification. (jaar onbekend). "*What is Waterfall model- advantages, disadvantages and when to use it?"* http://istqbexamcertification.com/what-is-waterfall-model-advantages-disadvantages-and-when-to-use-it/ (geraadpleegd op 29 april 2016).

[2] Kruchten, P.(2009) T*he Rational Unified Process An Introduction*, Pearson Education. (geraadpleegd op 29 april 2016).

[3] Scrum.nl. (jaar onbekend) *"Wat is scrum":* http://www.scrum.nl/site/Wat-is-Scrum-agile-scrum (geraadpleegd op 29 april 2016).

[4] Scribbr.nl (jaar onbekend) *"Overzicht van onderzoek soorten"* https://www.scribbr.nl/category/onderzoeksmethoden/ (geraadpleegd 30 april 2016)

Bijlage C

Onderzoeksplan

Onderzoeksplan

Opdrachtgever: Qi ict bv.
Begeleider: Hans Suttorp
Afstudeerder: Frank van Eijk
Opleiding: Technische Informatica, HHS Delft
Datum: 03-10-2016
Versie: 1.0

Versiebeheer

Versie	Datum	Opmerking
0.1	13-5-2016	Eerste versie
0.2	23-5-2016	Aanpassingen doorgevoerd na feedback van dhr. Hans Suttorp
0.3	17-6-2016	Aanpassingen doorgevoerd na feedback van dhr. Hans Suttorp
1.0	30-9-2016	Opmaak consistent gemaakt

Inhoudsopgave

1. Inleiding

Het onderzoek is opgedeeld worden in twee aparte onderzoeken, een literatuuronderzoek en een experimenteel onderzoek. Uit beide onderzoeken komt een resultaat en aan de hand van deze resultaten zal een advies gegeven worden of het uit faseren van STP in switched-core netwerken gewenst is.

In dit onderzoeksplan zal de aanleiding van dit onderzoek naar voren komen, hiernaast zal er ook verteld worden wat op dit moment het kennisgebied is op het onderwerp van de opdracht. Hierop volgt de probleemstelling die is opgedeeld in de hoofd- en deelvragen. Uiteindelijk zal hier een resultaat uit moeten komen en zal als laatste nog een globale planning worden vastgelegd over hoe de onderzoeksfasen volbracht zullen worden.

2. Aanleiding onderzoek

Qi ict bv. gebruikt op dit moment het spanning tree protocol(STP) voor het gebruik van redundantie in hun switched netwerken, deze keuze is gemaakt toen STP de meest voordehand liggende keuze was, maar is dit tegenwoordig nog steeds de meest logische keuze? De hoofdreden voor dit onderzoek is dat Qi over weinig kennis beschikt wat betreft de mogelijkheden van alternatieven zoals TRILL.

Het onderzoek is in twee delen op te delen; een literatuuronderzoek en een experimenteel onderzoek.

De reden dat er een literatuuronderzoek wordt gedaan is: er moet kennis worden opgedaan over de protocollen die voor het experimentele onderzoek nodig zijn. Het literatuuronderzoek wordt uitgevoerd omdat het van essentieel belang is dat de protocollen al enigszins bekend zijn als zij geconfigureerd moeten worden.

De reden van het experimentele onderzoek is het bevestigen of ontkrachten van de theorieën die uit het literatuuronderzoek voortkomen. Ook wordt er geëxperimenteerd of het mogelijk is om STP uit een switched-core netwerk te migreren. Hieruit zullen een aantal stappen volgen die tot het uiteindelijke resultaat zullen leiden.

De resultaten van beide onderzoeken zullen ervoor zorgen dat de hoofdvraag beantwoordt kan worden en dat er een advies kan worden gegeven aan de hand van dit resultaat.

3. Kennisgebied

Het kennisgebied dat betrekking heeft tot het literatuuronderzoek zijn Spanning Tree Protocol (STP), Transparent Interconnection of Lots of Links (TRILL) en de varianten van TRILL; Virtual Cluster Switching (VCS) van Brocade en FabricPath van Cisco. Hiernaast worden ook netwerken aangeleverd door Qi ict bv. waarnaar enig onderzoek gedaan moet worden wat de verwachtingen zijn van het netwerk.

Uit de eerste oriëntatie onderzoeken blijkt dat TRILL een vervangend protocol is voor STP. Hierbij is TRILL voornamelijk bedacht om de nadelen van STP op te lossen, zo gebruikt TRILL routering in Layer 2 met behulp van Intermediate System-to-Intermadiate System (IS-IS) routing protocol waar STP poorten zal blokken om loops te voorkomen.[4]

Dit houdt mede in dat niet alle verbindingen optimaal gebruikt worden en dat deze manier van redundantie niet efficiënt is. Verder bleek ook dat TRILL gebruik maakt van MAC adressen om te routeren. Ook hebben de meeste switch fabrikanten hun eigen TRILL variant zoals VCS van Brocade[1], FabricPath van Cisco[2] en SPB van Alcatel[3].

Bij de netwerken zal het voornaamste kennisgebied zijn dat de werking van de apparatuur duidelijk is en wat deze doet tijdens het werken met STP, TRILL, VCS of FabricPath. Ook zit hierin het deel configuratie dat bij elke switch anders zal zijn.

Bij het experimenteel onderzoek wordt er gebruik gemaakt van de kennis die is opgedaan tijdens het literatuuronderzoek. Zodat er bij het uitvoeren van de experimenten een verwachtingspatroon zal zijn. Als deze verwachting niet klopt, kan het zijn dat de literatuur niet juist is of dat er instellingen niet juist zijn ingesteld.

4. Probleemstelling

Doordat er nog geen uitgebreid onderzoek is gedaan, kan Qi niet zeggen of zij op de meest efficiënte manier redundantie uitvoeren. Daarmee komt dus de opdracht tot stand. Onderzoek verschillende protocollen om redundantie uit te voeren in een switched core netwerk en adviseer of het mogelijk is om STP uit dit switched core netwerk te faseren. Hierbij kunnen de volgende vragen worden gesteld.

4.1 Hoofdvraag

“Onder welke voorwaarden Is het met TRILL mogelijk om STP uit een door Qi ict bv. gebruikt switched-core netwerk te faseren?”

4.2 Deelvragen

In deze paragraaf zullen de deelvragen en de eventuele sub-vragen ervan beschreven worden. Hierbij worden de vragen voor het literatuuronderzoek en het experimentele onderzoek gescheiden.

Literatuur onderzoek

Deelvraag 1: “Wat is STP?”

Reden: Voordat gezegd kan worden of STP uit de huidige switched core netwerken gefaseerd wordt, moet er wel duidelijk zijn wat STP precies inhoudt. Denk hierbij aan waarom is STP ooit ontworpen en waarom is er op dit moment zoveel vraag naar alternatieven.

> **Sub-vraag1.1: “Hoe werkt STP in een switched core netwerk?”**
> *Reden:* De grootste vraag bij STP is “wat doet STP?” Bij deze vraag wordt onderzocht wat STP aan een netwerk toevoegt, maar ook wat er gebeurt als STP uitgeschakeld staat en er geen alternatief op het netwerk actief is.
>
> **Sub-vraag1.2: “Wat zijn nadelen van het Spanning Tree Protocol”**
> *Reden:* Om de kwestie omtrent de vraag naar alternatieven van STP, moet er wel duidelijk zijn waarom deze vraag er is. Dit zal voornamelijk te maken hebben met het feit dat STP bepaalde keuzes maakt waarbij een aantal nadelen aan deze keuzes hangen.

Deelvraag 2: “Wat is TRILL?“

Reden: Bij deze deelvraag geldt hetzelfde als bij de deelvraag “Wat is STP?”. Voordat er een conclusie kan worden getrokken uit de hoofdvraag moet niet alleen het oude protocol (STP) bekend zijn, maar ook de eventuele vervanger (TRILL).

> **Sub-vraag2.1: “Hoe werkt TRILL in een switched core netwerk?”**
> *Reden:* Net als STP, is het logisch dat duidelijk moet zijn hoe TRILL werkt in een switched core netwerk.
>
> **Sub-vraag 2.2: “Welke varianten van TRILL zijn er?”**
> *Reden:* Uit het onderzoek blijkt dat TRILL een open standaard is en door verschillende bedrijven gebruikt is om hun eigen versie van TRILL te creëren. Hierbij wordt gekeken welke varianten eventueel relevant zijn voor Qi ict bv.
>
> **Sub-vraag 2.3: “Wat zijn de verschillen tussen de varianten en TRILL?”**
> *Reden:* Om een duidelijk overzicht te krijgen wat er precies verschilt tussen de varianten van TRILL en TRILL zelf. Hierbij kan gedacht worden aan de werking en toepassing van de protocollen.

Sub-vraag 2.4: “Welke randvoorwaarden zijn er om TRILL te implementeren?”
Reden: Bij de deelvraag kan de vraag worden gesteld, aan welke randvoorwaarden moet er worden voldaan om TRILL of een variant te implementeren. Hierbij kan gedacht worden aan apparatuur en welke configuratie.

Sub-vraag 2.5: “Waar kunnen TRILL en de varianten het beste worden toegepast in een netwerk?”
Reden: Deze deelvraag is ontstaan uit het deel van de hoofdvraag of TRILL STP uit de huidig gebruikte switched core netwerken faseert. Hierbij wordt gekeken waar TRILL het best in een netwerk kan worden geïmplementeerd.

Deelvraag 3: “Wat zijn de verschillen tussen STP en TRILL?”
Reden: Nu alle protocollen (die behandeld worden) duidelijk zijn, kan de vergelijking opgemaakt worden. Hierbij worden een aantal kenmerken van de protocollen naast elkaar gezet Hierbij kan gedacht worden aan de manier van loops voorkomen en de schaalbaarheid van de netwerken waar de protocollen worden toegepast. Met deze deelvraag kan al een groot deel van de hoofdvraag beantwoordt worden.

Deelvraag 4: “Kan TRILL in de reeds bestaande infrastructuren worden geïmplementeerd?”
Reden: Als laatste wordt er onderzocht of TRILL direct zonder aanpassingen aan de huidige netwerken kan worden toegevoegd. Denk hierbij dat alleen de configuratie aangepast hoeft te worden. Geen verandering van de infrastructuur of apparatuur.

Sub-vraag 4.1: “Hoe ziet deze infrastructuur eruit?”
Reden: Om deze deelvraag te beantwoorden moet wel eerst duidelijk worden om wat voor soort infrastructuur het hier gaat. Hoe ziet de infrastructuur eruit en welke apparatuur wordt er gebruikt; “Is deze apparatuur wel TRILL compatible?”

Sub-vraag4.2: “Wat zijn de huidig gebruikte protocollen?”
Reden: Naast de vraag hoe de infrastructuur eruit ziet, moet er ook duidelijk worden hoe de infrastructuur werkt. Met welke protocollen wordt het huidige netwerk draaiend gehouden.

Sub-vraag 4.3: “Is er compatibiliteit mogelijk met de huidig gebruikte protocollen?”
Reden: Ook moet duidelijk zijn of TRILL of de varianten compatible zijn met de huidig gebruikte protocollen. Met andere woorden, is het bijvoorbeeld mogelijk om een TRILL-core te hebben met een STP-access? Of moet de hele infrastructuur aangepast worden?

Experimenteel onderzoek

Deelvraag 5: "Hoe werkt de huidige situatie?"

Reden: Voordat STP uit het huidige netwerk kan worden gefaseerd, moet eerst duidelijk zijn wat de functionaliteiten zijn van de huidige situatie. Zonder beginsituatie is het ook niet mogelijk om de vergelijking met de nieuwe situatie aan het eind van het onderzoek uit te voeren.

Sub-vraag 5.1: "Werken de gebruikte protocollen zoals uit de literatuur naar voren kwam?"

Reden: Hierbij wordt de gevonden literatuur vergeleken met de werkelijkheid op het netwerk. Hierbij kan de literatuur bevestigd worden of ontkracht. Hierbij kan het geval zijn dat de literatuur een andere werking van een protocol weergeeft dan wat het protocol op het netwerk daadwerkelijk doet. De nadruk ligt hierbij op RSTP.

Sub-vraag 5.2: "Wat zijn de waardes van het huidige netwerk?"

Reden: Hierbij wordt een Nulmeting uitgevoerd. Bij een nulmeting worden verschillende waardes van het huidige netwerk achterhaald, om aan het eind van het onderzoek de waardes van de nieuwe en oude situatie met elkaar te kunnen vergelijken. Voorbeelden van deze waardes zijn: Latency, Reliability en Down time.

Deelvraag 6: "Hoe werkt de nieuwe situatie?"

Reden: Voordat er gemigreerd kan worden naar de nieuwe situatie, moet de nieuwe situatie wel bekend zijn. Op deze manier kan ook de werking van de protocollen op de nieuwe situatie worden getest.

Sub-vraag 6.1: "Werken de gebruikte protocollen zoals uit de literatuur naar voren kwam?"

Reden: Hierbij wordt de gevonden literatuur vergeleken met de werkelijkheid op het netwerk. Hierbij kan de literatuur bevestigd worden of ontkracht. In de nieuwe situatie gaat het vooral om de werking van SPB. De andere protocollen zijn al getest.

Sub-vraag 6.2: "Wat zijn de waardes van het nieuwe netwerk?"

Reden: Hierbij worden verschillende waardes van het nieuwe netwerk achterhaald, om aan het eind van het onderzoek de waardes van de beide situaties met elkaar te kunnen vergelijken. Voorbeelden van deze waardes zijn: Latency, Reliability en Down time.

Deelvraag 7: "Werkt de nieuwe situatie beter als de oude?"
Reden: Om een advies te kunnen geven of het wenselijk is om STP uit de huidige netwerk te faseren, moet wel duidelijk zijn of deze situatie beter werkt.

> **Sub-vraag 7.1: "In welk opzicht verschilt de nieuwe situatie met de oude situatie?"**
> *Reden:* Hierbij wordt er gekeken welke verschillen er zijn bij de metingen die bij de oude situatie en bij de nieuwe situatie zijn uitgevoerd. Uit deze metingen zullen verschillen komen, echter is het zo dat sommige waardes ook nog hetzelfde kunnen zijn. De gebieden waarnaar gekeken wordt zijn: Scalability, Availability, Manageability, Maintainability en Performance.

Deelvraag 8: "Hoe wordt de oude situatie naar de nieuwe situatie gemigreerd?"
Reden: Om van de oude situatie naar de nieuwe situatie te migreren moeten er een aantal handelingen worden uitgevoerd. Het is noodzakelijk om te weten hoe de migratie gedaan moet worden. Deze stappen zorgen ervoor dat de migratie op een efficiënte manier kan worden uitgevoerd.

> **Sub-vraag 8.1: "Welke stappen moeten hiervoor worden genomen?"**
> *Reden:* Hierbij zijn de stappen van groot belang, als er niet stapsgewijs gewerkt wordt kan het zijn dat er geen overzicht meer is in de migratie. Hierbij is het mogelijk dat er dan iets ontbreekt of niet op de juiste instellingen staat.

> **Sub-vraag 8.2: "Welke voorwaarden zitten er aan de migratie stappen?"**
> *Reden:* Hierbij kan gedacht worden aan de downtijd die het netwerk maximaal mag hebben. Ook moeten de risico's worden gedefinieerd die aanwezig kunnen zijn tijdens het migreren van het netwerk.

5. Resultaat

De resultaten van beide onderzoeken worden verwerkt in een aparte onderzoeksrapporten en uit de resultaten van deze rapporten zal een adviesrapport worden geschreven. In de resultaten worden de bevindingen van bovenstaande deelvragen gegeven en zal uiteindelijk een advies gegeven kunnen worden op de hoofdvraag en waarom dit wel of niet het geval is.

Naast het opleveren van het rapport zullen de resultaten worden gepresenteerd aan de begeleider en enkele andere (technische) collega's binnen Qi ict bv. De resultaten zullen een bijdrage leveren aan de adviezen die Qi ict bv. haar klanten geeft omtrent de keuze voor redundantie oplossingen en de engineers helpen om deze oplossing goed te kunnen implementeren.

6. Planning

De planningen geven aan hoe de onderzoeksfasen zullen worden ingedeeld. De planning geeft aan de besteden tijd aan in het aantal dagen dat er aan elke deel- of sub-vraag nodig is. De planningen zijn ook opgedeeld in het literatuuronderzoek en in het experimentele onderzoek. Deze planningen zijn op de volgende pagina te vinden. Hierbij is rekening gehouden met de Ontwerpfase die tussen deze beide onderzoeken plaatsvind en ook de vakantie van de afstudeerder is meegenomen in de data.

Naam	Vraag	Duur	Startdatum	9-5-2016			16-5-2016			23-5-2016			30-5-2016			6-6-2016		
				maan	woe	vrij	maan	woe	vrij	maan	woe	vrij	maan	woe	vrij	maan	woe	vrij
Onderzoeksfase		25 dagen	9-5-2016															
Deelvraag 1	Wat is STP?	5 dagen	9-5-2016															
Sub-vraag 1.1	Hoe werkt STP in een switched core netwerk?	3 dagen	9-5-2016															
Sub-vraag 1.2	Wat zijn nadelen aan STP?	2 dagen	12-5-2016															
Deelvraag 2	Wat is TRILL?	10 dagen	16-5-2016															
Sub-vraag 2.1	Hoe werkt TRILL in een switched core netwerk?	3 dagen	16-5-2016															
Sub-vraag 2.2	Welke varianten van TRILL zijn er?	2 dagen	19-5-2016															
Sub-vraag 2.3	Wat zijn de verschillen tussen TRILL en de varianten?	3 dagen	23-5-2016															
Sub-vraag 2.4	Welke randvoorwaarden zijn er om TRILL of de varianten te implementeren?	2 dagen	26-5-2016															
Sub-vraag 2.5	Waar kan TRILL het beste worden toegepast in het netwerk?	2 dagen	30-5-2016															
Deelvraag 3	Wat zijn de verschillen tussen STP en TRILL?	3 dagen	1-6-2016															
Deelvraag 4	Kan TRILL in de bestaande infrastructuur worden geimplementeerd?	5 dagen	6-6-2016															
Sub-vraag 4.1	Hoe ziet deze infrastructuur eruit?	2 dagen	6-6-2016															
Sub-vraag 4.2	Wat zijn de huidig gebruikte protocollen?	2 dagen	8-6-2016															
Sub-vraag 4.3	Is er compatibiliteit mogelijk met de huidig gebruikte protocollen?	1 dag	10-6-2016															

Naam	Vraag	Duur	Startdatum	4-7-2016			11-7-2016			18-7-2016			25-7-2016			8-8-2016			15-8-2016		
				maan	woe	vrij	maan	woe	vrij	maan	woe	vrij	maan	woe	vrij	maan	woe	vrij	maan	woe	vrij
Experimentsfase		30 dagen	4-7-2016																		
Deelvraag 5	Hoe werkt de huidige situatie?	10 dagen	4-7-2016																		
Sub-vraag 5.1	Werken de gebruikte protocollen zoals in de literatuur naar voren kwam?	5 dagen	4-7-2016																		
Sub-vraag 5.2	Wat zijn de waardes in het huidige netwerk?	5 dagen	11-7-2016																		
Deelvraag 6	Hoe werkt de nieuwe situatie?	10 dagen	18-7-2016																		
Sub-vraag 6.1	Werken de gebruikte protocollen zoals in de literatuur naar voren kwam?	5 dagen	18-7-2016																		
Sub-vraag 6.2	Wat zijn de waardes in het nieuwe netwerk?	5 dagen	25-7-2016																		
Deelvraag 7	Werkt de nieuwe situatie beter als de oude?	3 dagen	8-8-2016																		
Sub-vraag 7.1	In welk opzicht verschilt de oude situatie met de nieuwe situatie?	3 dagen	8-8-2016																		
Deelvraag 8	?Hoe wordt de oude situatie naar de nieuwe situatie gemigreerd	7 dagen	11-8-2016																		
Sub-vraag 8.1	Welke stappen moeten hiervoor worden genomen?	4 dagen	11-8-2016																		
Sub-vraag 8.2	Welke voorwaarden zitten er aan de migratie stappen?	3 dagen	17-8-2016																		

Literatuurlijst

[1] Brocade Communications Systems. (2012). *Brocade VCS Fabric Technical Architecture*. Retrieved april 20, 2016, from Brocade.com: http://www.brocade.com/en/backend-content/pdf-page.html?/content/dam/common/documents/content-types/architecture-guide/vcs-technical-architecture-tb.pdf

[2] Cisco Systems. (2012). *Cisco FabricPath*. Retrieved april 20, 2016, from Cisco.com: http://www.cisco.com/c/dam/en/us/products/collateral/switches/nexus-7000-series-switches/at_a_glance_c45-605626.pdf

[3] Fedyk, D. (2012, Oktober). *Introduction to Shortest Path Bridging.* Retrieved from www.netnod.se: https://www.netnod.se/sites/default/files/SPB-fedyk-091012.pdf

[4] Rouse, M. (2011, Juni). *Transparent Interconnection of Lots of Links (TRILL)*. Retrieved april 20, 2016, from TechTarget: http://searchnetworking.techtarget.com/definition/Transparent-Interconnection-of-Lots-of-Links-TRILL

Bijlage D

Literatuur Onderzoeksrapport

Literatuur onderzoeksrapport

Opdrachtgever: Qi ict bv.
Begeleider: Hans Suttorp
Afstudeerder: Frank van Eijk
Opleiding: Technische Informatica, HHS Delft
Datum: 03-10-2016
Versie: 1.0

Versiebeheer

Versie	Datum	Opmerking
0.1	17-6-2016	Eerste versie
0.2	05-7-2016	Aanpassingen doorgevoerd na feedback van dhr. Hans Suttorp
1.0	30-9-2016	Opmaak consistent gemaakt

Inhoudsopgave

Tabellen

Figuren

1. Inleiding

Het onderzoek is opgedeeld in twee aparte onderzoeken, een literatuuronderzoek en een experimenteel onderzoek. Uit beide onderzoeken komt een resultaat en aan de hand van deze resultaten zal een advies gegeven worden of het uit faseren van STP in switched-core netwerken gewenst is.

Om de hoofdvraag te kunnen beantwoorden, zijn er meerdere deelvragen opgesteld. In dit rapport zullen alleen de deelvragen die aan het literatuuronderzoek zijn gesteld behandeld worden. Voor de beantwoording van de experimentele deelvragen, wordt verwezen naar het Experimentele onderzoeksrapport.

In het volgende hoofdstuk zal de aanleiding tot het literatuuronderzoek worden behandeld. Daarna zal het kennisgebied van de afstudeerder worden aangegeven. Als dit is uitgelegd volgt de probleemstelling waarin de deelvragen en eventuele sub-vragen worden uitgelegd en waarom deze vragen relevant zijn voor het onderzoek. Nadat de vragen duidelijk zijn zullen deze in de daarop volgende hoofdstukken behandeld worden. Uiteindelijk zal er een conclusie uit het literatuuronderzoek volgen.

2. Aanleiding literatuuronderzoek

De reden dat er een literatuuronderzoek wordt gedaan is, er moet kennis worden opgedaan over de protocollen die voor het experiment nodig zijn. Het literatuuronderzoek wordt uitgevoerd omdat het van essentieel belang is dat de protocollen al enigszins bekend zijn als zij geconfigureerd moeten worden. Dit zorgt er mede voor dat de simulatie op een efficiënte manier zal worden gebouwd. Ook zal door deze kennis van de protocollen een verwachtingspatroon zijn bij uitvoering van bepaalde handelingen. Op deze manier is er een verwachting bij elke configuratie en zal een afwijking direct opvallen.

3. Kennisgebied

Het kennisgebied dat betrekking heeft tot het literatuuronderzoek zijn het Spanning Tree Protocol (STP), Transparent Interconnection of Lots of Links (TRILL) en de varianten van TRILL. De varianten zijn: Virtual Cluster Switching (VCS) van Brocade, FabricPath van Cisco en Shortest Path Bridging (SPB) van Alcatel. Hiernaast wordt er ook een switched-core netwerk aangeleverd door Qi ict bv. waarnaar enig onderzoek gedaan moet worden over wat de werking is van de protocollen die naast deze redundantie protocollen aanwezig zijn op het netwerk.

Uit de eerste oriëntatie onderzoeken blijkt dat TRILL een vervangend protocol is voor STP. Hierbij is TRILL voornamelijk bedacht om de nadelen van STP op te lossen, zo gebruikt TRILL routering in Layer 2 met behulp van Intermediate System-to-Intermadiate System (IS-IS) routing protocol waar STP poorten zal blokken om loops te voorkomen

Dit houdt mede in dat niet alle verbindingen optimaal gebruikt worden en dat deze manier van redundantie niet efficiënt is. Verder bleek ook dat TRILL gebruik maakt van MAC adressen om te routeren. Ook hebben de meeste switch fabrikanten hun eigen TRILL variant zoals VCS van Brocade, FabricPath van Cisco en SPB van Alcatel.

Bij de netwerken zal het voornaamste kennisgebied zijn dat de werking van de apparatuur duidelijk is en wat deze doet tijdens het werken met STP, TRILL, VCS, FabricPath of SPB. Ook zit hierin het deel configuratie dat bij elk merk switch anders zal zijn.

4. Probleemstelling

In dit hoofdstuk zal de hoofdvraag en de deelvragen worden beschreven, deze vragen zullen in de loop van de literatuur onderzoeksfase onderzocht en beantwoordt worden.

4.1 Hoofdvraag

“Is het met TRILL mogelijk om STP uit een door Qi ict bv. gebruikt switched-core netwerk te faseren?”

4.2 Deelvragen

In deze paragraaf zullen de deelvragen en de eventuele sub-vragen die tijdens het literatuuronderzoek beantwoordt worden beschreven.

Deelvraag 1: “Wat is STP?”
Reden: Voordat gezegd kan worden of STP uit de huidige switched core netwerken gefaseerd wordt, moet er wel duidelijk zijn wat STP precies inhoudt. Denk hierbij aan waarom is STP ooit ontworpen en waarom is er op dit moment zoveel vraag naar alternatieven.

> **Sub-vraag1.1: “Hoe werkt STP in een switched core netwerk?”**
> *Reden:* De grootste vraag bij STP is “wat doet STP?” Bij deze vraag wordt onderzocht wat STP aan een netwerk toevoegt, maar ook wat er gebeurt als STP uitgeschakeld staat en er geen alternatief op het netwerk actief is.
>
> **Sub-vraag1.2: “Wat zijn nadelen van het Spanning Tree Protocol”**
> *Reden:* Om de kwestie omtrent de vraag naar alternatieven van STP, moet er wel duidelijk zijn waarom deze vraag er is. Dit zal voornamelijk te maken hebben met het feit dat STP bepaalde keuzes maakt waarbij een aantal nadelen aan deze keuzes hangen.

Deelvraag 2: “Wat is TRILL?“
Reden: Bij deze deelvraag geldt hetzelfde als bij de deelvraag “Wat is STP?”. Voordat er een conclusie kan worden getrokken uit de hoofdvraag moet niet alleen het oude protocol (STP) bekend zijn, maar ook de eventuele vervanger (TRILL).

> **Sub-vraag2.1: “Hoe werkt TRILL in een switched core netwerk?”**
> *Reden:* Net als STP, is het logisch dat duidelijk moet zijn hoe TRILL werkt in een switched core netwerk. Als dit duidelijk is kan er een vergelijking worden gemaakt over welk protocol in welke situatie het beste is. Dit is deelvraag 4.
>
> **Sub-vraag 2.2: “Welke varianten van TRILL zijn er?”**
> *Reden:* Uit het onderzoek blijkt dat TRILL een open standaard is en door verschillende bedrijven gebruikt is om hun eigen versie van TRILL te creëren. Hierbij wordt gekeken welke varianten eventueel relevant zijn voor Qi ict bv.
>
> **Sub-vraag 2.3: “Wat zijn de verschillen tussen de varianten en TRILL?”**
> *Reden:* Om een duidelijk overzicht te krijgen wat er precies verschilt tussen de varianten van TRILL en TRILL zelf. Hierbij kan gedacht worden aan de werking en toepassing van de protocollen.

Sub-vraag 2.4: “Welke randvoorwaarden zijn er om TRILL te implementeren?”
Reden: Bij de deelvraag kan de vraag worden gesteld, aan welke randvoorwaarden moet er worden voldaan om TRILL of een variant te implementeren. Hierbij kan gedacht worden aan apparatuur en welke configuratie.

Sub-vraag 2.5: “Waar kunnen TRILL en de varianten het beste worden toegepast in een netwerk?”
Reden: Deze deelvraag is ontstaan uit het deel van de hoofdvraag of TRILL STP uit de huidig gebruikte switched core netwerken faseert. Hierbij wordt gekeken waar TRILL het best in een netwerk kan worden geïmplementeerd.

Deelvraag 3: “Wat zijn de verschillen tussen STP en TRILL?”
Reden: Nu alle protocollen (die behandeld worden) duidelijk zijn, kan de vergelijking opgemaakt worden. Hierbij worden een aantal kenmerken van de protocollen naast elkaar gezet om te kijken hoe elk protocol in een situatie reageert. Hierbij kan gedacht worden aan de werking en toepassing van de protocollen. Met deze vraag kan al een groot deel van de hoofdvraag beantwoordt worden.

Deelvraag 4: “Kan TRILL in de reeds bestaande infrastructuren worden geïmplementeerd?”
Reden: Als laatste wordt er onderzocht of TRILL direct zonder aanpassingen aan de huidige netwerken kan worden toegevoegd. Denk hierbij dat alleen de configuratie aangepast hoeft te worden. Geen verandering van de infrastructuur of apparatuur.

Sub-vraag 4.1: “Hoe ziet deze infrastructuur eruit?”
Reden: Om deze deelvraag te beantwoorden moet wel eerst duidelijk worden om wat voor soort infrastructuur het hier gaat. Hoe ziet de infrastructuur eruit en welke apparatuur wordt er gebruikt; “Is deze apparatuur wel TRILL compatible?”

Sub-vraag 4.2: “Wat zijn de huidig gebruikte protocollen?”
Reden: Naast de vraag hoe de infrastructuur eruit ziet, moet er ook duidelijk worden hoe de infrastructuur werkt. Met welke protocollen wordt het huidige netwerk draaiend gehouden.

Sub-vraag 4.3: “Is er compatibiliteit mogelijk met de huidig gebruikte protocollen?”
Reden: Ook moet duidelijk zijn of TRILL of de varianten compatible zijn met de huidig gebruikte protocollen. Met andere woorden. Is het bijvoorbeeld mogelijk om een TRILL-core te hebben met een STP-access? Of moet de hele infrastructuur gemigreerd worden?

5. Spanning Tree Protocol

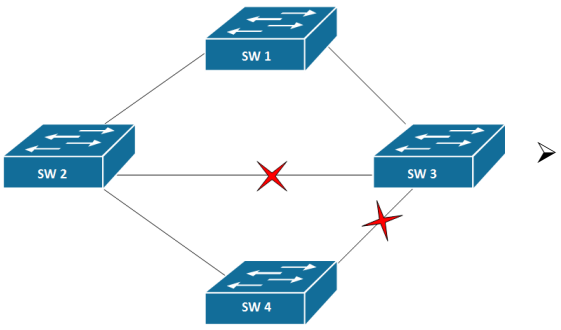
In dit hoofdstuk zal de deelvraag worden beantwoord: *"Wat is STP?"* Om deze vraag te onderzoeken wordt er onderzoek gedaan naar algemene informatie van STP, de werking van STP en de nadelen van STP. In het eerste subhoofdstuk wordt de algemene informatie van STP gegeven. Vervolgens wordt de werking van STP in het volgende subhoofdstuk behandeld worden. Dit zal duidelijk gemaakt worden aan de hand van verscheidene scenario's. Als laatste worden de nadelen van STP gegeven. Hieruit volgt de duidelijkheid waarom dit onderzoek is ontstaan.

5.1 Wat is het Spanning Tree Protocol

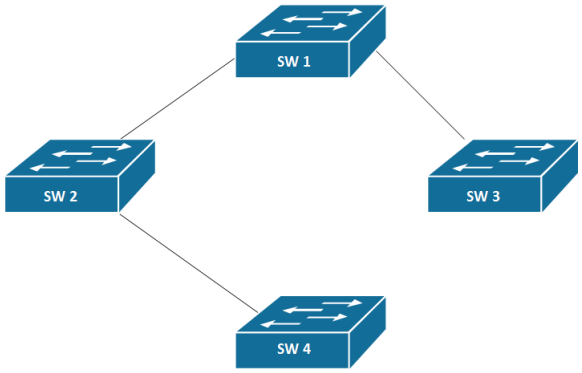
Het Spanning Tree Protocol, of afgekort STP, is een protocol dat in switched-netwerken wordt gebruikt om laag 2 switching loops en laag 2 broadcast storms te voorkomen[1][2]. STP is ontwikkeld door mevrouw Radia Perlman. STP wordt vooral in grotere netwerken gebruikt waarin veel gebruik wordt gemaakt van redundantie.

Redundantie is bijvoorbeeld het dubbel uitvoeren van een path of het gebruik van back-up switches. Redundantie wordt ingebouwd om de beschikbaarheid van het netwerk te verhogen. Echter kan dit er wel voor zorgen dat er fysieke loops ontstaan. Zonder STP zou het dataverkeer door deze loops blijven circuleren totdat één van de switches het begeeft.

STP voorkomt deze loops door het maken van een boom structuur. Hieronder wordt een layer 2 netwerk weergegeven en daarnaast het netwerk zoals STP dit netwerk logisch gebruikt.



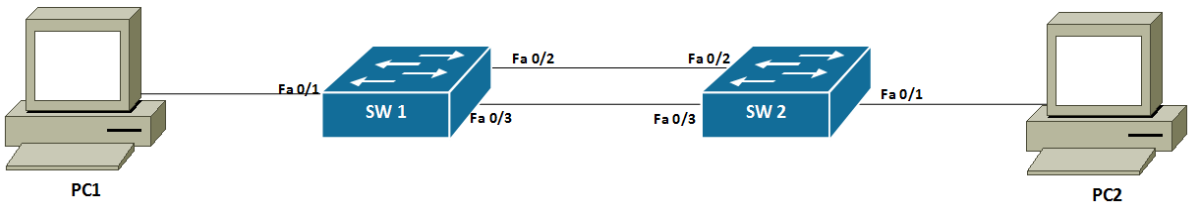
Figuur 1 Fysieke topologie met STP



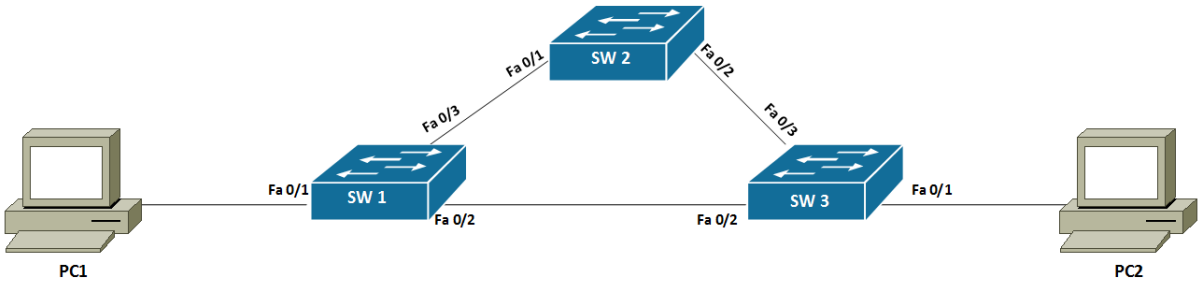
Figuur 2 Logische topologie met STP

Switching loops

Een switching loop ontstaat in een switched-netwerk als er een verbinding ontstaat tussen switches dat verkeer weer terug kan sturen bij de zendende switch. Vaak is dit het geval bij een netwerk dat redundantie ingebouwd heeft. Het geval kan zijn dat er maar twee switches met elkaar verbonden zijn, maar dat deze wel dubbele verbonden zijn om zo redundantie aan het netwerk toe te voegen. Dit is te zien in figuur 3.



Figuur 3 Redundantie tussen twee switches



Figuur 4 Switch loop met meerdere switches

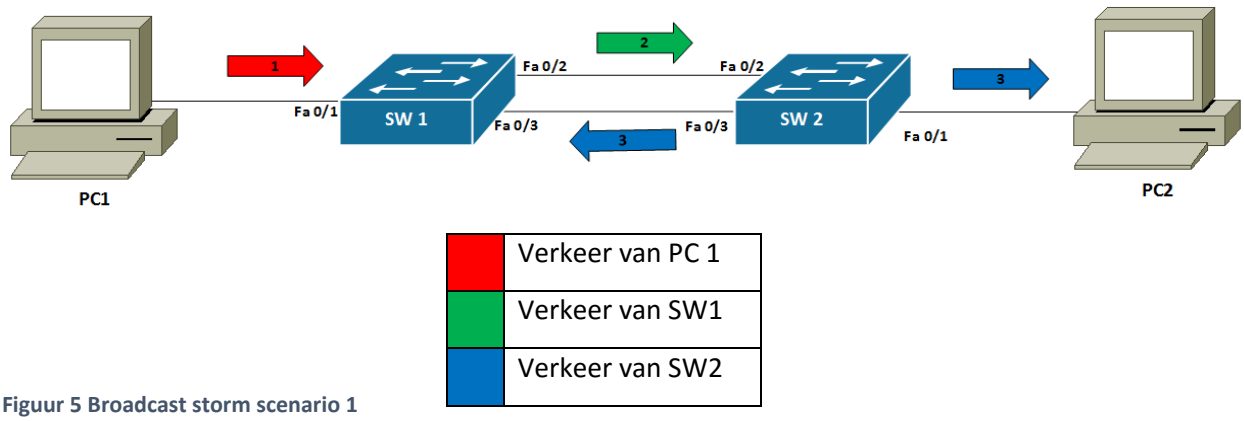
Maar een loop kan ook ontstaan als meerdere switches enkelvoudig met elkaar verbonden zijn. Hierbij is er redundantie gerealiseerd door het toevoegen van een back-up switch, zoals in figuur 4.

Zonder STP zouden deze switching loops de volgende gevolgen met zich mee kunnen brengen[1][2]:

- Broadcast storms
- Mac tabel instabiliteit
- Destinations zullen dezelfde frames meerdere malen ontvangen

Broadcast storm

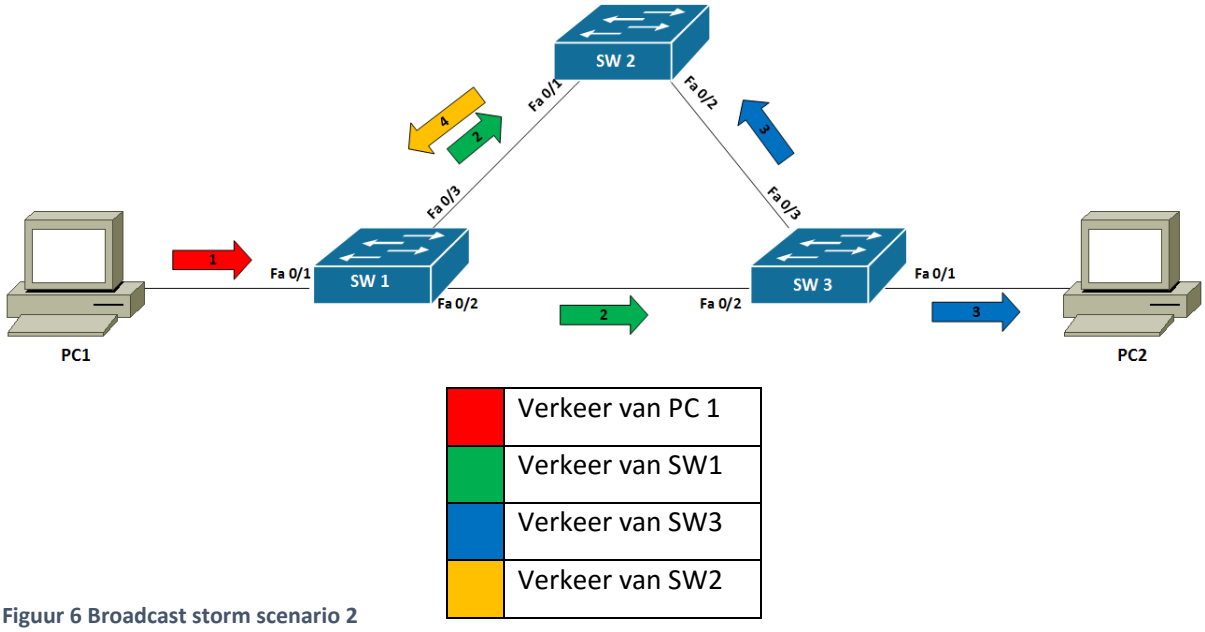
Bij broadcast verkeer in een switched netwerk wordt een frame via alle poorten doorgestuurd behalve op de port waar het frame op binnen is gekomen. Echter is het zo dat als dit switched netwerk een loop heeft. Dan is het zo dat het frame oneindig lang in het netwerk blijft loopen. Het oneindig loopen van deze frames wordt ook wel een broadcast storm genoemd[1][2]. In figuur 5 wordt er een scenario geschetst over hoe een broadcast storm ontstaat in een infrastructuur met maar twee switches. Deze switches zijn wel dubbel verbonden om redundantie toe te voegen aan het netwerk.



Figuur 5 Broadcast storm scenario 1

Op het moment dat PC1 broadcast verkeer stuurt naar SW1 dan zal SW1 dit verkeer doorsturen naar alle poorten, op de port na waar hij het verkeer van ontvangen heeft. SW1 zal dus het verkeer uit sturen op de poorten Fa0/2 en Fa0/3. *"In dit geval focussen we ons op het verkeer dat via Fa0/2 wordt verstuurd."* Hierbij wordt het broadcast verkeer ontvangen bij SW2 en zal SW2 net als SW1 het verkeer doorsturen naar alle poorten behalve de port waar hij het verkeer vandaan heeft[1][2]. Dit houdt in dat het SW2 het verkeer nu via port Fa0/1 naar PC2 stuurt, maar ook dat het verkeer via Fa0/3 teruggaat naar SW1. En SW1 zal het verkeer dan terugsturen naar PC1 en wederom het verkeer over Fa0/2 sturen. Als er naar bovenstaande figuur wordt gekeken, dan is de loop in het netwerk goed zichtbaar.

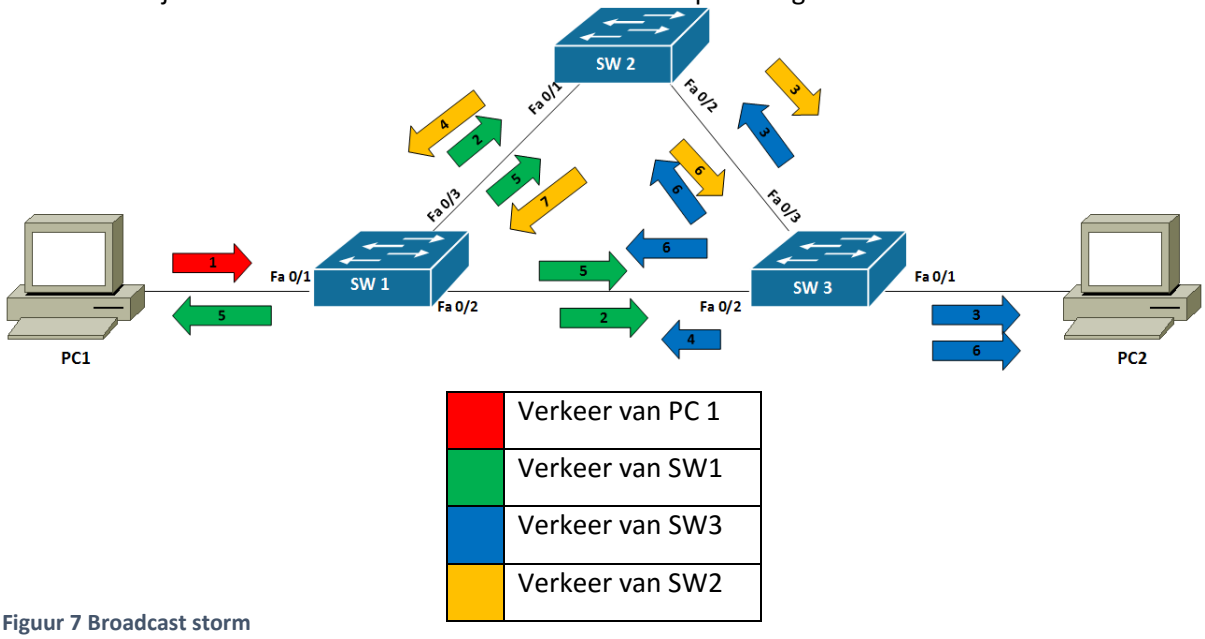
Als er maar een enkele lijn ligt tussen switches kan er nog steeds een loop ontstaan. In figuur 6 wordt een tweede scenario gegeven over hoe er een broadcast storm kan ontstaan. Ditmaal wordt er gebruik gemaakt van een netwerk waarbij drie switches enkelvoudig verbonden zijn.



Figuur 6 Broadcast storm scenario 2

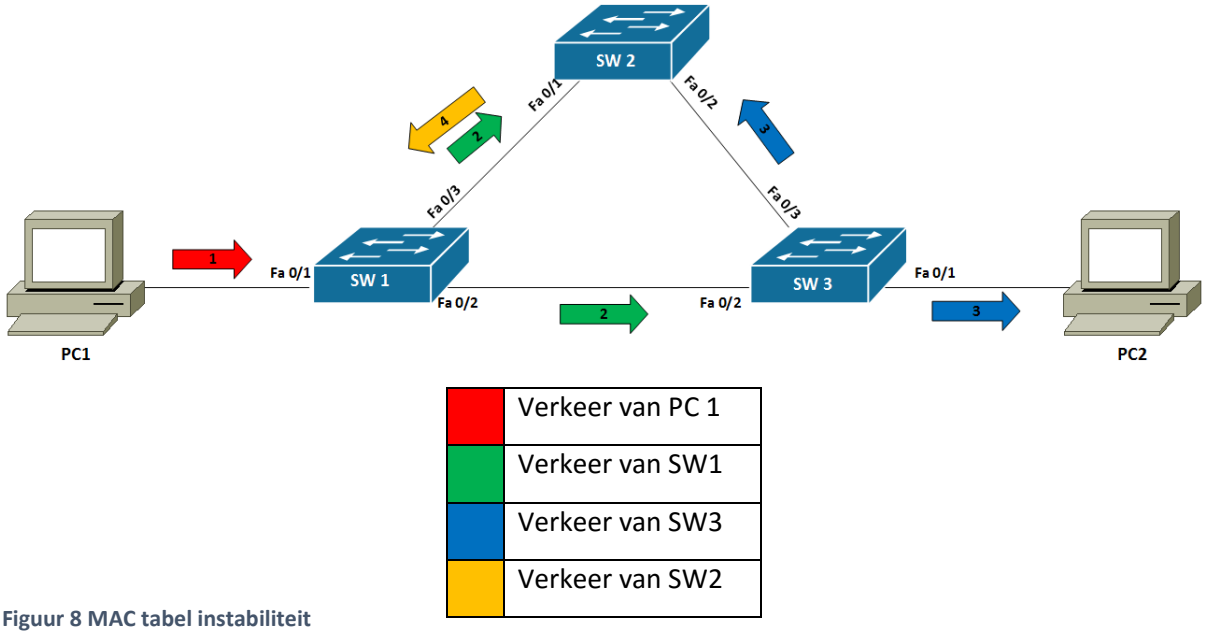
Zodra PC1 zijn broadcast frames verzendt naar SW1 zal deze switch kijken op welke port het verkeer is binnengekomen en zal het verkeer doorsturen op zijn andere poorten. Hierbij ontvangt SW1 het broadcast verkeer op Fa0/1 en zal dit verkeer doorsturen over de poorten Fa0/2 en Fa0/3. "*We zullen ons in deze situatie ons vooral focussen op verkeer dat via Fa0/2 wordt verzonden.*" Hierbij wordt het broadcast verkeer ontvangen door SW3 en zal SW3 net als SW1 het verkeer doorsturen naar alle poorten behalve de port waar hij het verkeer vandaan heeft[1][2]. Dit houdt in dat het SW3 het verkeer nu via port Fa0/1 naar PC2 stuurt, maar ook dat het verkeer via Fa0/3 doorstuurt naar SW2. In dit scenario is het dus niet het geval dat SW1 direct weer het verkeer ontvangt van SW3. Maar zal uiteindelijk het verkeer via SW2 alsnog bij SW1 uitkomen.

In onderstaande afbeelding worden alle frames die via SW1 worden verstuurt weergegeven en wordt duidelijk dat door een broadcast het netwerk niet optimaal gebruikt kan worden.



Figuur 7 Broadcast storm

Mac tabel instabiliteit
Om duidelijk te kunnen maken wat MAC instabiliteit inhoud wordt er gebruik gemaakt van onderstaande afbeelding.



Figuur 8 MAC tabel instabiliteit

Wanneer PC1 broadcast verkeer stuurt naar het netwerk zal deze aankomen bij SW1. Voordat SW1 het verkeer doorstuurt naar SW2 en naar SW3 zal hij de source MAC-adres van het frame opslaan in zijn MAC-tabel. Het opgeslagen MAC-adres zal gekoppeld worden aan de ontvangen switch port in dit geval is dat F0/1. Een voorbeeld van een MAC tabel is de onderstaande figuur.

```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0002.4a19.3802    DYNAMIC     Fa0/3
   1    000a.f3ab.2c02    DYNAMIC     Fa0/2
```

Figuur 9 Cisco Switch MAC tabel

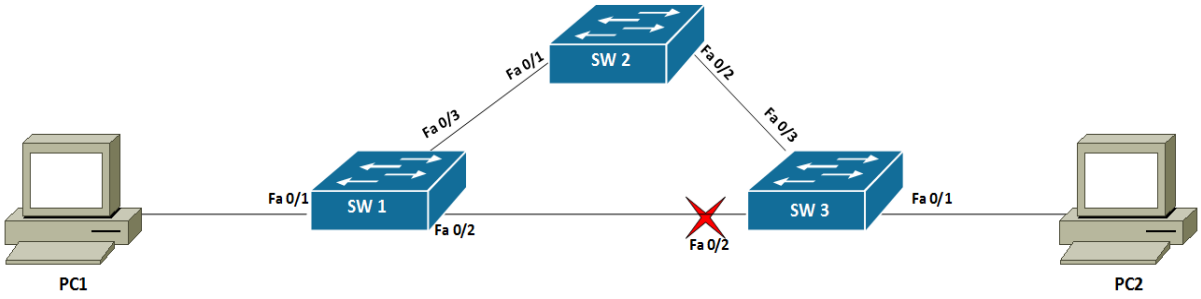
De MAC-tabel wordt gebruikt om gericht verkeer te sturen naar de destination. Door gebruik te maken van de MAC tabel weet een switch uit welke poort het ontvangen frame verstuurd moet worden, zodat het frame aankomt bij de juiste destination[1][2].

Nu dat SW1 het source MAC-adres heeft opgeslagen, zal SW1 beginnen met het doorsturen van het broadcast verkeer naar SW2 en SW3. Beide switches zullen ook het source MAC-adres van het frame opslaan in hun MAC-tabel. Nu is echter het geval dat SW2 en SW3 dit frame met het source MAC-adres naar elkaar zullen sturen. Dit houdt in dat er nu een duplicate MAC-adres komt te staan, alleen wordt deze aan een andere port gelinkt. Dit is op een switch echter niet mogelijk. De switch zal als hij een duplicate MAC-adres ontvangt op een andere port de andere port “cleanen”. Hierbij zal dan het MAC-adres op de nieuwe port worden toegevoegd en bij de andere port verwijderd worden. Dit zorgt ervoor dat de switch gaat “MAC flapping”. Hierbij zal het frame per keer een ander path kiezen om de PC te bereiken. Dit zorgt ervoor dat de MAC-tabel instabiel en onbetrouwbaar ofwel onbruikbaar wordt.

Naast de verandering in de MAC-tabellen zullen ook de destinations door loops in het netwerk meerdere malen hetzelfde frame opnieuw ontvangen[1][2]. Dit komt door het verkeer dat via meerdere switches verstuurd zal worden naar de destination. Nu de problemen en het ontstaan van loops in kaart zijn gebracht zal in de volgende paragraaf achterhaald worden hoe deze problemen opgelost kunnen worden door het Spanning Tree Protocol.

5.2 Werking van het Spanning Tree Protocol

In dit hoofdstuk wordt er antwoord gegeven op de deelvraag: “hoe werkt het Spanning Tree Protocol?”. Om dit toe te lichten wordt er gebruik gemaakt van verschillende scenario’s. STP blokkeert bepaalde poorten om loops te voorkomen. Onderstaande figuur geeft een voorbeeld van een switched netwerk met STP.



Figuur 10 Switched netwerk met STP

Doordat Fa0/2 van SW3 in Blocking state geplaatst is, zal op deze manier de loop in het netwerk voorkomen worden[1][2]. Op deze manier kan SW3 alleen nog maar bij PC 1 komen door gebruik te maken van port Fa0/3. De verbinding tussen SW1 en SW3 zal pas gebruikt worden als de verbinding tussen SW1 en SW2 of de verbinding tussen SW2 en SW3 down gaat.

In de volgende paragraven wordt er toegelicht hoe STP loops in een switched netwerk voorkomt. Dit wordt gedaan door middel van deze drie stappen[1][2]:

- Root switch van het netwerk bepalen
- Het beste path naar de Root switch vaststellen
- Het blokkeren van redundante verbindingen.

Root switch bepalen

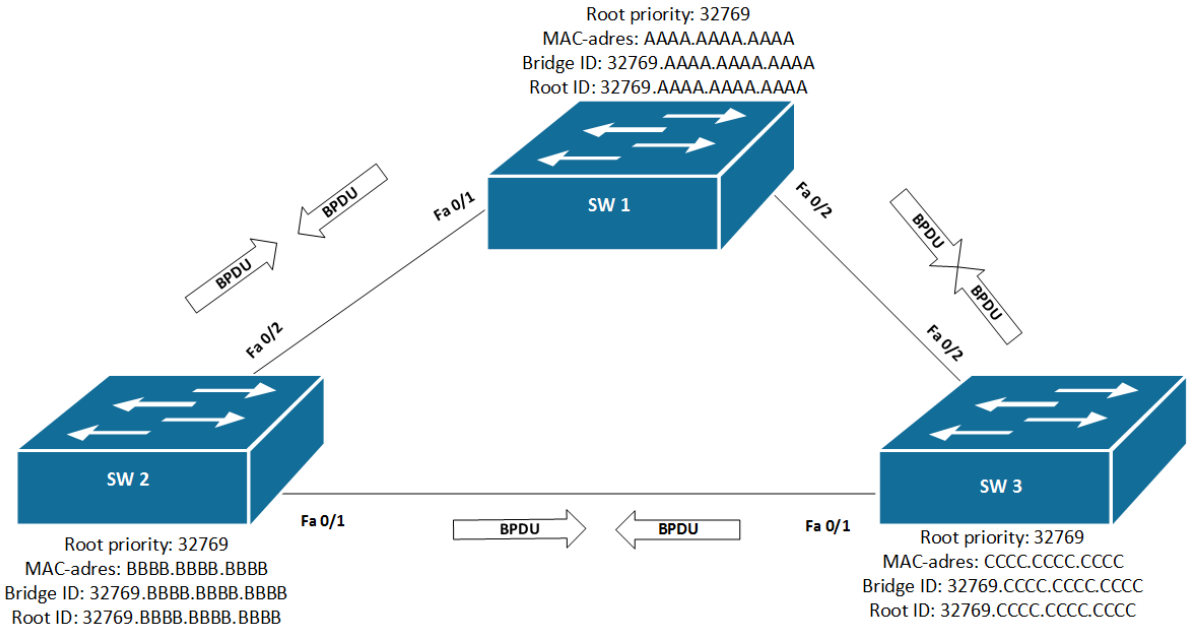
In deze paragraaf wordt er toegelicht hoe de root switch in een switched-netwerk wordt bepaald.

Wanneer switches opgestart worden, dan beginnen ze met het sturen van BPDU frames naar elkaar. BPDU staat voor Bridge Protocol Data Units (BDPU), in deze frames staat de volgende informatie[1][2]:

- Root prioriteit
- Switch MAC-adres

Deze BPDU frames worden gebruikt om te bepalen welke switch de root wordt. De root-prioriteit heeft een standaard waarde van 32.768+VLAN ID (op Cisco). De root-switch wordt aan de hand van deze waarde bepaald[1][2]. De switch met de laagste root-prioriteit zal aangewezen worden als de root-switch. De prioriteit waarde kan aangepast worden in de configuratie van het STP protocol. Wanneer de root-prioriteit waardes gelijk zijn, zal er naar het MAC-adres van de switches gekeken worden om te bepalen wie de root-switch wordt. De switch met het laagste MAC-adres wordt dan verkozen tot root-switch.

Hierbij denkt elke switch dat hij de Root-switch kan zijn en stuurt dus een BPDU met zijn Bridge ID naar de andere switches zeggend: “Ik ben <Naam>; mijn Bridge ID is 32769+MAC-adres en ik ben dus de Root-switch.” Hierbij krijgen de andere switches dit frame binnen en vergelijken de Bridge ID van <Naam> met hun eigen Bridge ID. Mocht het Bridge ID van <Naam> lager zijn, dan zal de ontvanger ook BPDU’s sturen zeggende: “<Naam> is de root met dit Bridge ID: 32769+MAC-adress”.



Figuur 11 BPDU zenden en Root switch kiezen

In bovenstaande figuur zijn de Root prioriteit, het MAC-adres, de Bridge ID en de Root ID te zien van de switches SW1, SW2 en SW3. Hierin zijn alle drie de Root prioriteit waardes gelijk en zal de beslissing van wie de Root switch wordt vallen in de vergelijking van de MAC-adressen. Als SW2 als eerste zijn BPDU’s stuurt naar SW1 en SW3 dan zullen deze switches de ontvangen Root ID vergelijken met hun eigen Root ID. Voor SW1 geldt dan dat SW1 het BPDU van SW2 negeert, omdat zijn eigen Root ID lager is. Voor SW3 geldt echter dat SW3 het Root ID van SW2 overneemt en zegt dat SW2 de root is. Dit omdat de Root ID van SW2 lager is dan de Root ID van SW3. Als SW1 zijn BPDU’s gaat sturen dan zal zowel SW2 als SW3 tot de conclusie komen dat het Root ID van SW1 lager is als de eigen Root ID en hierbij is dan de root gekozen en dat is SW1. Hierbij zal alleen de Root ID aangepast worden bij de switches. De Bridge ID kan niet door andere switches aangepast worden, alleen een gebruiker kan de Root prioriteit aanpassen. Als de keuze van wie de Root switch is afgelopen, zullen er geen BPDU’s meer worden gestuurd door de switches behalve door de Root switch[1][2].

Beste path naar de Root-switch vaststellen
Nu dat de Root-switch is gekozen voor het netwerk, moet elke niet Root-switch uitzoeken welk path het beste is om bij de Root-switch te komen. Om dit path vast te kunnen stellen zijn er drie mogelijkheden:

- Laagste cost van het path
- Laagste Bridge ID
- Laagste interface nummer

De cost van een path wordt bepaald aan de hand van de bandwidth van de verbinding[[1][2]. Zie afbeelding hieronder voor een indicatie van Cost per bandwidth.

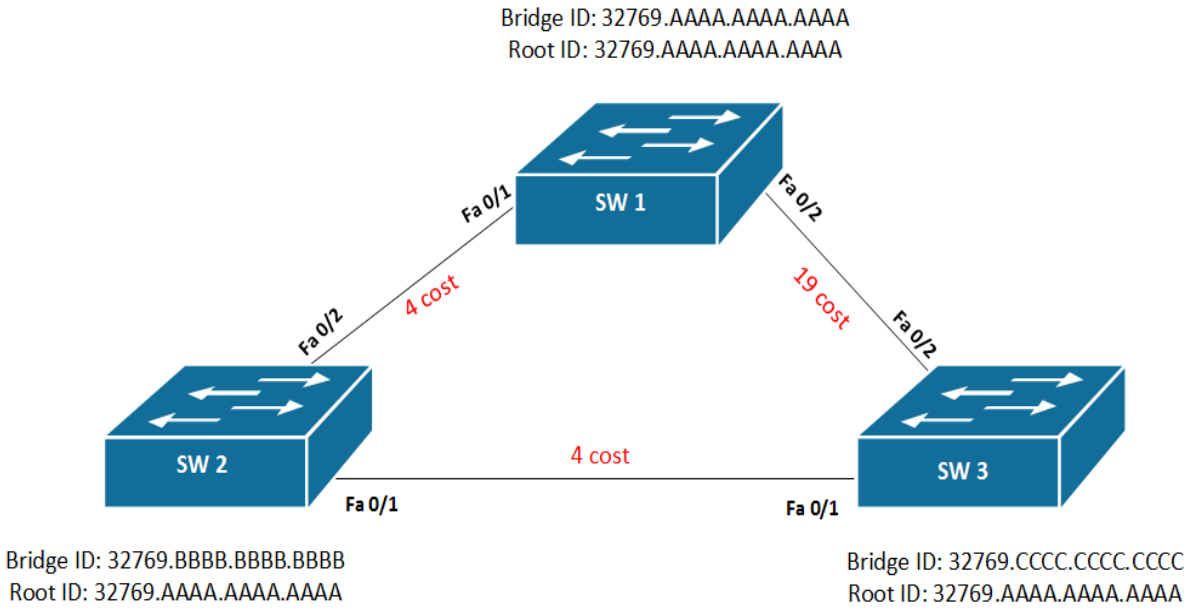
Link Bandwidth	Old STP Cost	New STP Cost
4 Mbps	250	250
10 Mbps	100	100
16 Mbps	63	62
45 Mbps	22	39
100 Mbps	10	19
155 Mbps	6	14
622 Mbps	2	6
1 Gbps	1	4
10 Gbps	0	2

Figuur 12 Path Cost[1].

In de tijd van de oude STP cost werd er nog geen rekening gehouden met een snelheid sneller als 1 Gbps. Hierdoor zijn de oude waardes niet meer van toepassing op de netwerken van de tegenwoordige tijd en daarom zijn deze waardes aangepast[1][2].

Wanneer er een gelijke cost is in een netwerk en daardoor het beste path naar de Root-switch niet kan worden bepaald, zal STP aan de hand van de volgende Switch zijn BID bepalen welk path het beste is. Echter als hier ook nog geen beslissing uitkomt, zal aan de hand van het laagste interfacenummer bepaald worden welk path het beste is om naar de Root-switch te gaan. In de komende scenario's waarin het beste path wordt vastgesteld zal er gebruikt worden van een path cost van 4 (1 Gbps verbinding) en de cost van 19 (100 Mbps verbinding).

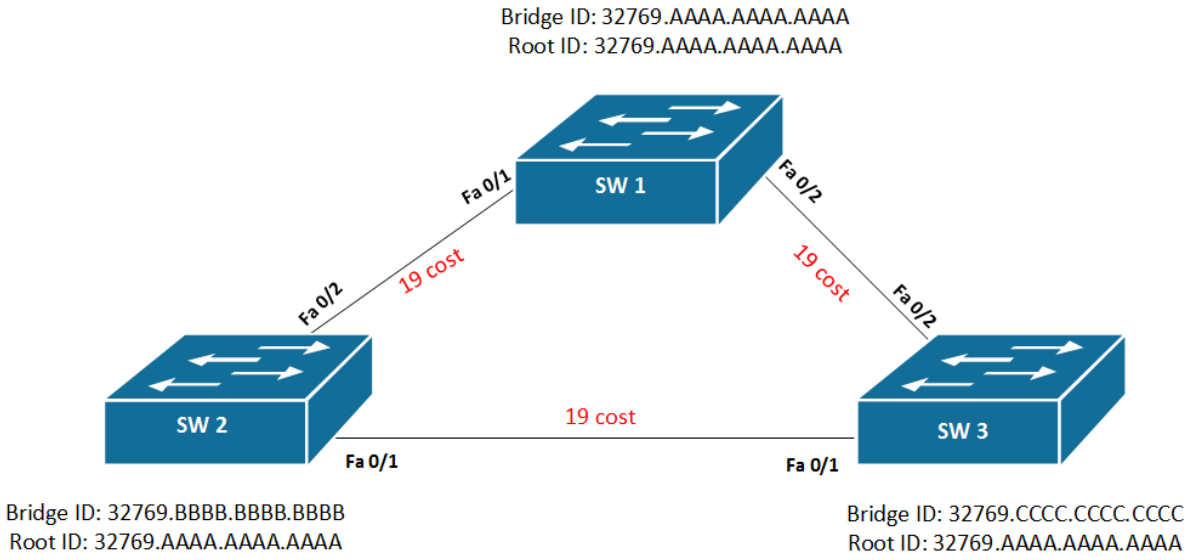
Met onderstaande opstelling zal begonnen worden met het uitleggen van hoe de switches hun beste path naar de Root-switch bepalen.



Figuur 13 Beste path vinden d.m.v. Path cost

In bovenstaande figuur in een netwerk aangegeven waarin SW1 de Root-switch zal worden na het uitwisselen van de BPDU. SW1 heeft het laagste Bridge ID. Nu dat alle switches in het netwerk weten dat SW1 de Root-switch is, zullen de switches SW2 en SW3 het beste path naar SW1 proberen te vinden. Hierin wordt als eerste gekeken naar de path cost[1][2]. Voor SW2 geldt in dit geval dat hij zijn directe link naar SW1 over Fa0/2 gebruikt omdat deze een cost heeft van 4. Als hij via SW3 zou gaan dan zou hij een waarde van 4+19 = 23 hebben en in deze afweging geld: 4<23. Daarmee wint het path van SW2 naar SW1 via Fa0/2 het over het path van Fa0/1. Als dan het path van SW3 naar SW1 wordt bepaald zal weer dezelfde afweging worden gemaakt. Het path van SW3 over Fa0/2 heeft een cost van 19. Nu is het geval daar dat als SW3 via SW2 naar SW1 wil de cost van het path slechts 4+4=8 is. Hierbij is dus het path over Fa0/1 via SW2 beter als de directe verbinding naar SW1 via Fa0/2. Want de cost vergelijking is dan 8<19[[1][2].

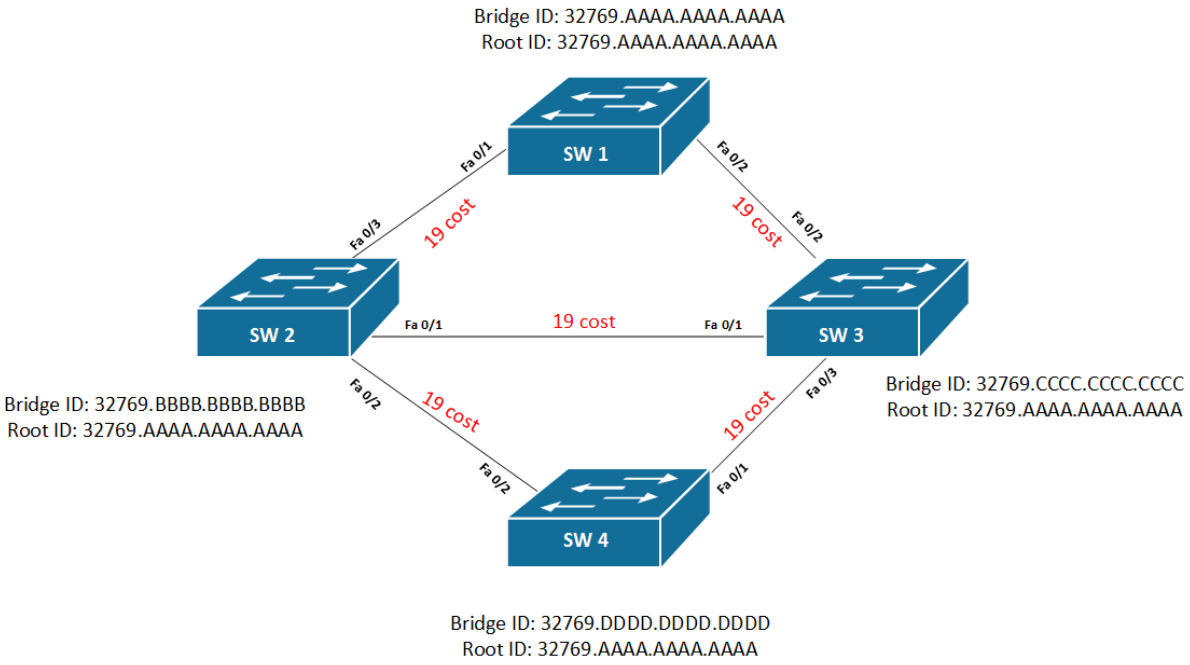
Echter kan het geval ook zo zijn dat alle path dezelfde cost hebben en daarmee valt bovenstaande manier van het beste path vinden af. Nu zal er gekeken worden naar de andere mogelijkheden met als tweede optie. Welke switch heeft de laagste Bridge ID.



Figuur 14 Path bepalen naar de Root

In figuur 14 hierboven is zoals al aangegeven geen sprake van het beste path bepalen door middel van de cost. Hierbij geldt voor zowel SW2 als SW3 dat het beste path naar de Root-switch, de directe verbinding is. Hierbij is het namelijk het geval dat deze verbinding een Path Cost heeft van 19. Terwijl als het path via de andere switch gebruikt wordt de cost 19+19 = 38 is. Hieruit wordt dan de vergelijking gemaakt dat 19<38 en daarmee wint het directe path het over het path via de andere switch[1][2].

Omdat in bovenstaande figuur beide switches in directe verbinding staan met de Root-switch kan hier geen andere manier uitgelegd worden. Hiervoor wordt de volgende scenario gebruikt:

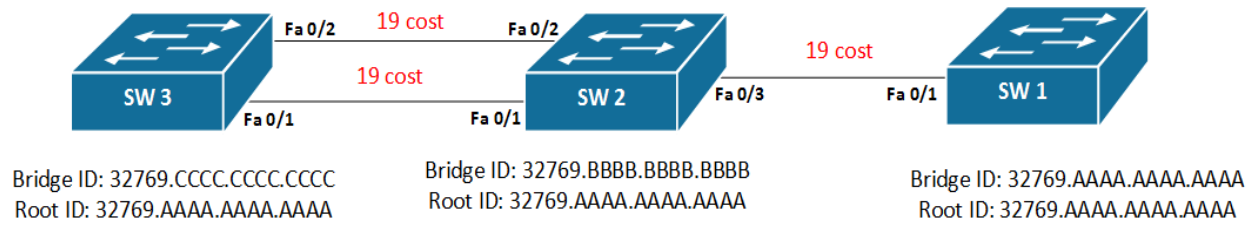


Figuur 15 Path bepalen d.m.v. Bridge ID

In dit scenario is SW4 niet direct verbonden met de Root-switch dat in dit geval wederom SW1 is. Nu kan er dus geen path gekozen kan worden die op basis van alleen de cost. In dit geval zijn er namelijk twee paths die beide de cost hebben van 19+19 = 38 en geen van beide is direct verbonden aan de Root Switch.

Hierdoor wordt de keuze van het beste path op de tweede manier bepaald; het kiezen van het path via de switch met de laagste Bridge ID. Hierbij zal SW4 de afweging moeten maken tussen de Bridge ID's van SW2 en SW3[1,2] In het geval van het kiezen welk path hiervoor het beste is, wordt dezelfde vergelijking gemaakt als bij het kiezen van de Root-switch. De switch met de laagste Bridge ID wint de verkiezing. Hierbij heeft SW2 een Bridge ID van 32769.BBBB.BBBB.BBBB en heeft SW3 een Bridge ID van 32769.CCCC. CCCC. CCCC. De vergelijking is snel duidelijk en wint SW2 de verkiezing want na het gelijke begin zal de B van SW2 winnen over de C van SW3 want hier geldt B<C[1][2].

Echter kan het ook nog het geval zijn dat ook deze manier van path bepalen niet van toepassing kan zijn. Hiervoor is onderstaande scenario gebruikt:



Figuur 16 Path bepalen d.m.v. Interface nummer

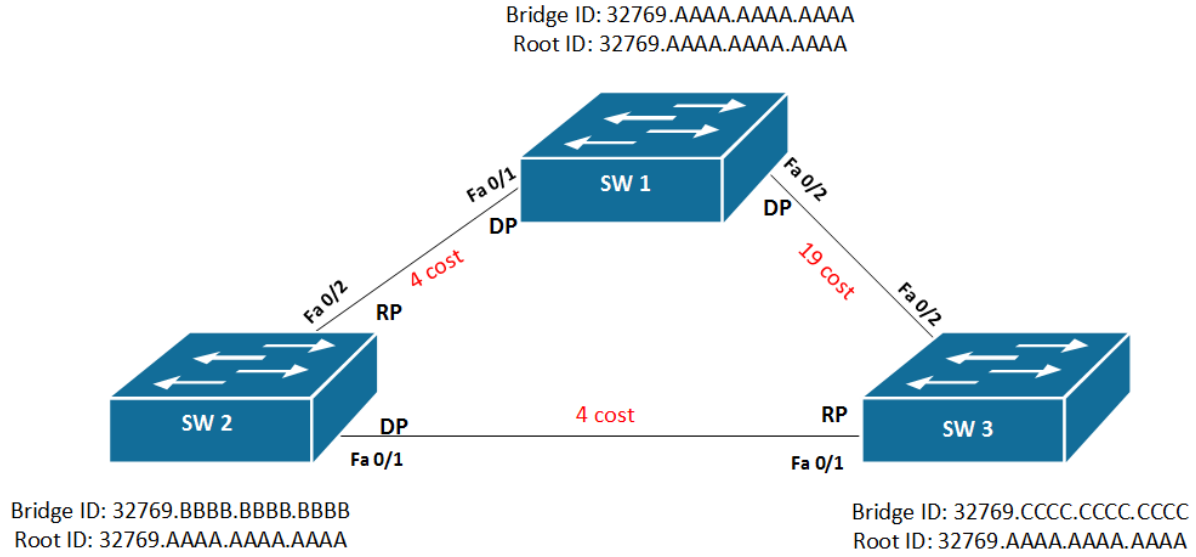
Bij dit figuur gelden de eerder besproken manier niet, de cost van de verbindingen zijn hetzelfde en ook het Bridge ID is hetzelfde omdat dit dezelfde switch is. Hierbij moet dus de laatste manier van path bepaling gebruikt worden en dat is het kiezen van het beste path op basis van de laagste interface[1][2]. In dit scenario is SW1 wederom de Root-switch en kijken we vanuit SW3 hoe er bij SW1 gekomen kan worden. SW3 moet in ieder geval door SW2 heen voordat SW1 bereikt kan worden. Nu heeft SW3 twee paths die naar SW2 gaan met ieder de cost van 19. Hierbij zal SW3 kijken welke interface het laagste is en de afweging zal in dit geval gaan tussen Fa0/1 en Fa0/2. Hierin wordt duidelijk dat 1<2 is en daarmee zal Fa0/1 de voorkeur krijgen over Fa0/2.

Nu is er duidelijk gemaakt hoe switches het beste path naar de Root-switch bepalen. In de volgende paragraaf zal uitgelegd worden hoe het netwerk achterhaald welke verbindingen geblokkeerd worden om loops te voorkomen. Hierbij wordt ook uitgelegd in welke statussen de verbinding zich kan bevinden en wanneer deze status van toepassing is.

Blokkeren van redundante verbindingen

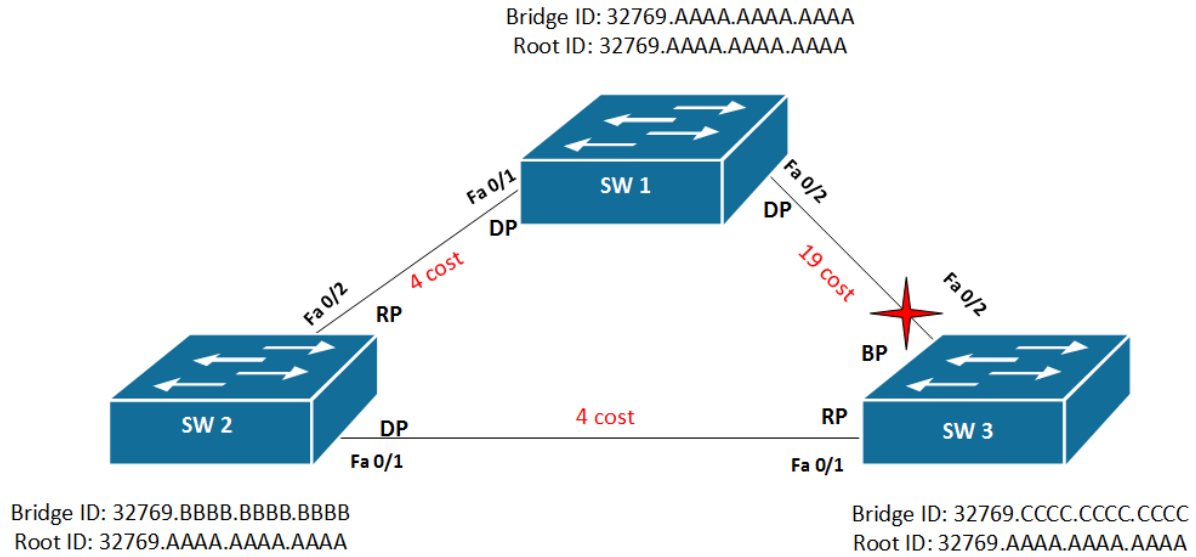
Het laatste wat STP doet bij het creëren van een boom structuur is het blokkeren van verbindingen waardoor loops zouden ontstaan[1][2]. Het blokkeren van deze verbinding wordt net als het kiezen van het beste path gedaan, er wordt een afweging gemaakt welke verbinding in Blocking State gaat en welke in Forwarding state gaat.

De manieren waarop bepaald wordt welke port in Blocking State gaat zijn dezelfde manieren als die gebruikt worden voor het path naar de Root-switch[1][2]. Alleen is het nu het geval dat de hoogste waarde in de Blocking State gaat. Dit wordt uitgelegd aan de hand van de eerder gebruikte scenario's.



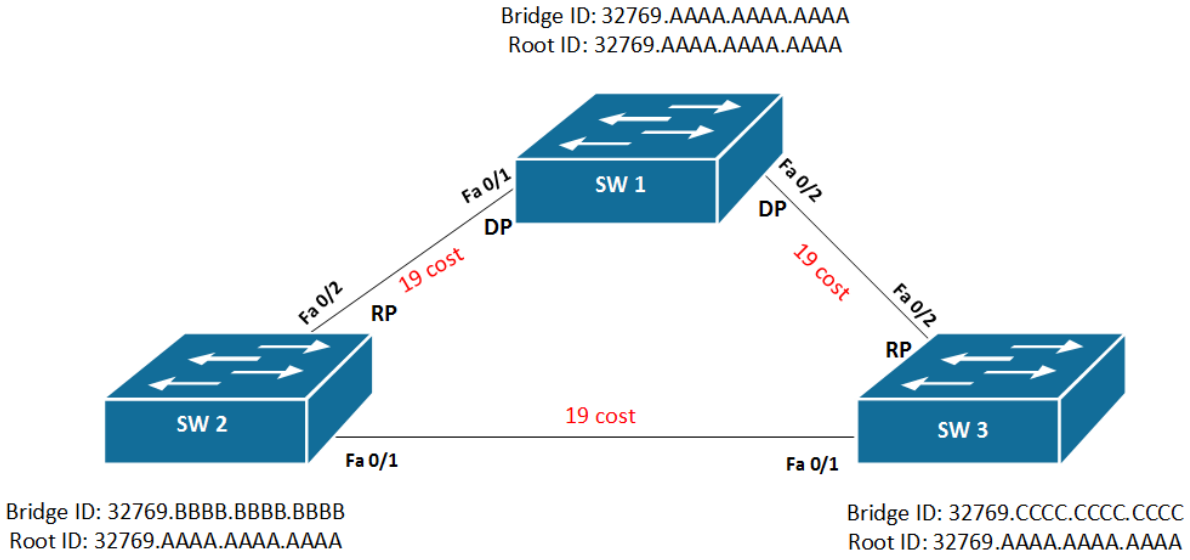
Figuur 17 Scenario met verschillend cost

In bovenstaand figuur wordt een scenario weergegeven waarin de beslissing al gevallen is op de verbinding die de hoogste path cost heeft. Hierbij zijn de Root paths aangegeven als RP en de poorten van de Root-switch staan in Forwarding State of ook wel de Designated Ports (DP). Doordat de directe verbinding duurder is, zal de verbinding van SW3 via SW2 naar SW1 lopen. Hierdoor moet SW2 port Fa0/1 in Forwarding State om SW3 met SW1 te laten communiceren[1][2]. Mede hierdoor wordt automatisch Fa0/2 van SW3 in Blocking State gezet. Dit geeft het volgende resultaat:



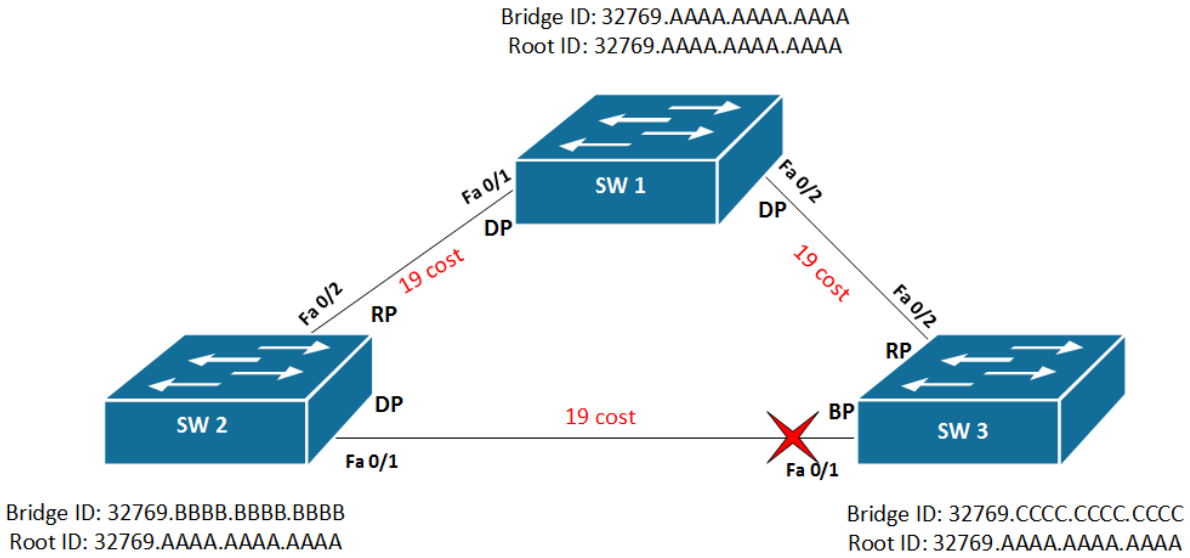
Figuur 18 STP resultaat bij ongelijke cost

Maar als de cost in bovenstaande scenario wel hetzelfde was, dan had het scenario er zo uit gezien:



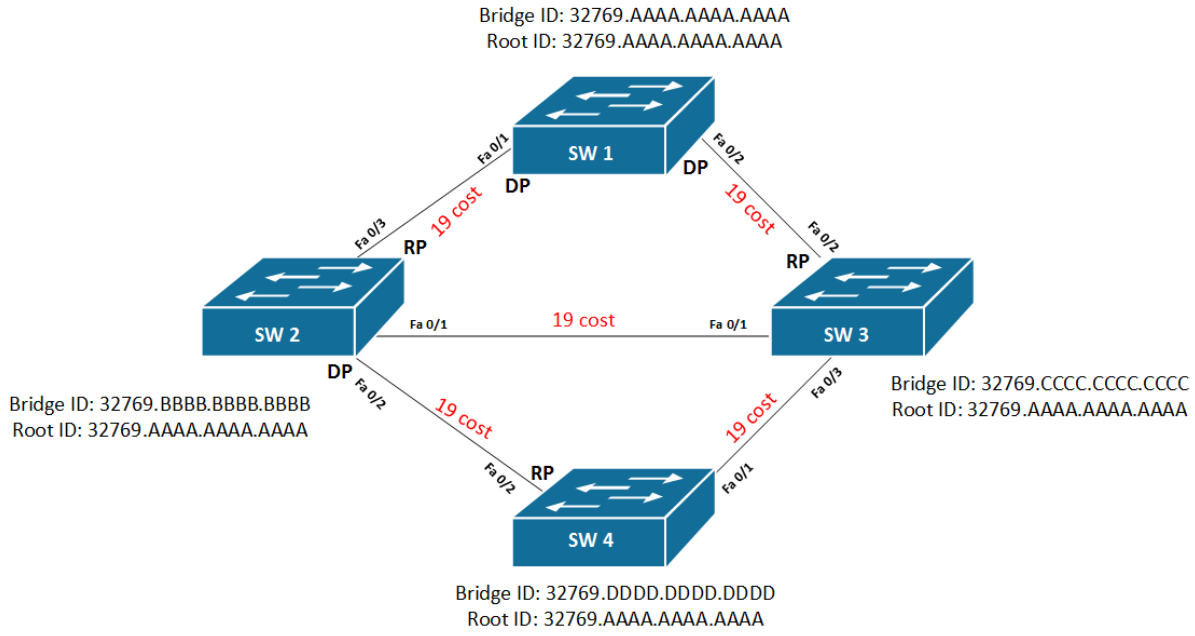
Figuur 19 Blocking paths met zelfde Cost

In dit scenario zijn de Root poorten aangegeven (RP) en deze zijn logische wijs de directe verbindingen naar de Root-switch. Hierbij zijn de poorten van de Root-switch wederom Designated poorten (DP). Nu volgt de afweging of SW2 of SW3 zijn port in Blocking State moet zetten. Hierbij wordt de afweging gemaakt in wie het laagste Bridge ID heeft. De switch met het laagste Bridge ID zet zijn port in Forwarding State ofwel de port als Designated[1][2]. Als naar de Bridge ID's wordt gekeken, is duidelijk te zien dat SW2 een lager Bridge ID heeft en daarmee de afweging wint.



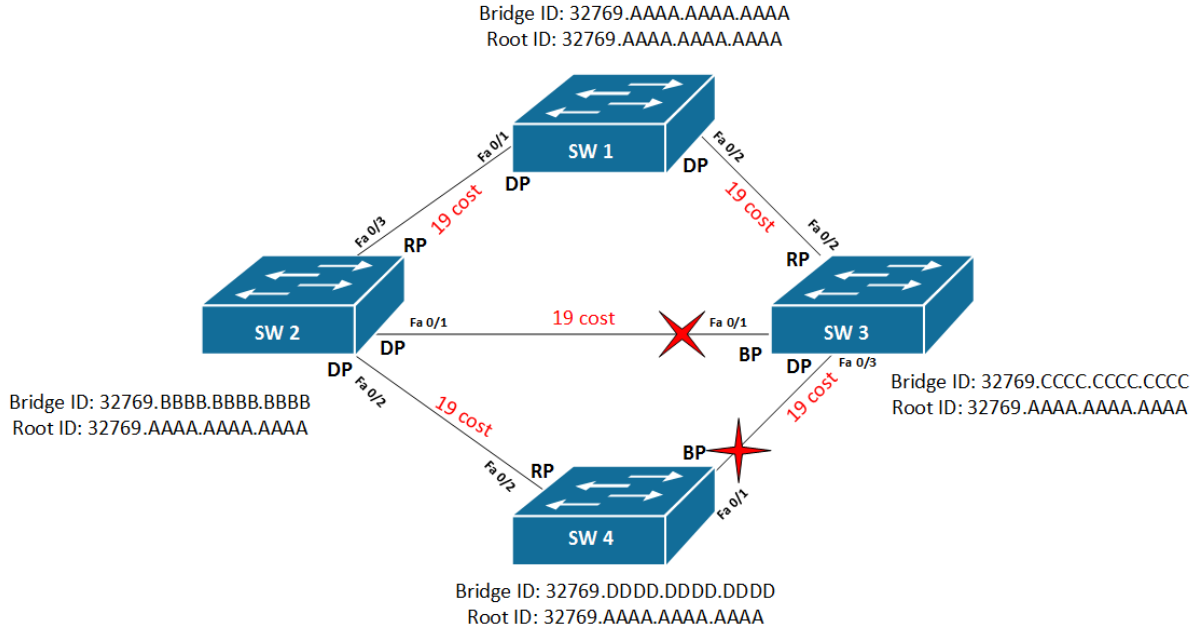
Figuur 20 STP resultaat aan de hand van Bridge ID

In het volgende scenario moeten er meerdere poorten in Blocking State gezet worden, omdat in dit netwerk er meerdere loops zijn.



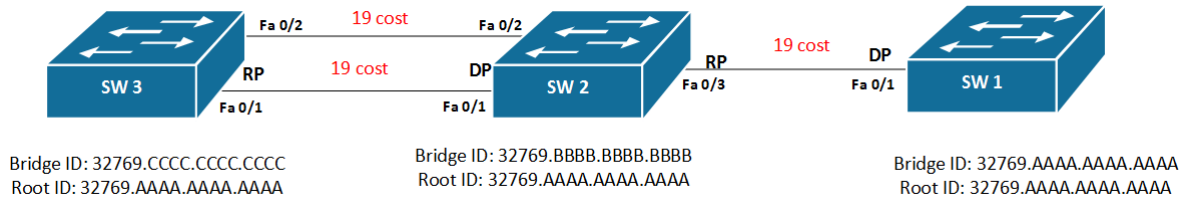
Figuur 21 Meerdere loops in het netwerk

In bovenstaand scenario staan wederom de Root poorten en de Designated poorten al aangegeven die al bekend zijn. Deze zijn bepaald aan de hand van het bepalen van het beste path naar de Root-switch[1][2]. Nu moeten er nog twee lijnen aangepast worden om de loops ter voorkomen. Hierbij gaat het tussen de verbinding van SW2 en SW3 en de verbinding tussen SW3 en SW4. In beide gevallen kan de afweging weer gemaakt worden aan de hand van de Bridge ID's van de switches[1][2]. Hierbij wint SW2 het van SW3 en wint SW3 het van SW4. Hieruit volgt dan het volgende resultaat.



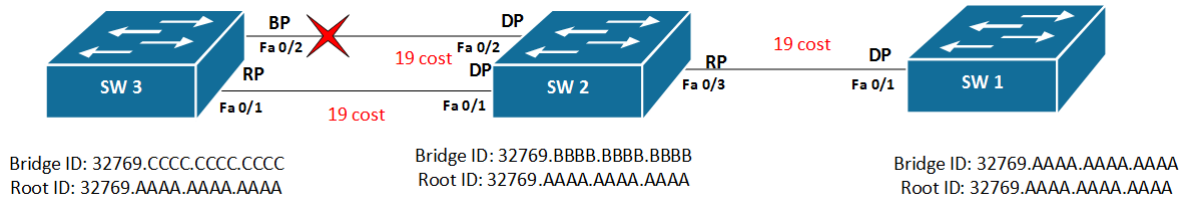
Figuur 22 STP resultaat bij meerdere loops

Als laatste komt het scenario aan bod waarbij ook de Bridge ID doorslag geeft, ondanks dat dit dezelfde switch is[1,2]. Hieronder is dit scenario afgebeeld met de Root poorten en Designated poorten al aangegeven.



Figuur 23 Port status bij redundante verbinding

In dit scenario is het net als in het scenario hierboven het geval dat er een verbinding is die een tweede verbinding heeft om bij de root te komen. Hierbij is het echter het geval dat beide verbindingen bij dezelfde switch uitkomen, in dit geval SW2. Omdat de bepaling van het beste path naar de Root-switch al een verbinding heeft gekozen blijft er nu nog één verbinding over waarin de afweging moet worden gemaakt welke switch zijn port in Blocking State moet zetten. Hierbij komt de beslissing wederom door het vergelijken van de Bridge ID's, waarbij SW2 wint van SW3. Dit leidt tot het volgende resultaat.



Figuur 24 STP resultaat bij redundante verbinding

Nu duidelijk is geworden hoe STP loops voorkomt in een layer 2 netwerk, zal er beschreven worden welke nadelen STP heeft met deze manier van oplossen. Naast het Spanning Tree Protocol zijn er nog verschillende vormen van STP; zo is er het Rapid Spanning Tree Protocol (RSTP) en het Multiple Spanning Tree Protocol (MSTP). Deze vormen van STP voorkomen loops op dezelfde manier als STP zelf en daarom zal er aan deze protocollen verder geen aandacht worden besteed[1][2].

5.3 Nadelen van het Spanning Tree Protocol

Door het blokkeren van de redundante verbindingen kan er niet optimaal gebruik gemaakt worden van de bandbreedte. Hierbij is het ook het geval dat het verkeer niet efficiënt door het netwerk wordt gerouteerd. Doordat er redundante verbindingen geblokkeerd worden zal het verkeer via een omweg naar hun bestemming gaan[1][2].

Ook is het geval er dat als de verbinding uitvalt de omschakelingstijd van STP er lang duurt[1][2]. Hierbij wacht de switch 10 Hello frames af, waarbij elk Hello frame om de 2 seconden wordt gestuurd. Dan zal de switch in Listening State en gaat 15 seconden luisteren over zijn andere lijnen of hij hier wel een Hello frame ontvangt. Als dit het geval is dan gaat de switch in Learning State en leert dan het alternatieve path voor de uitgevallen verbinding. De Learning State duurt ook weer 15 seconden. Als de switch het nieuwe path heeft geleerd zal hij deze pas gebruiken. Ondertussen zijn er al 50 seconden verstreken en is de verbinding deze tijd down. Dit is ook de reden dat RSTP en MSTP ontwikkelt zijn. RSTP en MSTP hebben een snellere omschakelingstijd dan STP[1][2].

Als laatste kwam uit het onderzoek naar de protocollen naar voren dat STP slecht schaalbaar is. Als het netwerk uitgebreid moet worden, waarbij het aantal VLANs oploopt tot in de honderden, zal het configureren van nieuwe switches veel tijd kosten. Hiervoor is ook een protocol bedacht door de IEEE groep, namelijk Multi Spanning Tree Protocol (MSTP)[1]. MSTP wordt vooral gebruikt als het netwerk met meerdere VLANs werkt, maar er niet voor elk VLAN een aparte Distribution Tree moet komen. MSTP maakt Distribution Trees per “instance” en per “instance” worden VLANs toegevoegd.

5.4 Conclusie Spanning Tree Protocol

Als resultaat uit het onderzoek naar het Spanning Tree Protocol blijkt dat zonder STP er loops ontstaan in een switched netwerk en dat er broadcast storms kunnen ontstaan. Hierdoor kan een netwerk vastlopen en zal het netwerk frames rond blijven sturen over het netwerk totdat er een switch crasht.

Ook werd duidelijk dat STP loops voorkomt door het blokkeren van de redundante verbindingen. Hierbij wordt een Root-switch gekozen waarlangs al het verkeer gaat. Nadat de Root-switch bepaalt is, kiest elke niet Root-Switch een path naar de Root-switch. Hierbij worden afwegingen gemaakt om te kijken welk path het efficiënts is. Als laatste worden de overgebleven paths vanaf één kant geblokkeerd door een switch. Hierbij wordt hetzelfde selectieproces uitgevoerd als voor het vinden van het beste path naar Root-switch. Als al deze stappen doorlopen zijn, kan er gesproken worden over een STP netwerk. Fysiek gezien zitten er nog loops in het netwerk maar logisch gezien niet meer.

Echter zorgt deze manier van loops voorkomen voor een aantal nadelen. Zo maakt STP door het blokkeren van de redundante verbinding niet optimaal gebruikt van de bandbreedte. Ook de omschakelingstijd als er een verbinding uitvalt, is langzaam bij STP. Hier zijn daarentegen wel het RSTP en MSTP ontwikkelt, dit zijn snellere vormen van STP. Als laatste is STP slecht schaalbaar (als het netwerk meerdere VLANs gebruikt), zal bij uitbreiding van het netwerk alle switches de VLANs handmatig geconfigureerd worden.

6. Transparent Interconnection of Lots of Links

In dit hoofdstuk zal de deelvraag worden beantwoord: *"Wat is TRILL?"* Om deze vraag te onderzoeken wordt er onderzoek gedaan naar algemene informatie van TRILL en de werking van TRILL. In het eerste subhoofdstuk wordt de algemene informatie van TRILL gegeven. Vervolgens wordt de werking van TRILL in het volgende subhoofdstuk behandeld worden. Dit zal duidelijk gemaakt worden aan de hand van verscheidene scenario's.

6.1 Wat is het TRILL protocol

TRILL staat voor Transparent Interconnection of Lots of Links. TRILL is een verzamelnaam voor het gebruik van Ethernet en het IS-IS protocol. Hierbij zorgt ethernet ervoor dat de switches de frames rondsturen door het netwerk en zorgt IS-IS ervoor dat de switches weten waar de frames naartoe worden gestuurd door middel van het opstellen en uitwisselen van Forwarding tabellen. TRILL is ontwikkeld door mevrouw Radia Perlman. Mevrouw Perlman was naast de ontwikkelaar van TRILL ook de ontwikkelaar van STP[3].

Mevrouw Perlman was in eerste instantie met haar idee van TRILL naar de leergroep van IEEE gegaan, dit waren ook de uiteindelijke uitgevers van STP. Deze groep was echter van mening dat er niets mis was met STP en dat TRILL eerder meer schade aan zou kunnen richten door het routeren van frames door het netwerk. Over dit routeren wordt in het volgende hoofdstuk "Werking van TRILL" verder op ingegaan. Nadat ze hier was afgewezen ging ze naar de Internet Engineering Task Force (IETF). Hier werd haar idee wel geaccepteerd en mede hierdoor is TRILL een IETF standaard geworden in plaats van een IEEE standaard. Indirect kan worden gezegd dat TRILL ontstaan is uit de nadelen die STP met zich meebracht en had de volgende kunnen zijn van in de reeks van STP protocollen.

TRILL maakt gebruik van het beste van twee lagen. TRILL maakt namelijk gebruik van de Data-link laag (Layer 2) en de Netwerk laag(Layer 3). De data-link laag, ook wel bekend als de ethernet laag, hier wordt adressering gedaan door middel van de MAC-adressen. Bij de netwerk laag wordt voornamelijk gebruik gemaakt van het routeren van pakketten door het netwerk door middel van routing protocollen. Zo gebruikt TRILL het IS-IS (Intermediate System-to-Intermadiate System) protocol voor het opstellen en uitwisselen van de Forwarding tabellen om de beste paths naar de switches op basis van de MAC-adressen te kiezen[3].

IS-IS wordt gebruikt omdat de andere routing protocollen gebruik maken van IP-adressen, maar switches hebben geen IP-adressen. IS-IS werkt direct op Layer 2 netwerken, zonder configuratie. Het IS-IS protocol zorgt voor het uitwisselen van Forwarding tabellen van de switches. Hierdoor weet elke Rbridge de verbindingen tussen de alle Rbridges en wat hun locatie is. Door IS-IS kan elke Rbridge het beste path tussen zijn neighbors en elke andere Rbridge berekenen[3].

TRILL maakt gebruik van Rbridges in plaats van de standaard switches, hierbij gaat het voornamelijk over switches die TRILL kunnen implementeren. Verder hebben standaard switches weinig verschil met de gebruikte Rbridges[4][5].

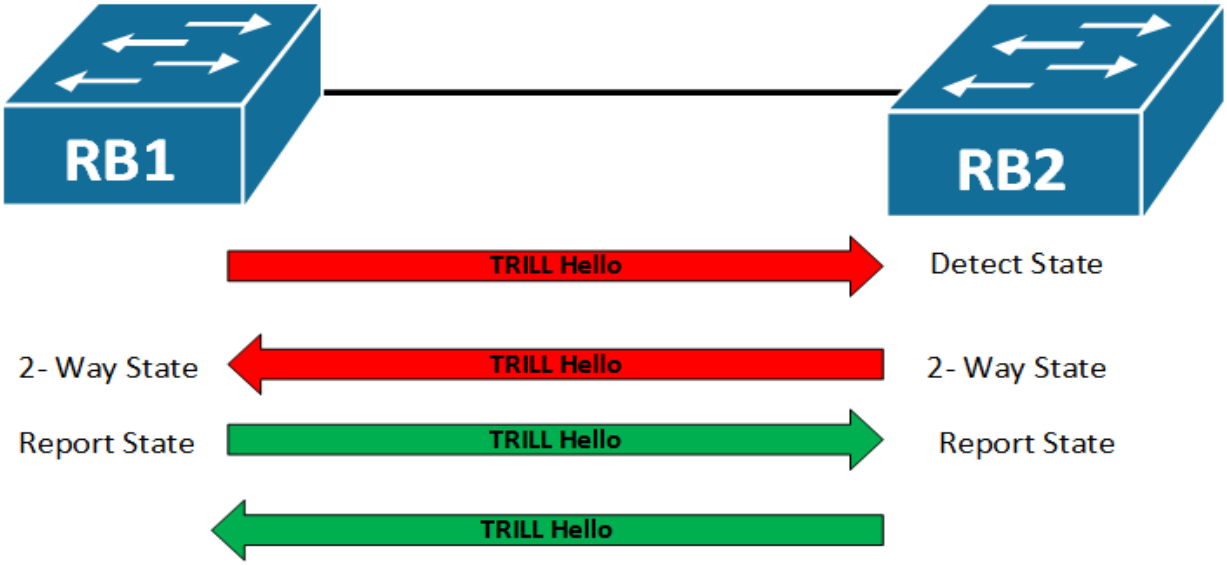
Nu alle algemene informatie duidelijk is wordt nu de werking van TRILL uitgelegd. Ook wordt uitgelegd hoe Rbridges hierbij werken.

6.2 Werking van TRILL

Voordat Rbridges met elkaar kunnen communiceren, moeten Rbridges wel weten wat de waardes zijn van de andere Rbridge. Deze verbinding zullen ze proberen te leggen door middel van het sturen van Hello frames.

Rbridge communicatie

Deze manier van communicatie leggen zal met behulp van het volgende scenario uitgelegd worden:



Figuur 25 Rbridges onderhandeling

TRILL heeft vier staten waarin de Rbridges zich kunnen begeven[4][5][6]:

- Down state
- Detect state
- 2-Way state
- Report state

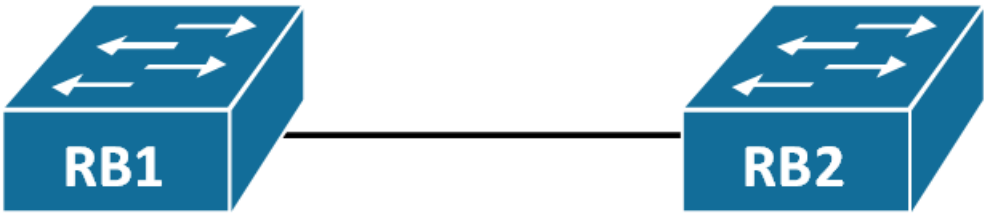
Wanneer RBridges in Down state staan betekent dit dat er geen onderhandeling heeft plaatsgevonden of dat er geen TRILL neighbors zijn. Wanneer de status van de verbinding verandert naar up is zal RB1 een TRILL Hello frame sturen naar RB2. Nadat RB2 het frame heeft ontvangen zal RB2 zichzelf in het Detect state plaatsen. RB2 zal vervolgens een Hello frame terugsturen naar RB1 met daarin wat zijn Nickname is[4][5][6].

"Een Nickname is te vergelijken met het Router-ID dat gebruikt wordt bij OSPF." Bij TRILL is het ook mogelijk om deze Nickname per Rbridge handmatig aan te passen. Als dit niet gedaan wordt, zal de Rbridge een willekeurige Nickname aannemen. Deze Nickname dient uniek te zijn in een broadcast netwerk. Mocht het zo zijn dat er twee Rbridges zijn met dezelfde Nickname, dan zal de Rbridge met het laagste MAC-adres zijn Nickname moeten veranderen."

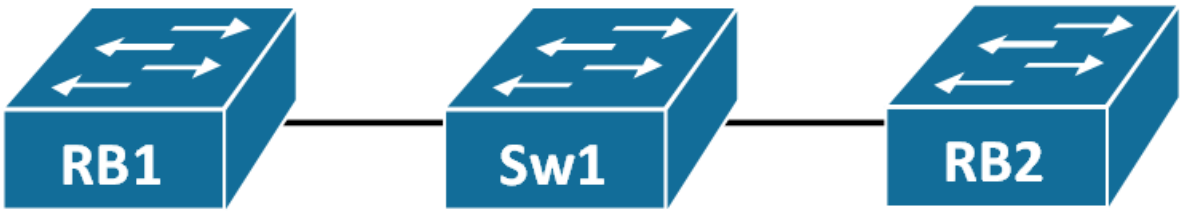
Als RB1 het Hello frame heeft ontvangen zal hij zich in 2-way state plaatsen. In deze state stuurt RB1 een Hello frame terug naar RB2 en verandert daarna zijn state naar de Report state. Op dat moment zullen beide Rbridges zich in de Report state bevinden. Als dit het geval is dan zullen de Rbridges om de 5 seconden Hello frames blijven sturen. Dit is als controle bedoeld om te kijken of de neighbor nog in leven is[4].

Designated Rbridge selecteren
Tijdens het Hello frames uitwisselen in een broadcast implementatie van TRILL, bepaald TRILL welke Rbridge de Designated Rbridge wordt, ook wel afgekort tot DRB[4][5][6]. Deze DRB wordt gekozen op basis van de interface prioriteit. Als deze interface prioriteiten gelijk zijn, zal het MAC-adres van de Rbridges gebruikt worden om te bepalen wie de DRB wordt. Hierbij geldt dat de Rbridge met de laagste waarde de DRB wordt van dit netwerk. Zodra de DRB bepaalt is, zal de DRB een VLAN kiezen die gebruikt zal worden voor onderlinge communicatie tussen de Rbridges. Alle Rbridges zullen deze VLAN gebruiken voor de communicatie onder elkaar. De DRB zal hiernaast ook het aanspreekpunt worden voor de netwerktopologie informatie. Ook kiest de DRB de Appointed Forwarders(AF), hierover wordt verderop meer verteld.

Onderstaande figuren geven voorbeeld van zowel een point-to-point implementatie van TRILL als van een broadcast implementatie van TRILL. Hierbij geld wel dat bij een point-to-point implementatie er geen DRB wordt bepaald. Ook is hier geen sprake van een AF. Dit wordt alleen gedaan in een broadcast omgeving.

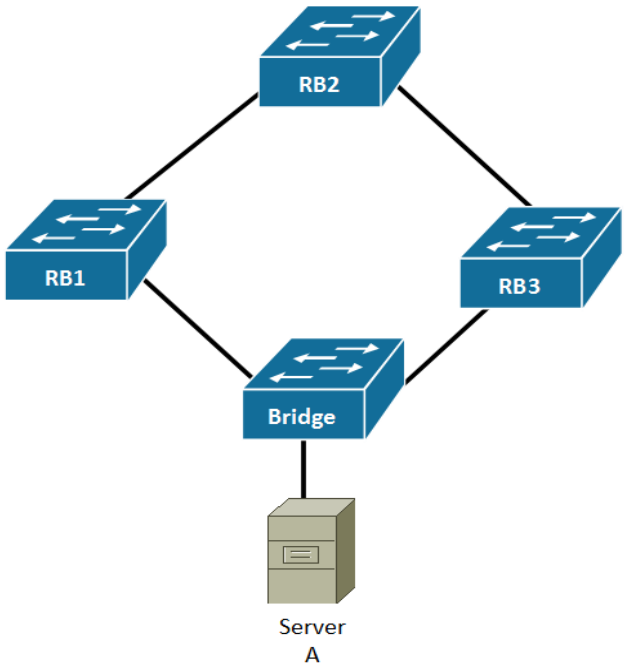


Figuur 26 Point-to-Point TRILL



Figuur 27 Broadcast implementatie TRILL

Het kiezen van een Appointed Forwarder
Een Appointed Forwarder wordt gekozen om een loop in het netwerk te voorkomen, dit wordt gedaan voor een bepaalde VLAN[3][5][7]. Deze situatie zal worden uitgelegd aan de hand van het volgende scenario:



Figuur 28 Appointed Forwarder selecteren

In bovenstaande figuur is een scenario waarbij er drie Rbridges op een Layer 2 bridge zijn aangesloten. Op deze bridge is ook een server aangesloten. In dit netwerk kunnen er loops ontstaan als er een broadcast of een multicast met een onbekende destination wordt gestuurd. Want als de Bridge een broadcast/multicast ontvangt zal hij deze doorsturen naar zowel RB1 als RB3. Deze Rbridges zullen dit frame verwerken en deze opsturen naar de DRB van dit netwerk. Deze DRB zal dit verkeer ontvangen en opsturen naar alle Rbridges in hetzelfde VLAN van het netwerk. Op deze manier komen de frames opnieuw bij RB1 en RB3 terecht. Op dat moment zullen de Rbridges het frame bekijken en zien dat het van hun server afkomt en opnieuw naar de DRB moet. Op deze manier ontstaat er een loop in het netwerk. Om deze loop te verhelpen wordt er een AF aangewezen door de DRB. Deze AF wordt gekozen aan de hand van de interface prioriteit en het MAC-adres van de desbetreffende Rbridge. Wanneer de AF gekozen is, zal alleen deze Rbridge nog de frames ontvangen en doorsturen van een bepaald VLAN. En de andere Rbridges in deze VLAN zullen niet met het ontvangen frame doen.

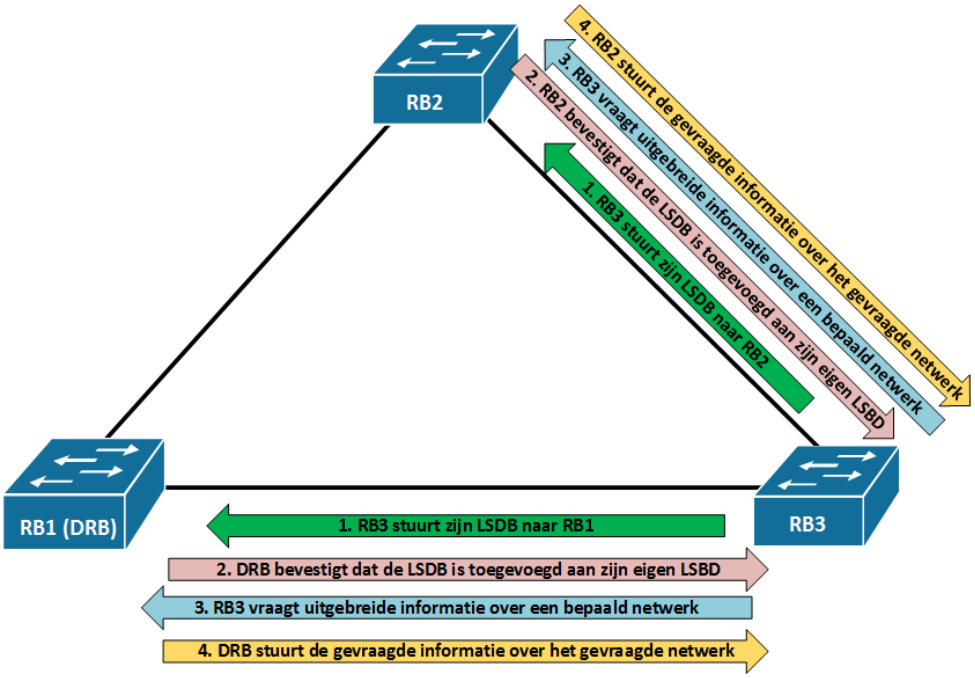
Rbridge database synchronisatie

Als twee Rbridges van elkaar weten waar ze zich bevinden, zullen de Rbridges hun Link State Database (LSDB) naar elkaar opsturen. Dit wordt gedaan aan de hand van het IS-IS protocol. De uitwisseling van de LSDB zorgt ervoor dat elke Rbridge dezelfde Forwarding tabel kan genereren en op deze manier het hele netwerk kent[5][6]. Voor elk soort netwerk verschilt dit. In onderstaande afbeelding is het synchroniseren van een point-to-point verbinding weergegeven:

Figuur 29 LSDB uitwisseling Point-to-point

Als eerste stuurt RB1 zijn LSDB naar RB2, hieruit zal RB2 een netwerk selecteren waarvan die geen informatie heeft. Als tweede zal RB2 een verzoek indienen van het netwerk waarvan hij onvoldoende informatie heeft. Als laatste zal RB1 op het verzoek van RB2 reageren en de gevraagde informatie van het desbetreffende netwerk sturen. Deze synchronisatie zal zich blijven herhalen tot er in het netwerk elke Rbridge hetzelfde LSDB heeft.

In onderstaand figuur wordt een scenario gegeven waarin de LSDB wordt uitgewisseld bij het toevoegen van een nieuwe Rbridge (RB3).

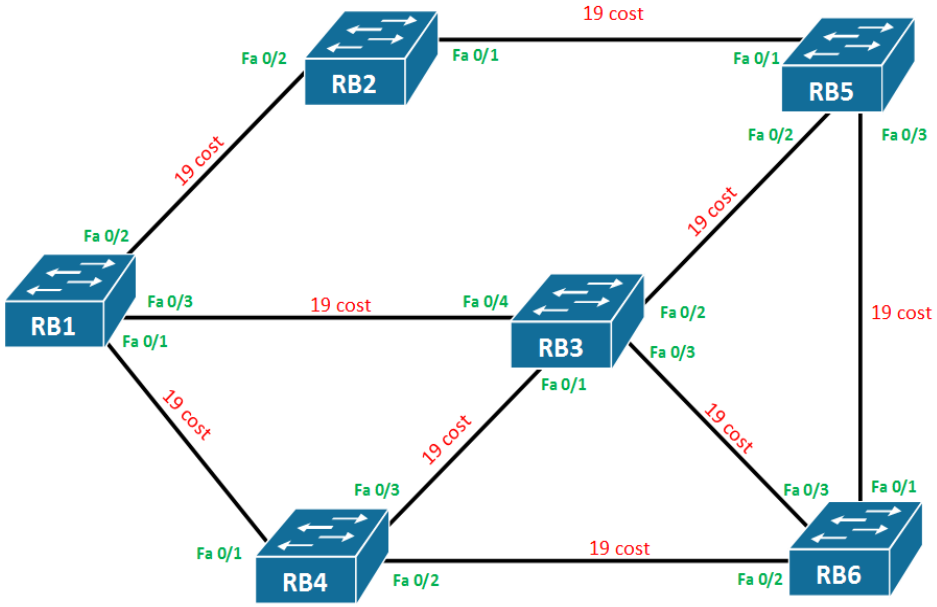


Figuur 30 Uitwisseling LSDB broadcast netwerk

Net als bij het uitwisselen van de LSDB bij een Point-to-Point verbinding zal de nieuwe Rbridge zijn LSDB sturen naar zijn neighbor bridges. Echter zal in dit geval alleen de Designated Rbridge reageren op het LSDB frame van de nieuwe Rbridge. De Designated Rbridge, hierin RB1, zal naar de nieuwe Rbridge (RB3) verkeer sturen waarin hij meedeelt dat hij de LSDB van RB3 heeft toegevoegd. Hierna zal RB3 kijken van welk netwerk hij nog onvoldoende informatie heeft. Dit frame wordt opnieuw naar alle neighbor bridges gestuurd. Alle bridges zullen op dit frame antwoord geven door middel van het sturen van de gevraagde informatie van het desbetreffende netwerk. Deze synchronisatie blijft zich herhalen tot dat elke Rbridge in het netwerk hetzelfde LSDB heeft. Elke keer als een nieuwe Rbridge wordt toegevoegd zal dit scenario zich herhalen[5][6].

Beste path selectie

Nadat alle Rbridges de LSDB tabellen hebben uitgewisseld beschikt dus iedere Rbridge over een volledige LSDB[3][4][5]. Aan de hand van deze LSDB kan het beste path gekozen worden. Dit wordt uitgelegd aan de hand van het volgende netwerk:



Figuur 31 Path selectie

Aan de hand van figuur 7 kunnen de volgende LSDB tabellen worden gehaald. Hierbij worden niet alle waardes weergegeven die in deze LSDB staan, alleen de waardes die voor dit onderzoek belangrijk zijn.

Tabel 1 LSDB tabel

Link State Database van alle Rbridges uit bovenstaand netwerk																	
RB1			RB2			RB3			RB4			RB5			RB6		
NN	Int	Cost	NN	Int	Cost	BNN	Int	Cost	NN	Int	Cost	NN	Int	Cost	NN	Int	Cost
RB2	Fa0/2	19	RB1	Fa0/2	19	RB1	Fa0/4	19	RB1	Fa0/1	19	RB2	Fa0/1	19	RB4	Fa0/2	19
RB3	Fa0/3	19	RB5	Fa0/1	19	RB4	Fa0/1	19	RB3	Fa0/3	19	RB3	Fa0/2	19	RB5	Fa0/1	19
RB4	Fa0/1	19				RB5	Fa0/2	19	RB6	Fa0/2	19	RB6	Fa0/3	19	RB3	Fa0/3	19
						RB6	Fa0/3	19									
NN = Nickname																	
Int = Interface																	

De LSDB tabel helpt de Rbridges om het beste path naar andere Rbridges te bepalen. Voor het bepalen van dit path zullen de Rbridges gebruik maken van het Shortest Path First(SPF) algoritme[3][5][6]. Ook het SPF algoritme is onderdeel van het IS-IS protocol. Door gebruik te maken van het SPF algoritme zullen alle RBridges instaat zijn om het beste path naar elk Rbridge te berekenen. Vervolgens zullen deze paths opgeslagen worden in de TRILL routing tabel van de Rbridges. In onderstaande tabel wordt hier een voorbeeld van gegeven.

Tabel 2 TRILL routing tabel

TRILL Routing Tabel van RB1		
Source	**Destination**	**Via Interface**
RB1	**RB2**	**Fa0/2**
RB1	**RB3**	**Fa0/3**
RB1	**RB4**	**Fa0/1**
RB1	**RB5**	**Fa0/2 & Fa0/3**
RB1	**RB6**	**Fa0/1 & Fa0/3**

In bovenstaande tabel worden het beste path van RB1 gegeven. De beste waarde wordt bepaald aan de hand van de cost van het path[3,5]. Zo is het beste path van RB1 naar RB2 op de volgende manieren te verwezenlijken, met de bijbehorende kosten.

- Route 1: RB1 → RB2 = 19 Cost
- Route 2: RB1 → RB3 → RB5 → RB2 = 57 cost
- Route 3: RB1 → RB3 → RB6 → RB5 → RB2 = 76 Cost
- Route 4: RB1 → RB4 → RB3 → RB5 → RB2 = 76 Cost
- Route 5: RB1 → RB4 → RB6 → RB5 → RB2 = 76 Cost
- Route 6: RB1 → RB4 → RB3 → RB6 → RB5 → RB2 = 95 Cost
- Route 7: RB1 → RB3 → RB4 → RB6 → RB5 → RB2 = 95 Cost

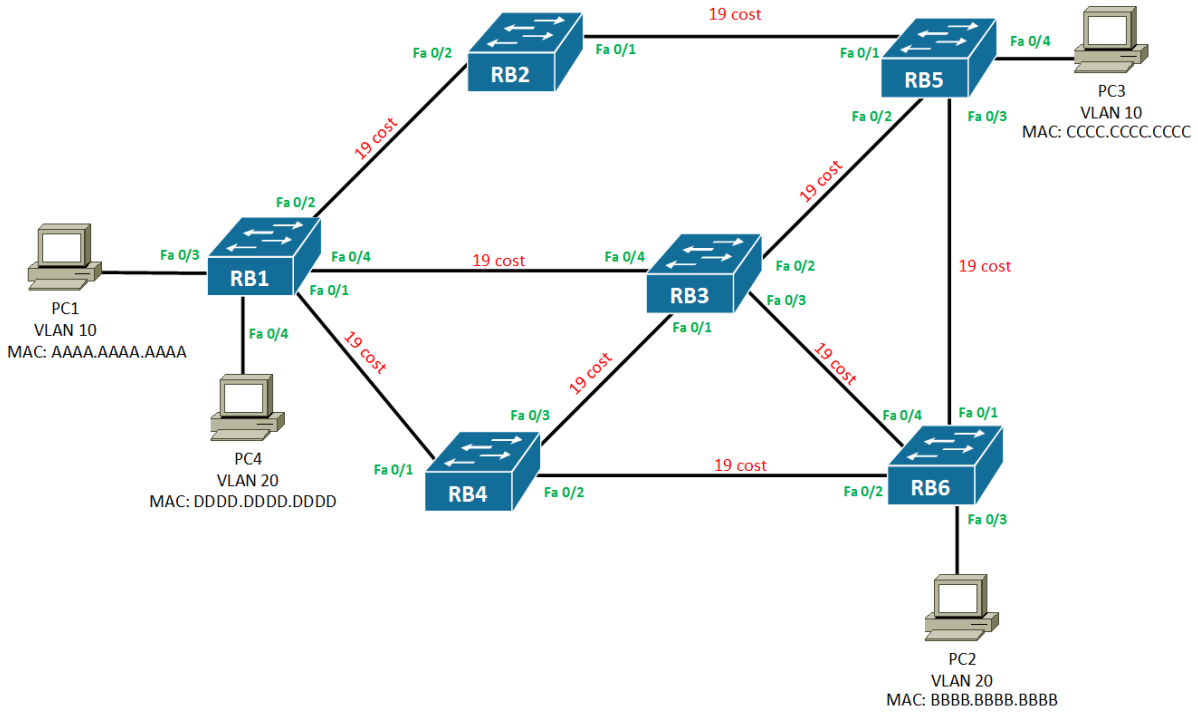
Omdat path 1 de laagste Path Cost heeft zal SPF dit path kiezen als de beste optie. Dit path zal in de TRILL routing tabel geplaatst worden[3][5]. Dit path zal nu gebruikt worden als RB1 verkeer naar RB2 wil sturen. Als de beste paths voor alle Rbridges zijn berekend, dan weet elke Rbridge hoe hij verkeer beste naar een andere Rbridge kan sturen. In tabel 2, een TRILL routing tabel, is te zien dat het path naar RB5 en naar RB6 twee interfaces heeft. Wanneer twee paths dezelfde Cost hebben zullen beide interfaces in de TRILL tabel worden opgenomen. Dit zorgt ervoor dat het verkeer verdeeld kan worden over meerdere paths. Dit is onder TRILL ook wel bekend als Equal Cost Multipath (ECMP). Zo zal het bij het path van RB1 naar RB5 en naar RB6 ECMP toegepast worden[3][5].

Rbridge communicatie tabellen

In een TRILL netwerk zijn er twee soorten Rbridges te onderscheiden. De eerste soort Rbridge zit aan een End node aangesloten en wordt ook wel een Edge Rbridge genoemd. De tweede soort zijn de Rbridges die zich tussen de Edge Rbridges bevinden, deze Rbridges worden de Core Rbridges genoemd. Op de Edge Rbridges wordt naast de routing tabel ook een TRILL MAC tabel bijgehouden. In deze tabel wordt de volgende informatie bijgehouden[5]:

- Local End Node informatie; Dit is een End node die aan de switch zelf zit aangesloten.
  - VLAN
  - MAC-adres
  - Lokale Interface port
- Remote End Node informatie; Dit is een End node die aan een andere switch zit aangesloten.
  - VLAN
  - MAC-adres
  - Nickname van destination Rbridges.

Deze informatie kan op twee manier verkregen worden. De eerste manier is de traditionele manier, bij deze manier wordt er gebruik gemaakt van de ontvangen frames. Aan de hand van deze frames kan de TRILL MAC-tabel gevuld worden met de bovenstaande informatie. Het volgende scenario zal gebruikt worden om een voorbeeld te geven van een TRILL MAC-tabel.



Figuur 32 TRILL MAC-tabel scenario

Als een End node, of in bovenstaand geval, een PC aangesloten wordt op een switch/Rbridge zullen deze proberen verbinding te maken. Tijdens dit proces zal de Rbridge, in dit geval, de frames gebruiken om zijn TRILL MAC-tabel te vullen met de juiste informatie. Zo zullen de Rbridges RB1, RB5 en RB6 in bovenstaand scenario een TRILL MAC-tabel bijhouden met de informatie van de PCs.

Een voorbeeld van een TRILL MAC-tabel wordt in onderstaande tabel weergegeven.

Tabel 3 TRILL MAC-tabel RB1

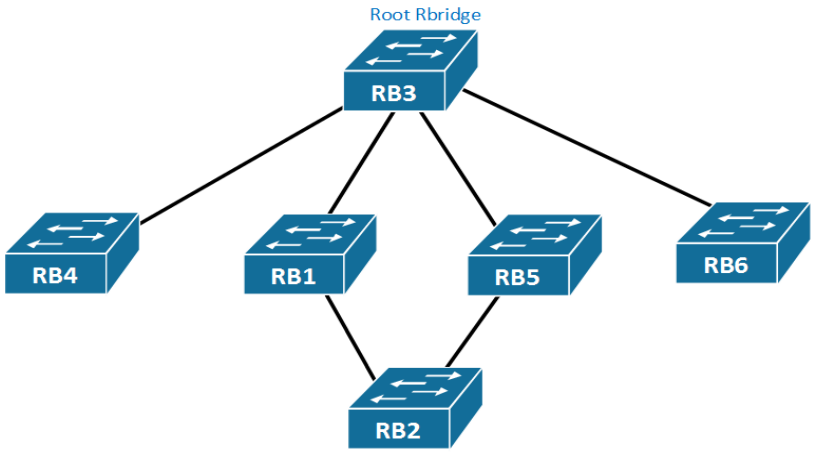
TRILL MAC Tabel RB1				
End Node	**MAC adres**	**VLAN**	**Interface**	**Destination Rbridge**
PC 1	**AAAA.AAAA.AAAA**	**10**	**F0/3**	
PC 4	**DDDD.DDDD.DDDD**	**20**	**F0/4**	
PC 2	**BBBB.BBBB.BBBB**	**20**		**RB5**
PC 3	**CCCC.CCCC.CCCC**	**10**		**RB6**

Edge Rbridges zullen standaard hun MAC-tabel om de 5 minuten legen en opnieuw vullen[5].Dit is om ervoor te zorgen dat er geen black hole ontstaat in het netwerk. Een black hole ontstaat als er data verstuurd wordt uit een verbinding waar een End node zich bevond maar zich daar niet meer bevindt.

Naast de traditionele manier die hierboven is uitgelegd is het ook mogelijk om de TRILL MAC-tabel te vullen met het ESADI protocol. Het ESADI is een optionele manier om de TRILL MAC-tabel bij te werken[5]. ESADI staat voor End Station Address Distribution Information. Dit is een protocol die informatie over End Nodes doorgeeft aan andere Edge Rbridges in het netwerk. Een update zal plaatsvinden als er een End Node aangesloten wordt of verplaatst wordt. Op deze manier zorgt ESADI ervoor dat de TRILL MAC-tabel up-to-date blijft en betrouwbaar blijft. Hierdoor zal er ook geen onnodige data verstuurd worden naar een Rbridge waar geen End node zich meer bevindt. Bij het ESADI protocol zal de TRILL MAC-tabel niet geleegd worden, dit omdat ESADI de tabel up-to-date houdt en dus het legen en opnieuw vullen overbodig wordt.

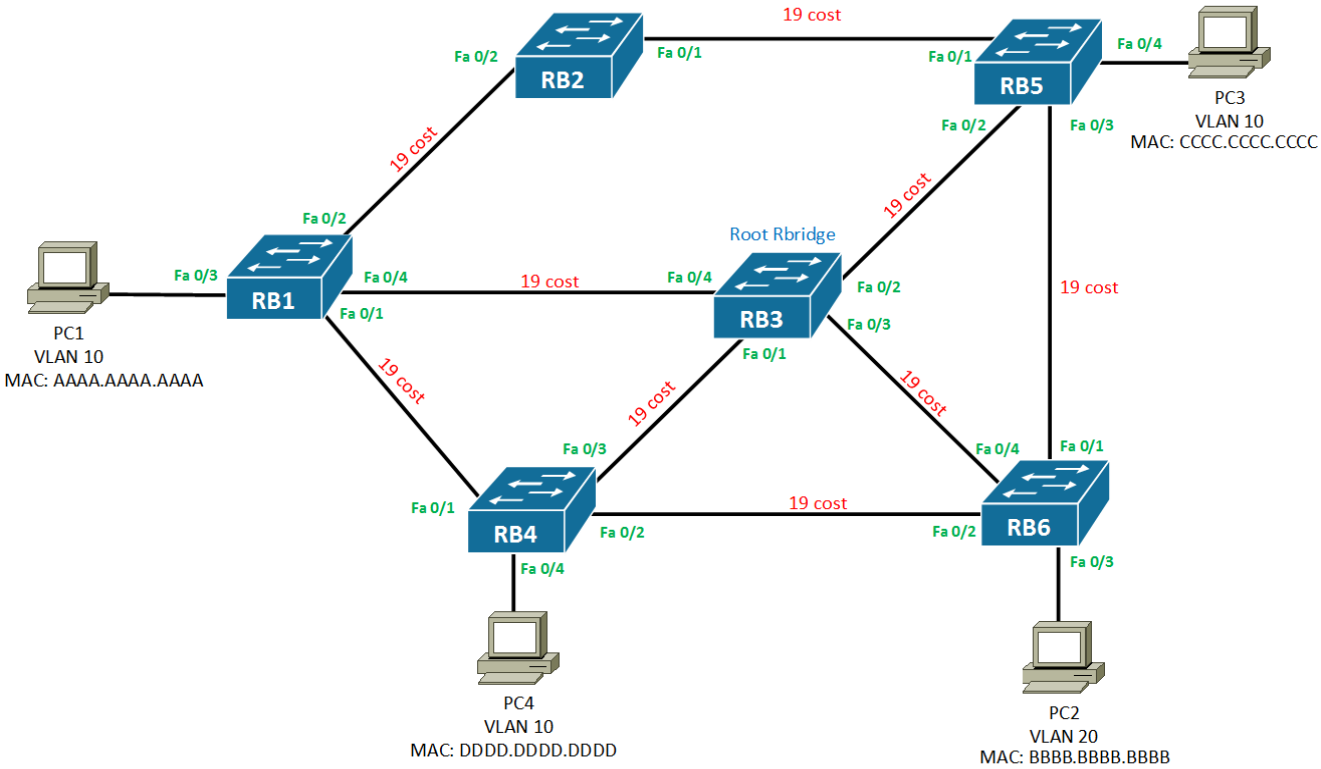
Naast de TRILL MAC-tabel hebben de Rbridges ook een Multi-destination routing tabel nodig[5].Deze tabel wordt gebruikt wanneer een broadcast, multicast of een verkeer met een onbekende destination verstuurd moet worden. Als er gebruik gemaakt wordt van het ESADI protocol, zal de tabel niet gebruikt worden voor onbekende destinations verkeer. Dit komt doordat alle Edge Rbridges al weten waar alle End Nodes zich bevinden in het netwerk.

Voor het versturen van een multicast, broadcast of een verkeer met een onbekende destination maakt TRILL gebruik van Distribution Trees[3][5][6].Om een Distribution Tree te maken moet er een Root Rbridge worden aangewezen. De Root Rbridge wordt gekozen tijdens het onderhandeling proces van TRILL. Hierbij wordt de Rbridge met de hoogste Root prioriteit gekozen. Als het geval zo is dat er meerdere Rbridges dezelfde Root prioriteit heeft, dan zal de Rbridge met het laagste MAC-adres de Root Rbridge worden. Zo een Distribution Tree ziet er als volgt uit; hierbij is RB3 gekozen als Root Rbridge



Figuur 33 Distribution Tree

De Root Rbridge zal met behulp van het SPF algoritme bepalen hoe alle andere Rbridges het best te bereiken zijn, wat is het beste path naar deze Rbridges. In een LSDB update zal worden aangegeven dat de Root Rbridge de destination wordt voor het versturen van broadcast, multicast en verkeer met onbekende destination. Daarnaast kan een Root Rbridge meerdere Distribution Trees maken en delen met het netwerk. Als deze Distribution Trees aangemaakt zijn, kan er gebruik gemaakt worden van ECMP bij het verzenden van broadcast, multicast en onbekende destination verkeer. Om dit proces wat te verduidelijken zal het volgende scenario geschetst worden.



Figuur 34 Multi-destination scenario

In bovenstaande afbeelding is te zien dat RB3 als Root Rbridge gekozen is. Zoals ook hierboven is uitgelegd zal deze Rbridge het beste paths berekenen naar alle andere Rbridges. RB3 zal zichzelf ook aangeven als Root Rbridge voor de Distribution Tree. Alle andere Rbridges zullen nu RB3 in hun Multi-destination tabel opnemen als destination voor de broadcast en multicast verkeer. De tabel hieronder is een voorbeeld van deze tabel.

Tabel 4 Multi-destination routing tabel

Multi-destination routing tabel					
End node	**Destination MAC adres**	**VLAN**	**Interface**	**Distribution tree**	**Destination Rbridge**
PC 1	**FFFF.FFFF.FFFF**	**10**	**F0/4**	**Tree 1**	**RB3**

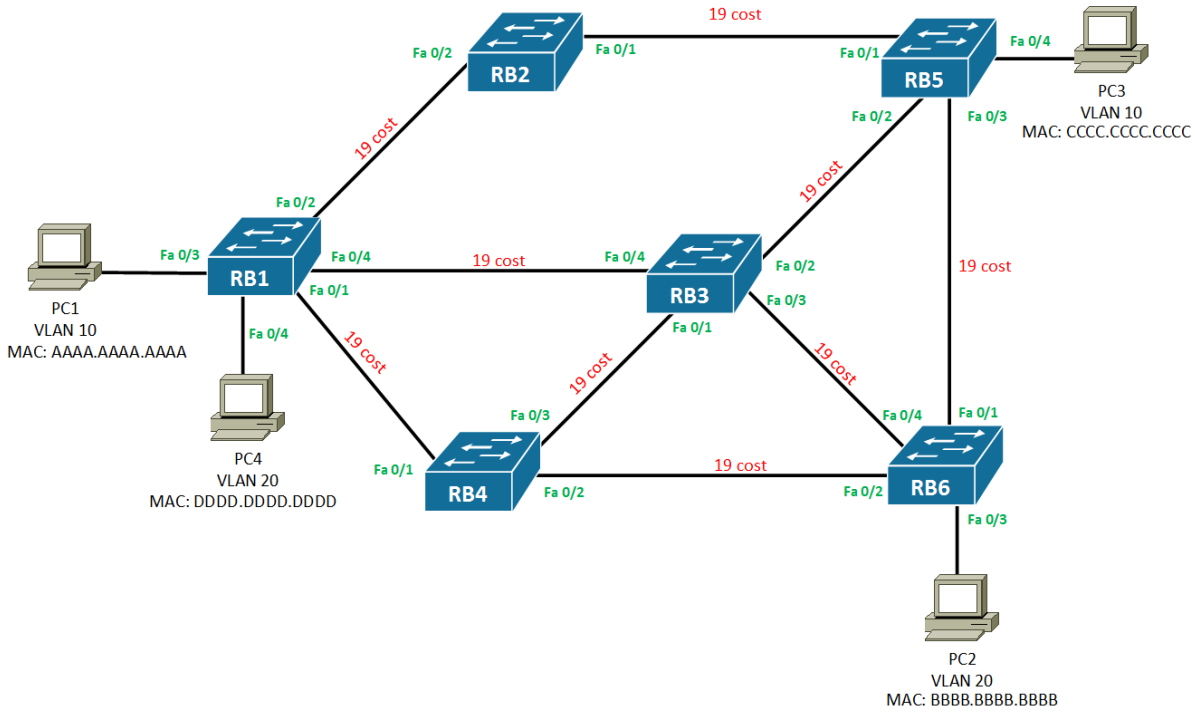
Als PC1 een broadcast frame wil sturen naar alle PCs die op VLAN 10 met elkaar communiceren, dan zal PC1 het verkeer als een broadcast frame markeren en opsturen naar RB1. RB1 zal zien dat het frame als een broadcast is gemarkeerd en hij zal dit frame dan opsturen naar RB3. Dit omdat RB3 in de tabel staat als destination bij een broadcast of multicast frame.

RB3 zal dit frame doorsturen naar alle Rbridges die communiceren over VLAN 10 [3][5][6].In bovenstaand scenario geldt dit voor RB4 en RB5. Het verkeer zal niet naar alle andere Rbridges gestuurd worden. Zo zal het frame niet naar RB6 gestuurd worden omdat deze op VLAN 20 communiceert. Alle Rbridges in het netwerk weten van elkaar welke VLANs op het netwerk geconfigureerd zijn. Dit is een van de waardes die tijdens het uitwisselen van LSDB tabellen wordt meegegeven.

Data communicatie tussen end nodes
Nu duidelijk is gemaakt hoe het proces van TRILL werkt zal er beschreven worden hoe de verschillende typen data frames verwerkt worden door TRILL RBridges[3][5][6].

De verschillende typen data frames zijn de volgende:
- Unicast data verkeer;
- Onbekend unicast, multicast en broadcast data frames;

Unicast
Voor de toelichting van het unicast dataframe zal er gebruik gemaakt worden van het onderstaande scenario.

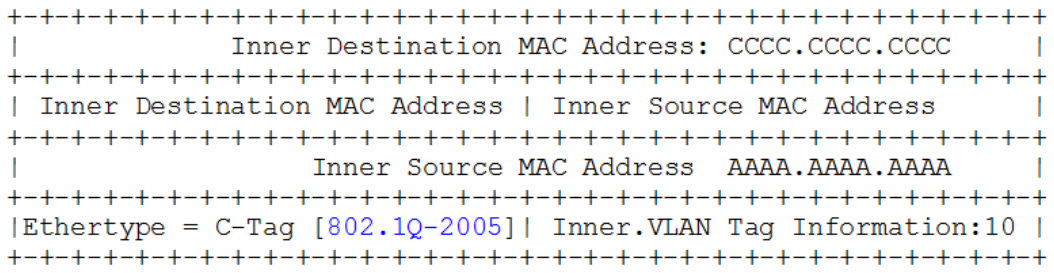


Figuur 35 Unicast End Node communicatie

In dit scenario zal het de bedoeling worden dat de TRILL tabel, de MAC-tabel en multicast tabel uitgewisseld en up-to-date zijn [3][5][6].

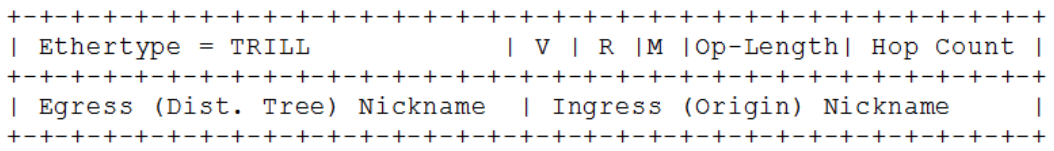
In deze paragraaf wordt er toegelicht hoe de frames verwerkt worden door TRILL op de Rbridges wanneer datacommunicatie plaatsvindt tussen PC1 en PC3. Als PC1 data wilt uitwisselen met PC3 dan zal PC1 eerst een frame opsturen naar RB1. In dit ethernet frame wordt het source MAC-adres en het destination MAC-adres gegeven.

Een voorbeeld van dit frame is hieronder te zien.



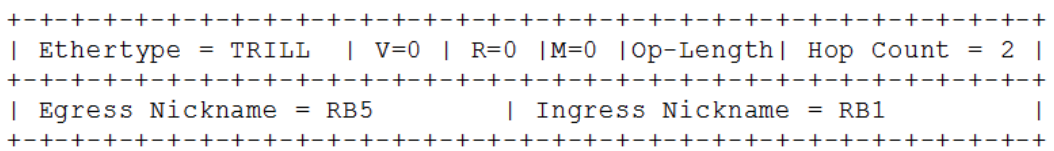
Figuur 36 Inner Ethernet Header (bewerkte afbeelding) [5]

Wanneer RB1 dit frame ontvangt zal er gekeken worden naar het destination MAC-adres en zal RB1 aan dit frame een TRILL header plakken. Een TRILL header ziet er als volgt uit:



Figuur 37 TRILL header

Zoals te zien is in bovenstaande afbeelding, bestaat een TRILL header uit 8 velden. Met het TRILL Ethertype wordt aangegeven wat voor type frame het is. TRILL type wordt ook wel aangegeven met 0x22F3. Dit geeft dan aan dat het een TRILL frame is. Daarnaast bevindt zich een V veld. In dit veld wordt aangegeven welke versie van TRILL wordt gebruikt. Het veld daarnaast, Veld R, is gereserveerd voor toekomstige toevoegingen. Deze beide velden hebben een standaard van 0[5].Met het M-veld wordt er aangegeven of het gaat om een multicast/broadcast verkeer. Bij een waarde van 1 zal de Rbridge weten dat dit een multicast/broadcast frame is en zal dit frame naar de Root Rbridge sturen. De Root Rbridge zal dan het frame weer doorsturen naar de juiste Rbridges. Als de waarde van het M-veld 0 is, zal het om een unicast frame gaan. Het Op-length veld geeft aan hoe groot de TRILL header is. Het Hop count veld geeft aan hoeveel hops het frame mag nemen voordat het bij zijn destination Rbridge aankomt. Wanneer het Hop count veld 0 wordt, zal het frame gedropt worden door de ontvangen Rbridge. Dit zorgt ervoor dat het frame niet oneindig in het netwerk blijft loopen. Naast deze velden heeft de TRILL header ook nog de Egress en Ingress velden. In het Egress veld wordt de Nickname van het destination Rbridge genoteerd. En bij het Ingress veld wordt de Nickname van de source Rbridge opgenomen. Een TRILL header die ingevuld is na aanleiding van bovenstaande topologie is hieronder weergegeven.

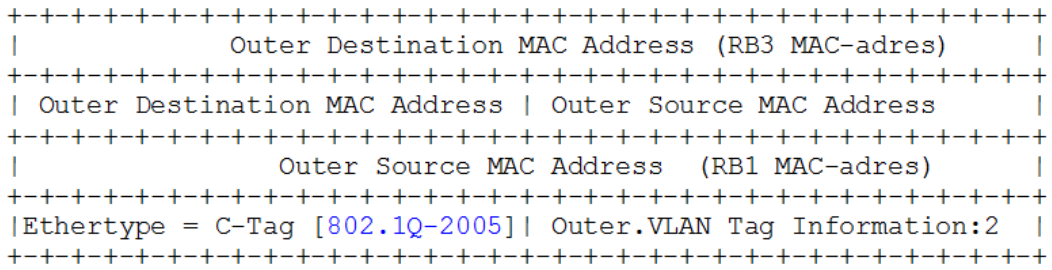


Figuur 38 TRILL header gevuld (bewerkte afbeelding)[5]

Hierbij wordt M op 0 gezet omdat, in dit geval het gaat om een unicast frame. Het veld van de Hop count is op 2 gezet omdat het frame dan al aangekomen moet zijn bij RB5.

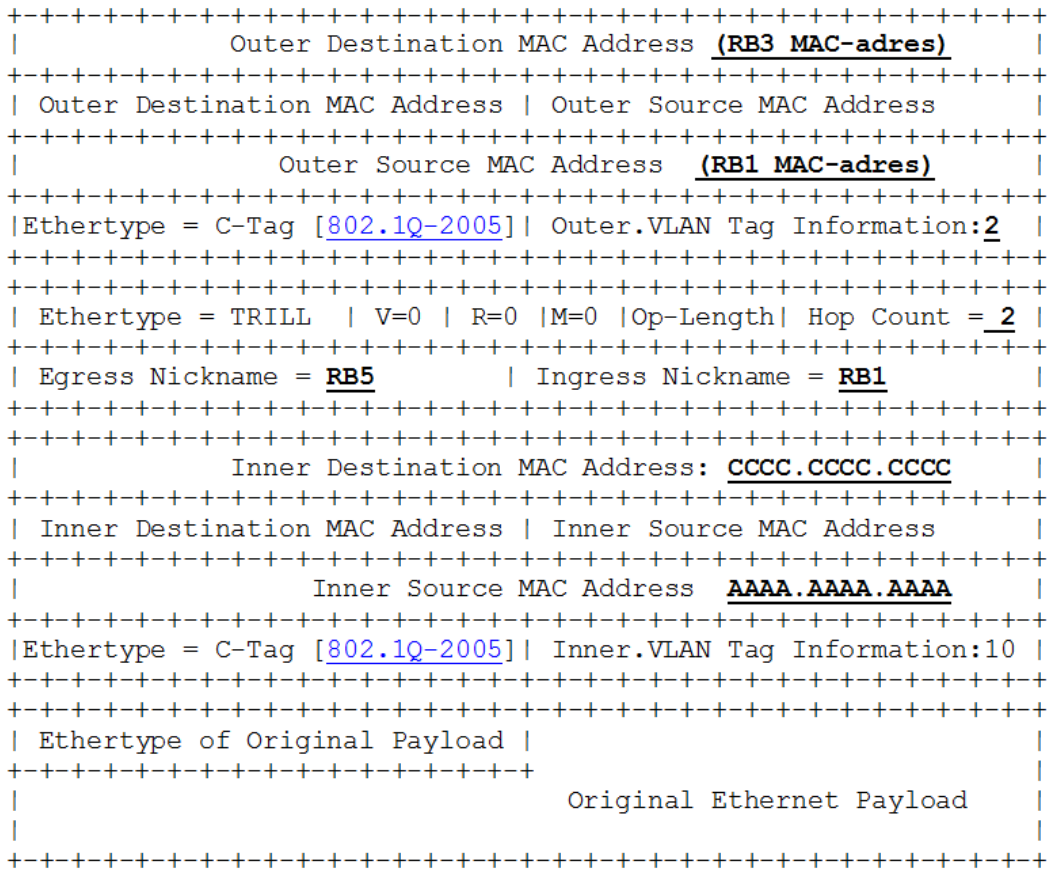
Nu de TRILL header gekoppeld is aan het frame zal RB1 een Outer Ethernet Header aan het frame koppelen[5].In het Outer Ethernet Header wordt het source Rbridge MAC-adres en het next hop Rbridge MAC-adres verwerkt. Om te achterhalen wat de next hop is, zal er gebruikt gemaakt worden van de TRILL routing tabel. Hiernaast wordt er een TRILL communicatie VLAN aangegeven. In een TRILL broadcast netwerk wordt deze VLAN bepaald door de DRB. In een P2P wordt er onderling gehandeld welke VLAN hiervoor het beste geschikt is. De VLAN van de Rbridge met de hoogste interface prioriteit zal gebruikt worden als Designated VLAN. Als echter de interface prioriteit geen doorslag geeft, zal er gekeken worden naar het laagste MAC-adres.

Hieronder is een voorbeeld weergegeven van een Outer Ethernet Header.



Figuur 39 Outer Ethernet Header (bewerkte afbeelding) [5]

Nu dat de Outer Ethernet Header ook aan het frame is toegevoegd, zal het frame opgestuurd worden naar RB3. Hieronder wordt het geheel van het frame weergegeven.

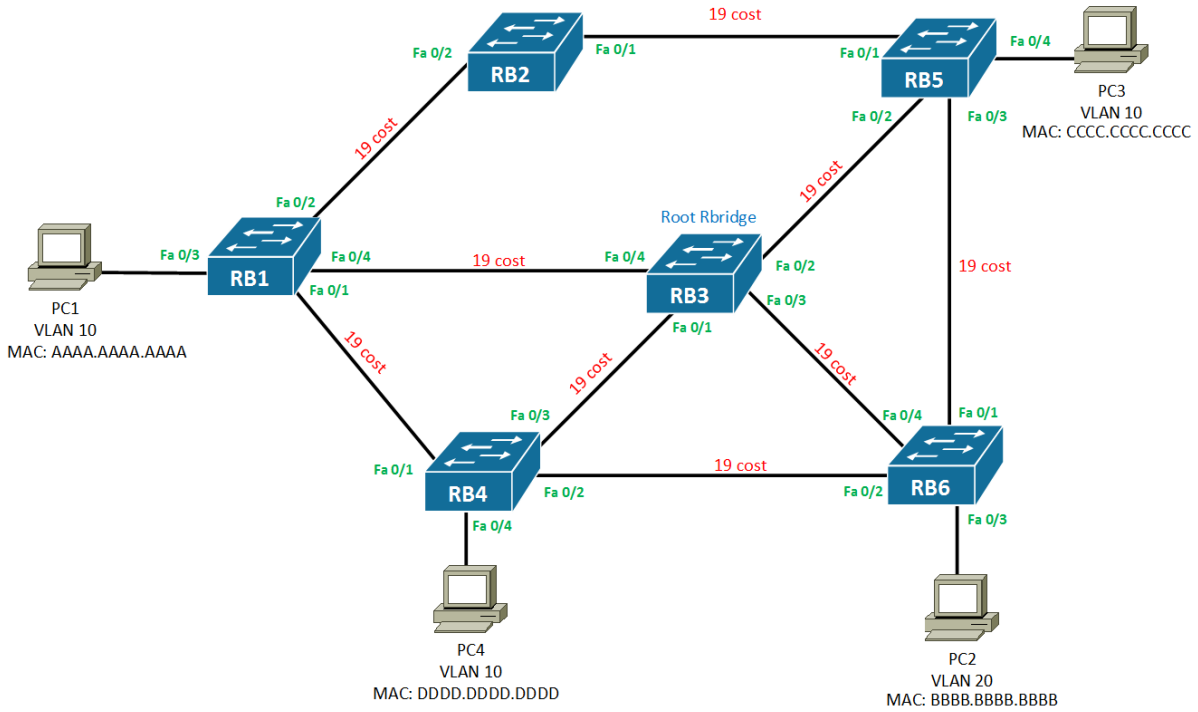


Figuur 40 TRILL frame (bewerkte afbeelding) [5]

RB3 zal dit frame ontvangen en de Outer Ethernet Header van het frame halen. Verder zal hij de Hop count verlagen naar 1. Aangezien de Egress Nickname RB5 is en niet RB3, zal RB3 een nieuwe Outer Header op het frame plakken met zijn MAC-adres als source. Nadat RB3 de nieuwe header heeft toegevoegd aan het frame, zal het frame worden doorgestuurd naar RB5. Vervolgens zal RB5 de Outer Header eraf halen en daarna ook de TRILL header. Dit komt omdat het Egress Nickname hetzelfde is als de Nickname van RB5. In de Inner header zal RB5 zien dat het frame bedoeld is voor MAC-adres CCCC. CCCC. CCCC. Aan de hand van deze informatie zal RB5 het frame doorsturen naar PC3.

Multicast

Nu er behandeld is hoe TRILL unicast frames afhandelt, zal er nu toegelicht worden hoe TRILL omgaat met broadcast, multicast en verkeer met een onbekende destination. Hiervoor zal gebruikt worden van het volgende scenario.



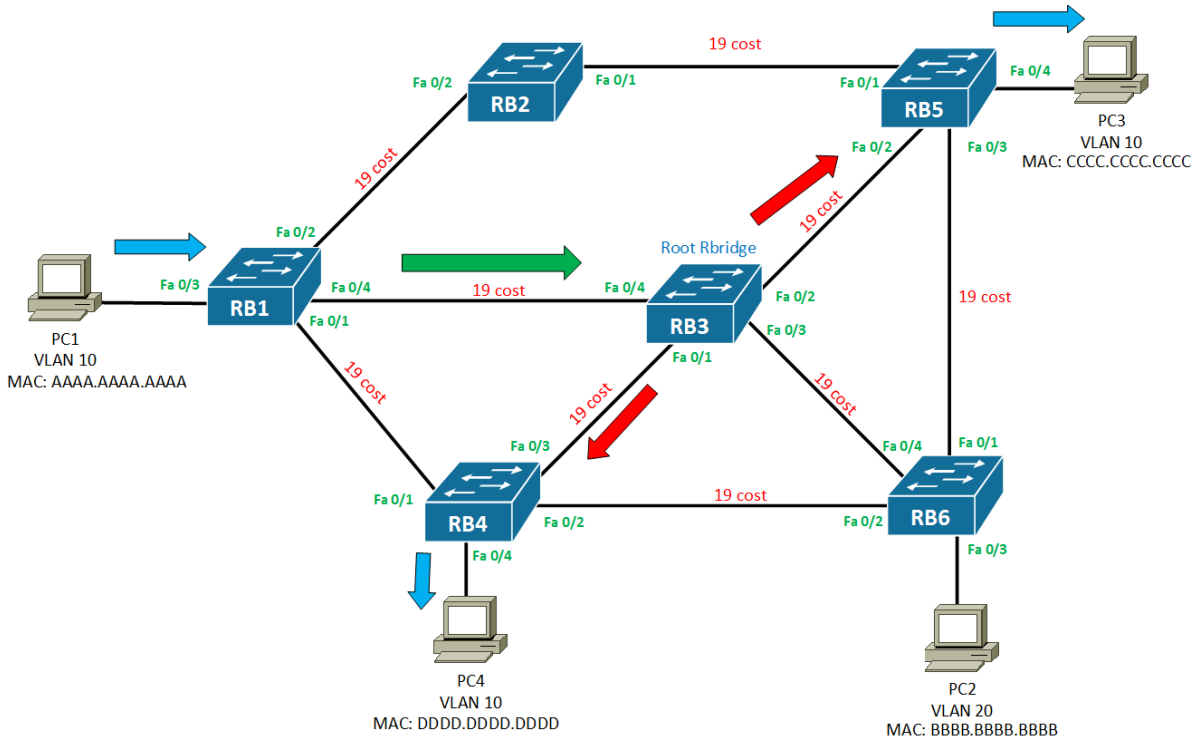
Figuur 41 Multicast communicatie

Bij het versturen van een multicast/broadcast of een onbekend unicast frame is een root Rbridge nodig. Daarom is in dit scenario gekozen voor RB3 als Root Rbridge. Als PC1 een multicast/broadcast wil sturen naar alle andere PCs in het netwerk van VLAN 10, dan zal hiervoor een ethernet frame worden aangemaakt. In dit frame worden de source MAC-adres en het destination MAC-adres van het frame meegegeven. RB1 zal het frame ontvangen en zal aan de hand van het destination MAC-adres zien dat het hierbij gaat om een multicast/broadcast frame. RB1 zal de TRILL header aan het frame plakken en zal het M bit op 1 zetten. Dit geeft aan dat het frame een multicast/broadcast verkeer is. In de TRILL header zal RB3 als Egress Nickname worden ingevuld. Als laatste zal RB1 de Outer Ethernet Header toevoegen en het frame naar RB3 sturen.

RB3 zal het frame ontvangen en de Outer Header eraf halen. In de TRILL header kan RB3 zien dat het frame voor hem bedoelt is als Root Rbridge. Ook ziet RB3 dat het frame verder gemulticast/ gebroadcast moet worden. Nu zal RB3 Reverse Path Forwarding (RPF) controle uitvoeren. Deze controle is om loops te voorkomen waarbij gecontroleerd wordt of het frame ontvangen is via de juiste interface. Voor deze controle wordt de Multi-destination tabel van RB3 gebruikt. Hierin staat welke Rbridge frames ontvangen mag via welke interface.

Als dit frame via de verkeerde interface binnenkomt, zal RB3 het frame droppen. RB3 zal de TRILL header van het frame loskoppelen van het frame. Vervolgens zal RB3 verschillende kopieën maken van het ethernet frame. RB3 zal aan het frame een nieuwe TRILL header en Outer header toevoegen. De source en destination Nickname van de frames zullen verschillen van elkaar. Dit omdat deze frames naar verschillende Rbridges gezonden zullen worden. Het is wel het geval dat deze frames alleen naar Rbridges worden gestuurd die VLAN 10 gebruiken om te communiceren.

In dit scenario geldt dat voor RB4 en RB5. Deze Rbridges zullen het frame ontvangen en vervolgens de Outer header en de TRILL header los halen van het frame. Na het controleren van het destination MAC-adres zullen RB4 en RB5 uit alle actieve poorten van VLAN 10 het frame versturen. Zie onderstaande figuur voor een voorbeeld van dit multicast frames uitwisselen.



	Frames van en naar End Nodes
	Frames naar Root Rbridge
	Frames naar AF Rbridge van VLAN 10

Figuur 42 Proces Multicast frame VLAN 10

6.3 Varianten van TRILL

TRILL is een open standaard dat door sommige fabrikanten gebruikt is om een eigen versie te ontwikkelen. Drie relevante voorbeelden van deze varianten zijn VCS van Brocade, FabricPath van Cisco en SPB van Alcatel. Hieronder zullen deze varianten kort besproken worden en worden de overeenkomsten met TRILL gegeven. De verschillen worden in een volgend hoofdstuk behandeld.

Deze varianten zijn relevant voor Qi ict bv. om de volgende reden: de apparatuur fabrikant. Zo werkt Qi ict bv. al jaren met deze fabrikanten. Brocade, Cisco en Alcatel zijn dan ook de fabrikanten die een groot deel van het netwerk circuit beheersen. Daarnaast draait alles om de werking van de protocollen, hierbij zijn redundantie en loops voorkomen de hoofdzaken. Doordat dit al de bedoeling is van TRILL, zullen ook de varianten dit als doelstelling hebben.

6.3.1 Brocade Virtual Cluster Switching

Virtual Cluster Switching, of afgekort VCS, is de Brocade proprietary van TRILL[15][16]. Brocade ondersteunt ook de standaard TRILL, maar heeft daarnaast nog gekozen voor een uitbreiding voor op de VDx switches. Toch houden VCS en TRILL er veel overeenkomsten op na:

Ontstaan uit het elimineren van STP
Het meest voor de hand liggende overeenkomst is dat VCS ontstaan is uit het idee dat STP uit switched core netwerken moet worden geëlimineerd. Hierbij zorgt VCS ook voor het gebruik van de hele bandbreedte in plaats van het blokkeren van verbindingen[15][16].

Snelle omschakeling bij een down verbinding
De snelle omschakeling is één van de hoofdredenen waarom een TRILL variant boven STP wordt gekozen. Zelfs bij RSTP is de omschakelingstijd hoger als bij TRILL. Zo heeft FabricPath een omschakelingstijd van ~500ms [15]terwijl RSTP een aantal seconden nodig heeft[2].

Het gebruik van een Distribution Tree
Dit is het geval bij Broadcast/Multicast/frames met onbekende destination. Hierbij zal een Root worden aangewezen en hieruit een Distribution Tree gevormd worden om op deze manier een loop te voorkomen[15][16].

Gebruik van Equal Cost Multipathing (ECMP)
Het is de bedoeling dat VCS in tegenstelling tot STP al zijn verbindingen gebruikt. Hierbij wordt de volle bandbreedte beschikbaar en kunnen op deze manier frames verstuurd worden via meerdere paths om bij de destination te komen. Hiervoor wordt het ECMP protocol gebruikt[15][16].

Plug & Play configuratie
Als er een switch wordt toegevoegd aan het netwerk, dan zal VCS alles binnen het netwerk regelen. Er is dus geen configuratie nodig[15][16].

6.3.2 Cisco FabricPath

FabricPath (FP) is de Cisco proprietary versie van TRILL[11][14].Cisco ondersteunt ook standaard TRILL, maar heft ervoor gekozen om een eigen versie te ontwikkelen voor op hun Nexus switches. FP en TRILL hebben de volgende overeenkomsten:

Ontstaan uit het elimineren van STP
Het meest voor de hand liggende overeenkomst is dat FabricPath ontstaan is uit het idee dat STP uit switched core netwerken moet worden geëlimineerd. Hierbij zorgt FabricPath ook voor het gebruik van de hele bandbreedte in plaats van het blokkeren van verbindingen[9][12].

Gebruik van IS-IS routing algoritme
FabricPath bepaalt zijn routering aan de hand van het IS-IS algoritme. Hierbij worden de Forwarding tabellen van de switches met elkaar gedeeld om op deze manier het beste path naar elke switch of end node te vinden[9][12].

Snelle omschakeling bij een down verbinding
De snelle omschakeling is één van de hoofdredenen waarom een TRILL variant boven STP wordt gekozen. Zelfs bij RSTP is de omschakelingstijd hoger als bij TRILL. Zo heeft FabricPath een omschakelingstijd van <300ms[10] terwijl RSTP een aantal seconden nodig heeft[2].

Het gebruik van een Distribution Tree
Dit is het geval bij Broadcast/Multicast/frames met onbekende destination. Hierbij zal een Root worden aangewezen en hieruit een Distribution Tree gevormd worden om op deze manier een loop te voorkomen[9][10].

Gebruik van Reverse Path Forwarding bij Multi-destination verkeer
Hierbij heeft elke switch een interface gelinkt aan een andere switch en laat hierop de frames van die switch binnenkomen. Als verkeer van een switch niet op de juiste interface binnenkomt dan zal RPF ervoor zorgen dat het verkeer gedropt wordt[9][12].

Gebruik van Equal Cost Multipathing (ECMP)
Het is de bedoeling dat FabricPath in tegenstelling tot STP al zijn verbindingen gebruikt. Hierbij wordt de volle bandbreedte beschikbaar en kunnen op deze manier verkeer verstuurd worden via meerdere paths om bij de destination te komen. Hiervoor wordt het ECMP protocol gebruikt[9][12].

Plug & Play configuratie
Als er een switch wordt toegevoegd aan het netwerk, dan zal FabricPath alles binnen het netwerk regelen. Er is dus geen configuratie nodig[9][12].

6.3.3 Shortest Path Bridging

De werkgroep van IEEE had Radia Perlman afgewezen over het idee van TRILL, zij waren van mening dat er niets mis was met STP. Later kwamen zij erachter dat er toch wat nadelen zaten aan STP, maar nu TRILL al een IETF standaard is moest IEEE een eigen variant bedenken. Hiermee is Shortest Path Bridging (SPB) tot ontwikkeling gekomen[17][19].De basis van SPB ligt bij het IETF standaard TRILL, echter wordt dit ontkent door de IEEE groep. SPB wordt ook gezien als de grootste concurrent van TRILL en niet echt als een variant[20][21].Toch wordt SPB in dit hoofdstuk meegenomen omdat beide protocollen bijna op dezelfde manier werken. Zo hebben SPB en TRILL de volgende overeenkomsten:

Ontstaan uit het elimineren van STP
Het meest voor de hand liggende overeenkomst is dat SPB ontstaan is uit het idee dat STP uit switched core netwerken moet worden geëlimineerd. Hierbij zorgt SPB ook voor het gebruik van de hele bandbreedte in plaats van het blokkeren van verbindingen[17][18][19].

Gebruik van IS-IS routing algoritme
SPB bepaalt zijn routering aan de hand van het IS-IS algoritme. Hierbij worden de Forwarding tabellen van de switches met elkaar gedeeld om op deze manier het beste path naar elke switch of end node te vinden[17][18].

Snelle omschakeling bij een down verbinding
De snelle omschakeling is één van de hoofdredenen waarom een TRILL variant boven STP wordt gekozen. Zelfs bij RSTP is de omschakelingstijd hoger als bij TRILL. Zo heeft SPB een omschakelingstijd van <1s [17] terwijl RSTP een aantal seconden nodig heeft[2].

Gebruik van Reverse Path Forwarding bij Multi-destination verkeer
Hierbij heeft elke switch een interface gelinkt aan een andere switch en laat hierop de frames van die switch binnenkomen. Als een verkeer van een switch niet op de juiste interface binnenkomt dan zal RPF ervoor zorgen dat het frame gedropt wordt[17][19].

Gebruik van Equal Cost Multipathing (ECMP)
Het is de bedoeling dat SPB in tegenstelling tot STP al zijn verbindingen gebruikt. Hierbij wordt de volle bandbreedte beschikbaar en kunnen op deze manier verkeer verstuurd worden via meerdere paths om bij de destination te komen. Hiervoor wordt het ECMP protocol gebruikt[17][18].

Plug & Play configuratie
Als er een switch wordt toegevoegd aan het netwerk, dan zal SPB alles binnen het netwerk regelen. Er is dus geen configuratie nodig[17][18][19].

6.4 Verschillen tussen TRILL en FabricPath

Naast de hierboven genoemde overeenkomsten hebben TRILL en FabricPath ook verschillen. Deze worden hieronder één voor één kort uitgelegd:

- FabricPath is Cisco proprietary oplossing[11][14].
- FabricPath heeft geen outer header[11][14].
- STP en IGMP snooping is nodig op de edge om loops te voorkomen[9][13].
- FabricPath leert niet alle remote node MAC-adressen[12][13].
- FabricPath maakt geen gebruik van ESADI protocol[12].

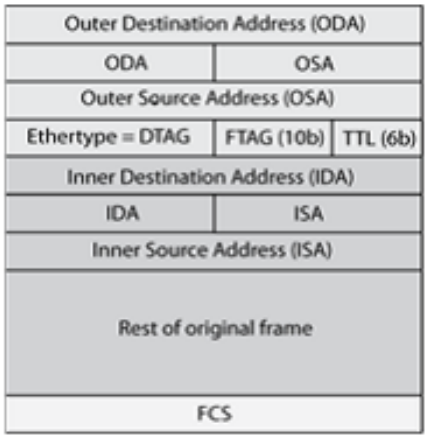
Naast deze verschillen zijn er geen andere verschillen als het gaat om protocol mechanisme. Verder zijn alleen de naamgeving bij FP anders dan bij TRILL maar de functionaliteiten blijven hetzelfde.

FabricPath is Cisco proprietary oplossing

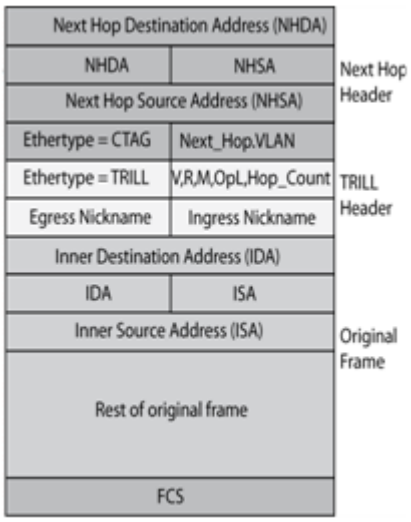
Dit houdt in dat FabricPath alleen te gebruiken is op Cisco apparatuur[12] [14].Cisco FabricPath is speciaal ontwikkeld voor op hun Nexus switches. Op dit moment zijn dat de Nexus 7000 en de Nexus 5500.

FabricPath heeft geen outer header

Het ethernet frame dat gestuurd wordt bij de communicatie tussen end nodes is verschillend zo is te zien in onderstaande afbeeldingen:

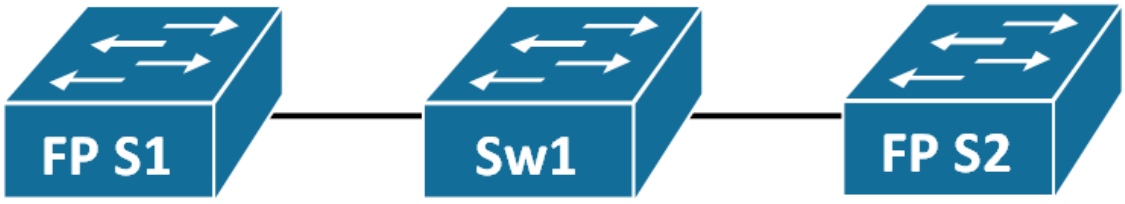


Figuur 43 FabricPath frame [14].



Figuur 44 TRILL frame [14].

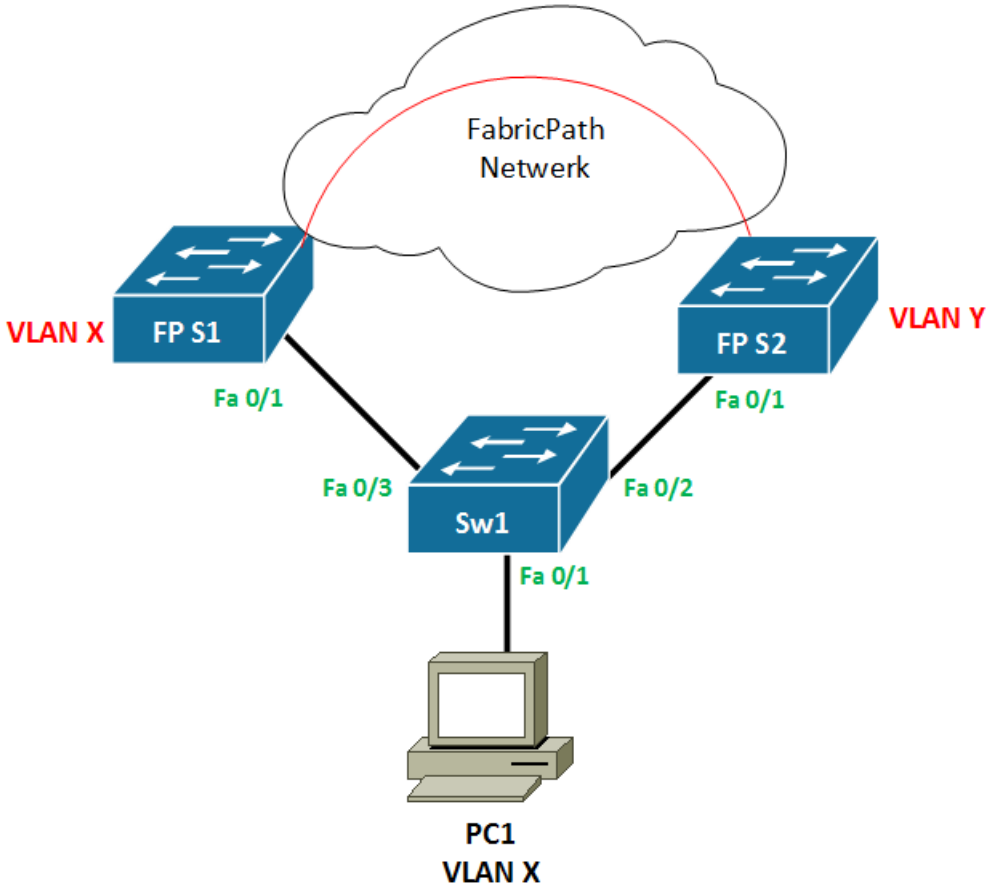
Hierboven is te zien dat het frame van FabricPath in tegenstelling tot het frame van TRILL geen outer header heeft. Dit betekend dat dat FabricPath niet in een scenario gebruikt kan worden waar een Layer 2 switch zich tussen 2 FabricPath bevindt. Een voorbeeld hiervan is hieronder weergegeven:



Figuur 45 onmogelijk scenario FabricPath

Dit scenario wordt wel door TRILL ondersteund. Hieruit kan geconcludeerd worden dat FabricPath alleen gebruikt kan worden bij een P2P implementatie model[11] [12].

STP en IGMP snooping zijn op de edge nodig om loops te voorkomen
In onderstaande afbeelding wordt een scenario geschetst die bij TRILL gebruikt kan worden om met een AF loops te voorkomen. In dit soort scenario's kunnen loops alleen ontstaan als er multicast frames worden verstuurd. Daarentegen maakt FabricPath gebruik van STP protocollenen van IGMP snooping om dit soort loops te voorkomen[9][13].



Figuur 46 FabricPath loop scenario

In het geval van bovenstaand scenario moet er met het gebruik van STP aangegeven worden welke switch de Rootswitch wordt voor een bepaald VLAN[9][13].Als FP S1 als Rootswitch gekozen wordt, dan zal Sw1 zijn Fa0/3 port als RP markeren en deze in FWD state plaatsen. Dit houdt ook in dat Fa0/2 in Blocking state geplaatst worden. Doordat Fa0/2 in Blocking state staat zal er geen verkeer naar FP S2 ontvangen worden.

Naast STP moet er ook op alle edge FP switches IGMP snooping geconfigureerd worden. IGMP zal analyseren welke VLANs gebruik maken van de switch. Door het IGMP snooping zullen de FP switches een lijst maken waarin aangegeven wordt voor welk VLAN ze multicast verkeer willen ontvangen. De FP switches zullen zichzelf markeren als ontvanger van een bepaald VLAN en zullen dit doorgeven aan de Multi-destination Rootswitch. In bovenstaand scenario zal FP2 geen verkeer ontvangen van VLAN X. Dit komt doordat STP voorkomt dat de verkeer van PC1 naar FP S2 gestuurd worden. Door deze situatie zal FP S2 zich niet registreren als ontvanger van VLAN X. Wanneer de Multi-destination Rootswitch een multicast frame ontvangt zal hij dit frame alleen opsturen naar de ontvangers van dat VLAN. Op deze manier worden loops voorkomen door FabricPath.

FabricPath leert niet alle remote node MAC-adressen
Naast de twee bovenstaande verschillen is ook het verschil er dat FP niet alle remote node MAC-adressen leert. Bij TRILL worden alle remote host gegevens opgeslagen op de destination Rbridges. Bij FabricPath is dit echter niet het geval. Bij FabricPath wordt door middel van het frame type bepaald of de gegevens opgeslagen moeten worden in de MAC tabel. De gegevens van de remote host worden alleen opgeslagen als het gaat om een unicast frame. Bij al het overige verkeer worden de remote host gegevens niet opgeslagen, dit zorgt ervoor dat de MAC-tabel van FP schaalbaar blijft[12][13].

FabricPath maakt geen gebruik van het ESADI protocol
Uit het onderzoek bleek dat FabricPath ESADI protocol niet ondersteunt om remote FP switches en End Node gegevens te leren[12].

6.5 Verschillen tussen TRILL en VCS

Naast de hierboven genoemde overeenkomsten hebben TRILL en VCS ook verschillen. Deze worden hieronder één voor één kort uitgelegd:

- VCS is Brocade proprietary oplossing[15].
- VCS maakt gebruik van Fabric Shortest Path First (FSPF) routing protocol[15][16].
- Ethernet Name Service(eNS) wordt er gebruikt voor MAC learning i.p.v. ESADI [15][16].

VCS is een Brocade proprietary oplossing
Net als FabricPath is VCS ook een proprietary protocol. Wat inhoud dat het alleen toegepast kan worden op apparaten van Brocade[15].De apparatuur waarop VCS werkt is de VDX serie; hieronder vallen onder andere de VDX 6710 en de VDX 8770.

VCS maakt gebruik van het Fabric Shortest Path First (FPSF) routing protocol
VCS maakt in tegenstelling tot TRILL geen gebruik van het IS-IS algoritme. VCS maakt gebruik van het FSPF protocol. FSPF is een linkstate routing protocol wat ontwikkeld is door Brocade. Aangezien FSPF een linkstate protocol is wordt dit protocol door VCS op hetzelfde manier gebruik als IS-IS in TRILL[15][16].Hieruit kan geconcludeerd worden dat TRILL en VCS op beide manieren het routeren bepalen, echter heet het protocol anders.

Ethernet Name Services (eNS) wordt gebruikt voor MAC learning i.p.v. ESADI
Behalve de twee bovenstaande verschillen werd ook duidelijk dat VCS geen gebruik maakt van ESADI voor MAC learning van het Ethernet Name Service(eNS). Dit is een service dat op dezelfde manier werkt als het ESADI protocol. Het eNS wordt gebruikt om End Node informatie uit te wisselen tussen Edge Rbridges. Dit zorgt ervoor dat alle edge Rbridges op de hoogte zijn van waar alle End Nodes zich bevinden in een netwerk[15][16].

6.6 Verschillen tussen TRILL en SPB

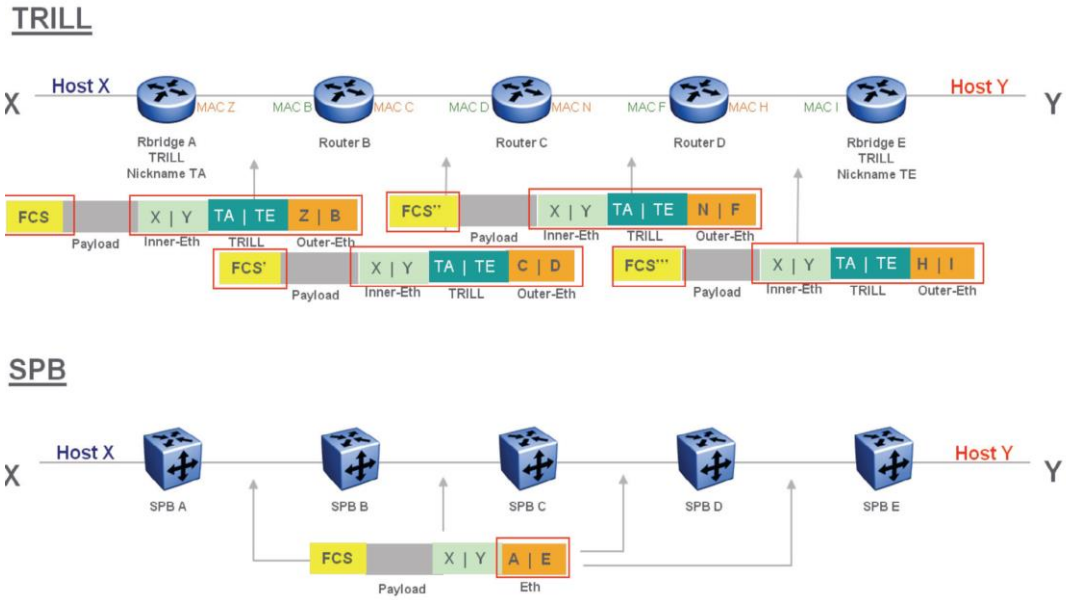
Naast de hierboven genoemde overeenkomsten hebben TRILL en SPB ook verschillen. Deze worden hieronder één voor één kort uitgelegd:

- SPB maakt de hele topologie bekend bij de edge switches[20][21].
- SPB gebruikt geen Rootswitch bij Multi-destination verkeer[20][21].
- SPB gebruikt een andere Header[20][21].
- SPB gebruikt een andere OAM[20].
- SPB gebruikt voor unicast een andere loop prevention[20].
- SPB is een IEEE standaard.

SPB maakt de hele topologie bekend bij de edge switches
Waar TRILL het paths tussen twee Rbridges probeert te optimaliseren, zorgt SPB ervoor dat alle Edge switches het hele netwerk kennen. Op deze manier hoeft er geen aparte Distribution Tree gemaakt te worden voor Multi-Destination verkeer[20][21].

SPB gebruikt geen Rootswitch bij Multi-destination verkeer
TRILL vormt bij Multi-Destination verkeer een Distribution Tree met een Rootswitch. De Rootswitch wordt gekozen door middel van een verkiezing op basis van Root prioriteit en MAC-adres. Bij SPB wordt er geen gebruik gemaakt van een Rootswitch maar wordt het kortste path gekozen door middel van de Path Cost. Dit wordt bij TRILL gebruikt voor alleen de unicast verkeer. SPB gebruikt op deze manier voor alle soorten verkeer dezelfde manier van path bepaling en daardoor zullen de paths ook altijd hetzelfde zijn[20][21].

SPB maakt gebruik van een andere header
Waar TRILL gebruikt maakt van een eigen header, gebruikt SPB een eigen eenvoudigere header. Hierbij dienen alleen het destination en de laatste Switch MAC-adressen toegevoegd worden aan het frame en alle andere switches weten waar het frame naar toe gestuurd moet worden. Terwijl TRILL iedere keer het frame opnieuw moet vormen[20][21].Zie onderstaande figuur als voorbeeld.



Figuur 47 TRILL vs. SPB Header[20]

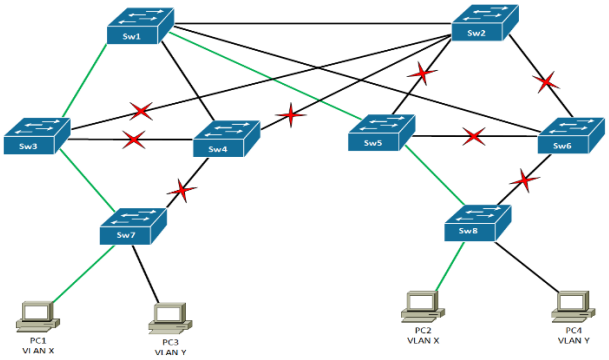
SPB gebruikt een ander OAM
SPB maakt gebruik van het IEEE standaard OAM, waar TRILL gebruik maakt van een eigen ontwikkeld OAM[20].

SPB gebruikt voor unicast een andere loop prevention
SPB gebruikt RPFC voor al zijn verkeer, waar TRILL Time-To-Live (TTL) gebruikt in zijn header om ervoor te zorgen dat de frames niet rond blijft loopen in het netwerk. Beide protocollen gebruiken wel RPFC voor multicast, broadcast en verkeer met een onbekende destination[20].

SPB is een IEEE standaard
SPB is in tegenstelling van TRILL een IEEE standaard. SPB is als opvolger van STP ontwikkeld. TRILL is daarentegen een IETF standaard[24].

6.7 Implementeren van TRILL

Voor het beantwoorden van de sub-vragen: "*Welke randvoorwaarden zijn er om TRILL te implementeren?"* en *"Waar kan TRILL worden toegepast in een netwerk?"* zal het onderstaande scenario gebruikt worden.



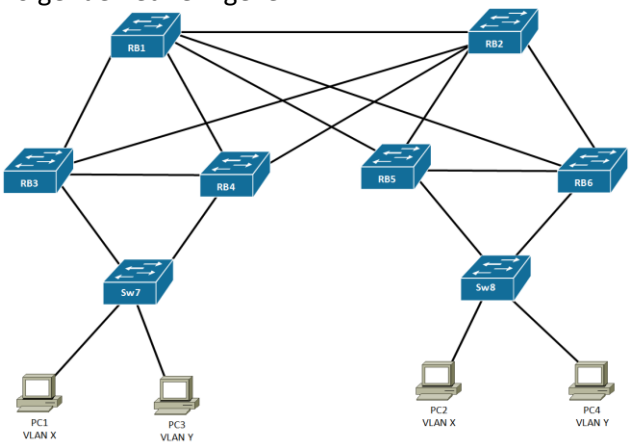
Figuur 48 STP netwerk

Dit netwerk maakt gebruik van het traditionele Spanning Tree Protocol om loops in het netwerk te voorkomen. Dit betekent dat niet de volledige bandbreedte wordt gebruikt omdat STP verbindingen blokkeert. Door TRILL toe te passen zullen we dit probleem oplossen.

Als eerste moet er gekeken worden wat er nodig is om TRILL te kunnen implementeren in dit netwerk. Hiervoor zullen de switches vervangen worden door Rbridges. Nu is het geval dat niet alle switches vervangen moeten worden. Dit wordt wel aangeraden om het netwerk op een efficiëntere manier te laten communiceren. Hierbij zullen beide implementatie methode toegelicht worden. Naast deze implementatie mogelijkheden zijn er nog talloze andere mogelijkheden. Elke implementatie methode heeft zo zijn voor- en nadelen. Hierbij is gekozen voor deze twee implementatie methoden omdat, deze het meest betrekking hebben tot het onderzoek.

Scenario 1: Alleen switches 1 t/m 6 vervangen

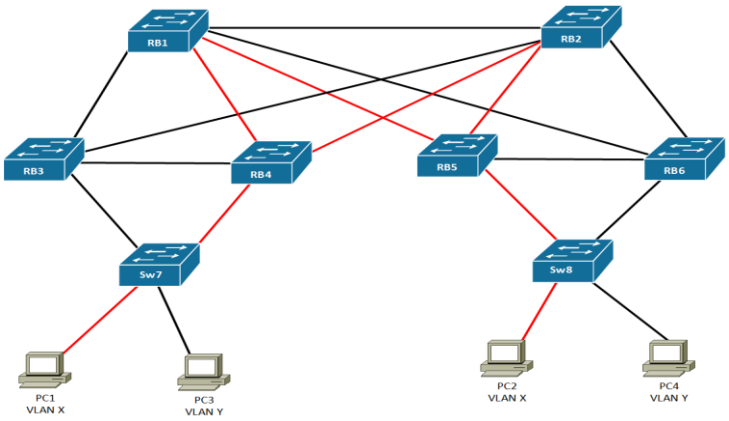
In het eerste scenario zullen we de switches 1 t/m 6 vervangen door Rbridges, dit zal dan het volgende netwerk geven:



Figuur 49 Toepassing TRILL switches 1-6

Hierbij is duidelijk te zien dat de switches 1-6 nu Rbridges zijn, Rbridges zullen in dit netwerk met elkaar communiceren en bepalen hoe ze het best elkaar kunnen bereiken. Deze manier van communiceren is in een vorig hoofdstuk al uitgebreid toegelicht, daarom zal er nu niet zo veel aandacht eraan besteed worden.

Wanneer PC1 data wilt uitwisselen met PC 2 zal het verkeer geloadbalanced worden over verschillende verbindingen. Dit alleen als de Cost van het beste paths gelijk zijn aan elkaar. Hierbij wordt ook een Appointed Forwarder bepaalt door de Rootswitch, de verkiezing van beide rollen binnen dit netwerk wordt niet verder uitgelegd. Dit is in een eerder hoofdstuk al uitgebreid behandelt. Op de volgende pagina staat een netwerk weergegeven die het path van PC1 naar PC2 aangeeft door middel van de rode verbindingen. Hierbij wordt duidelijk dat in dit scenario de AF voor VLAN X RB4 en RB5 zijn. Dit omdat wel gebruik gemaakt wordt van deze Rbridges maar niet van de Rbridges RB3 en RB6. De noodzaak van een AF staat ook eerder toegelicht en zal niet opnieuw uitgelegd worden.

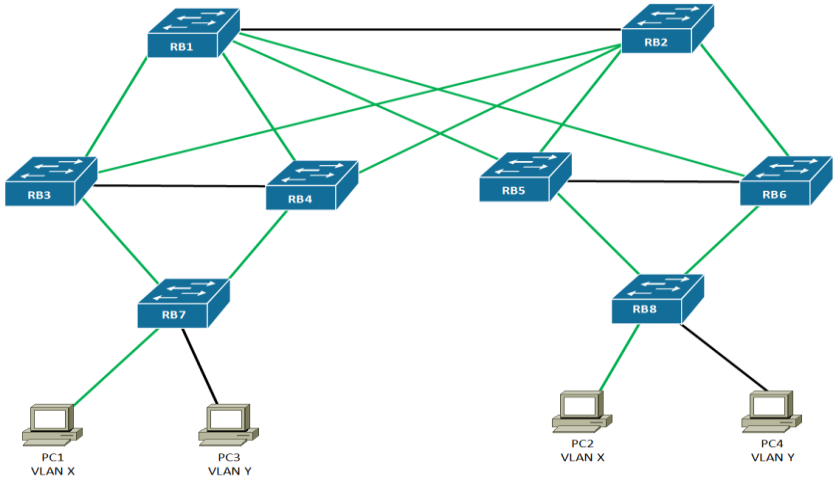


Figuur 50 Beste paths van PC1 naar PC2 (1)

Uit bovenstaande figuur wordt duidelijk dat hier niet gebruik wordt gemaakt van de volledige infrastructuur. Als dit wel wenselijk is, dan zullen alle switches vervangen moeten worden. Dit wordt in het volgende scenario uitgelegd.

Scenario 2: Alle switches vervangen

In onderstaande figuur is duidelijk te zien dat ook de switches 7 en 8 vervangen zijn door Rbridges en dat daardoor de mogelijkheden van beste paths is vergroot. Hierbij worden RB7 en RB8 de AF van zowel VLAN X als van VLAN Y. Op deze manier wordt er op een efficiënte manier gebruik gemaakt van de infrastructuur.



Figuur 51 Beste paths van PC1 naar PC2 (2)

6.8 Conclusie TRILL

Als resultaat uit het onderzoek naar TRILL blijkt dat TRILL geen verbindingen blokkeert om loops te voorkomen. TRILL maakt gebruik van het IS-IS routing protocol. Hierbij wordt het verkeer tussen de switches gerouteerd. Ook blijkt dat TRILL niet gebruik maakt van de standaard switches maar van switches die TRILL implementatie ondersteunen. Deze switches worden ook wel Rbridges genoemd.

Werking TRILL

Uit het onderzoek bleek ook dat Rbridges gebruik maken van een Hello conversatie om te achterhalen wie zijn neighbor is en waar deze zich bevindt. Bij TRILL wordt er een verzendende Rbridge gekozen deze staat ook wel bekend als een Designated Rbridge. De DRB wordt gekozen aan de hand van de interface prioriteit. De DRB zal een VLAN kiezen waarin de Rbridges onderling met elkaar communiceren. Hiernaast kiest de DRB ook een Appointed Forwarder(AF). Een AF zorgt ervoor dat een fysieke loop niet zorgt voor een broadcast storm. Een AF zal als enige Rbridge nog verkeer van een bepaald VLAN ontvangen en doorsturen. De andere Rbridges zullen niets met het frame doen.

Als twee Rbridges van elkaar weten waar ze zich bevinden, dan zullen de Rbridges hun Link State Database (LSDB) naar elkaar opsturen. LSDB zorgt ervoor dat alle Rbridges dezelfde Forwarding tabel hebben. Op deze manier weten alle Rbridges hoe zij de andere Rbridges in het netwerk kunnen bereiken.

Nu alle Rbridges van elkaar weten waar ze zich bevinden, moet het beste path naar de desbetreffende Rbridge nog vastgesteld worden. Het beste path wordt gekozen aan de hand van de LSDB. Hierin weet de Rbridge aan welke interface welke Rbridge zit. Ook weet de Rbridge hoe hij naar een andere Rbridge kan, die niet direct verbonden is, door de LSDB van de direct verbonden Rbridge. Het beste path wordt uiteindelijk gekozen door het Shortest Path First(SPF) algoritme. Het SPF zal het path van de Rbridges opslaan in een TRILL routing tabel. Als er meerdere paths zijn die dezelfde Cost hebben en deze hebben de laagste Cost. Dan zal TRILL gebruik maken van het Equal Cost Multipath(ECMP) protocol. Hierbij zal het verkeer over meerdere verbindingen gestuurd kunnen worden en de data over deze verbindingen verdeeld wordt.

Naast de LSDB en de routing tabel, houdt TRILL ook een TRILL MAC-tabel bij. Hierin zijn nog twee soorten te onderscheiden, de Edge Rbridges en de Core Rbridges. De Edge Rbridges zitten verbonden aan de End nodes, dit kan een server of PC zijn. De Core Rbridges zitten aan andere Rbridges verbonden. Een TRILL MAC-tabel beschikt over de informatie van de End Nodes, hierbij gaat het om de naam, MAC-adres, VLAN en naar welke interface of Rbridge het frame verstuurd moet worden. Elke Rbridge zal Hello-frames blijven sturen om te kijken of de End Node of Rbridge nog in leven is. Dit is de traditionele manier om de TRILL MAC-tabel te vullen. Hiernaast is er ook de optionele manier om de tabel te vullen met het End Station Address Distribution Information (ESADI) protocol. Dit is een protocol die informatie over End Nodes doorgeeft aan andere Edge Rbridges in het netwerk. Een update zal plaatsvinden als er een End Node aangesloten wordt of verplaatst wordt. Op deze manier zorgt ESADI ervoor dat de TRILL MAC-tabel up-to-date blijft en betrouwbaar blijft.

Naast de TRILL MAC-tabel hebben de Rbridges ook een Multi-destination routing tabel nodig. Deze tabel wordt gebruikt wanneer broadcast, multicast of verkeer met een onbekende destination verstuurd moet worden

Voor het versturen van multicast, broadcast of verkeer met een onbekende destination maakt TRILL gebruik van Distribution Trees. Om een Distribution Tree te maken moet er een Root Rbridge worden aangewezen. De Root Rbridge wordt gekozen tijdens het onderhandeling proces van TRILL. Hierbij wordt de Rbridge met de hoogste Root prioriteit gekozen. Als het geval zo is dat er meerdere Rbridges dezelfde Root prioriteit heeft, dan zal de Rbridge met het laagste MAC-adres de Root Rbridge worden. De Root Rbridge zal met behulp van het SPF algoritme bepalen hoe alle andere Rbridges het best te bereiken zijn, wat is het beste path naar deze Rbridges. In een LSDB update zal worden aangegeven dat de Root Rbridge de destination wordt voor het versturen van broadcast, multicast en verkeer met onbekende destination.

Als twee End Nodes met elkaar willen communiceren, zal TRILL een frame sturen met een aantal headers. Als eerste krijgt de Rbridge een Ethernet frame binnen waarin de source en destination MAC-adressen zijn meegegeven. Hier plakt een Rbridge een TRILL header op met de informatie die uit zijn tabellen kunnen worden gehaald. Als laatste zal de Rbridge er nog een Outer Ethernet Header aan het frame koppelen. Hierin staan de gegevens van de volgende hop. Als de volgende hop het frame ontvangt zal hij de Outer Ethernet Header eraf halen en kijken in de TRILL header waar het frame naar toe moet. Dan zal deze Rbridge de TRILL header aanpassen en er een nieuwe Outer Ethernet Header aan toe voegen. Dit zal gedaan worden tot het frame bij de End Node is aangekomen. Bij multicast verkeer zal het frame naar de Root-Rbridge gestuurd worden en deze zal wederom de Outer Frame Header eraf halen en de TRILL Header aanpassen. Hierna zal hij er een nieuwe Outer Ethernet Header aanhangen en naar de juiste Rbridges sturen.

Naast de werking van TRILL op de Rbridges is er ook onderzoek gedaan naar relevante varianten van TRILL. Hieruit kwamen drie resultaten. FabricPath van Cisco, VCS van Brocade en SPB van Alcatel. Deze varianten zijn gekozen omdat Qi ict bv. veelal gebruik maakt van apparatuur van deze fabrikanten. In de netwerken van Qi ict bv. zal het dus mogelijk zijn om een van deze varianten te kunnen testen. Naast meerdere overeenkomsten tussen TRILL en de varianten zijn er ook nog een aantal verschillen.

Cisco FabricPath vs. TRILL

- FabricPath is Cisco proprietary oplossing
- FabricPath heeft geen outer header
- STP en IGMP snooping is nodig op de edge om loops te voorkomen
- FabricPath leert niet alle remote node MAC-adressen
- FabricPath maakt geen gebruik van ESADI protocol

Eén van de verschillen is dat TRILL een open standaard is en FP een Cisco proprietary. Dit houdt in dat FP alleen op Cisco hardware gebruikt kan worden. Daarnaast gebruikt FP geen outer header, dit houdt in dat er geen Layer 2 switch tussen twee FP switches geïmplementeerd kan worden of in een broadcast model. Daarnaast kwam naar voren dat er gebruik gemaakt wordt van STP en IGMP snooping om loops te voorkomen. Een ander verschil wat naar voren kwam was dat FabricPath niet alle MAC-adressen van remote End Node opneemt in het MAC tabel. Ook bleek dat FabricPath geen gebruik maakt van ESADI protocol.

Brocade VCS vs. TRILL

- VCS is Brocade proprietary oplossing.
- VCS maakt gebruik van Fabric Shortest Path First (FSPF) routing protocol
- Ethernet Name Service(eNS) wordt er gebruikt voor MAC learning i.p.v. ESADI

Uit het onderzoek kwam naar voren dat het VCS een Brocade proprietary protocol is. Ook bleek dat VCS gebruik maakt van FSPF routing protocol en niet van IS-IS zoals FabricPath en TRILL. Tevens maakt VCS gebruik van eNS service om MAC tabellen onderling uit te wisselen. Deze services is gelijk aan de optionele MAC learning protocol ESADI van TRILL.

SPB vs. TRILL

- SPB maakt de hele topologie bekend bij de edge switches.
- SPB gebruikt geen Rootswitch bij Multi-destination verkeer
- SPB gebruikt een andere Header
- SPB gebruikt een andere OAM
- SPB gebruikt voor unicast een andere loop prevention
- SPB is een IEEE standaard

Waar TRILL de paths tussen twee Rbridges probeert te optimaliseren, zorgt SPB ervoor dat alle Edge switches het hele netwerk kennen. Ook kwam uit het onderzoek dat SPB geen Root-switch gebruikt bij Multi-destination verkeer. Bij SPB wordt er gebruik gemaakt van de Path Cost onderling en iedere switch weet de hele topologie. TRILL gebruikt dit alleen bij unicast, waar SPB het bij al het verkeer gebruikt. Hierdoor zijn de paths van SPB van Switch A naar Switch B hetzelfde, ongeacht het verkeerstype. Ook werd duidelijk dat waar TRILL gebruik maakt van een eigen header, gebruikt SPB een eigen eenvoudigere header. Hierbij dienen alleen het destination en de laatste Switch MAC-adressen toegevoegd worden aan het frame en alle andere switches weten waar het frame naar toe gestuurd moet worden. Daarnaast gebruikt SPB het IEEE standaard OAM, waar TRILL gebruik maakt van een eigen ontwikkeld OAM. SPB gebruikt RPFC voor al zijn verkeer, waar TRILL Time-To-Live (TTL) gebruikt in zijn header om ervoor te zorgen dat het verkeer niet rond blijft loopen in het netwerk. Beide protocollen gebruiken wel RPFC voor multicast, broadcast en verkeer met een onbekende destination.

Implementatie TRILL

Als laatste werd bij het onderzoek naar TRILL gekeken welke randvoorwaarden er zijn om TRILL te kunnen implementeren. Hierbij is de standaard TRILL protocol gebruikt. Hierbij werd al duidelijk dat net als bij alle varianten er gebruik moet worden gemaakt van aparte switches. In het geval van de standaard TRILL, zal er gebruik worden gemaakt van Rbridges. Hierbij moet er gekeken worden welke switch fabrikanten TRILL ‘ready’ apparatuur leveren.

Naast de apparatuur is er ook nog configuratie, echter is het zo dat TRILL gebruik maakt van een Plug&Play configuratie. Dit houdt in dat er geen configuratie nodig is om het te laten functioneren.

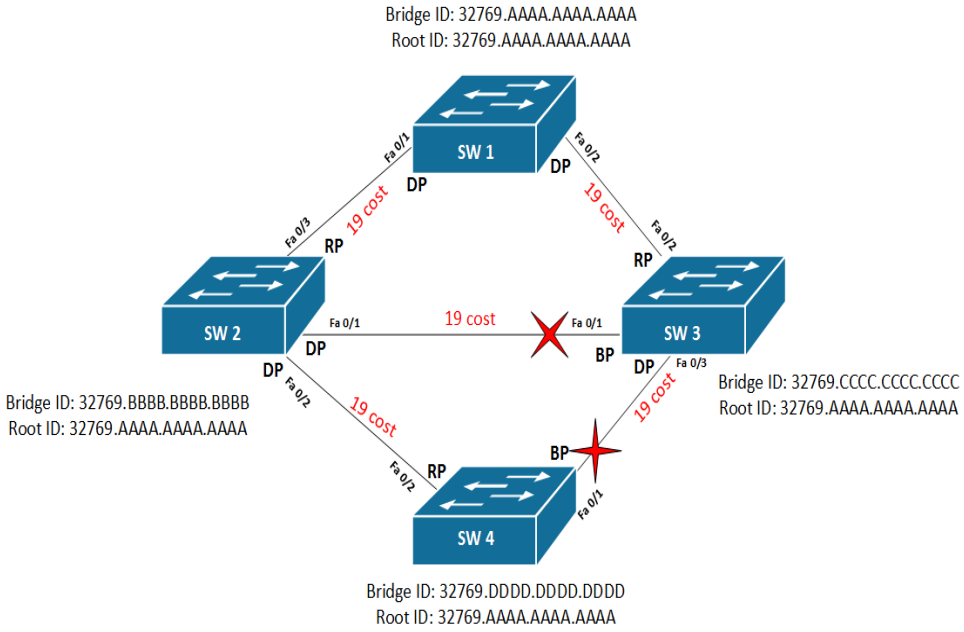
Als laatste kan er nog gedacht worden aan waar TRILL geïmplementeerd wordt. Zo kan TRILL in alleen de Core worden geïmplementeerd of voor een efficiëntere manier van routeren in het hele netwerk.

7. Verschillen tussen STP en TRILL

Na het onderzoeken van STP, TRILL en de varianten van TRILL kan de vergelijking worden opgezet: “wat zijn de verschillen tussen STP en TRILL?” Hierbij worden de varianten van TRILL buiten beschouwing gelaten omdat de vergelijking tussen standaard TRILL en de varianten al in een eerder hoofdstuk zijn behandeld. Hieruit is gebleken dat de werking van de varianten grotendeels overeenkomen met de open standaard TRILL.

Bij het onderzoek naar TRILL viel op dat ondersteunt moet TRILL worden door de switches, en dit is niet bij alle switches het geval. Deze TRILL ondersteunende switches worden ook wel Rbridges genoemd. STP daarentegen werkt wel op de standaard switches[4][5].

Uit het onderzoek van STP kwam naar voren dat er gebruikt wordt gemaakt van het blokkeren van verbindingen om loops te voorkomen[1][2].Hierbij wordt niet de hele bandbreedte gebruikt. TRILL daarentegen maakt wel gebruik van de gehele bandbreedte. TRILL gebruikt IS-IS routing op Layer 2 om verkeer naar de juiste Rbridge te sturen[3][6].Elke Rbridge weet hoe hij bij een andere Rbridge kan komen en welk path hiervoor nodig is. Door het toepassen van MAC-routing kan elke Rbridge zien waar het verkeer vandaan kwam en wat de destination is waar het verkeer naartoe moet.



Figuur 52 STP loops voorkomen

Bij TRILL is het door het gebruik van alle verbindingen ook mogelijk om verkeer te loadbalancen over meerdere verbindingen. Dit wordt gedaan door het Equal Cost Multipath algoritme[3][5][6]. Hierbij wordt, als er meerdere beste paths zijn, het verkeer opgedeeld en over de verbindingen gestuurd. Dit is bij STP niet mogelijk omdat er gebruik wordt gemaakt van het blokkeren van verbindingen. Mede hierdoor wordt er ook inefficiënt gerouteerd van verkeer. Zie ook bovenstaande figuur om dit te zien. Als SW3 een frame wil sturen naar SW4 dan zal het frame via SW1 (de Root) en SW2 bij SW4 uitkomen. Dit komt omdat SW4 frames die direct van SW3 komen blokkeert om loops te voorkomen[1][2].

Het blokkeren van verbindingen om loops voorkomen brengt bij STP nog een nadeel met zich mee. Als er een verbinding down gaat, moet er omgeschakeld worden door de switches omdat er nu de mogelijkheid is dat deze switch geen frames meer ontvangt. Zo is het geval als de verbinding tussen SW1 en SW2 wegvalt. Dit zorgt ervoor dat zowel SW2 als SW4 de Rootswitch niet kunnen bereiken. Nu is het bij STP het geval dat een switch standaard 10 Hello frames afwacht, ieder Hello frame wordt om de 2 seconden gestuurd. Dan moet de switch op zijn andere verbindingen luisteren of hier wel reactie komt op Hello frames, deze fase duurt 15 seconden. Als laatste moet switch dit path leren, deze fase duurt ook weer 15 seconden. Zo zal STP na het uitvallen van een verbinding 50 seconden verder zijn voordat het hele netwerk weer werkt. Hiervoor is al een ander protocol bedacht, het Rapid Spanning Tree Protocol (RSTP)[1][2].]. RSTP werkt net als STP nog steeds met het blokkeren van verbindingen, maar de omschakelingstijd is vele malen sneller dan die van STP. In plaats van 10 Hello frames wacht RSTP 1 Hello frame af en wordt er meteen geleerd wat de verbinding is. Hiermee doet RSTP er maar een aantal seconden over in plaats van 50 seconden[2].Nu is het wel het geval dat TRILL er maar een aantal milliseconden over doet in plaats van seconden[6].

Als laatste kwam er uit het onderzoek naar de protocollen dat STP slecht schaalbaar is. Als het netwerk uitgebreid moet worden, maar de huidige netwerkconfiguratie (Root, interface prioriteiten e.d.) hetzelfde moet blijven, dan zal de nieuwe switch helemaal geconfigureerd worden. Ook de andere switches zullen geconfigureerd worden om deze nieuwe switch te kunnen bereiken. Hiervoor is ook een protocol bedacht door de IEEE groep, namelijk Multi Spanning Tree Protocol (MSTP)[1]. MSTP wordt vooral gebruikt als het netwerk met meerdere VLANs werkt, maar niet voor elk VLAN een aparte Distribution Tree moet worden gecreëerd. MSTP maakt Distribution Trees per “instance” en aan een “instance” kunnen VLANs worden toegevoegd. Zo is bij 1000 VLANs het niet nodig om 1000 Distribution Trees aan te maken(zoals wel bij RSTP gebeurd), maar kan er bijvoorbeeld per 200 VLANs een instance aangemaakt worden. Nu heeft dit netwerk 5 Distribution Trees in plaats van 1000. TRILL hoeft daarentegen helemaal geen Distribution Trees te maken, omdat er geen verbindingen geblokkeerd worden.

Ook omdat er geen verbindingen geblokkeerd worden, is er minder configuratie nodig om TRILL te implementeren. De Rbridge zal zijn gegevens aan zijn neighbors laten weten door middel van Hello uitwisseling en daarna met het synchroniseren van de Link State Database (LSDB). Hierdoor weet de nieuwe Rbridge hoe hij de andere Rbridges kan bereiken en welk path de laagste Path Cost heeft[5][6].

7.1 Conclusie verschillen tussen STP en TRILL

Een eerste conclusie die kan worden getrokken is dat de switches waarop TRILL moet worden geconfigureerd wel TRILL moeten ondersteunen. Waar STP op de switches standaard al werkt. Hierbij is het verschil dat voor TRILL in sommige situaties aparte hardware moet worden geregeld.

Uit het onderzoek van STP kwam naar voren dat er gebruikt wordt gemaakt van het blokkeren van verbindingen om loops te voorkomen. Hierbij wordt niet de hele bandbreedte gebruikt. TRILL daarentegen maakt wel gebruik van de gehele bandbreedte. TRILL gebruikt IS-IS routing op Layer 2 om verkeer naar de juiste destination te sturen.

Bij TRILL is het door het gebruik van alle verbindingen ook mogelijk om verkeer te loadbalancen over meerdere verbindingen. Dit wordt gedaan door het Equal Cost Multipath algoritme. Hierbij wordt, als er meerdere beste paths zijn, het verkeer opgedeeld en over de verbindingen gestuurd. Dit is bij STP niet mogelijk omdat er gebruik wordt gemaakt van het blokkeren van verbindingen. Mede hierdoor wordt er ook inefficiënt gerouteerd van verkeer.

Het blokkeren van verbindingen om loops voorkomen brengt bij STP een nadeel met zich mee. Als er een verbinding down gaat, moet er omgeschakeld worden door de switches omdat er nu de tijdelijk geen verkeer meer worden ontvangen door andere switches. STP zal na het uitvallen van een verbinding 50 seconden verder zijn voordat het hele netwerk weer werkt. Hiervoor is al een ander protocol bedacht, het Rapid Spanning Tree Protocol (RSTP). RSTP werkt net als STP nog steeds met het blokkeren van verbindingen, maar de omschakelingstijd is vele malen sneller dan die van STP. RSTP doet er maar een aantal seconden over in plaats van de 50 seconden die STP nodig heeft. Nu is het wel het geval dat TRILL er maar een aantal milliseconden over doet in plaats van seconden.

Als laatste kwam er uit het onderzoek naar de protocollen dat STP slecht schaalbaar is. Als het netwerk uitgebreid moet worden, maar de huidige netwerkconfiguratie hetzelfde moet blijven, dan zal de nieuwe switch helemaal geconfigureerd worden.. Hiervoor is ook een protocol bedacht door de IEEE groep, namelijk Multi Spanning Tree Protocol (MSTP)[1]. MSTP wordt vooral gebruikt als het netwerk met meerdere VLANs werkt, maar niet voor elk VLAN een aparte Distribution Tree moet worden gecreëerd. MSTP maakt Distribution Trees per “instance” en aan een “instance” kunnen VLANs worden toegevoegd.

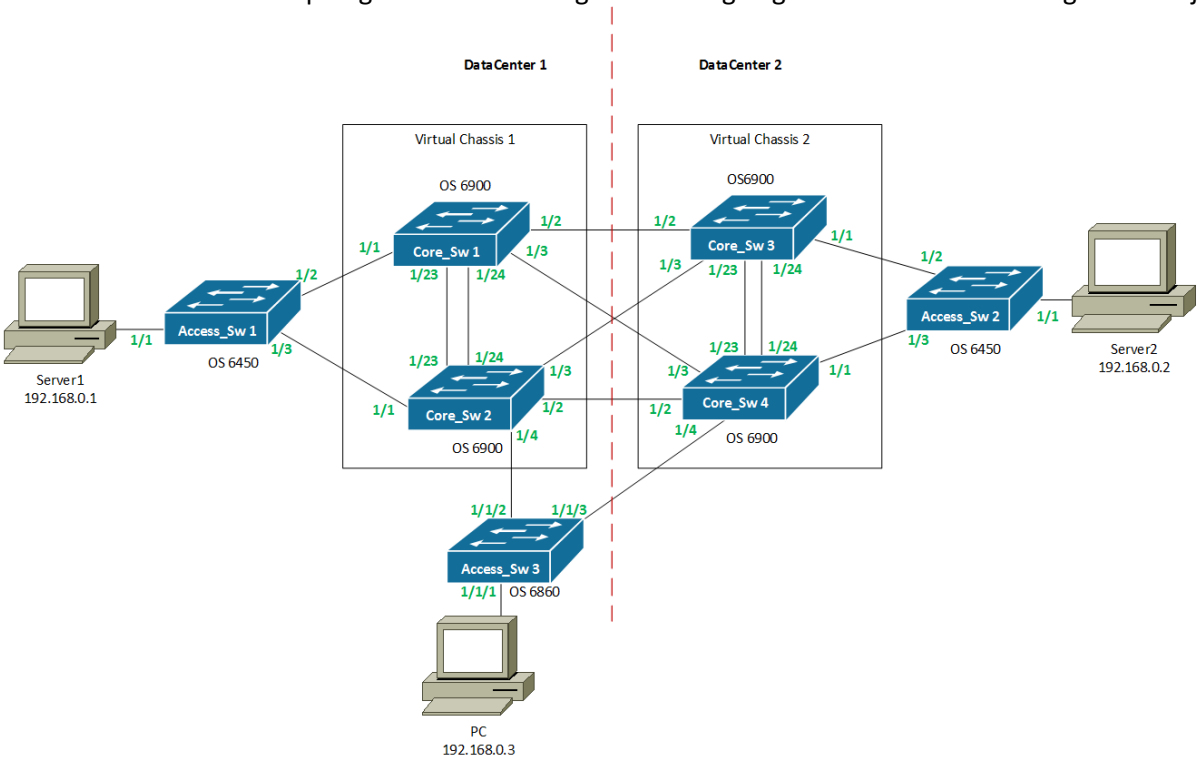
Ook omdat er geen verbindingen geblokkeerd worden, is er minder configuratie nodig om TRILL te implementeren. De Rbridge zal zijn gegevens aan zijn neighbors laten weten door middel van Hello uitwisseling en daarna met het synchroniseren van de Link State Database (LSDB). Hierdoor weet de nieuwe Rbridge hoe hij de andere Rbridges kan bereiken en welk path de laagste Path Cost heeft[5][6].

8. De huidige infrastructuur

In dit hoofdstuk zal de deelvraag: *"Kan TRILL in de reeds bestaande infrastructuren worden geïmplementeerd?".* Bij deze deelvraag horen meerdere sub-vragen die in onderstaande sub-hoofdstukken behandeld worden.

8.1 Topologie huidig netwerk

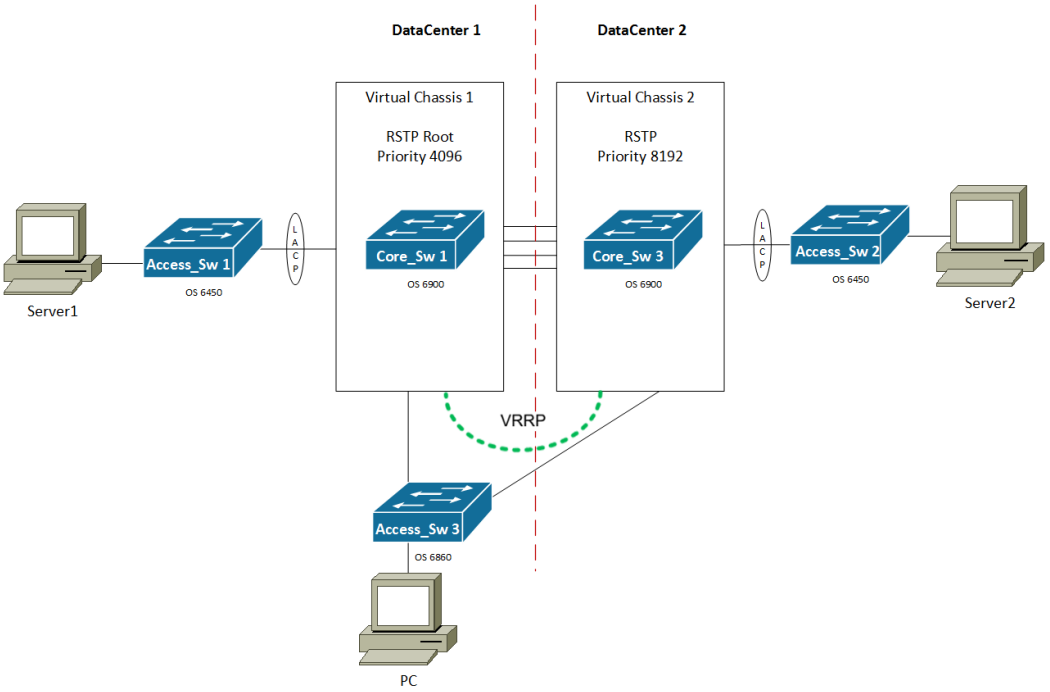
De huidige infrastructuur kan in twee aparte topologiën worden opgedeeld. Een fysieke topologie en de logische topologie. De fysieke topologie geeft de apparatuur met de poorten weer, daarentegen staan alleen de verbindingen en de apparatuur zoals deze door het netwerk zelf worden gezien. Hieronder zullen beide topologiën worden weergeven en uitgelegd waarom deze keuzes gemaakt zijn.



Figuur 53 Fysieke topologie huidige situatie

Te zien is dat de infrastructuur verdeeld is in twee aparte datacenters. Beide datacenters zijn met elkaar verbonden door de verbintenis van de beide Cores. Ieder datacenter heeft een eigen core bestaand uit een Virtual Chassis. Uit de fysieke topologie is te halen via welke poorten elke switch met elkaar verbonden is. Te zien is dat de Core switches full-mesh verbonden zijn. Dit is gedaan om de verbindingen redundant te maken. Ook staan de IP-adressen van de PCs in deze topologie weergegeven. Er staat een PC in Datacenter1 die verbonden is met beide Virtual Chassis.

Voor de protocollen moet er echter gebruik gemaakt worden van een logische topologie. Door beide topologiën te gebruiken kan bijna het hele netwerk begrepen worden. Hiervoor zou echter nog een gedetailleerde omschrijving moeten komen voor de instellingen. Deze instellingen zullen in het ontwerprapport vermeldt worden.



Figuur 54 Logische topologie huidige situatie

Uit beide topologiën is te herleiden dat er gebruik gemaakt wordt van Alcatel apparatuur. De keuze voor Alcatel apparatuur is gekomen door de volgende redenen:

- Alcatel is de meest gebruikte fabrikant van Qi ict bv.
- De infrastructuur is op basis van het netwerk van een klant van Qi ict bv.

Uit bovenstaande topologiën kunnen geen protocollen worden gehaald. Deze protocollen zijn wel bekend. Zo wordt er bij Access_Sw 2 gebruik gemaakt wordt van een Link Aggregation. Hierbij worden 2 fysieke verbindingen gebundeld tot één logische verbinding. Hiervoor wordt het Link Aggregation Control Protocol gebruikt. De core van elke datacenter bestaat uit twee switches die samen een Virtual Chassis vormen. Access_Sw3 gebruikt het Virtual Router Redundancy Protocol om bij het uitvallen van één van de beide Virtual Chassis toch nog een server te kunnen benaderen. In deze infrastructuren zal in de huidige situatie gebruik gemaakt worden van RSTP, dit is ook het protocol dat bij de klant gebruikt wordt. Al deze protocollen zullen in het volgende sub-hoofdstuk worden behandeld.

Voor de nieuwe situatie die gemigreerd wordt vanuit bovenstaande situatie geldt dat de functionaliteiten hetzelfde moeten blijven. Hierbij moet het geval nog steeds zijn dat wat er ook gebeurt (afgezien van een netwerk meltdown) PC1 moet data naar PC2 kunnen sturen. Hierbij wordt dan RSTP vervangen door SPB. In deze infrastructuur is de keuze gemaakt tussen TRILL en de verschillende varianten, waaronder SPB en is tot de conclusie gekomen dat SPB het beste protocol is om te gebruiken voor deze simulatie. En wel om de volgende redenen:

- Qi ict bv. maakt veel gebruik van Alcatel apparatuur
- De simulatie is op basis van de klant die Alcatel gebruikt en daarbij is SPB best toepasbaar
- Brocade en Cisco switches worden nauwelijks gebruikt door Qi ict bv.

Nu er een overzicht is van de topologie van de huidige infrastructuur, zullen de gebruikte protocollen van deze infrastructuur uitgelegd worden. Hierbij kan gedacht worden aan wat het protocol inhoudt, hoe het protocol werkt, waarom gebruik gemaakt wordt van het protocol en hoe deze geconfigureerd moet worden op switches.

8.2 Gebruikte protocollen

Hier wordt de sub-vraag behandeld: *"Wat zijn de huidig gebruikte protocollen?"*. De protocollen die worden gebruikt bij bovenstaand netwerk zijn: Virtual Chassis, VRRP, LACP en RSTP Deze protocollen hieronder ieder apart behandeld worden.

8.2.1 Virtual Chassis

Hieronder wordt uitgelegd wat een Virtual Chassis is, waarom er gebruik gemaakt wordt van een Virtual Chassis en hoe een Virtual Chassis werkt.

Wat is een Virtual Chassis?

Virtual Chassis(VC) is een technologie die gebruik maakt van stack switches, hierbij worden meerdere switches met elkaar verbonden en worden de switches logische wijs gezien als één switch. De switches hebben samen één switch Fabric, één Control Plane, één Configuratie bestand, één Operating System, er is geen Spanning Tree Protocol nodig voor het voorkomen van lussen en er is een Any-to-Any Port Connectivity[22].

Waarom wordt een Virtual Chassis gebruikt?

Virtual Chassis worden gebruikt vanwege een aantal voordelen[22][23]:

Redundantie: Als er met een enkele switch gewerkt word ten deze valt uit, dan is je network volledig down. Als er een stack van switches is en één switch valt om, dan blijft er nog steeds connectiviteit bestaan. Als je je netwerk op de juiste manier ontwerpt, dan kan het netwerk het uitvallen van een enkele switch overleven.

Beheer: Als er toegang voor 400 servers of computers moet worden voorzien, wordt liever gebruik gemaakt van 10 kleinere switches dan van één grote, dit vanwege de kosten en ruimte. Als switches worden opgestapeld, dan kunnen ze beheert worden als een enkele switch, waardoor het beheren van de switches een stuk eenvoudiger wordt.

Schaalbaar: Het is mogelijk om meerdere switches toe te voegen aan het Virtual Chassis, zonder configuratie, hierdoor is het netwerk beter schaalbaar.

Kabelbeheer: In plaats van honderden kabels nodig te hebben voor een specifieke switch in een rack, kan er ook een chassis gebruikt worden die bestaat uit meerdere switches. Dit geeft meer ruimte voor degelijk kabel beheer.

Kosten: Er zijn misschien geen honderden poorten direct nodig, maar misschien wel over een jaar gezien. Het aanschaffen van meerdere kleine switches als nodig, die onderdeel worden van een virtual chassis, zorgt voor de spreiding van kosten. Ook is door het stapelen van de switches minder ruimte nodig in een rack, mede hierdoor is er ook minder koeling en elektriciteit nodig.

Hoe werkt een Virtual Chassis?

Een Virtual Chassis werkt met een Master-Slave principe. Hierbij is een switch in de VC de Master en de andere switches zijn Slaves. De Master bekijkt waar het verkeer naartoe moet en bepaalt de paths naar de volgende hop. De meerdere switches werken logisch gezien als één switch.

Als de Master uitvalt, zal een Slave zijn Master rol overnemen. Als een Slave uitvalt, blijft de huidige Master switch de Master.

8.2.2 Virtual Router Redundancy Protocol

Hieronder wordt uitgelegd wat het Virtual Router Redundancy Protocol (VRRP) is, waarom er gebruik gemaakt wordt van VRRP en hoe VRRP werkt.

Wat is VRRP

VRRP zorgt voor een redundante oplossing voor de default gateway. Hierbij gebruikt VRRP een virtuele router die uit meerdere routers of switches kan bestaan. Deze virtuele router kan met een IP-adres de default gateway worden[24][26]. De master gebruikt het virtuele MAC-adres om het verkeer naar zich toe te halen. Wanneer de Master wegvalt neemt de back-up switch het virtuele MAC-adres over om het verkeer naar zich toe te trekken.

Waarom wordt VRRP gebruikt?

Virtual Router Redundancy Protocol wordt gebruikt voor het elimineren van het 'single point of failure' mede door het handmatig configureren van een virtual default gateway adres op een virtuele router die kan bestaan uit meerdere switches. Er kan niet op meerdere switches hetzelfde IP-adres worden geconfigureerd. De Master van het VRRP gebruikt als enige dit virtuele IP-adres. Zonder VRRP zullen alle hosts in het netwerk opnieuw geconfigureerd moeten worden als de default gateway uitvalt[25]. VRRP wordt in deze situatie gebruikt door beide Virtual Chassis aan de virtuele router toe te voegen. Dit wordt gedaan om bij het uitvallen van een Virtual Chassis Slave de andere server te kunnen bereiken.

Hoe werkt VRRP?

VRRP werkt met een Master-Slave principe, hierbij krijgt de Master het verkeer binnen. De Slave staat op *stand-by* en zal niets doen voor dit VRRP netwerk. Pas als de Master uitvalt, zal de Slave actie ondernemen. De Slave zal op dat moment frames sturen met het MAC-adres van de Virtuele router, die aangeven dat de Virtuele router nu achter een andere port zit. Hierdoor kan de switch/router zijn MAC-tabel aanpassen met waar de default gateway zich bevindt.

8.2.3 Link Aggregation Control Protocol

Hieronder wordt uitgelegd wat het Link Aggregation Control Protocol (LACP) is, waarom er gebruik gemaakt wordt van LACP en hoe LACP werkt.

Wat is een Link Aggregation

Een Link Aggregation is het bundelen van meerdere parallelle verbindingen tot een enkele (logische) verbinding om de doorvoer van het netwerk verkeer te verhogen. De vertaling van "Aggregate" is samenvoegen. Voor het samenvoegen van Ethernet verbindingen is het LACP protocol de standaard[1].LACP en andere vormen van Link Aggregation zijn bijna identiek, alleen is het met LACP het geval dat deze poorten zichzelf kunnen configureren in trunk groepen zonder dat er tussenkomst is van een persoon. LACP is de IEEE standaard, terwijl Link Aggregation meer als overkoepelende term wordt gebruikt[27].

Waarom wordt LACP gebruikt?

LACP wordt gebruikt om twee hoofdredenen[28]:

- Capaciteit verhogen; hierbij kan de data over meerdere verbindingen gestuurd worden terwijl logisch gezien er nog maar één verbinding is. Op deze manier kan verkeer geloadbalanced worden. Ook wordt hiermee de bandbreedte verhoogt. Bij het bundelen van de verbindingen hoeft geen fysieke verandering plaats te vinden. De verbindingen die al in de apparatuur zit hoeft alleen nog geconfigureerd te worden tot een Link Aggregation.

- Redundantie; Als één van de verbindingen uitvalt, kunnen de overige verbindingen gewoon door met het versturen van de data. Hierbij hoeft geen tussenkomst plaats te vinden van een gebruiker. Echter als de verbinding weer up is, moet er wel gecontroleerd worden of deze weer onderdeel is van de Link Aggregation.
- Er vindt een onderhandeling plaats om de link aggregatie op te stellen.
- Bij een statische link aggregatie zal de verbinding direct actief worden met de kans dat het verkeer naar een verkeerde port wordt gestuurd (bij een path of config fout)

Hoe werkt het Link Aggregation Control Protocol
LACP gebruikt het bundelen van de verbindingen en zorgt hiermee voor redundantie en capaciteit verhoging (bandbreedte verhoging). Op het moment dat LACP gebruikt wordt, zal de switch de gebundelde verbindingen zien als één verbinding in plaats van meerdere. Alle data zal logisch gezien over deze verbinding gaan, fysiek gezien gaat de data geloadbalanced over alle verbindingen heen[28].

8.2.4 Rapid Spanning Tree Protocol

Hieronder wordt uitgelegd wat het Rapid Spanning Tree Protocol(RSTP) is, waarom er gebruik gemaakt word van RSTP en hoe RSTP werkt.

Wat is het Rapid Spanning Tree Protocol
Het Rapid Spanning Tree Protocol is de snellere versie van de standaard Spanning Tree Protocol. Hierbij heeft STP het grote nadeel dat de omschakelingstijd bij het uitvallen van een verbinding hoog is. Door dit nadeel is er nagedacht over een nieuw protocol, maar wel met dezelfde werking. Hiermee is RSTP ontwikkeld door de IEEE groep[29].

Waarom wordt RSTP gebruikt?
RSTP wordt in netwerken gebruikt om loops te voorkomen. Hierbij zal RSTP net als STP een verbinding blokkeren om de loop te verwijderen uit het netwerk. Echter heeft RSTP een snellere omschakelingstijd dan STP. Waar STP er tussen de 30 en 50 seconden over doet, is RSTP omgeschakeld in minder dan 2 seconden[29].

Hoe werkt
Zoals hierboven al verteld wordt, de werking van RSTP is bijna identiek aan de werking van STP. Hierbij blokkeert RSTP een verbinding om loops uit netwerken te halen. De keuzes van welke verbinding er geblokkeerd wordt is hetzelfde als die van STP. Omdat STP al uitgebreid uitgelegd is zal er nu niet opnieuw uitgelegd worden hoe deze keuzes gemaakt worden[29].

Echter gebruikt RSTP naast de standaard port statussen ook nog twee extra port statussen:
- Alternate port: het beste alternatieve path naar de Rootswitch. Dit path is anders dan de Root port. Vaak is het path van dan ook anders dan die van de Root port.
- Back-up port; een back-up/redundant path naar een andere switch die al met een andere verbinding verbonden is. Hierbij is het niet de hoofdverbinding van bijvoorbeeld Switch A naar B. Het gaat hier over een redundante verbinding. Deze wordt pas gebruikt als de hoofdlijn naar deze switch uitvalt.

Naast de extra port statussen gebruikt RSTP ook andere verbinding statussen dan STP. Bij STP kan de status van een verbinding zijn: Blocking, Listening, Learning en Forwarding. RSTP maakt gebruik van de volgende statussen:

- Discarding; de port forward geen frames, verwerkt geen verkeer en leert ook geen MAC-adressen, maar luistert wel of er BPDU's binnenkomen. (dit doet de Blocking status bij STP)
- Learning; Ontvangt en verstuurt frames, ook worden MAC-adressen geleerd. Er forward geen frames. (Zelfde als bij STP)
- Forwarding; ontvangt en stuurt frames, MAC-adressen worden geleerd en er worden BPDU's ontvangen en gestuurd. (Zelfde als bij STP)

Ondanks dat de Learning status hetzelfde wordt gebruikt als bij STP, duurt het bij RSTP maar een aantal seconden. Dit komt doordat er bij RSTP met alle poorten wordt geconvergeerd als de poorten in Forwarding of Discarding status staan

8.3 Compatibiliteit met de huidig gebruikte protocollen

Als laatste zal in dit hoofdstuk de laatste sub-vraag behandeld worden. Namelijk de vraag: "*Is er compatibiliteit mogelijk met de huidig gebruikte protocollen?*". Hierbij worden de protocollen die hierboven besproken zijn en gebruikt worden in de huidige infrastructuur behandeld. Ieder protocol wordt apart behandeld of deze inderdaad compatible is met SPB of dat er een extra handeling nodig is om de infrastructuur naar de nieuwe situatie te migreren. SPB is gekozen als TRILL variant omdat, er gewerkt wordt met Alcatel apparatuur. Dit zorgt ervoor dat er geen hardware verandering plaats hoeft te vinden in het netwerk.

SPB met Virtual Chassis

Een Virtual Chassis is het stacken (verbinden) van switches en het als één logische switch te laten werken. De Virtual Chassis kijkt als één logische switch naar welke protocollen er op hem draaien. Hierbij kan dus zowel RSTP (huidige situatie) als SPB (Proof of Concept) compatible zijn[30].

SPB met VRRP

Net als bij de oude situatie, zal VRRP werken tussen de Virtual Chassis en zal geen last hebben van het protocol dat tussen de overige switches draait. Ook omdat VRRP gebruik maakt van IP-adressen en RSTP/SPB gebruik maken van routering op basis van MAC-adressen. Hiermee kan worden vastgesteld dat VRRP en SPB los van elkaar draaien en daarmee dus compatible zijn[31].

SPB met LACP

LACP is het bundelen van een verbinding, hierbij maakt het echter niet uit van wat voor protocol de verbinding is voorzien. LACP ziet niet of een verbinding met RSTP of met SPB werkt. Hierbij is er dus compatibiliteit aanwezig tussen SPB en LACP[32].

SPB met RSTP

Als SPB in het netwerk alleen in bijvoorbeeld de core wordt geplaatst en RSTP blijft op de Access switches werken, dan moet er compatibiliteit zijn tussen de protocollen. Nu is het zo dat beide protocollen bedacht zijn door de groep van IEEE. Zelfs is het zo dat SPB de functionaliteiten van RSTP in zijn eigen protocol heeft verworven[18][33].

8.4 Conclusie huidige infrastructuur

Topologie huidig netwerk

De topologie van de huidige infrastructuur is gebaseerd op één van de klanten waar Qi ict bv. het netwerk heeft aangelegd en beheerd. Hierbij gaat het om een netwerk dat de redundantie van de verbindingen beheert door middel van het Rapid Spanning Tree Protocol. In dit hoofdstuk wordt de topologie in twee delen opgedeeld, een fysieke topologie en een logische topologie.

Uit de fysieke topologie werd duidelijk dat het netwerk in twee aparte datacenters kon worden opgedeeld. De apparatuur die gebruikt wordt zijn Alcatel Omniswitches. De beide datacenters hebben ieder een eigen Virtual Chassis dat de core vormt voor dat datacenter. Beide Virtual Chassis zijn full-mesh verbonden en vormen samen een collapsed core voor het gehele netwerk.

Uit de logische tekening kan worden gehaald dat VRRP wordt gebruikt om een Single point-of-Failure uit de core te voorkomen. Ook wordt duidelijk dat Access_Sw2 gebruik maakt van een Link Aggregation voor de verbindingen naar de Virtual Chassis.

Voor de nieuwe situatie die gemigreerd wordt vanuit bovenstaande situatie geldt dat de functionaliteiten hetzelfde moeten blijven. Hierbij moet PC1 data naar PC2 kunnen sturen. Hierbij wordt dan RSTP vervangen door SPB. In deze infrastructuur is de keuze gemaakt tussen TRILL en de verschillende varianten, waaronder SPB en is tot de conclusie gekomen dat SPB het beste protocol is om te gebruiken voor deze simulatie.

Gebruikte protocollen

Virtual Chassis(VC) is een technologie die gebruik maakt van stack switches, hierbij worden meerdere switches met elkaar verbonden en worde de switches logische wijs gezien als 1 switch. De switches hebben samen 1 switch Fabric, 1 Control Plane, 1 Configuratie bestand en 1 Operating System. Virtual Chassis wordt gebruikt vanwege een aantal voordelen:

- Zorgt voor redundantie door meerdere switches te ‘stacken;
- Beter beheerbaar doordat alle switches 1 Config file gebruikt;
- Beter schaalbaard door de mogelijkheid om meerdere switches toe te voegen aan het Virtual Chassis, zonder configuratie;
- Efficiënter kabelbeheer, in plaats van honderden kabels nodig te hebben voor één specifieke switch in een rack, kan er ook een chassis gebruikt worden die bestaat uit meerdere switches
- Lagere kosten, het aanschaffen van meerdere kleine switches, die onderdeel worden van een virtual chassis, zorgt voor de spreiding van kosten. Ook is door het stapelen van de switches minder ruimte nodig in een rack, mede hierdoor is er ook minder koeling en elektriciteit nodig.

Een Virtual Chassis werkt met een Master-Slave principe. Hierbij is een switch in de VC de Master en de andere switches zijn Slaves. De Master bekijkt waar het verkeer naartoe moet en bepaalt de paths naar de volgende hop. Als de Master uitvalt, zal een Slave zijn Master rol overnemen. Als een Slave uitvalt, blijft de huidige Master switch de Master. De Master wordt in de logische verbinding weergegeven.

Er zijn poorten op een aantal Alcatel Omniswitches die ingesteld kunnen worden op “automatic Virtual Fabric Link (VFL). Deze moeten echter wel vooraf ingesteld worden. Hierbij zijn echter wel een aantal voorwaarden om dit werkend te krijgen.

Virtual Router Redundancy Protocol(VRRP) is lid van de First-Hop Redundancy Protocol familie en is de IETF standaard. VRRP is een layer 3 redundantie protocol dat meerdere routers/switches voorziet van redundante routing services naar gebruikers. Virtual Router Redundancy Protocol wordt gebruikt voor het elimineren van het 'single point of failure' mede door het handmatig configureren van een default gateway adres op elke host in het netwerk. VRRP werkt net als Virtual Chassis met een Master-Slave principe, hierbij wordt de Master de router/switch die de frames ontvangt. De Slave staat op *stand-by* en zal niets doen voor dit VRRP netwerk. Pas als de Master uitvalt, zal de Slave actie ondernemen.

Een Link Aggregation is het bundelen van meerdere parallelle verbindingen tot een enkele (logische) verbinding om de doorvoer van het netwerk verkeer te verhogen. Voor het samenvoegen van Ethernet verbindingen is het LACP protocol de standaard. LACP en andere vormen van Link Aggregation zijn bijna identiek, alleen is het met LACP het geval dat deze poorten zichzelf kunnen configureren in trunk groepen zonder dat er tussenkomst is van een persoon. LACP is de IEEE standaard, terwijl Link Aggregation meer als overkoepelende term wordt gebruikt. LACP wordt vanwege twee hoofdredenen gebruikt:

- Het verhogen van de capaciteit;
- Redundantie;

LACP gebruikt het bundelen van de verbindingen en zorgt hiermee voor redundantie en capaciteit verhoging (bandbreedte verhoging). Op het moment dat LACP op de verbinding gebruikt wordt zal de switch de gebundelde verbindingen zien als één verbinding in plaats van meerdere. LACP moet op beide switches worden uitgevoerd, hierbij kan er nog gekozen worden in welk mode de switchpoorten staan waar LACP op draait.

Het Rapid Spanning Tree Protocol is de snellere versie van de standaard Spanning Tree Protocol. Hierbij heeft STP het grote nadeel dat de omschakelingstijd bij het uitvallen van een verbinding hoog is. Dit is dan ook de reden waarom RSTP de voorkeur krijgt boven STP.RSTP gebruikt naast de standaard port statussen ook nog twee extra port statussen:

- Alternate port;
- Back-up port;

Naast de extra port statussen gebruikt RSTP ook andere verbinding statussen dan STP. Bij STP kan de status van een verbinding zijn: Blocking, Listening, Learning en Forwarding. RSTP maakt gebruik van de volgende statussen:

- Discarding;
- Learning;
- Forwarding;

Ondanks dat de Learning status hetzelfde wordt gebruikt als bij STP, duurt het bij RSTP maar een aantal seconden. Dit komt doordat er bij RSTP met alle poorten wordt geconvergeerd als de poorten in Forwarding of Discarding status staan

Compatibiliteit protocollen met SPB

Alle protocollen die hierboven zijn besproken zijn compatible met het Shortest Path Bridging protocol. Hierbij is het geval dat Virtual Chassis en VRRP niets met SPB te maken hebben. Deze protocollen draaien apart van elkaar. Het Link Aggregation Control Protocol (LACP) ziet niet welk protocol er over een verbinding loopt. LACP bundelt alleen verbindingen en is daarmee dus compatible met SPB. Als SPB in het netwerk alleen in bijvoorbeeld de core wordt geplaatst en RSTP blijft op de Access switches werken, dan moet er compatibiliteit zijn tussen de protocollen. Nu is het zo dat beide protocollen bedacht zijn door de groep van IEEE. Ook vallen beide protocollen onder de categorie van 802.1 protocollen. Zo is SPB 802.1aq en is RSTP 802.1w.

9. Conclusie onderzoek

Uit het Literatuuronderzoek kan geconcludeerd worden dat het mogelijk is om STP uit een switched core netwerk van Qi ict bv. te faseren.

Allereerst is het mogelijk om STP uit een netwerk te faseren. Eén van de voorwaarden is wel dat TRILL gebruik maakt van Rbridges in plaats van standaard switches. Hierdoor moet de hardware die in het netwerk gebruik wordt wel TRILL 'ready' zijn. Als dit niet het geval is zouden deze nog vervangen kunnen worden, echter kost dit wel meer tijd en geld.

Nadat duidelijk werd dat STP uit te faseren is, moest er gekeken worden naar wat voor een netwerk er gebruikt wordt voor deze opdracht. In het netwerk waar STP uit gefaseerd moet worden draait niet de standaard STP, maar het Rapid Spanning Tree Protocol. Dit protocol werkt in principe hetzelfde als STP, alleen heeft RSTP een snellere omschakelingstijd bij het uitvallen van een verbinding.

Ook werd duidelijk dat de apparatuur fabrikant waarmee gewerkt word Alcatel is. Een eis bij het uit faseren van STP was, dat de apparatuur hetzelfde zou blijven. Hierdoor zullen de TRILL varianten FabricPath en VCS afvallen, omdat dit TRILL proprietary varianten van Cisco en van Brocade zijn. SPB daarentegen wordt wel ondersteund door Alcatel. Hierdoor is de keuze gevallen op SPB om RSTP uit het huidige netwerk te faseren.

Naast RSTP werken er nog meerdere protocollen, deze protocollen moeten ook compatible zijn met een variant van TRILL. Anders is de uitfasering van STP lastiger uit te voeren. De protocollen waar het hier om gaat zijn Virtual Chassis, Virtual Router Redundancy Protocol(VRRP) en het Link Aggregation Control Protocol(LACP). Uit het onderzoek kwam naar voren dat alle protocollen op het netwerk compatible zijn met SPB. Hierdoor zullen er geen conflicten ontstaan, omdat de protocollen naast elkaar of met elkaar werken.

Terminologielijst

Term	Definitie
STP	Spanning Tree Protocol; protocol gebruikt in switched netwerken om loops te voorkomen.
TRILL	Transparent Interconnection of Lots of Links (TRILL), de IETF standaard om STP te vervangen
IS-IS	Intermediate System-to-Intermadiate System; het routing protocol dat gebruikt wordt door TRILL.
FP	FabricPath; de Cisco proprietary variant van TRILL.
VCS	Virtual Cluster Switching; de Brocade proprietary variant van TRILL.
SPB	Shortest Path Bridging; de IEEE standard ontwikkelt als vervanger van STP.
ECMP	Equal Cost Multipath; het verdelen van de data over meerdere verbindingen.
SPF	Shortest Path First; protocol om het beste path naar een destination te bepalen.
RB	Root Bridge; De switches die TRILL ondersteunen.
DRB	Designated Router Bridge; bepaalt de VLAN voor onderlinge communicatie, ook kiest de Appointed Forwarder.
AF	Appointed Forwarder; een switch die alleen verkeer ontvangt en doorstuurt van een bepaalde VLAN.
RSTP	Rapid Spanning Tree Protocol; STP variant, wordt gebruikt vanwege de snellere omschakelingstijd in vergelijking met STP.
MSTP	Multi Spanning Tree Protocol; STP variant, wordt gebruikt vanwege de betere schaalbaarheid in vergelijking met STP.
LACP	Link Aggregation Control Protocol; een protocol gebruikt om meerdere fysieke verbindingen te bundelen tot één logische verbinding.
VRRP	Virtual Router Redundancy Protocol; protocol voor het elimineren van ‘single point of failure’ in een netwerk.
VC	Virtual Chassis; het stapelen van meerdere fysieke switches en de switches logischer wijs als één enkele switch te laten werken/configureren.

Literatuurlijst

[1] Hucaby, D. (2010, februari) *CCNP SWITCH 642-813 Official Certification Guide,* Pearson Education. (geraadpleegd op 11 mei 2016).

[2] Odom, W. (2015, februari). *Cisco CCNA Routing and Switching Official Cert Guide,* Pearson Education. (geraadpleegd op 9 mei 2016).

[3] Perlman, R., Eastlake, D. (2011, september) *Introduction to TRILL, The Internet Protocol Journal, Volume 14, No.3.* http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_14-3/143_trill.html (geraadpleegd op 16 mei 2016).

[4] Perlman, R., Eastlake, D., Ghanwani, A., Dutt, D., Manral, V. (2011, juli) *Routing Bridges (RBridges): Adjacency*. RFC 6327. http://tools.ietf.org/search/rfc6327 (geraadpleegd op 16 mei 2016).

[5] Perlman, R., Eastlake, D., Ghanwani, A., Dutt, D., Gai, S. (2011, juli) *Routing Bridges (RBridges): Base Protocol Specification*. RFC 6325. http://tools.ietf.org/search/rfc6325 (geraadpleegd op 18 mei 2016).

[6] Huawei Technologies co. LTD. (2013, maart) *Technology White paper – TRILL.* http://enterprise.huawei.com/ilink/cnenterprise/download/HW_259594 . (geraadpleegd op 18 mei 2016).

[7] Perlman, R., Eastlake, D., Li, Y., Banerjee, A., Hu, F. (2011, november) *Routing Bridges (RBridges): Appointed Forwarders*. RFC 6439. http://tools.ietf.org/html/rfc6439 (geraadpleegd op 18 mei 2016).

[8] Eastlake, D. (2013, oktober) *TRILL Tutorial Transparent Interconnection of Lots of Links.* RIPE TRILL Tutorial. https://ripe67.ripe.net/presentations/135-TRILLtutorial44a.pdf (geraadpleegd op 18 mei 2016).

[9] Cisco systems. (jaar onbekend) *FabricPath Forwarding*. http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/fabricpath/configuration/guide/fp_forwarding.pdf (geraadpleegd op 23 mei 2016)

[10] Schönekerl, J-A. (2014, februari) *FabricPath :: Part I – The basics.* http://www.cloudstructured.com/network/fabricpath/fabricpath-deep-dive/ (geraadpleegd op 23 mei 2016)

[11] Dawani, A. (2010) *FabricPath/TRILL/OTV*. http://www.cisco.com/web/JP/event/es/postevent/123/iaf2012/thankyou/docs/4_iaf_FabricPathTrillOTV.pdf (geraadpleegd op 23 mei 2016)

[12] Day, S. (2010, november) *Scaling the DC Architecture: Be Ready for the Cloud Evolution*. http://www.cisco.com/web/DK/assets/docs/presentations/A1-Scaling-the-DC-external.pdf (geraadpleegd op 23 mei 2016)

[13] Cisco systems. (2013, oktober) *Nexus 7000 FabricPath White Paper Version 2.0*. http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9402/white_paper_c11-687554.html#wp9000496 (geraadpleegd op 23 mei 2016)

[14] Fuller, R. (2010, oktober) *Full-tilt boogie networking: Cisco`s FabricPath vs. IETF TRILL.* http://www.networkworld.com/article/2227471/cisco-subnet/full-tilt-boogie-networking--cisco-s-fabricpath-vs--ietf-trill.html (geraadpleegd op 26 mei 2016)

[15] Brocade Communication Systems. (2012) *DATA CENTER Brocade VCS Fabric Technical Architecture.* http://www.brocade.com/downloads/documents/technical_briefs/vcs-technical-architecture-tb.pdf (geraadpleegd op 24 mei 2016)

[16] Brocade Communication Systems. (2013, december) *Network OS Administrator`s Guide*. http://www.brocade.com/downloads/documents/product_manuals/B_VDX/NOS_AdminGuide_v400.pdf (geraadpleegd op 24 mei 2016)

[17] Fedyk, D. (2012, oktober). *Introduction to Shortest Path Bridging.* https://www.netnod.se/sites/default/files/SPB-fedyk-091012.pdf (geraadpleegd op 25 mei 2016)

[18] Ashwood-Smith, P. (2010, oktober). *Shortest Path Bridging IEEE802.1aq Tutorial and Demo*. https://www.nanog.org/meetings/nanog50/presentations/Sunday/IEEE_8021aqShortest_Path.pdf (geraadpleegd op 25 mei 2016).

[19] Fedyk, D. (2010, juli). *Shortest Path Bridging IEEE802.1aq Overview.* https://www.internet2.edu/presentations/jt2010july/20100712-Shortest_Path_Bridgingv3-Fedyk.pdf (geraadpleegd 25 mei 2016)

[20] Avaya Inc. (2010) *Compare and Contrast SPB and TRILL.* http://techdata.com/business/avaya/DataCenterSolutions/files/A%20- %20Why%20Avaya/2%20-%20Learn%20More%20About%20VENA/SPB-TRILL_Compare_Contrast-DN4634.pdf (geraadpleegd 27 mei 2016)

[21] DeCusatis, C. J., Carranza, A., DeCusatis, C.M.(2012) *Communication within Clouds: Open Standards and Proprietary Protocols for Data Center Networking.* http://ms14.voip.edu.tw/~sandra/paper/CwC.pdf (geraadpleegd 27 mei 2016)

[22] Juniper Networks. (2015, september) *Network Simplification with Juniper Networks Virtual Chassis Technology.* https://www.juniper.net/us/en/local/pdf/whitepapers/2000427-en.pdf (geraadpleegd 1 juni 2016)

[23] Alcatel-Lucent. (jaar onbekend) *Configuring Virtual Chassis.* http://enterprise.alcatel-lucent.com/assets/documents/userguides/AOS-Release-8-Switch-Management-Guide/!SSL!/Multiscreen_HTML5/desktop/os8_sw/s_vc/s_vc.htm#XREF_73939_Virtual_Chassis (geraadpleegd 1 juni 2016)

[24] TechTarget. (2006, augustus) *VRRP (Virtual Router Redundancy Protocol).* http://searchnetworking.techtarget.com/definition/VRRP (geraadpleegd 6 juni 2016)

[25] Extreme networks. (2014) *Data Center Solutions Guide.* http://learn.extremenetworks.com/rs/extreme/images/Data-Center-Solutions-Guide-WP.pdf (geraadpleegd 6 juni 2016) (geraadpleegd 6 juni 2016)

[26] R. Hinden. (2004, april) *Virtual Router Redundant Protocol (VRRP).* RFC 3768. http://tools.ietf.org/html/rfc3768 (geraadpleegd 6 juni 2016)

[27] Rajesh K, excitingip.com. (2012, mei) *LAG (Link Aggregation Group) & LACP (Link Aggregation Control Protocol) – An Intro.* http://www.excitingip.com/3015/lag-link-aggregation-group-lacp-link-aggregation-control-protocol-an-intro/ (geraadpleegd 7 juni 2016)

[28] The Network Way. (2015, mei) *An Overview of Link Aggregation and LACP.* https://thenetworkway.wordpress.com/2015/05/01/an-overview-of-link-aggregation-and-lacp/ (geraadpleegd 7 juni 2016)

[29] 9tut. (2015, juni) *Rapid Spanning Tree Protocol RSTP tutorial.* http://www.9tut.com/rapid-spanning-tree-protocol-rstp-tutorial (geraadpleegd 7 juni 2016)

[30] Alcatel-Lucent. (jaar onbekend) *Configuring Shortest Path Bridging.* http://enterprise.alcatel-lucent.com/assets/documents/userguides/OmniSwitch-AOS-Release-8-Network-Configuration-Guide/!SSL!/Multiscreen_HTML5/desktop/os8_nt/n_spb/n_spb.htm (geraadpleegd 10 juni 2016)

[31] Boe. G, Faltinsen. V, Lillebrygfjeld, E. (2011, december) *Recommendations for a redundant campus network.* http://services.geant.net/cbp/Knowledge_Base/Campus_Networking/Documents/gn3-na3-t4-ufs114.pdf (geraadpleegd 10 juni 2016)

[32] Alcatel-Lucent. (2015, april) *Auto Fabric Workflow on Alcatel-Lucent OmniSwitch.* Auto_fabric_workflow_Application_Note.pdf (geraadpleegd 10 juni 2016)

[33] TechPowerUp. (2012, mei) *IEEE approves new IEEE 802.1aq Shortest Path Bridging Standard.* http://www.techpowerup.com/165594/ieee-approves-new-ieee-802-1aq-shortest-path-bridging-standard (geraadpleegd 10 juni 2016)

Bijlage E

Ontwerprapport

Ontwerprapport

Opdrachtgever: Qi ict bv.
Begeleider: Hans Suttorp
Afstudeerder: Frank van Eijk
Opleiding: Technische Informatica, HHS Delft
Datum: 03-10-2016
Versie: 1.0

Versiebeheer

Versie	Datum	Opmerking
0.1	24-6-2016	Eerste versie
0.2	06-7-2016	Aanpassingen doorgevoerd na feedback van dhr. Hans Suttorp
1.0	30-9-2016	Opmaak consistent gemaakt

Inhoudsopgave

Figuren

Tabellen

1. Inleiding

Om het onderzoek te ondersteunen zal er een huidige situatie worden gebouwd. Deze huidige situatie is gebaseerd op één van de vele klanten waar Qi ict bv. haar diensten levert. Aan de hand van de huidige situatie zal een Proof of Concept gerealiseerd worden waarna deze verderop in het onderzoek met elkaar vergeleken kunnen worden.

In dit rapport zal de huidige situatie in het kort uitgelegd worden in betrekking tot apparatuur, protocollen en bekabeling. Ook zullen de fysieke en logische ontwerpen van het huidige netwerk behandeld worden.

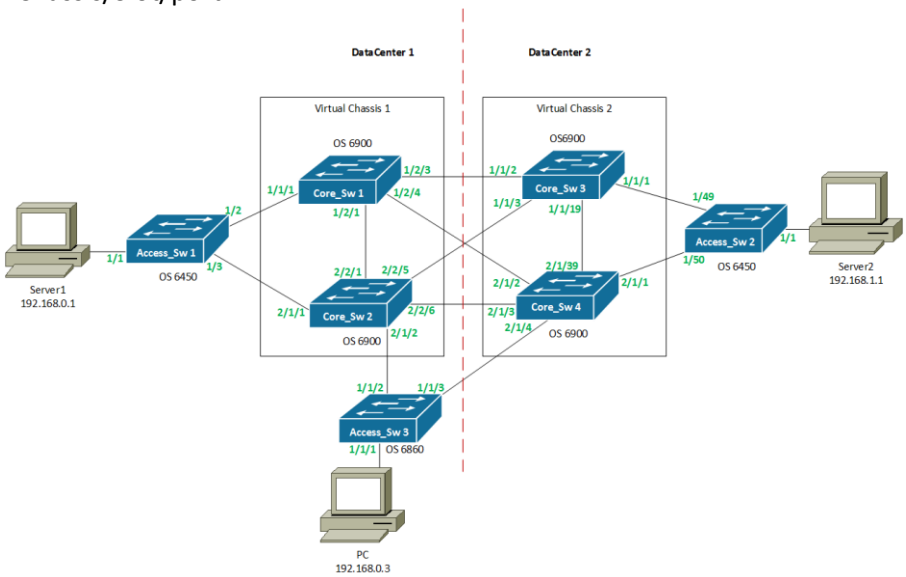
Voordat het Proof of Concept netwerk ontworpen kan worden zullen er eisen worden opgesteld waaraan het Proof of Concept moet voldoen. Aan de hand van de huidige situatie en de eisen zal het Proof of Concept ontworpen worden. Ook deze ontwerpen worden opgedeeld in een fysiek en een logisch ontwerp.

2. Ontwerp huidige situatie

Voordat de huidige situatie gebouwd kan worden zal deze eerst geanalyseerd moeten worden. De benodigdheden worden onder de fysieke topologie genoemd. Van de huidige situatie zijn twee ontwerpen verkregen: een fysiek ontwerp en een logisch ontwerp. Hierbij geeft de fysieke topologie alle tastbare elementen weer van het ontwerp. Het logische ontwerp laat zijn hoe het netwerk de protocollen gebruikt. De huidige situatie is ook in het literatuuronderzoek behandeld.

2.1 Fysieke topologie

Onderstaande topologie weergeeft de huidige fysieke situatie. Aan de hand van deze topologie kunnen de apparatuur en bekabeling geconcludeerd worden. De poorten worden aangeduid in "Chassis/Slot/port".



Figuur 1 Fysieke topologie huidig netwerk

Apparatuur

In dit netwerk wordt gebruik gemaakt van 4 Core switches en 3 Access switches. De apparatuur die gebruikt word zijn Alcatel switches. Dit kan gezien worden aan de OS die staat voor OmniSwitch. Hierbij zijn de versies 6450, 6860 en 6900 gebruikt. Hierbij zijn van de OS6900 de volgende versies gebruikt: T20, T40, X20, X40.

Bekabeling

Voor de bekabeling moet er duidelijk worden wat voor aansluitingen elke switch beschikt en hoe deze aan elkaar aangesloten kunnen worden. In onderstaande opsomming worden de poorten per switch weergegeven:

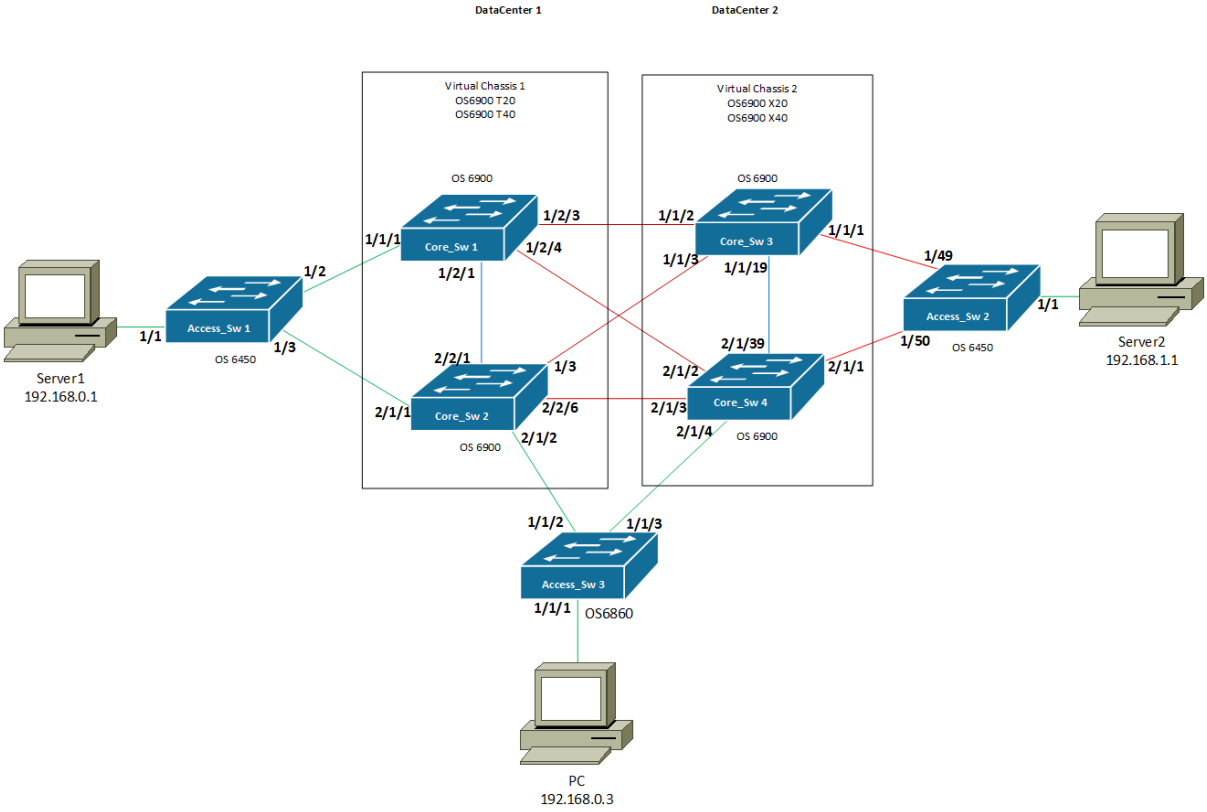
- De OS6450-24 beschikt over 24 RJ45 poorten, dit zijn koper poorten. Ook beschikt de OS6450 over 2 SFP poorten[1].
- De OS6450-48 beschikt over 48 RJ45 poorten, dit zijn koper poorten. Ook beschikt de OS6450 over 2 SFP poorten[1].
- De OS6860-24 beschikt over 24 Base-T poorten, dit zijn ook koper poorten. Ook beschikt de OS6860-24 over 4 SPF poorten[2].
- De OS6900-T20 beschikt over 20 10GBase-T poorten, dit zijn koper poorten[3].
- De OS6900-T40 beschikt over 40 10GBase-T poorten, dit zijn koper poorten[3].
- De OS6900-X20 beschikt over 20 SFP poorten[3].
- De OS6900-X40 beschikt over 40 SFP poorten[3].

Voor de bekabeling van het netwerk blijkt dat de OS6900-X20 en de OS6900-X40 alleen maar over SFP+ poorten beschikken. Op deze poorten kunnen niet direct kabels worden gepatcht, maar zal op deze poorten een SFP module aangesloten worden. Er wordt dus gebruik gemaakt van 1 koper en 16 fiber SFP's. Waarvan 4 SFP's 10 Gig ondersteunen en 12 SFP's 1 Gig ondersteunen.

De OS6900-X20 en OS6900-X40 beschikken over een module binnen in de switches waardoor zij met behulp van 10 gig SFP's als Virtual Chassis geconfigureerd kunnen worden. Voor de OS6900-T20 en OS6900-T40 moet er een extra module gebruikt worden, omdat Virtual Chassis alleen met 10 Gig glasvezel gerealiseerd kunnen worden. Hiervoor worden de expansion module OS-HNI-U6 en OS-XNI-U12 gebruikt. De SFP poorten zullen worden voorzien van de 10 Gig glasvezel SFP's en deze poorten zijn geconfigureerd om als VF-links te dienen. Mede hierdoor bestaat er één Virtual Chassis uit de OS6900-T20 met de OS6900-T40 en bestaat de andere Virtual Chassis uit de OS6900-X20 met de OS6900-X40.

Door bovenstaande kenmerken ziet de bekabeling er als volgt uit:

- Virtual Chassis verbinding (10 Gig fiber)
- Koper
- Glasvezel

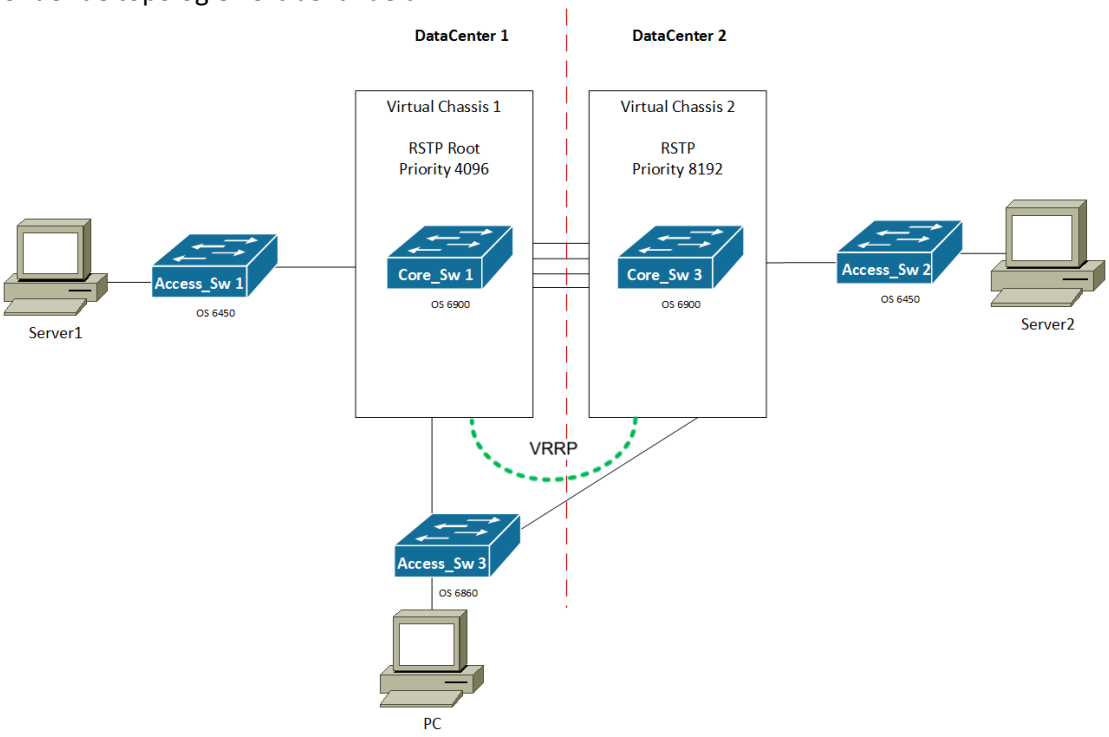


Figuur 2 Bekabeling netwerk

Uit bovenstaande afbeelding kan gehaald worden dat de 10 Gig fiber SFP's gebruikt zullen worden op de OS6900; waarbij elke switch één 10 Gig SFP krijgt. Twee fiber SFP's zullen op de OS6450 geplaatst worden die als Access_Sw2 gebruikt wordt. De overige fiber SFP's zullen in de OS6900 geplaatst worden om de core te verbinden. De koper SFP zullen gebruikt worden op de OS6900-X20 om de switch met Access_Sw3 te verbinden.

2.2 Logische topologie

De logische topologie geeft weer hoe het netwerk gebruik maakt van de aanwezige verbindingen. Hierbij hebben de werking van de protocollen een grote rol. Om onderstaande logische topologie te begrijpen moet er duidelijk zijn welke protocollen er gebruikt worden. Deze protocollen worden onder de topologie kort behandeld.



Figuur 3 Logische topologie huidig netwerk

Protocollen

De protocollen die op het huidige netwerk werken zijn

- Virtual Chassis
- Virtual Router Redundancy Protocol
- Link Aggregation Control Protocol
- Rapid Spanning Tree Protocol

Elk protocol is in het literatuuronderzoek uitgebreider behandeld. Hierin wordt uitgelegd wat elk protocol is, waarom het protocol wordt gebruikt, hoe het protocol werkt en hoe het protocol geconfigureerd kan worden.

In onderstaande tabel wordt aangegeven welke protocollen ondersteunt worden door de gebruikte switches[1][2][3]:

	OS6450-24	OS6450-48	OS6860	OS6900-T20	OS6900-T40	OS6900-X20	OS6900-X40
Virtual Chassis	X	X	X	X	X	X	X
VRRP	X	X	X	X	X	X	X
LACP	X	X	X	X	X	X	X
RSTP	X	X	X	X	X	X	X

Tabel 1 Compatibiliteit huidige protocollen op switch

3. Requirements Proof of Concept

De functionaliteit van het netwerk blijft dat de PC de servers kan bereiken, zelfs bij het uitvallen van een switch of een verbinding. Hierbij zijn een aantal uitzonderingen, zoals de Acces switches. Om deze werking te verwezenlijken zullen er een aantal eisen worden gesteld aan het Proof of Concept.

- *De functionaliteit van het netwerk blijft hetzelfde.*
- *SPB gaat RSTP in het netwerk vervangen*
- *Apparatuur zal niet vervangen worden*

Hieronder worden de eisen kort toegelicht:
De functionaliteit blijft hetzelfde; Hierbij gaat het erom dat vanaf de PC nog steeds beide servers kan bereiken door middel van ICMP-berichten.

SPB gaat RSTP in het netwerk vervangen; In de huidige situatie wordt er door het hele netwerk RSTP gebruikt om de frames door het netwerk te switchen. In het Proof of Concept zal dit gedaan worden door SPB. Dit om te achterhalen of SPB op de plek van RSTP kan draaien.

Apparatuur zal niet vervangen worden; in overleg met de begeleider vanuit Qi ict bv. is er besloten om geen verandering in het netwerk toe te passen wat betreft apparatuur. Hierdoor zal alleen de werking en daarmee het logische ontwerp verandert worden. De fysieke opstelling blijft hetzelfde.

4. Ontwerp Proof of Concept

Voordat het Proof of Concept gebouwd kan worden zal deze situatie eerst ontworpen moeten worden. De benodigdheden blijven hetzelfde als in de huidige situatie. Echter is het wel zo dat Rapid Spanning Tree Protocol vervangen zal worden door Shortest Path Bridging. Hiermee kan geconcludeerd worden dat de ontwerpen van de oude situatie en de nieuwe situatie bijna identiek zijn.

Protocollen

Het enige verschil qua protocollen is dat het Rapid Spanning Tree Protocol vervangen gaat worden door het Shortest Path Bridging protocol. Door deze verandering zullen de volgende protocollen gebruikt worden in de nieuwe situatie: Virtual Chassis, VRRP, LACP en SPB.

SPB is een opvolger van de IEEE standaard Spanning Tree Protocol. SPB gebruikt in tegenstelling tot de STP varianten de gehele bandbreedte, hierbij worden geen verbindingen geblokkeerd. SPB voorkomt layer 2 loops in een netwerk door middel van het IS-IS routing protocol. SPB kan als een variant van TRILL gezien worden door de overeenkomsten in werking. Echter is SPB een IEEE standaard en TRILL is de IETF standaard. Zoals eerder vermeld is elk protocol is in het literatuuronderzoek uitgebreider behandeld. Alleen de werking van SPB is niet uitgebreid behandeld. Hierbij is TRILL echter wel uitgebreid behandeld. Dit omdat TRILL het hoofdonderwerp was van het onderzoek.

Apparatuur

Naast dat de protocollen vast staan, staat ook de apparatuur vast. Er zal namelijk geen verandering komen in de apparatuur en dit betekent dat er nog steeds gebruik gemaakt word van de Alcatel switches. Er zal nog steeds gebruik gemaakt worden van 4 Core switches en 3 Access switches.

In onderstaande tabel wordt aangegeven welke protocollen ondersteunt worden door gebruikte switches[1][2][3]:

	OS6450-24	OS6450-48	OS6860-24	OS6900-T20	OS6900-T40	OS6900-X20	OS6900-X40
Virtual Chassis	X	X	X	X	X	X	X
VRRP	X	X	X	X	X	X	X
LACP	X	X	X	X	X	X	X
RSTP	X	X	X	X	X	X	X
SPB			X *	X	X	X	X

Tabel 2 Compatibiliteit nieuwe protocollen op switch

**om SPB te gebruiken op de OS6860 is een software licentie nodig*

Hieruit wordt duidelijk dat beide OS6450 geen SPB ondersteunen. Ook is duidelijk geworden dat er een software licentie nodig is om SPB op de OS6860 te configureren. Hierdoor is het niet mogelijk om een geheel SPB netwerk te maken met de huidige apparatuur.

4.1 Fysieke topologie

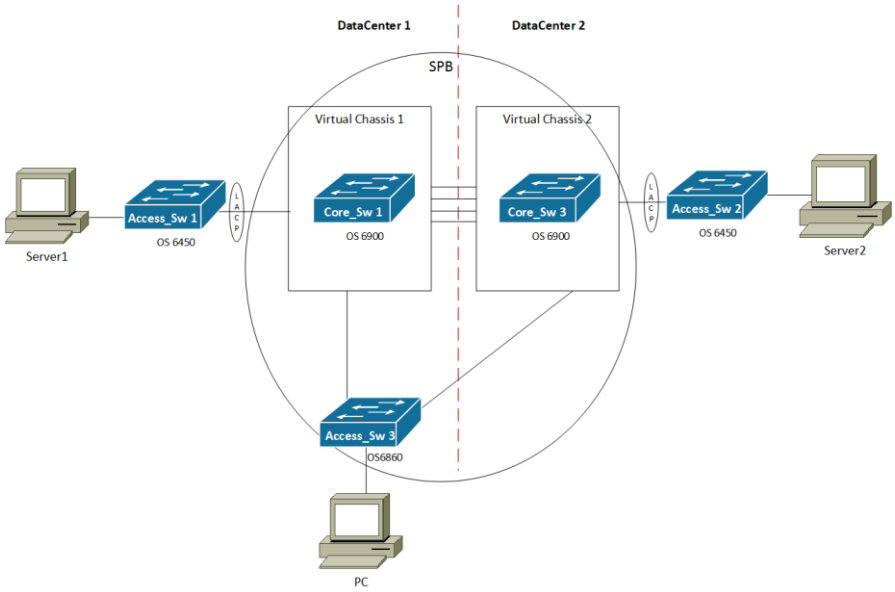
Uit de requirements wordt duidelijk dat de netwerk in fysiek opzicht niet zal veranderen. Het netwerk zal blijven bestaan uit dezelfde apparatuur met dezelfde aansluitingen als in de huidige situatie. Echter is het wel zo dat het netwerk in logisch opzicht zal veranderen.

4.2 Logische topologie

De logische topologie geeft weer hoe het netwerk gebruik maakt van de aanwezige verbindingen. Hierbij hebben de werking van de protocollen een grote rol. Om onderstaande logische topologie te begrijpen moet er duidelijk zijn welke protocollen er gebruikt worden.

In de huidige situatie werd bij de OS6860 gebruik gemaakt van RSTP, hierdoor werd één van de verbindingen geblokkeerd. Bij SPB wordt er echter gebruik gemaakt van alle verbindingen. Uit het onderzoek van de apparatuur blijkt dat de OS6450 geen SPB ondersteunen[1]. Hierdoor zullen deze switches nog steeds gebruik blijven maken van LACP.

Deze verandering in werking verandert echter niets aan de topologie. Beide topologiën blijven op deze manier hetzelfde echter is de verwachting dat de werking van het netwerk wel verandert. Deze verwachting zal getest worden in de experimentele fase.



Figuur 4 Logische topologie Proof of Concept

Literatuurlijst

[1] Alcatel Lucent. (2016, januari) *Alcatel-Lucent Omniswitch 6450*.
http://enterprise.alcatel-lucent.com/assets/documents/OmniSwitch_6450_24-48_datasheet_EN.pdf
(geraadpleegd 14 juni 2016)

[2] Alcatel Lucent. (2015, september) *Alcatel-Lucent Omniswitch 6860.*
http://enterprise.alcatel-lucent.com/assets/documents/OmniSwitch_6860_Datasheet_EN.pdf
(geraadpleegd 14 juni 2016)

[3] Alcatel Lucent. (2016, maart) *Alcatel-Lucent Omniswitch 6900*.
http://enterprise.alcatel-lucent.com/assets/documents/omniswitch_6900_stackable_LAN_switches_datasheet_EN.pdf
(geraadpleegd 14 juni 2016)

Bijlage F

Testdocument

LIVING UPTIME

Testdocument

Opdrachtgever: Qi ict bv.
Begeleider: Hans Suttorp
Afstudeerder: Frank van Eijk
Opleiding: Technische Informatica, HHS Delft

Datum: 03-10-2016
Versie: 1.0

Versiebeheer

Versie	Datum	Opmerking
0.1	1-7-2016	Eerste versie
0.2	6-7-2016	Aanpassingen doorgevoerd na feedback van dhr. Hans Suttorp
1.0	30-9-2016	Aanpassingen doorgevoerd na feedback van dhr. Hans Suttorp Opmaak consistent gemaakt

Inhoudsopgave

Figuren

1. Inleiding

Gedurende de afstudeerstage zal een onderzoek uitgevoerd worden voor Qi ict.

Qi ict is een gespecialiseerde leverancier van hoogwaardige ict infrastructuur oplossingen en diensten. De missie van Qi ict is een zo'n hoog mogelijke uptime realiseren bij zijn klanten. Qi ict realiseert dit door gebruik te maken van producten van technologie leaders (Alcatel, Checkpoint) en met de professionaliteit van hoog opgeleide engineers. Als afstudeerder van Qi ict heb ik de opdracht gekregen om onderzoek te doen of het Spanning Tree Protocol door middel van TRILL uit de gebruikte switched-core netwerken van Qi ict bv. kan worden gefaseerd.

Om dit onderzoek te ondersteunen zal er een Proof of Concept worden gebouwd op basis van het huidige netwerk. Deze huidige situatie is gebaseerd op één van de vele klanten waar Qi ict bv. haar diensten levert.

In dit document wordt weergegeven hoe de beide situaties getest gaan worden. Hierbij worden er verschillende testcases op gesteld en uitgevoerd. Een onderdeel is het testen van de werking van de gebruikte protocollen. Hierin wordt gekeken of de protocollen daadwerkelijk werken zoals uit het literatuuronderzoek is gebleken. Een ander onderdeel van het testen, is het meten van de huidige waardes van de situaties. Hierbij kan gedacht worden aan performance en availability. Deze waardes zullen uiteindelijk met elkaar vergeleken worden om te kunnen concluderen of de nieuwe situatie meer gewenst is als de oude situatie.

2. Test doelstelling

De doelstelling van het testen, is het bevestigen of ontkrachten van de theorie die uit het literatuuronderzoek is voortgekomen. Hierbij werkt het testen ondersteunend om tot een conclusie te komen of het mogelijk en wenselijk is om STP (RSTP) uit netwerken te migreren door middel van een TRILL variant (SPB).

Het testen van de protocol werking is bedoeld om te achterhalen of de gevonden literatuur overeenkomt met de werkelijkheid. Als dit niet het geval is kan de conclusie van het literatuuronderzoek totaal verschillen met de conclusie van het experimentele onderzoek.

De nulmetingen zijn bedoeld om de beide situaties met elkaar te kunnen vergelijken. Op deze manier kan aangegeven worden of één van de twee situaties een meer gewenste werking heeft dan de ander.

3. Test aanpak

Voor ieder protocol is een apart testontwerp ontworpen, op deze manier kan de werking van het specifieke protocol duidelijk vast gesteld worden. Hierbij hebben SPB en RSTP hetzelfde testontwerp. Dit komt omdat beide protocollen hetzelfde het doel hebben.

Om de nulmeting uit te voeren zal er gebruik gemaakt worden van de gehele opstelling die bij de situatie hoort en op deze situatie een aantal testen op uit te voeren aan de hand van een aantal vooraf vastgestelde gebieden. Aangezien het fysieke ontwerp hetzelfde is zal het ontwerp hetzelfde zijn, echter zal de configuratie verschillen.

Voor elke meting en protocoltest is een testcase opgesteld. Hierbij wordt er gebruik gemaakt van dezelfde soort testcase, zowel bij de metingen als bij de werking van de protocollen. Hierbij wordt een beschrijving gegeven van de testcase, over wat er getest gaat worden. Hierna worden de voorwaarden gegeven waaraan de beginsituatie moet voldoen, naast de werking van het algehele netwerk dat in hoofdstuk 4 hieronder wordt behandeld. Als de voorwaarden vast staan, zullen de teststappen uitgelegd worden. Deze stappen zullen uitgevoerd worden om zo tot het uiteindelijke resultaat te kunnen komen. Het resultaat is hier een verwachting, deze verwachting is voortgekomen uit het literatuuronderzoek naar de werking van de protocollen. Bij de meting van het netwerk zal hier uit komen of dat het geteste gebied wel/niet voldoet aan de eis.

De uiteindelijke resultaten zullen woorden weergegeven in het laatste hoofdstuk van dit document: hoofdstuk 7 *“Conclusie resultaten”.* Hierin wordt doormiddel van vinkjes en kruisen aangegeven of het verwachte resultaat ook het definitieve resultaat was. Eventuele opmerkingen worden hierachter geplaatst.

4. Test afbakening

Aan de testopstelling en de simulatie worden een aantal voorwaardes gesteld waaraan het netwerk moet voldoen als er begonnen wordt met testen. Het netwerk moet als basis aan de volgende voorwaarden voldoen:

- Alle componenten werken
- Access switches mogen niet uitvallen; de Access switches zijn Single Point of Failure
- De verbinding tussen PC en servers werkt
    - Hiermee is ICMP-berichten uitwisselen tussen de PC en de servers mogelijk
- Alle verbindingen zijn aangesloten zijn zoals in de ontwerpen zijn aangegeven
- Duurtest wordt gedaan op weekend basis

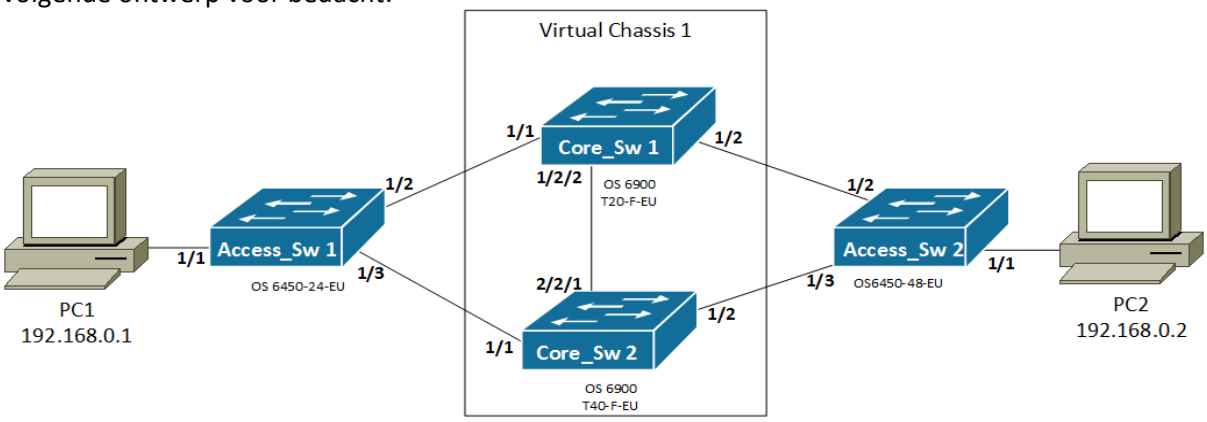
5. Protocol Tests

Om de werking van de protocollen op de netwerken te achterhalen is er gekozen om het netwerk op te delen in deelontwerpen. Uit deze experimenten kan geconcludeerd worden of deze protocollen daadwerkelijk werken zoals in het literatuuronderzoek naar voren kwam. In de deelontwerpen worden alleen de specifieke protocollen getest en geconfigureerd. De andere te testen protocollen worden hier buiten beschouwing gelaten. Zo zullen alle default instellingen van de switches gebruikt worden.

5.1 Virtual Chassis

Uit de literatuur blijkt dat twee fysieke switches als één logische switch werken. Deze Virtual Chassis beheert dan alle switches door middel van één switch Fabric, één Control Plane en één Configuratie bestand. De bekabeling die de switches verbinden om het Virtual Chassis te vormen, hoeven geen STP te ondersteunen. Nu moet dit in de praktijk nog bevestigd of tegengesproken worden.

Het eerste deelontwerp is om te testen hoe een Virtual Chassis werkt. Voor dit experiment is het volgende ontwerp voor bedacht:



Figuur 1 Deelontwerp Virtual Chassis

De apparatuur die gebruikt is om deze deeltestopstelling te bouwen ziet er als volgt uit:

- 1x Alcatel OmniSwitch 6900-T20-F met expansion module OS-HNI-U6
- 1x Alcatel OmniSwitch 6900-T40-F-EU met expansion module OS-XNI-U12
- 1x Alcatel OmniSwitch 6450-24-EU
- 1x Alcatel OmniSwitch 6450-48-EU
- 2x Dell Latitude, OS Windows 7 (laptop)
- 6x UTP kabel
- 1x glasvezel kabel

Met als configuratie op de componenten:

PC1	***PC2***
IP-adres 192.168.0.1 met subnetmask 255.255.255.0	IP-adres 192.168.0.2 met subnetmask 255.255.255.0

Access_Sw1	***Access_Sw2***

Core_Sw1	***Core_Sw2***
Interfaces 1/2/1 als VFL port Chassis-ID 1 (Master switch) EMP adres 192.168.0.10/24	Interfaces 2/2/1 als VFL port Chassis-ID 2 (Slave switch) EMP adres 192.168.0.11/24

Hoe wordt een Virtual Chassis geconfigureerd?
Configuratie van Virtual Chassis op de OS6900[1][2]:
Allereerst zal er een Virtual Chassis ID aan de switch gehangen worden; Hierop zal elke switch een ander nummer hebben.

➔ ***virtual-chassis configured-chassis-id*** <id>

Dan zal de VF-link mode op statisch gezet worden om zelf poorten toe te kunnen voegen:

➔ ***virtual-chassis vf-link-mode*** static

Hierna zal er een VF-link aangemaakt worden en zullen hierbij de poorten worden toegevoegd:

➔ ***virtual-chassis vf-link*** <VFL> ***create***
➔ ***virtual-chassis vf-link*** <VFL> ***member-port*** <port>

Ook moeten de beide switches in dezelfde chassis-group zitten; de groep kan gewijzigd worden door middel van het volgende commando:

➔ ***virtual-chassis chassis-group*** <group-id>

Als laatste wordt er gebruik gemaakt van een EMP-adres. Deze zorgt ervoor dat de switches van elkaar weten of ze nog active zijn als de VF-link wegvalt. De switches zijn alleen met deze link verbonden:

➔ ***ip interface local chassis-id*** <id> ***emp address*** <adres> ***mask*** <mask>

Ook zal er een emp adres voor het virtual-chassis gegeven worden.

➔ ***ip interface master emp address*** <adres> ***mask*** <mask>

De uiteindelijke configuratie stappen:

Op de Master (OS6900-T20)	Op de Slave (OS6900-T40)
virtual-chassis chassis-id *1* ***configured-chassis-id*** *1*	***virtual-chassis chassis-id*** *2* ***configured-chassis-id*** *2*
Virtual-chassis vf-link-mode *static*	***Virtual-chassis vf-link-mode*** *static*
virtual-chassis chassis-id *1* ***vf-link*** *0* ***create***	***virtual-chassis chassis-id*** *2* ***vf-link*** *0* ***create***
virtual-chassis vf-link *0* ***member-port*** *1/2/1*	***virtual-chassis vf-link*** *0* ***member-port*** *2/2/1*
virtual-chassis chassis-group *1*	***virtual-chassis chassis-group*** *1*
ip interface local chassis-id *1* ***emp address*** *192.168.0.10* ***mask*** *255.255.255.0*	***ip interface local chassis-id*** *1* ***emp address*** *192.168.0.11* ***mask*** *255.255.255.0*
ip interface master emp address *192.168.0.20* ***mask*** *255.255.255.0*	

Ook kan gekeken worden hoe de Virtual Chassis configuratie ingesteld staat:

➔ ***show virtual-chassis topology.***

Ook kan er gekeken worden welke poorten er gebruikt worden voor de link tussen de switches:

➔ ***show virtual-chassis vf-link***

Nu deze instellingen zijn doorgevoerd zal er nu getest worden aan de hand van de volgende testcases.

Testcase P1	Is de Virtual Chassis correct geconfigureerd?
Beschrijving	Als eerste test moet er gecontroleerd worden of de Virtual Chassis configuratie in de switch is doorgevoerd. Dit wordt gedaan door te controleren op de switches of de Virtual Chassis is aangemaakt.
Voorwaarden	• Virtual Chassis is geconfigureerd zoals hierboven is aangegeven • Er wordt gebruik gemaakt van het Deelontwerp Virtual Chassis

Teststappen

1	Op beide switches die de Virtual Chassis vormen zal het commando: ***show virtual-chassis topology*** uitgevoerd worden.
2	Hierin wordt gekeken of de beide switches in het Virtual Chassis zitten
3	Op beide switches die de Virtual Chassis vormen zal het commando: ***show virtual-chassis vf-link*** en ***show virtual-chassis vf-link member-port*** uitgevoerd worden.
4	Nu wordt er gekeken of de juiste poorten zijn gebruikt voor de verbinding van de switches.

Verwachte Resultaat

Op de Master switch zal het volgende moeten staan na het invoeren van het commando ***"show virtual-chassis topology"***:

```
Local Chassis: 1

                                          Config
Chas    Role          Status              Chas ID   Pri   Group   MAC-Address
-----+------------+------------------+--------+-----+-----+------------------
 1      Master        Running               1      100     1    <mac address master>
 2      Slave         Running               2      100     1    <mac address slave>
```

Op de Mater switch zal het volgende moeten staan na het invoeren van het commando ***"show virtual-chassis vf-link"***:

```
                                  Primary   Config   Active     Def       Speed
Chassis/VF-Link ID   Oper         Port      Port      Port      Vlan       Type
-------------------+--------+---------+-------+---------+---------+----------
1/0                   Up        1/2/1     1          1         1         10G
2/0                   Up        2/2/1     1          1         1         10G
```

Behaalde Resultaat

```
-> show virtual-chassis topology
Local Chassis: 1
 Oper                                Config   Oper
 Chas  Role         Status           Chas ID  Pri   Group  MAC-Address
-----+-----------+------------------+--------+-----+------+-----------------
 1     Master       Running          1        100   1      e8:e7:32:e6:a0:91
 2     Slave        Running          2        100   1      e8:e7:32:c1:76:29


-> show virtual-chassis vf-link
VFLink mode: Static

                           Primary  Config  Active  Def       Speed
 Chassis/VFLink ID  Oper   Port     Port    Port    Vlan      Type
------------------+-------+--------+-------+-------+---------+----------
1/0                Up      1/2/1    1       1       1         10G
2/0                Up      2/2/1    1       1       1         10G

-> show virtual-chassis vf-link member-port
VFLink mode: Static

 Chassis/VFLink ID  Chassis/Slot/Port  Oper      Is Primary
------------------+------------------+---------+------------
 1/0                1/2/1              Up        Yes
 2/0                2/2/1              Up        Yes
```

Na het configureren en het herstarten van de beide switches zijn de commando's uitgevoerd op de OS6900-T20 (Master) en zijn de resultaten in de afbeelding hiernaast weergegeven.

Hieruit wordt duidelijk dat beide switches geconfigureerd zijn als onderdeel van het Virtual Chassis en dat de juiste poorten geselecteerd zijn als VFL-link.

Testcase P2	Neemt de Slave switch de functionaliteiten over van de Master als deze uitvalt?
Beschrijving	Volgens het literatuuronderzoek zal de Slave switch de functionaliteiten van de Master switch overnemen als deze uitvalt. In deze testcase wordt dit geverifieerd door het spanningsloos maken van de Master switch.
Voorwaarden	• Virtual Chassis is geconfigureerd zoals hierboven is aangegeven. • Er wordt gebruik gemaakt van het Deelontwerp Virtual Chassis • Testcase P1 is geslaagd

Teststappen

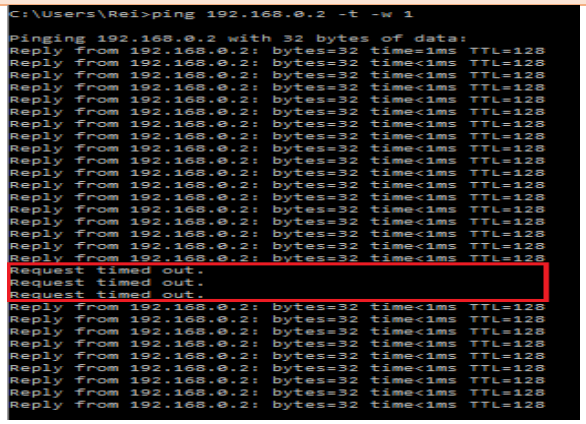
1	Op PC1 wordt een ICMP-bericht gestuurd naar PC2 met een wait van 1 sec.
2	De Master switch wordt losgekoppeld van de netstroom. Op deze manier wordt de switch spanningsloos.
3	Er wordt gecontroleerd of de ICMP-berichten tussen PCs nog verzonden worden. Er wordt gecontroleerd of de ICMP-berichten onderbroken zijn of dat de latency verhoogd is.
4	Op de Slave switch zal het commando: ***show virtual-chassis topology*** uitgevoerd worden. Om te kijken of de Slave de Master is geworden en er maar één switch in het Virtual Chassis bevind.

Verwachte Resultaat

De Slave switch in de Virtual Chassis neemt de rol over van de Master switch. Uit het commando ***"show virtual-chassis topology"*** zal het volgende resultaat komen.

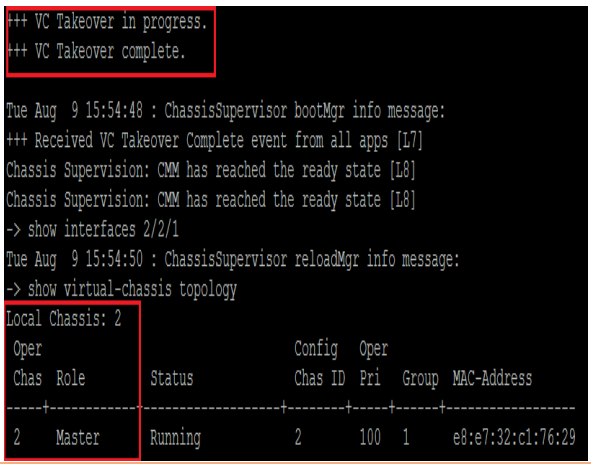
```
Local Chassis: 1
                                                  Config
Chas    Role           Status                Chas ID   Pri    Group   MAC-Address
-----+------------+--------------------+--------+-----+------+------------------
 2      Master        Running                2          100    1      e8:e7:32:c1:76:29
```

Behaalde Resultaat



Uit de afbeelding hiernaast blijkt dat het Virtual Chassis een drietal secondes nodig heeft om te switchen tussen Master en Slave.

← Loskoppelen van de netstroom switch OS6900-T20.



Uit de afbeelding hiernaast wordt duidelijk dat de master switch wordt uitgeschakeld. Er wordt namelijk een *"VC Takeover"* uitgevoerd en Chassis-ID 2 is nu nog de enige switch in het Virtual Chassis en daarmee automatisch Master.

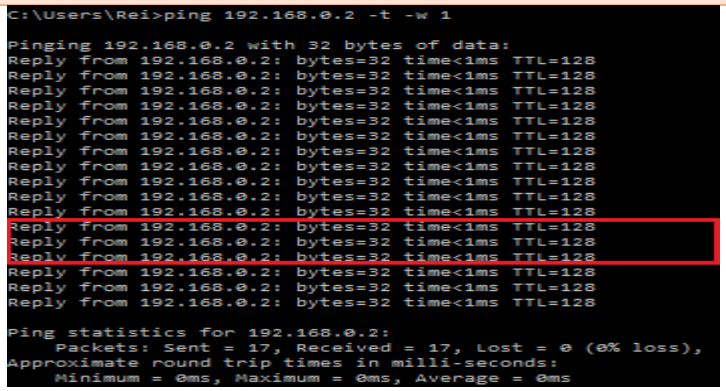
Testcase P3	Blijft het netwerk actief bij het uitvallen van de Slave?
Beschrijving	Volgens de literatuur gebeurt er niets aan de werking van de Virtual Chassis als de Slave uitvalt. De Slave is alleen van waarde als de Master uitvalt en zal anders een redundant component zijn. Hierdoor zal het netwerk geen effect merken bij het uitvallen van de Slave switch.
Voorwaarden	• Virtual Chassis is geconfigureerd zoals hierboven is aangegeven • Gebruik gemaakt van Deelontwerp Virtual Chassis • Testcase P1 is geslaagd
Teststappen	
1	Op PC1 wordt een ping gestuurd naar PC2 met een wait van 1 sec.
2	De Slave switch wordt losgekoppeld van de netstroom. Op deze manier wordt de switch spanningsloos.
3	Er wordt gecontroleerd of de berichten tussen PCs nog verzonden worden. Er wordt ook gecontroleerd of de ping berichten onderbroken zijn of dat de latency verhoogd is. Ook wordt er gecontroleerd of de Virtual Chassis nu alleen uit de Master bestaat.

Verwachte Resultaat

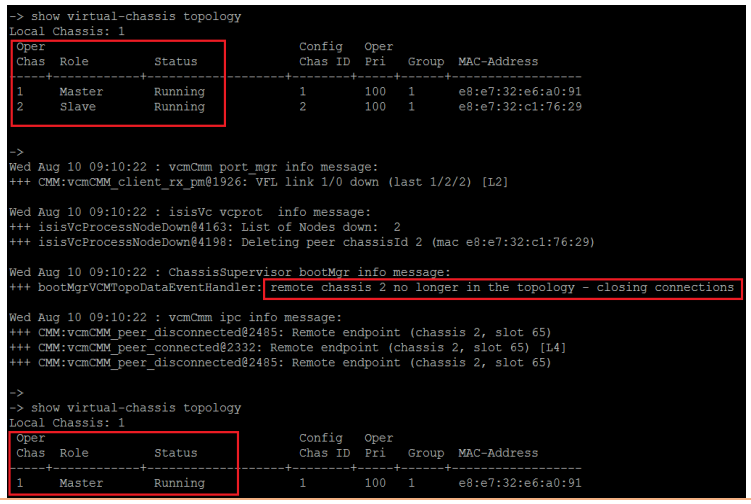
Het netwerk blijft de ICMP-berichten sturen.
De Virtual Chassis gaat verder als een enkele switch. De gebruiker merkt niets van deze verandering. Uit het commando "***show virtual-chassis topology***" zal het volgende resultaat komen:

```
Local Chassis: 1
                                                  Config
Chas    Role          Status                Chas ID  Pri    Group  MAC-Address
-----+------------+--------------------+--------+-----+------+-----------------
 1      Master        Running                1         100    0      e8:e7:32:e6:a0:91
```

Behaalde Resultaat



Er wordt geen downtime ondervonden omdat alles via de Master switch zal verlopen. Hierbij ondervindt de gebruiker geen onderbreking als de Slave switch uitvalt.
← *Loskoppelen van de netstroom switch OS6900-T40.*

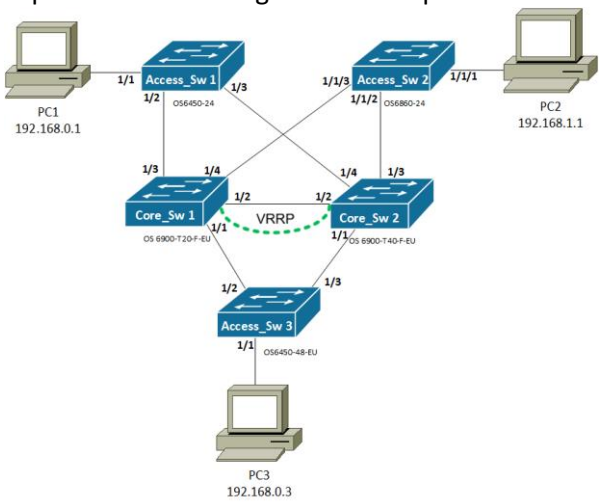


Uit de afbeelding hiernaast is te zien dat bij het uitvoeren van het eerste commando beide switches nog aanwezig zijn. Na het loskoppelen van de Slave switch geeft de switch meerdere meldingen dat de Slave is uitgevallen. Als dit gecontroleerd wordt met het ***show virtual-chassis topology*** commando blijkt inderdaad dat alleen de Master switch nog aanwezig is.

5.2 Virtual Router Redundancy Protocol

Uit de literatuur komt dat VRRP gebruikt wordt om het 'single point of failure' te elimineren. Dit wordt gedaan door het handmatig configureren van een default gateway op elke host in het netwerk.

Het tweede deelontwerp is om te testen hoe het Virtual Router Redundancy Protocol werkt. Voor dit experiment is het volgende ontwerp voor bedacht:



Figuur 2 Deelontwerp VRRP

VRRP wordt op de Core_Sw1 en Core_Sw3 geïmplementeerd op de interfaces die met Access_Sw3 verbonden zijn.

De apparatuur die gebruikt is om deze deeltestopstelling te bouwen ziet er als volgt uit:

- 1x Alcatel OmniSwitch 6900-T20-F
- 1x Alcatel OmniSwitch 6900-T40-F-EU
- 1x Alcatel OmniSwitch 6860-24EU
- 1x Alcatel OmniSwitch 6450-24-EU
- 1x Alcatel OmniSwitch 6450-48-EU
- 3x Dell Latitude, OS Windows 7 (laptop)
- 10x UTP kabel

PC1	***PC2***	***PC3***
IP-adres 192.168.0.1 met subnetmask 255.255.255.0 Default gateway 192.168.0.100	IP-adres 192.168.1.1 met subnetmask 255.255.255.0 Default gateway 192.168.1.100	IP-adres 192.168.0.3 met subnetmask 255.255.255.0 Default gateway 192.168.0.100

Access_Sw1	***Access_Sw2***	***Access_Sw3***

Core_Sw1	***Core_Sw2***
VRRP op VRID 1 en VRID 2 enabled VRRP op VLAN 1 enabled VRID 1 adres 192.168.0.100 VRID 2 adres 192.168.1.100 IP-interface 192.168.0.100 op vlan 1 IP-interface 192.168.1.100 op vlan 1	VRRP op VRID 1 en VRID 2 enabled VRRP op VLAN 1 enabled VRID 1 adres 192.168.0.100 VRID 2 adres 192.168.1.100 IP-interface 192.168.0.101 op vlan 1 IP-interface 192.168.1.101 op vlan 1

Hoe wordt VRRP geconfigureerd?
Configuratie van VRRP op de OS6900[2]:
Als eerste zal er een Virtuele router gecreëerd moeten worden

➔ ***vrrp*** <VRID> <vlan>

Hierna moet er een IP-adres geconfigureerd worden voor de Virtual Router.

➔ ***vrrp*** <VRID> <vlan> ***address*** *<x.x.x.x>*

Als laatste moet VRRP dan nog op elke switch enabled worden.
Voor de OS6900:

➔ ***vrrp*** <VRID> <vlan> ***admin-state*** *enable*

Bovenstaande commando's moeten op alle fysieke switches gedaan worden die onderdeel zijn van de virtuele router.

Om te verifiëren of de VRRP configuratie gelukt is kan er ook nog gebruik worden gemaakt van het volgende commando's:

➔ ***show vrrp***

➔ ***show vrrp*** <VRID> ***statistics***

De uiteindelijke configuratie stappen:

Op de Master switch (VRRP)	Op de Back-up switch(VRRP)
ip interface *"vrrp"* **address** *192.168.0.100* **vlan** *1*	**ip interface** *"vrrp"* **address** *192.168.0.101***vlan** *1*
vrrp *1 1*	***vrrp*** *1 1*
vrrp *1 1* ***address*** *192.168.0.100*	***vrrp*** *1 1* ***address*** *192.168.0.100*
vrrp *1 1* ***admin-state*** *enable*	***vrrp*** *1 1* ***admin-state*** *enable*
ip interface *"vrrp2"* **address** *192.168.1.100* **vlan** *1*	**ip interface** *"vrrp2"* **address** *192.168.1.101* **vlan** *1*
vrrp *2 1*	***vrrp*** *1 1*
vrrp *2 1* ***address*** *192.168.1.100*	***vrrp*** *1 1* ***address*** *192.168.0.100*
vrrp *2 1* ***admin-state*** *enable*	***vrrp*** *1 1* ***admin-state*** *enable*

Nu deze instellingen zijn doorgevoerd zal er nu getest worden en wel aan de hand van testcases.

Testcase P4	Is VRRP correct geconfigureerd?
Beschrijving	Als eerste test moet er gecontroleerd worden of de VRRP configuratie in de switch is doorgevoerd. Dit wordt gedaan door te controleren op de switches of de VRRP instantie is aangemaakt.
Voorwaarden	• VRRP is geconfigureerd zoals hierboven is aangegeven • Gebruik gemaakt van Deelontwerp VRRP
Teststappen	
1	Op beide switches die de VRRP verbinding vormen zullen de commando's: ***show vrrp*** en ***show vrrp 1 statistics*** uitgevoerd worden.
2	Hierin wordt gekeken of de VRRP configuratie klopt
Verwachte Resultaat	

Op de switch zal dergelijk resultaat te zien moeten zijn na het invoeren van ***show vrrp***:

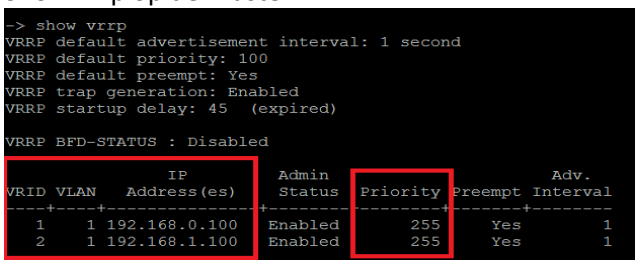
```
VRRP trap generation: Enabled
VRRP startup delay: 45 (expired)

IP Admin Adv.
VRID   VLAN      Address(es)     Status     Priority    Preempt  Interval
-----+-------+---------------+-----------+----------+--------+-------
1       1       192.168.0.100    Enabled    100 OF 255     Yes       1
2       1       192.168.1.100    Enabled    100 OF 255     Yes       1
```

Op de switch zal dergelijk resultaat te zien moeten zijn na het invoeren van ***show vrrp 1 statistics***:

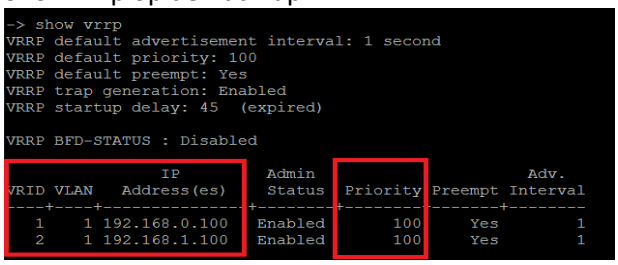
```
-> show vrrp 1 statistics
Virtual Router VRID = 1 on VLAN = 1
State = Master / Backup
UpTime (1/100th second) = 378890
Become master = 1
Advertisements received = 0
```

Behaalde Resultaat

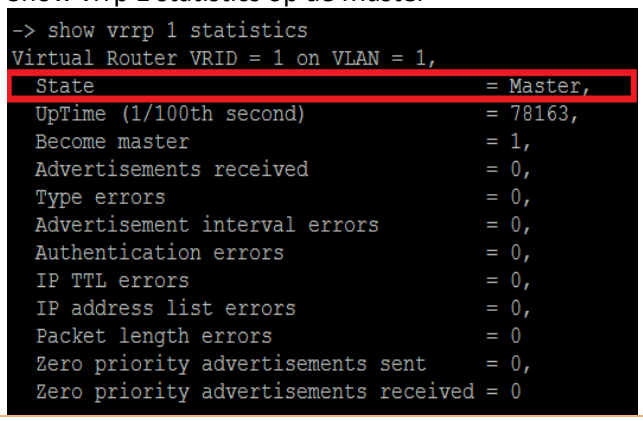
Show vrrp op de Master



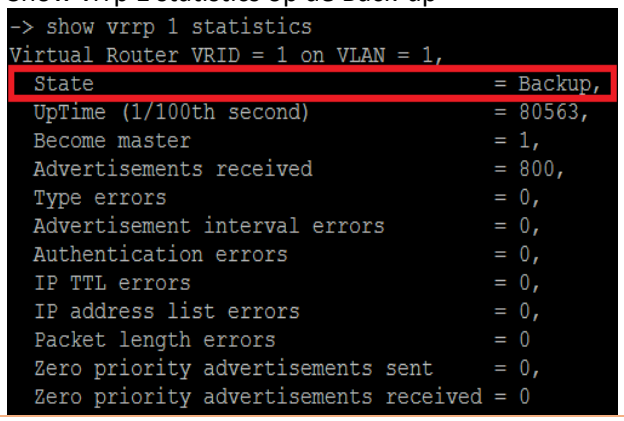
Show vrrp op de Back-up



Show vrrp 1 statistics op de Master



Show vrrp 1 statistics op de Back-up



Testcase P5	**Neemt de Back-up switch de werkzaamheden van de Active switch over?**
Beschrijving	Uit het literatuuronderzoek naar VRRP kwam naar voren, dat als de Active switch uitvalt de Back-up switch de functionaliteiten overneemt. Hierdoor zal de gebruiker zijn werkzaamheden door blijven voeren zonder effect te ondervinden van de verandering.
Voorwaarden	• VRRP is geconfigureerd zoals hierboven is aangegeven • Gebruik gemaakt van Deelontwerp VRRP • Testcase P4 is geslaagd
Teststappen	
1	Op PC3 wordt een ICMP-bericht gestuurd naar PC2 met een wait van 1 sec.
2	De Active switch (OS6900-T20) wordt losgekoppeld van de netstroom. Op deze manier wordt de switch spanningsloos.
3	Er wordt gecontroleerd of de ICMP-berichten tussen PCs nog verzonden worden. Er wordt gecontroleerd of de ICMP-berichten onderbroken zijn of dat de latency verhoogd is.
Verwachte Resultaat	
De Access switch weet nu dat de Active switch niet te bereiken is en zal via de Back-up switch proberen alsnog de server te kunnen bereiken. De Back-up heeft hiermee de rol als Active overgenomen.	
Behaalde Resultaat	

```
C:\Users\qiict>ping 192.168.1.1 -t -w 1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
```

In de afbeelding hiernaast is te zien dat er geen time-out is ondervonden tijdens het loskoppelen van de VRRP master switch.

← Loskoppelen van de netstroom switch OS6900-T20.

```
-> show vrrp 1 statistics
Virtual Router VRID = 1 on VLAN = 1,
  State                                     = Backup,
  UpTime (1/100th second)                   = 272762,
  Become master                             = 3,
  Advertisements received                   = 2351,
  Type errors                               = 0,
  Advertisement interval errors             = 0,
  Authentication errors                     = 0,
  IP TTL errors                             = 0,
  IP address list errors                    = 0,
  Packet length errors                      = 0
  Zero priority advertisements sent         = 0,
  Zero priority advertisements received = 0

-> show vrrp 1 statistics
Virtual Router VRID = 1 on VLAN = 1,
  State                                     = Master,
  UpTime (1/100th second)                   = 274753,
  Become master                             = 4,
  Advertisements received                   = 2368,
  Type errors                               = 0,
  Advertisement interval errors             = 0,
  Authentication errors                     = 0,
  IP TTL errors                             = 0,
  IP address list errors                    = 0,
  Packet length errors                      = 0
  Zero priority advertisements sent         = 0,
  Zero priority advertisements received = 0
```

In de hiernaast gegeven afbeelding is te zien hoe de Back-up switch gewijzigd is naar de Master. Tussen de beide commando's in is de Master switch spanningsloos gemaakt en daardoor is bij het uitvoeren van het tweede commando deze switch nu de Master in plaats van de Back-up

Testcase P6	**Blijft het netwerk actief bij het uitvallen van de Back-up?**
Beschrijving	Volgens de literatuur gebeurt er niets als de Back-up switch uitvalt. De Active switch heeft al de hoogste rechten en zal nog steeds alles regelen. De Back-up is alleen van waarde als de Active uitvalt.
Voorwaarden	• VRRP is geconfigureerd zoals hierboven is aangegeven • Gebruik gemaakt van Deelontwerp VRRP • Testcase P4 is geslaagd

Teststappen

1	Op PC3 wordt een ICMP-bericht gestuurd naar PC2 met een wait van 1 sec.
2	De Back-up switch wordt losgekoppeld van de netstroom. Op deze manier wordt de switch spanningsloos.
3	Er wordt gecontroleerd of de ICMP-berichten tussen PCs nog verzonden worden. Er wordt gecontroleerd of de ICMP-berichten onderbroken zijn of dat de latency verhoogd is.

Verwachte Resultaat

De ICMP-berichten hebben geen down tijd ondervonden. Dit komt omdat, de uitschakeling van de Back-up switch geen effect heeft op de werking van het netwerk.

Behaalde Resultaat

```
C:\Users\qiict>ping 192.168.0.1 -t -w 1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
```

Er wordt geen downtime ondervonden omdat alles via de Master switch zal verlopen. Hierbij ondervindt de gebruiker geen onderbreking als de Back-up switch uitvalt.

🡐 *Loskoppelen van de netstroom switch OS6900-T40.*

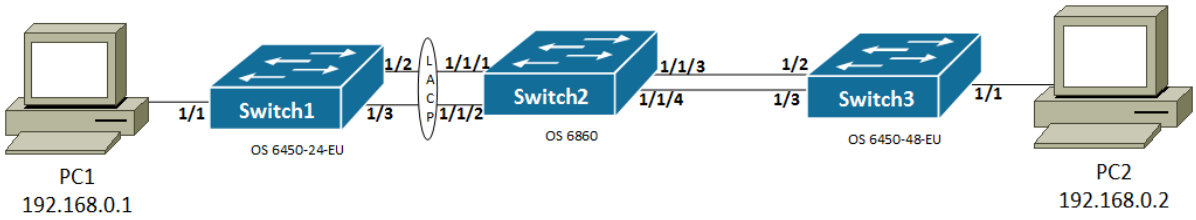
```
-> show vrrp 1 statistics
Virtual Router VRID = 1 on VLAN = 1,
  State                                 = Master,
  UpTime (1/100th second)               = 25550,
  Become master                         = 1,
  Advertisements received               = 0,
  Type errors                           = 0,
  Advertisement interval errors         = 0,
  Authentication errors                 = 0,
  IP TTL errors                         = 0,
  IP address list errors                = 0,
  Packet length errors                  = 0
  Zero priority advertisements sent     = 0,
  Zero priority advertisements received = 0

-> show vrrp 1 statistics
Virtual Router VRID = 1 on VLAN = 1,
  State                                 = Master,
  UpTime (1/100th second)               = 27322,
  Become master                         = 1,
  Advertisements received               = 0,
  Type errors                           = 0,
  Advertisement interval errors         = 0,
  Authentication errors                 = 0,
  IP TTL errors                         = 0,
  IP address list errors                = 0,
  Packet length errors                  = 0
  Zero priority advertisements sent     = 0,
  Zero priority advertisements received = 0
```

In de hiernaast gegeven afbeelding is te zien dat de Master switch niet gewijzigd is en nog steeds de Master switch is. Tussen de beide commando's in is de Back-up switch spanningsloos gemaakt. Echter heeft het uitvallen van de Back-up geen gevolgen voor de Master. Dit wordt pas een probleem als de Master switch uitvalt voordat de Back-up switch weer werkend is.

5.3 LACP

Uit de literatuur kwam naar voren dat LACP een Link Aggregation aanmaakt. Een Link Aggregation is het bundelen van meerdere parallelle verbindingen tot een enkele (logische) verbinding om de doorvoer van het netwerk verkeer te verhogen.

Het volgende deelontwerp is om te testen hoe het Link Aggregation Control Protocol werkt. Voor dit experiment is het volgende ontwerp voor bedacht:



Figuur 3 Deelontwerp LACP

Hier zal tussen Switch1 en Switch 2 wel gebruik gemaakt worden van LACP en tussen Switch2 en Switch3 niet. Op deze manier kan de werking getest worden en kan meteen duidelijk worden in welke opzichten LACP verschilt met een verbinding die los gebruikt worden. Hierbij kan het gedrag geconstateerd worden van de switches als bijvoorbeeld een verbinding wegvalt.

De apparatuur die gebruikt is om deze deeltestopstelling te bouwen ziet er als volgt uit:

- 1x Alcatel OmniSwitch 6900-T20-F
- 1x Alcatel OmniSwitch 6860-24-EU
- 1x Alcatel OmniSwitch 6450-24-EU
- 2x Dell Latitude, OS Windows 7 (laptop)
- 6x UTP kabel

De configuratie ziet er als volgt uit op de componenten:

PC1	***PC2***
IP-adres 192.168.0.1 met subnetmask 255.255.255.0	IP-adres 192.168.0.2 met subnetmask 255.255.255.0

Switch1	***Switch2***	***Switch3***
LACP group 10; Interfaces 0/2 en 0/3 toevoegen aan LACP group 10;	LACP group 10; Interfaces 0/2 en 0/3 toevoegen aan LACP group 10;	

Hoe wordt LACP geconfigureerd?
Op de OS6450 wordt LACP op de volgende manier geconfigureerd[3]:
Eerst zal er een LACP groep aan worden gemaakt:

➔ ***lacp linkagg*** *<id>* ***size*** *<size>* ***actor admin key*** *<key>*

Vervolgens zullen er poorten toegevoegd moeten worden:

➔ ***lacp agg*** *<port>* ***actor admin key*** *<key>*

Als laatste zal er een VLAN aangewezen worden waar deze link agg overheen gaat:

➔ ***vlan*** *<vlan>* ***port default*** *<id>*

Om te controleren of de Link Aggregation is gemaakt en de poorten zijn toegevoegd kunnen de volgende commando's worden gebruikt:

➔ ***show linkagg*** *<id>*

➔ ***show linkagg port*** *<port>*

Op de OS6860 wordt LACP op een andere manier geconfigureerd, namelijk als volgt[4]:
Eerst zal er een LACP groep aan worden gemaakt:

➔ ***linkagg lacp agg*** *<id>* ***size*** *<size>* ***actor admin-key*** *<key>*

Vervolgens zullen er poorten toegevoegd moeten worden:

➔ ***linkagg lacp port*** *<port>* ***actor admin-key*** *<key>*

Als laatste zal er een VLAN aangewezen worden waar deze link agg overheen gaat:

➔ ***vlan*** *<vlan>* ***members linkagg*** *<id>* ***untagged***

Om te controleren of de Link Aggregation is gemaakt en de poorten zijn toegevoegd kunnen de volgende commando's worden gebruikt:

➔ ***show linkagg agg*** *<id>*

➔ ***show linkagg port*** *<port>*

De uiteindelijke configuratie stappen:

configuratie op Switch 1 (OS6450)	configuratie op Switch2 (OS6860)
lacp linkagg *10* ***size*** *2* ***actor admin key*** *5*	***linkagg lacp agg*** *10* ***size*** *2* ***actor admin-key*** *5*
lacp agg *1/2* ***actor admin key*** *5*	***linkagg lacp port*** *1/1/1* ***actor admin-key*** *5*
lacp agg *1/3* ***actor admin key*** *5*	***linkagg lacp port*** *1/1/2* ***actor admin-key*** *5*
vlan *1* ***port default*** *10*	***vlan*** *1* ***members linkagg*** *10* ***untagged***

Nu deze instellingen zijn doorgevoerd zal er nu getest worden en wel aan de hand van testcases.

Testcase P7	Is LACP correct geconfigureerd?
Beschrijving	Als eerste test moet er gecontroleerd worden of de LACP configuratie in de switch is doorgevoerd. Dit wordt gedaan door te controleren op de switches of de Link Aggregation is aangemaakt.
Voorwaarden	• LACP is geconfigureerd zoals hierboven is aangegeven • Er wordt gebruik gemaakt van het Deelontwerp LACP
Teststappen	
1	Op de OS6450 zal het commando: ***show linkagg*** *en* ***show linkagg 10***uitgevoerd worden. En op de OS6860 zal het commando**: *show linkagg* en *show linkagg agg 10*** uitgevoerd worden.
2	Hierin wordt gekeken of het aanmaken van de LACP bundel is gelukt
3	Op de beide switches zal het commando: ***show linkagg port*** uitgevoerd worden.
4	Nu wordt er gekeken of de poorten aan de LACP bundel zijn toegevoegd.

Verwachte Resultaat

Uit het commando ***show linkagg*** zal een uitkomst komen zoals hieronder:

```
Number    Aggregate     SNMP Id      Size      Admin State    Oper State    Att/Sel Ports
------+-----------+------------+-------+---------------+-----------+---------------
10        Dynamic      40000001      2           ENABLED         UP             2   2
```

Uit het commando ***show linkagg port*** <*port*> zal een uitkomst komen zoals hieronder:

Op de 6860

```
Dynamic Aggregable Port
SNMP Id : 1001,
Chas/Slot/Port : 1/1/1,
Administrative State : ENABLED,
Operational State : UP,
Port State : ATTACHED,
Link State : UP,
Selected Agg Number : 10,
Port position in the aggregate: 0,
Primary port : YES,
```

Op de 6450

```
Dynamic Aggregable Port
SNMP Id : 1002,
Slot/Port : 1/1,
Administrative State : ENABLED,
Operational State : UP,
Port State : ATTACHED,
Link State : UP,
Selected Agg Number : 10,
Port position in the aggregate: 0,
Primary port : YES,
```

Behaalde Resultaat

Op de OS6450:

```
-> show linkagg

Number  Aggregate  SNMP Id   Size Admin State  Oper State     Att/Sel Ports
-------+----------+---------+----+------------+-------------+------------
  10      Dynamic   40000010   2   ENABLED      UP              2   2
->
-> show linkagg 10

Dynamic Aggregate
  SNMP Id                 : 40000010,
  Aggregate Number        : 10,
  SNMP Descriptor         : Dynamic Aggregate Number 10 ref 40000010 size 2,
  Name                    : ,
  Admin State             : ENABLED,
  Operational State       : UP,
  Aggregate Size          : 2,
  Number of Selected Ports : 2,
  Number of Reserved Ports : 2,
  Number of Attached Ports : 2,
  Primary Port            : 1/2
LACP
  MACAddress              : [e8:e7:32:9d:0e:cf],
  Actor System Id         : [00:00:00:00:00:00],
  Actor System Priority   : 0,
  Actor Admin Key         : 5,
  Actor Oper Key          : 5,
  Partner System Id       : [00:00:00:00:00:00],
  Partner System Priority : 0,
  Partner Admin Key       : 0,
  Partner Oper Key        : 5
  Wait-To-Restore Timer   : 0

-> show linkagg port

Slot/Port Aggregate SNMP Id   Status   Agg  Oper Link Prim
---------+---------+-------+----------+----+----+----+----
  1/2     Dynamic     1002  ATTACHED    10  UP   UP   YES
  1/3     Dynamic     1003  ATTACHED    10  UP   UP   NO
```

Op de OS6860:

```
-> show linkagg

Number  Aggregate     SNMP Id   Size Admin State  Oper State     Att/Sel Ports
-------+-------------+---------+----+------------+-------------+------------
  10      Dynamic      40000010   2   ENABLED      UP              2   2

-> show linkagg agg 10

Dynamic Aggregate
  SNMP Id                 : 40000010,
  Aggregate Number        : 10,
  SNMP Descriptor         : Dynamic Aggregate Number 10 ref 40000010 size 2,
  Name                    : ,
  Admin State             : ENABLED,
  Operational State       : UP,
  Aggregate Size          : 2,
  Number of Selected Ports : 2,
  Number of Reserved Ports : 2,
  Number of Attached Ports : 2,
  Primary Port            : 1/1/1,
  Port Selection Hash     : Source Destination Ip,
  Wait To Restore Time    : 0 Minutes
LACP
  MACAddress              : [e8:e7:32:fa:89:9a],
  Actor System Id         : [00:00:00:00:00:00],
  Actor System Priority   : 0,
  Actor Admin Key         : 5,
  Actor Oper Key          : 5,
  Partner System Id       : [00:00:00:00:00:00],
  Partner System Priority : 0,
  Partner Admin Key       : 0,
  Partner Oper Key        : 5

-> show linkagg port

Chassis/Slot/Port  Aggregate   SNMP Id   Status    Agg  Oper   Link Prim
------------------+---------+--------+---------+----+------+----+----
         1/1/1     Dynamic      1001   ATTACHED     10  UP   UP    YES
         1/1/2     Dynamic      1002   ATTACHED     10  UP   UP    NO
```

Testcase P8 — **Heeft het uitvallen van een verbinding binnen een bundel effect op het netwerk?**

Beschrijving

Volgens de literatuur is een LACP verbinding een bundel van meerdere verbindingen. Als één van de verbindingen wegvalt, wat voor gevolgen heeft dit dan voor het verkeer dat over deze verbinding gaat.

Voorwaarden

- LACP is geconfigureerd zoals hierboven is aangegeven
- Er wordt gebruik gemaakt van het Deelontwerp LACP
- Testcase P7 is geslaagd

Teststappen

1	Op PC1 wordt een ICMP-bericht gestuurd naar PC2 met een wait van 1 sec.
2	De kabel van Switch2 op port ***1/1/2*** wordt losgekoppeld van de switch.
3	Er wordt gecontroleerd of de ICMP-berichten tussen de PCs nog verzonden worden
4	Er wordt op Switch1 gecontroleerd of de LACP bundel effect heeft ondervonden van de uitgevallen verbinding door middel van het ***show linkagg port*** commando.

Verwachte Resultaat

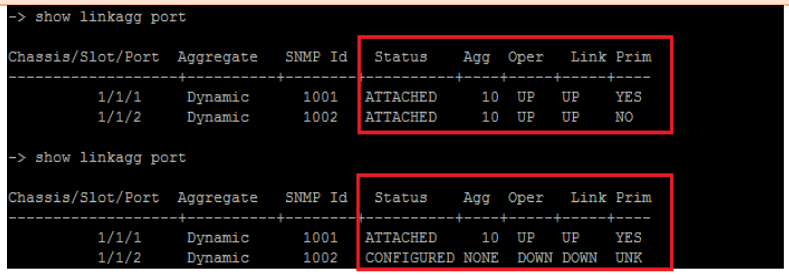
Het netwerk zal een korte onderbreking (<1sec.) ondervinden van het uitvallen van een enkele verbinding. Dit is alleen het geval als het de verbinding is waar het verkeer over heen wordt gestuurd.
Op de switch is te zien dat als de verbinding die het verkeer stuurde wordt losgekoppeld, deze niet langer de verbinding is met de prioriteit. Dit is te zien aan de verandering in de ***show linkagg port*** tabel.
Voor het loskoppelen van de verbinding:

```
Chassis/Slot/Port  Aggregate SNMP Id   Status    Agg Oper Link Prim
------------------+---------+-------+----------+----+----+----+------
1/1/1               Dynamic   1001    ATTACHED   10   UP   UP   YES
1/1/2               Dynamic   1002    ATTACHED   10   UP   UP   NO
```

Na het los koppelen van de verbinding:

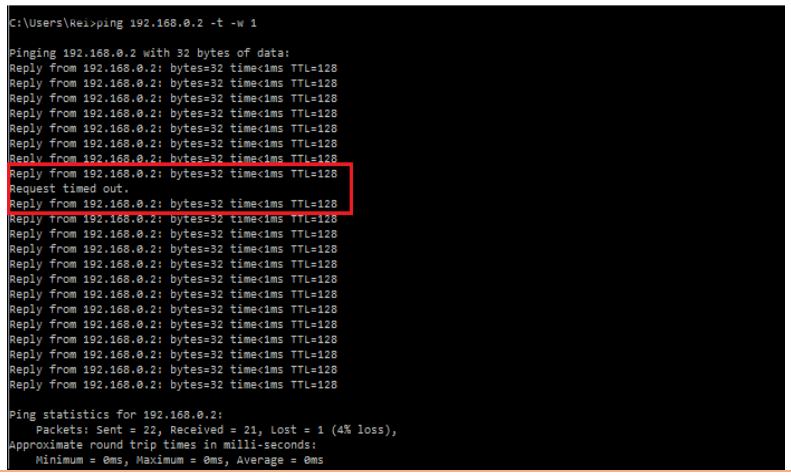
```
Chassis/Slot/Port  Aggregate SNMP Id   Status     Agg     Oper   Link   Prim
------------------+---------+-------+-----------+-------+-----+-------+------
1/1/1               Dynamic   1001    ATTACHED     10     UP     UP     YES
1/1/2               Dynamic   1002    CONFIGURED   NONE   DOWN   DOWN   UNK
```

Behaalde Resultaat



```
-> show linkagg port

Chassis/Slot/Port  Aggregate   SNMP Id  Status     Agg  Oper   Link Prim
------------------+----------+--------+----------+----+-----+-----+----
          1/1/1     Dynamic      1001  ATTACHED     10  UP    UP     YES
          1/1/2     Dynamic      1002  ATTACHED     10  UP    UP     NO

-> show linkagg port

Chassis/Slot/Port  Aggregate   SNMP Id  Status     Agg  Oper   Link Prim
------------------+----------+--------+----------+----+-----+-----+----
          1/1/1     Dynamic      1001  ATTACHED     10  UP    UP     YES
          1/1/2     Dynamic      1002  CONFIGURED NONE  DOWN DOWN   UNK
```

Hiernaast is te zien dat op de switch de loskoppeling van de kabel te zien is. Ook is uit de ICMP berichten te halen dat de verbinding down is geweest want er is een Time out opgetreden.



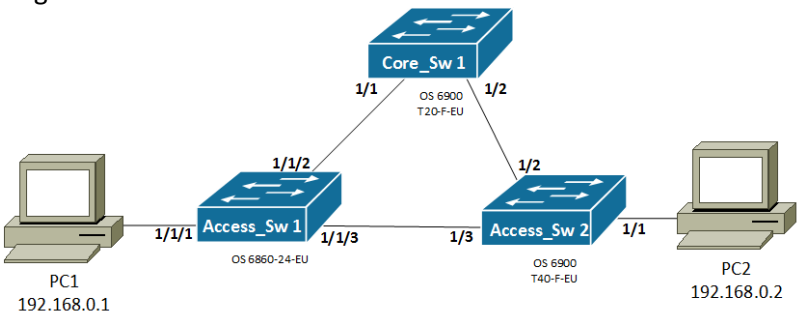
```
C:\Users\Rei>ping 192.168.0.2 -t -w 1

Pinging 192.168.0.2 with 32 bytes of data:
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Request timed out.
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 22, Received = 21, Lost = 1 (4% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

← Loskoppeling van één verbinding van de bundel

Hiermee kan geconcludeerd worden dat het down gaan van een verbinding wel degelijk effect heeft op het netwerk. Ondanks dat de downtijd minder als een seconde is, zal deze downtijd wel aanwezig.

5.4 RSTP en SPB

Bij onderstaand deelontwerp kunnen zowel RSTP als SPB getest worden. Dit ontwerp is gekozen omdat, er op deze manier getest kan worden hoe beide protocollen reageren als er verbindingen wegvallen tussen switches. Alle switches zullen geconfigureerd zijn met één van de beide protocollen. Zo zal één testomgeving zijn dat alle switches RSTP ondersteunen. En er zal een testomgeving zijn dat alle switches met SPB geconfigureerd zijn. De testcases zullen om en om uitgevoerd worden.



Figuur 4 Deelontwerp RSTP & SPB

De apparatuur die gebruikt is om deze deeltestopstelling te bouwen ziet er als volgt uit:

- 1x Alcatel OmniSwitch 6900-T20-F
- 1x Alcatel OmniSwitch 6900-T40-F-EU
- 1x Alcatel OmniSwitch 6860-48-EU met Advanced routing license
- 2x Dell Latitude, OS Windows 7 (laptop)
- 5x UTP kabel

De configuratie voor een RSTP situatie ziet er als volgt uit:

PC1	***PC2***
IP-adres 192.168.0.1 met subnetmask 255.255.255.0	IP-adres 192.168.0.2 met subnetmask 255.255.255.0

Access_Sw1 (OS6860)	***Access_Sw2* (OS6900-T40)**	***Core_Sw1* (OS6900-T20)**
Root priority 12288	Root priority 8192	Root priority 4096

Hoe wordt RSTP geconfigureerd?

Op Alcatel switches staat over het algemeen het Spanning Tree Protocol als standaard ingesteld. Op zowel de OmniSwitch OS6450[3], OmniSwitch OS6860[4] en de OmniSwitch OS6900[2] staat RSTP als default ingesteld. Dit is te controleren door het volgende commando:

➔ ***show spantree***

Als dit echter niet het geval is kan het volgende commando gebruikt worden om als nog RSTP in te stellen als STP mode.

➔ ***spantree mode rstp***

Nu zal alleen op de Core_Sw1 de root prioriteit aangepast worden en dat wordt gedaan met het volgende commando

➔ ***spantree vlan*** *<vlan ID>* ***priority*** *<priority>*

De uiteindelijke configuratie stappen als RSTP niet als default staat ingesteld:

Core_Sw1 (OS6900-T20)	***Access_Sw1 (OS6860)***	***Access_Sw2 (OS6900-T40)***
spantree mode rstp	***spantree mode rstp***	***spantree mode rstp***
***spantree vlan** 1 **priority** 4096*	***spantree vlan** 1 **priority** 12288*	***spantree vlan** 1 **priority** 8192*

De configuratie voor een SPB situatie ziet er als volgt uit:

PC1	***PC2***
IP-adres 192.168.0.1 met subnetmask 255.255.255.0	IP-adres 192.168.0.2 met subnetmask 255.255.255.0

***Access_Sw1* (OS6860)**	***Access_Sw2* (OS6900-T40)**	***Core_Sw1* (OS6900-T20)**
SPB bvlan 4001 SPB poorten 1/1/2 & 1/1/3 SPB service 1 isid 500 SAP port 1/1/1:all	SPB bvlan 4001 SPB poorten 1/1/2 & 1/1/3 SPB service 1 isid 500 SAP port 1/1/1 :all	SPB bvlan 4001 SPB poorten 1/1/1 & 1/1/2

Hoe wordt SPB geconfigureerd?

SPB wordt op de OS6860 en de OS6900[5] hetzelfde geconfigureerd, de commando's komen overeen:
Eerst zal er een SPB BVLAN aangemaakt moeten worden om de switches onderling te communiceren:

➔ ***spb bvlan*** *<vlan ID>*

Vervolgens zal er een bvlan gekozen worden waarop SPB de frames uitwisselt met de neighbor switches:

➔ ***spb isis control-bvlan*** *<vlan ID>*

Er moeten nu nog poorten aan de SPB instantie toegevoegd worden:

➔ ***spb isis interface port*** *<port>*

En als laatste wordt de SPB instantie enabled op e switch; door dit te doen wordt de Hello conversatie tussen de switches begonnen:

➔ ***spb isis admin-state*** *enable*

Nadat SPB op alle switches is geconfigureerd en enabled, moet er nog een SPB service aangemaakt worden op de switches die verbonden zijn met endpoints. Eerst moet de port naar de endpoint geconfigureerd worden:

➔ ***service access port*** *<port naar de endpoint>*

Hierna zal er een SPB BVLAN gelinkt worden aan de service; deze service moet een Service id en een ISID krijgen:

➔ ***service*** *<id>* ***spb isid*** *<isid>* ***bvlan*** *<vlan ID>* ***admin-state*** *enable*

Vervolgens zal er een Service access point toegewezen worden waarop SPB de frames uitwisselt met de endpoint. Hierbij is de SAP-port de port naar de PC en zal al het verkeer doorgelaten worden, omdat er geen scheiding is qua verkeer:

➔ ***service*** *<id>* ***sap port*** *<port naar de endpoint>****:all admin-state*** *enable*

De uiteindelijke configuratie stappen:

Core_Sw1 (OS6900-T20)	***Access_Sw1 (OS6860)***	***Access_Sw2 (OS6900-T40)***
spb bvlan *4001*	***spb bvlan*** *4001*	***spb bvlan*** *4001*
spb isis control-bvlan *4001*	***spb isis control-bvlan*** *4001*	***spb isis control-bvlan*** *4001*
spb isis interface port *1/1/1*	***spb isis interface port*** *1/1/2*	***spb isis interface port*** *1/1/2*
spb isis interface port *1/1/2*	***spb isis interface port*** *1/1/3*	***spb isis interface port*** *1/1/3*
spb isis admin-state enable	***spb isis admin-state*** *enable*	***spb isis admin-state*** *enable*
	Service access port *1/1/1*	***Service access port*** *1/1/1*
	Service spb *1* ***isid*** *500* ***bvlan*** *4001* ***admin-state*** *enable*	***Service*** *1* ***spb isid*** *500* ***bvlan*** *4001* ***admin-state*** *enable*
	Service spb *1* ***sap port*** *1/1/1:all* ***admin-state*** *enable*	***Service*** *1* ***sap port*** *1/1/1:all* ***admin-state*** *enable*

Testcase P9 RSTP	Staat RSTP als default ingesteld?
Beschrijving	Als eerste test moet er gecontroleerd worden of de RSTP daadwerkelijk als default staat ingesteld op de switches. Dit is namelijk uit het literatuuronderzoek naar voren gekomen.
Voorwaarden	• RSTP is geconfigureerd zoals hierboven is aangegeven • Gebruik gemaakt van Deelontwerp RSTP+SPB

Teststappen

1	Op alle switches zal het commando: ***show spantree vlan 1*** uitgevoerd worden.
2	Hierin wordt gekeken of RSTP als default staat ingesteld

Verwachte Resultaat

Uit het commando: "**show spantree vlan 1"** zal het volgende resultaat moeten volgen.

```
-> show spantree vlan 1
 Spanning Tree Parameters for Vlan 1
 Spanning Tree Status : ON,
 Protocol : IEEE STP,
 mode : Per VLAN (1 STP per-vlan),
 Priority : 32768 (0x8000),
 Bridge ID : 8000-00:d0:95:6a:f4:58,
 Designated Root : 0000-00:00:00:00:00:00,
 Current Parameters (seconds)
 Max Age = 20,
 Forward Delay = 15,
 Hello Time = 2
 Parameters system uses when attempting to become root
 System Max Age = 20,
 System Forward Delay = 15,
 System Hello Time = 2
```

Behaalde Resultaat

OS6860

```
-> show spantree vlan 1
Spanning Tree Parameters for Vlan 1
  Spanning Tree Status :                  ON,
  Protocol             :        IEEE Rapid STP,
  mode                 : Per VLAN (1 STP per Vlan),
  Priority             :         12288 (0x3000),
  Bridge ID            :    3000-e8:e7:32:fa:89:93,
  Designated Root      :    1000-e8:e7:32:e6:a0:91,
  Cost to Root Bridge  :                     4,
  Root Port            :                 1/1/2,
  Next Best Root Cost  :                     8,
  Next Best Root Port  :                 1/1/3,
  TxHoldCount          :                     3,
  Topology Changes     :                     9,
  Topology age         : 2 days and 16:50:54,
    Current Parameters (seconds)
      Max Age              =    20,
      Forward Delay        =    15,
      Hello Time           =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
      System Hello Time    =     2
```

OS6900-T20 (Rootswitch)

```
-> show spantree vlan 1
Spanning Tree Parameters for Vlan 1
  Spanning Tree Status :                  ON,
  Protocol             :        IEEE Rapid STP,
  mode                 : Per VLAN (1 STP per Vlan),
  Priority             :          4096 (0x1000),
  Bridge ID            :    1000-e8:e7:32:e6:a0:91,
  Designated Root      :    1000-e8:e7:32:e6:a0:91,
  Cost to Root Bridge  :                     0,
  Root Port            :                  None,
  Next Best Root Cost  :                     0,
  Next Best Root Port  :                  None,
  TxHoldCount          :                     3,
  Topology Changes     :                     2,
  Topology age         :              00:00:05,
    Current Parameters (seconds)
      Max Age              =    20,
      Forward Delay        =    15,
      Hello Time           =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
      System Hello Time    =     2
```

OS6900-T40

```
-> show spantree vlan 1
Spanning Tree Parameters for Vlan 1
  Spanning Tree Status :                  ON,
  Protocol             :        IEEE Rapid STP,
  mode                 : Per VLAN (1 STP per Vlan),
  Priority             :          8192 (0x2000),
  Bridge ID            :    2000-e8:e7:32:c1:76:29,
  Designated Root      :    1000-e8:e7:32:e6:a0:91,
  Cost to Root Bridge  :                     4,
  Root Port            :                   1/2,
  Next Best Root Cost  :                     0,
  Next Best Root Port  :                  None,
  TxHoldCount          :                     3,
  Topology Changes     :                    14,
  Topology age         :              00:01:32,
    Current Parameters (seconds)
      Max Age              =    20,
      Forward Delay        =    15,
      Hello Time           =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
      System Hello Time    =     2
```

Uit deze afbeeldingen blijkt dat op alle switches RSTP staat ingesteld. Ook is duidelijk te zien dat alle prioriteiten op de juiste switches staan ingesteld. En hiermee de Rootswitch ook daadwerkelijk de OS6900-T20 is.

Testcase P9.1 SPB	Is SPB correct geconfigureerd?
Beschrijving	Als eerste test moet er gecontroleerd worden of de SPB configuratie in de switch is doorgevoerd. Dit wordt gedaan door te controleren op de switches of SPB als type spantree is geselecteerd.
Voorwaarden	• SPB is geconfigureerd zoals hierboven is aangegeven • Gebruik gemaakt van Deelontwerp RSTP+SPB
Teststappen	
1	Op alle switches zullen de commando's: ***show vlan*** en ***show spb isis info*** uitgevoerd worden.
2	Hierin wordt gekeken of de verandering naar SPB is doorgevoerd.
Verwachte Resultaat	

Uit het commando: "***show spb isis info***" zal het volgende resultaat moeten volgen:

```
SPB ISIS Bridge Info:
System Id = <MAC>,
System Hostname = <HOSTNAME>
SPSourceID = <SourceID>,
SPBM System Mode = auto,
BridgePriority = 32768 (0x8000),
Control BVLAN = 4001,
Admin State = UP,
LSDB Overload = Disabled,
SPF Wait = Max: 1000 ms, Initial: 100 ms, Second: 300 ms,
LSP Lifetime = 1200,
LSP Wait = Max: 1000 ms, Initial: 0 ms, Second: 300 ms,
Control Address = 01:80:C2:00:00:14 (AllL1)
```

Behaalde Resultaat

OS6860

```
-> show vlan
 vlan    type   admin   oper    ip    mtu          name
------+-------+-------+------+------+------+------------------
1       std       Dis     Dis   Dis    1500    VLAN 1
4001    spb       Ena     Ena   Dis    1524    VLAN 4001
4094    vcm       Ena     Dis   Dis    1500    VCM IPC

-> show spb isis info
SPB ISIS Bridge Info:
  System Id             = e8e7.32fa.8993,
  System Hostname       = OS6860,
  SPSourceID            = 0a-89-93,
  SPBM System Mode      = auto,
  BridgePriority        = 32768 (0x8000),
  MT ID                 = 0,
  Control BVLAN         = 4001,
  Area Address          = 0
                        0.0.0,
  Level Capability      = L1,
  Admin State           = UP,
  LSDB Overload         = Disabled,
  Last Enabled          = Fri Jan  3 01:20:01 2014,
  Last SPF              = Fri Jan  3 01:33:10 2014,
  SPF Wait              = Max: 1000 ms  Initial: 100 ms  Second: 300 ms,
  LSP Lifetime          = 1200,
  LSP Wait              = Max: 1000 ms, Initial: 0 ms, Second: 300 ms,
  Graceful Restart      = Disabled,
  GR helper-mode        = Disabled,
  # of L1 LSPs          = 3
  Control Address       = 01:80:c2:00:00:14 (AllL1)
```

OS6900-T20

```
-> show vlan
 vlan    type   admin   oper    ip    mtu          name
------+-------+-------+------+------+------+------------------
1       std       Dis     Dis   Ena    1500    VLAN 1
4001    spb       Ena     Ena   Dis    1524    VLAN 4001
4094    vcm       Ena     Dis   Dis    1500    VCM IPC

-> show spb isis info
SPB ISIS Bridge Info:
  System Id             = e8e7.32e6.a091,
  System Hostname       = OS6900-T20,
  SPSourceID            = 06-a0-91,
  SPBM System Mode      = auto,
  BridgePriority        = 32768 (0x8000),
  MT ID                 = 0,
  Control BVLAN         = 4001,
  Area Address          = 0
                        0.0.0,
  Level Capability      = L1,
  Admin State           = UP,
  LSDB Overload         = Disabled,
  Last Enabled          = Sat Jul 23 13:32:08 2016,
  Last SPF              = Sat Jul 23 13:42:38 2016,
  SPF Wait              = Max: 1000 ms  Initial: 100 ms  Second: 300 ms,
  LSP Lifetime          = 1200,
  LSP Wait              = Max: 1000 ms, Initial: 0 ms, Second: 300 ms,
  Graceful Restart      = Enabled,
  GR helper-mode        = Enabled,
  # of L1 LSPs          = 3
  Control Address       = 01:80:c2:00:00:14 (AllL1)
```

OS6900-T40

```
-> show vlan
 vlan    type   admin   oper    ip    mtu          name
------+-------+-------+------+------+------+------------------
1       std       Dis     Dis   Dis    1500    VLAN 1
4001    spb       Ena     Ena   Dis    1524    VLAN 4001
4094    mcm       Ena     Dis   Dis    9198    MCM IPC

-> show spb isis info
SPB ISIS Bridge Info:
  System Id             = e8e7.32c1.7629,
  System Hostname       = OS6900-T40,
  SPSourceID            = 01-76-29,
  SPBM System Mode      = auto,
  BridgePriority        = 32768 (0x8000),
  MT ID                 = 0,
  Control BVLAN         = 4001,
  Area Address          = 0
                        0.0.0,
  Level Capability      = L1,
  Admin State           = UP,
  LSDB Overload         = Disabled,
  Last Enabled          = Sat Jul 23 15:29:32 2016,
  Last SPF              = Sat Jul 23 15:44:33 2016,
  SPF Wait              = Max: 1000 ms  Initial: 100 ms  Second: 300 ms,
  LSP Lifetime          = 1200,
  LSP Wait              = Max: 1000 ms, Initial: 0 ms, Second: 300 ms,
  Graceful Restart      = Enabled,
  GR helper-mode        = Enabled,
  # of L1 LSPs          = 3
  Control Address       = 01:80:c2:00:00:14 (AllL1)
```

Uit deze afbeeldingen blijkt dat SPB op alle drie de switches is enabled en werkt op BVLAN 4001. Het vlan met RSTP is disabled om er zeker van te zijn dat er geen conflict ontstaat tussen het RSTP en SPB protocol.

Testcase P10 RSTP	**Heeft het uitvallen van switch CoreSw1 effect op het netwerk?**
Beschrijving	In het geval van RSTP is CoreSw1 de Rootswitch, hierbij zou het betekenen dat als deze switch uitvalt dat RSTP moet omschakelen naar een andere Root en zal daardoor ook de verbinding op elke switch opnieuw moeten toewijzen. Hierdoor ondervindt het netwerk enige downtijd.
Voorwaarden	• RSTP is geconfigureerd zoals hierboven is aangegeven • Gebruik gemaakt van Deelontwerp RSTP+SPB • Testcase P9 is geslaagd

Teststappen

1	Op PC1 worden ICMP-berichten gestuurd naar PC2 met een wait van 1 sec.
2	Switch CoreSw1 wordt losgekoppeld van de netstroom. Op deze manier wordt de switch spanningsloos.
3	Er wordt gecontroleerd of er veranderingen zijn in het netwerk; dit wordt gedaan met de commando's: ***show spantree ports active*** en ***show spantree vlan 1***
4	Er wordt gecontroleerd of de ICMP-berichten tussen de PCs nog verzonden worden. Er wordt gecontroleerd of de ICMP-berichten onderbroken zijn of dat de latency verhoogd is.

Verwachte Resultaat

CoreSw1 is de Root switch, hierdoor zal RSTP moeten omschakelen naar de switch met de op één na laagste Root prioriteit. De schakel tijd van RSTP bedraagt ± 1 seconden om de nieuwe Rootswitch functionaliteiten over te laten nemen. Hierdoor zal er een downtijd ontstaan van 1 à 2 seconden.

Behaalde Resultaat

```
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Request timed out.
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
```

```
-> show spantree ports active
 Vlan  Port   Oper Status  Path Cost  Role    Note
-----+-------+------------+----------+-------+---------
    1  1/1/1      FORW             4   DESG
    1  1/1/2      FORW             4   ROOT
    1  1/1/3       BLK             4    ALT

-> show spantree ports active
 Vlan  Port   Oper Status  Path Cost  Role    Note
-----+-------+------------+----------+-------+---------
    1  1/1/1      FORW             4   DESG
    1  1/1/3      FORW             4   ROOT
```

```
Spanning Tree Parameters for Vlan 1
  Spanning Tree Status :                    ON,
  Protocol             :        IEEE Rapid STP,
  mode                 : Per VLAN (1 STP per Vlan),
  Priority             :          8192 (0x2000),
  Bridge ID            :   2000-e8:e7:32:c1:76:29,
  Designated Root      :   1000-e8:e7:32:e6:a0:91,
  Cost to Root Bridge  :                     2,
  Root Port            :                   1/2,
  Next Best Root Cost  :                     0,
  Next Best Root Port  :                  None,
  TxHoldCount          :                     3,
  Topology Changes     :                    36,
  Topology age         :              00:33:12,
    Current Parameters (seconds)
      Max Age             =    20,
      Forward Delay       =    15,
      Hello Time          =     2
    Parameters system uses when attempting to become root
      System Max Age      =    20,
      System Forward Delay =    15,
      System Hello Time   =     2

-> show spantree vlan 1
Spanning Tree Parameters for Vlan 1
  Spanning Tree Status :                    ON,
  Protocol             :        IEEE Rapid STP,
  mode                 : Per VLAN (1 STP per Vlan),
  Priority             :          8192 (0x2000),
  Bridge ID            :   2000-e8:e7:32:c1:76:29,
  Designated Root      :   2000-e8:e7:32:c1:76:29,
  Cost to Root Bridge  :                     0,
  Root Port            :                  None,
  Next Best Root Cost  :                     0,
  Next Best Root Port  :                  None,
  TxHoldCount          :                     3,
  Topology Changes     :                    36,
  Topology age         :              00:33:48,
    Current Parameters (seconds)
      Max Age             =    20,
      Forward Delay       =    15,
      Hello Time          =     2
    Parameters system uses when attempting to become root
      System Max Age      =    20,
      System Forward Delay =    15,
      System Hello Time   =     2
```

Uit de afbeeldingen hierboven blijkt dat bij het uitschakelen van de Rootswitch er een Time-out is opgetreden. In de afbeelding daarnaast is te zien dat de verbinding van OS6860 naar de Rootswitch is verdwenen en dat er een nieuw path is naar de Root.

Op de afbeelding hiernaast is te zien dat toen de Rootswitch nog aan stond de OS6900-T40 niet de Rootswitch had maar alleen een Port naar de Root. Daaronder is de verandering te zien dat OS6900-T40 nu de nieuwe Rootswitch is door zijn lagere prioriteit dan de Root prioriteit van de OS6860.

Testcase P10.1 SPB	Heeft het uitvallen van switch CoreSw1 effect op het netwerk?
Beschrijving	Als in het netwerk switch CoreSw1 uitvalt, mag dit bij SPB niet voor problemen zorgen. SPB blokkeert namelijk geen verbindingen zoals RSTP dit doet. Ook is uit de literatuur gebleken dat het omschakelen van verbinding bij SPB maar enkele milliseconden duurt. Hierdoor zal het netwerk niet tot nauwelijks effect ondervinden van de verandering.
Voorwaarden	• SPB is geconfigureerd zoals hierboven is aangegeven • Gebruik gemaakt van Deelontwerp RSTP+SPB • Testcase P9.1 is geslaagd

Teststappen

1	Op PC1 worden ICMP-berichten gestuurd naar PC2 met een wait van 1 sec.
2	Switch CoreSw1 wordt losgekoppeld van de netstroom. Op deze manier wordt de switch spanningsloos.
3	Er wordt gecontroleerd of de switch nog in de SPB omgeving aanwezig is door middel van het uitvoeren van het ***"show spb isis adjacency"*** commando
4	Er wordt gecontroleerd of de ICMP-berichten tussen de PCs nog verzonden worden. Er wordt gecontroleerd of de ICMP-berichten onderbroken zijn en of dat de latency verhoogd is.

Verwachte Resultaat

Het versturen van de ICMP-berichten zal geen onderbreking ondervinden van de uitgevallen verbinding. Op de OS6860 is te zien dat CoreSw1 (OS6900-T20) verdwijnt uit de SPB omgeving.

Behaalde Resultaat

```
-> show spb isis adjacency
SPB ISIS Adjacency:
 System
 (Name : SystemId)                     Type   State   Hold  Interface
-----------------------------------+------+-------+------+----------
 OS6900-T20          : e8e7.32e6.a091  L1    UP        24        1/1/2
 OS6900-T40          : e8e7.32c1.7629  L1    UP        20        1/1/3

Adjacencies : 2
```

← Voor het uitschakelen van CoreSw1

Op de afbeeldingen is te zien dat op de OS6860 het commando "*show spb isis adjacency*" is uitgevoerd. Dit commando laat de switches zien die in de topology ook SPB draaien.

Hierbij is te zien dat bij het uitschakelen van CoreSw1 (OS6900-T20) deze niet langer te zien is in de tabel.

```
-> show spb isis adjacency
SPB ISIS Adjacency:
 System
 (Name : SystemId)                     Type   State   Hold  Interface
-----------------------------------+------+-------+------+----------
 OS6900-T40          : e8e7.32c1.7629  L1    UP        25        1/1/3

Adjacencies : 1
```

← Na het uitschakelen van CoreSw1

```
Pinging 192.168.0.2 with 32 bytes of data:
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
```

In de afbeelding is het uitwisselen van ICMP-berichten weergegeven tussen de PCs. Hierbij is te zien dat het uitvallen van CoreSw1 geen effect heeft op deze uitwisseling.

← Het loskoppelen van CoreSw1

Testcase P11 RSTP	**Heeft het uitvallen van een willekeurige verbinding effect op het netwerk?**
Beschrijving	Volgens het literatuuronderzoek schakelt RSTP, net als STP, bij het uitvallen van een niet-Blocking verbinding. Er zal een downtijd van 1 à 2 seconden plaatsvinden, doordat RSTP dit als omschakeltijd nodig heeft.
Voorwaarden	• RSTP is geconfigureerd zoals hierboven is aangegeven • Gebruik gemaakt van Deelontwerp RSTP+SPB • Testcase P9 is geslaagd

Teststappen

1	Op PC1 worden ICMP-berichten gestuurd naar PC2 met een wait van 1 sec.
2	Een willekeurige verbinding tussen de switches wordt losgekoppeld van beide switches waarmee deze is verbonden.
3	Er wordt gecontroleerd of de ICMP-berichten tussen de PCs nog verzonden worden. Ook wordt er gecontroleerd of de ICMP-berichten onderbroken zijn of dat de latency verhoogd is.

Verwachte Resultaat

RSTP heeft een schakeltijd van 1 à 2 seconden om het path te wijzigen, hiermee zullen er gedurende 5 seconden geen ICMP-berichten gestuurd worden. Dit zal het geval zijn als er een verbinding wordt losgekoppeld die als Root verbinding of Designated verbinding wordt gebruikt. Bij het loskoppelen van een verbinding die in Blocking state staat zal er geen effect ondervonden worden.

Behaalde Resultaat

```
C:\Users\Rei>ping 192.168.0.2 -t -w 1

Pinging 192.168.0.2 with 32 bytes of data:
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Request timed out.
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Request timed out.
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Request timed out.
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Request timed out.
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
```

➔ *Kabel port 1/1/2 op de OS6860 losgekoppeld*

➔ *Kabel port 1/1/2 op de OS6860 terug geplaatst*

➔ *Kabel port 1/1/3 op de OS6860 losgekoppeld*

➔ *Kabel port 1/1/3 op de OS6860 terug geplaatst*

➔ *Kabel port 1/1 op de OS6900-T20 losgekoppeld*

➔ *Kabel port 1/1 op de OS6900-T20 terug geplaatst*

➔ *Kabel port 1/2 op de OS6900-T20 losgekoppeld*

➔ *Kabel port 1/2 op de OS6900-T20 terug geplaatst*

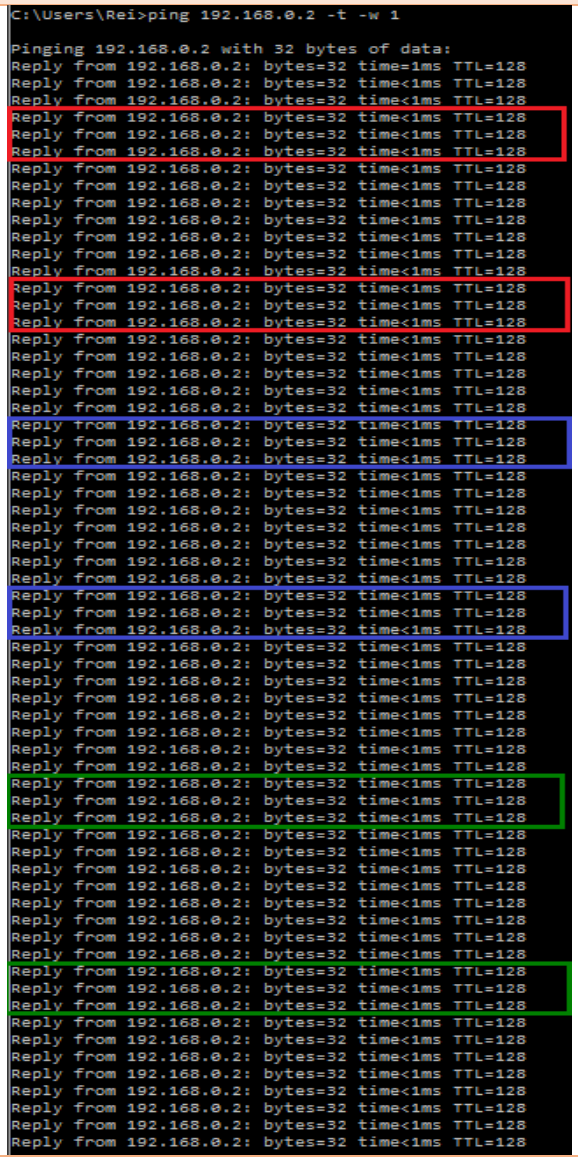
➔ *Kabel port 1/3 op de OS6900-T40 losgekoppeld*

➔ *Kabel port 1/3 op de OS6900-T40 terug geplaatst*

➔ *Kabel port 1/2 op de OS6900-T40 losgekoppeld*

➔ *Kabel port 1/2 op de OS6900-T40 terug geplaatst*

Testcase P11.1 SPB	Heeft het uitvallen van een willekeurige verbinding effect op het netwerk?
Beschrijving	Volgens het literatuuronderzoek gebruikt SPB alle verbindingen. Dit zorgt ervoor dat het netwerk een minimale downtijd ondervindt. SPB heeft maar een aantal milliseconden nodig en zal hierdoor alleen een hogere latency hebben.
Voorwaarden	• SPB is geconfigureerd zoals hierboven is aangegeven • Gebruik gemaakt van Deelontwerp RSTP+SPB • Testcase P9.1 is geslaagd
Teststappen	
1	Op PC1 worden ICMP-berichten gestuurd naar PC2 met een wait van 1 sec.
2	Een willekeurige verbinding tussen de switches wordt losgekoppeld van beide switches waarmee deze is verbonden.
3	Er wordt gecontroleerd of de ICMP-berichten tussen de PCs nog verzonden worden. Ook wordt er gecontroleerd of de ICMP-berichten onderbroken zijn of dat de latency verhoogd is.
Verwachte Resultaat	
Het netwerk zal bijna geen effect ondervinden van de uitgevallen verbinding. Er zal hoogstens een verhoging zijn in de latency.	
Behaalde Resultaat	



➔ *Kabel port 1/1/2 op de OS6860 losgekoppeld*

➔ *Kabel port 1/1/2 op de OS6860 terug geplaatst*

➔ *Kabel port 1/1/3 op de OS6860 losgekoppeld*

➔ *Kabel port 1/1/3 op de OS6860 terug geplaatst*

➔ *Kabel port 1/1 op de OS6900-T20 losgekoppeld*

➔ *Kabel port 1/1 op de OS6900-T20 terug geplaatst*

➔ *Kabel port 1/2 op de OS6900-T20 losgekoppeld*

➔ *Kabel port 1/2 op de OS6900-T20 terug geplaatst*

➔ *Kabel port 1/3 op de OS6900-T40 losgekoppeld*

➔ *Kabel port 1/3 op de OS6900-T40 terug geplaatst*

➔ *Kabel port 1/2 op de OS6900-T40 losgekoppeld*

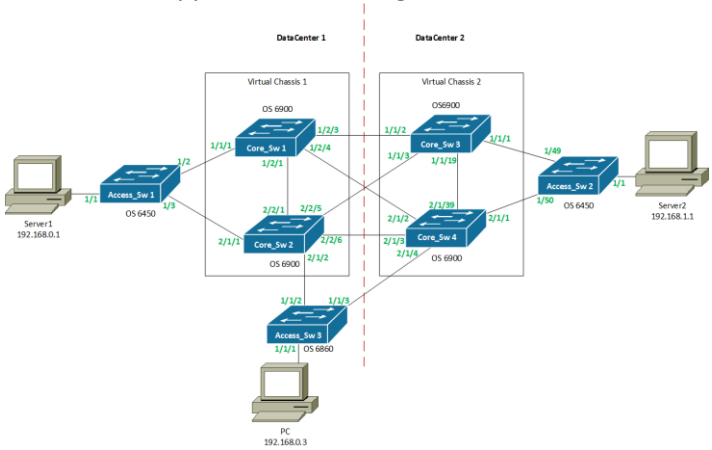
➔ *Kabel port 1/2 op de OS6900-T40 terug geplaatst*

6. Nulmeting

De metingen worden gedaan op het gehele netwerk om zo de uiteindelijke werkingen van het netwerk tegen elkaar af te wegen. Op deze manier kan er een duidelijk advies gegeven worden waarom er wel of niet gemigreerd moet worden naar een TRILL omgeving in plaats van een STP netwerk.

6.1 Ontwerp

Het netwerk waar de metingen op worden uitgevoerd zijn de beide situaties. Nu is het zo dat door de eis dat de apparatuur niet mag veranderen deze beide netwerken er fysiek gezien hetzelfde zijn.



Figuur 5 Fysiek ontwerp metingen

De instellingen die bij de huidige situatie horen zien er als volgt uit:

Server1	***Server2***	***PC***
IP-adres 192.168.0.1 met subnetmask 255.255.255.0 Default-GW 192.168.0.100	IP-adres 192.168.1.1 met subnetmask 255.255.255.0 Default-GW 192.168.1.100	IP-adres 192.168.0.3 met subnetmask 255.255.255.0 Default-GW 192.168.0.100

Core_Sw1	***Core_Sw2***
Virtual Chassis: Interface 1/2/1 als VFL port; Chassis ID 1 (Master switch); EMP chassis 1 adres 10.0.0.1 EMP master adres 10.0.0.10 **RSTP:** Root priority 4096	**Virtual Chassis:** Interface 2/2/1 als VFL port; Chassis ID 2 (Slave switch); EMP adres 10.0.0.2 **VRRP:** VRRP op VRID 1 en VRID 2 enabled VRRP op VLAN 1 enabled VRID 1 adres 192.168.0.100 VRID 2 adres 192.168.1.100

Core_Sw3	***Core_Sw4***
Virtual Chassis: Interface 1/1/19 als VFL port; Chassis ID 1 (Master switch); EMP chassis 1 adres 10.0.0.1 EMP master adres 10.0.0.10 **RSTP:** Root priority 8192	**Virtual Chassis:** Interface 2/1/39 als VFL port; Chassis ID 2 (Slave switch); EMP adres 10.0.0.2 **VRRP:** VRRP op VRID 1 en VRID 2 enabled VRRP op VLAN 1 enabled VRID 1 adres 192.168.0.100 VRID 2 adres 192.168.1.100

Access_Sw1	*Access_Sw2*	*Access_Sw3*
LACP: group 10 creëren; Interfaces 1/2 en 1/3 toevoegen aan LACP group 10;	**LACP:** group 11 creëren; Interfaces 1/49 en 1/50 toevoegen aan LACP group 11;	**RSTP**: Root priority 12288

De instellingen die bij het Proof of Concept horen zien er als volgt uit:

Server1	*Server2*	*PC*
IP-adres 192.168.0.1 met subnetmask 255.255.255.0 Default-GW 192.168.0.100	IP-adres 192.168.1.1 met subnetmask 255.255.255.0 Default-GW 192.168.1.100	IP-adres 192.168.0.3 met subnetmask 255.255.255.0 Default-GW 192.168.0.100

Core_Sw1	*Core_Sw2*
Virtual Chassis: Interfaces 1/2/1 als VFL port; Chassis ID 1 (Master switch); **SPB:** SPB bvlan 4001; SPB poorten 1/2/3 & 1/2/4; SPB service 1; ISID 500; SAP linkagg 10:all	**Virtual Chassis:** Interfaces 2/2/1 als VFL port; Chassis ID 2 (Slave switch); **SPB:** SPB bvlan 4001; ISID 500 SPB poorten 2/1/3 & 2/2/5 & 2/2/6;

Core_Sw3	*Core_Sw4*
Virtual Chassis: Interfaces 1/1/19 als VFL port; Chassis ID 1 (Master switch); **SPB:** SPB bvlan 4001; SPB poorten 1/1/2 & 1/1/3; SPB service 1; ISID 500; SAP linkagg 11:all	**Virtual Chassis:** Interfaces 2/1/39 als VFL port; Chassis ID 2 (Slave switch); **SPB:** SPB bvlan 4001; SPB poorten 2/1/2 & 2/1/3 & 2/1/4;

Access_Sw1	*Access_Sw2*	*Access_Sw3*
LACP: group 10 aanmaken; Interfaces 1/2 en 1/3 toevoegen aan LACP group 10; **IP:** ip interface 192.168.0.100/24 ip interface 192.168.1.100/24	**LACP:** group 11 aanmaken; Interfaces 1/49 en 1/50 toevoegen aan LACP group 11; **IP** ip interface 192.168.0.100/24 ip interface 192.168.1.100/24	**SPB:** SPB bvlan 4001; SPB poorten 1/1/2 & 1/1/3; SPB service 1; SAP port 1/1/1:all;

6.2 Configuratie huidige situatie

Virtual-Chassis

Op de Master VC1 (OS6900-T20)	Op de Slave VC1 (OS6900-T40)
***virtual-chassis chassis-id** 1 **configured-chassis-id** 1*	***virtual-chassis chassis-id** 2 **configured-chassis-id** 2*
***Virtual-chassis vf-link-mode** static*	***Virtual-chassis vf-link-mode** static*
virtual-chassis chassis-id** 1 **vf-link** 0 **create	***virtual-chassis chassis-id** 2 **vf-link** 0 **create***
***virtual-chassis vf-link** 0 **member-port** 1/2/1*	***virtual-chassis vf-link** 0 **member-port** 2/2/1*
***virtual-chassis chassis-group** 1*	***virtual-chassis chassis-group** 1*
***ip interface local chassis-id** 1 **emp address** 10.0.0.1 **mask** 255.255.255.0*	***ip interface local chassis-id** 1 **emp address** 10.0.0.2 **mask** 255.255.255.0*
***ip interface master emp address** 10.0.0.10 **mask** 255.255.255.0*	

Op de Master VC2 (OS6900-X20)	Op de Slave VC2 (OS6900-X40)
***virtual-chassis chassis-id** 1 **configured-chassis-id** 1*	***virtual-chassis chassis-id** 2 **configured-chassis-id** 2*
***Virtual-chassis vf-link-mode** static*	***Virtual-chassis vf-link-mode** static*
virtual-chassis chassis-id** 1 **vf-link** 0 **create	***virtual-chassis chassis-id** 2 **vf-link** 0 **create***
***virtual-chassis vf-link** 0 **member-port** 1/1/19*	***virtual-chassis vf-link** 0 **member-port** 2/1/39*
***virtual-chassis chassis-group** 1*	***virtual-chassis chassis-group** 1*
***ip interface local chassis-id** 1 **emp address** 10.0.0.2 **mask** 255.255.255.0*	***ip interface local chassis-id** 1 **emp address** 10.0.0.2 **mask** 255.255.255.0*
***ip interface master emp address** 10.0.0.10 **mask** 255.255.255.0*	

VRRP

Op de Master switch (VC1)	Op de Back-up switch(VC2)
ip interface *"vrrp"* **address** *192.168.0.100/24* **vlan** *1*	**ip interface** *"vrrp"* **address** *192.168.0.101/24* **vlan** *1*
***vrrp** 1 1*	***vrrp** 1 1*
***vrrp** 1 1 **address** 192.168.0.100*	***vrrp** 1 1 **address** 192.168.0.100*
***vrrp** 1 1 **admin-state** enable*	***vrrp** 1 1 **admin-state** enable*
ip interface *"vrrp2"* **address** *192.168.1.100/24* **vlan** *1*	**ip interface** *"vrrp2"* **address** *192.168.1.101/24* **vlan** *1*
***vrrp** 2 1*	***vrrp** 1 1*
***vrrp** 2 1 **address** 192.168.1.100*	***vrrp** 1 1 **address** 192.168.0.100*
***vrrp** 2 1 **admin-state** enable*	***vrrp** 1 1 **admin-state** enable*

LACP

configuratie op Access_Sw1 (OS6450)	configuratie op Switch2 (VC1)
***lacp linkagg** 10 **size** 2 **actor admin key** 5*	***linkagg lacp agg** 10 **size** 2 **actor admin-key** 5*
***lacp agg** 1/2 **actor admin key** 5*	***linkagg lacp port** 1/1/1 **actor admin-key** 5*
***lacp agg** 1/3 **actor admin key** 5*	***linkagg lacp port** 2/1/1 **actor admin-key** 5*
***vlan** 1 **port default** 10*	***vlan** 1 **members linkagg** 10 **untagged***

configuratie op Access_Sw2 (OS6450)	configuratie op Switch2 (VC2)
***lacp linkagg** 11 **size** 2 **actor admin key** 5*	***linkagg lacp agg** 11 **size** 2 **actor admin-key** 5*
***lacp agg** 1/1/49 **actor admin key** 5*	***linkagg lacp port** 1/1/1 **actor admin-key** 5*
***lacp agg** 1/1/50 **actor admin key** 5*	***linkagg lacp port** 2/1/1 **actor admin-key** 5*
***vlan** 1 **port default** 11*	***vlan** 1 **members linkagg** 11 **untagged***

RSTP

VC1 (OS6900-T20)	*Access_Sw3 (OS6860)*	*VC2 (OS6900-T40)*
spantree mode rstp	***spantree mode rstp***	***spantree mode rstp***
***spantree vlan** 1 **priority** 4096*	***spantree vlan** 1 **priority** 12288*	***spantree vlan** 1 **priority** 8192*

6.3 Configuratie Proof of Concept

De configuratie voor het realiseren van het Proof of Concept verandert in meerdere opzichten op die van de huidige situatie; zo is VRRP in de core niet mogelijk als de core SPB gebruikt. SPB gebruikt namelijk een extra tag in de frames die binnenkomen op de SAP port. Hierin wordt het VLAN aan een ISID gekoppeld. Het ISID is door middel van een SPB service aan een BVLAN gekoppeld binnen het SPB netwerk. Het ISID wordt uiteindelijk gebruikt voor het switchen binnen het SPB netwerk over het aangegeven BVLAN. Hierdoor is het gebruik van VRRP of iedere andere vorm van routeren binnen het SPB netwerk niet mogelijk. Dit wordt nu opgelost door de Access switches beide ip interfaces te geven om beide servers te kunnen bereiken.

De configuratie voor het Proof of Concept ziet er nu als volgt uit:

Virtual-Chassis

Op de Master VC1 (OS6900-T20)	Op de Slave VC1 (OS6900-T40)
***virtual-chassis chassis-id** 1 **configured-chassis-id** 1*	***virtual-chassis chassis-id** 2 **configured-chassis-id** 2*
***Virtual-chassis vf-link-mode** static*	***Virtual-chassis vf-link-mode** static*
virtual-chassis chassis-id** 1 **vf-link** 0 **create	***virtual-chassis chassis-id** 2 **vf-link** 0 **create***
***virtual-chassis vf-link** 0 **member-port** 1/2/1*	***virtual-chassis vf-link** 0 **member-port** 2/2/1*
***virtual-chassis chassis-group** 1*	***virtual-chassis chassis-group** 1*
***ip interface local chassis-id** 1 **emp address** 10.0.0.1 **mask** 255.255.255.0*	***ip interface local chassis-id** 1 **emp address** 10.0.0.2 **mask** 255.255.255.0*
***ip interface master emp address** 10.0.0.10 **mask** 255.255.255.0*	

Op de Master VC2 (OS6900-X20)	Op de Slave VC2 (OS6900-X40)
***virtual-chassis chassis-id** 1 **configured-chassis-id** 1*	***virtual-chassis chassis-id** 2 **configured-chassis-id** 2*
***Virtual-chassis vf-link-mode** static*	***Virtual-chassis vf-link-mode** static*
virtual-chassis chassis-id** 1 **vf-link** 0 **create	***virtual-chassis chassis-id** 2 **vf-link** 0 **create***
***virtual-chassis vf-link** 0 **member-port** 1/1/19*	***virtual-chassis vf-link** 0 **member-port** 2/1/39*
***virtual-chassis chassis-group** 1*	***virtual-chassis chassis-group** 1*
***ip interface local chassis-id** 1 **emp address** 10.0.0.2 **mask** 255.255.255.0*	***ip interface local chassis-id** 1 **emp address** 10.0.0.2 **mask** 255.255.255.0*
***ip interface master emp address** 10.0.0.10 **mask** 255.255.255.0*	

LACP

configuratie op Access_Sw1 (OS6450)	configuratie op VC1
***lacp linkagg** 10 **size** 2 **actor admin key** 5*	***linkagg lacp agg** 10 **size** 2 **actor admin-key** 5*
***lacp agg** 1/2 **actor admin key** 5*	***linkagg lacp port** 1/1/1 **actor admin-key** 5*
***lacp agg** 1/3 **actor admin key** 5*	***linkagg lacp port** 2/1/1 **actor admin-key** 5*
***vlan** 1 **port default** 10*	***vlan** 1 **members linkagg** 10 **untagged***

configuratie op Access_Sw2 (OS6450)	configuratie op VC2
***lacp linkagg** 11 **size** 2 **actor admin key** 5*	***linkagg lacp agg** 11 **size** 2 **actor admin-key** 5*
***lacp agg** 1/1/49 **actor admin key** 5*	***linkagg lacp port** 1/1/1 **actor admin-key** 5*
***lacp agg** 1/1/50 **actor admin key** 5*	***linkagg lacp port** 2/1/1 **actor admin-key** 5*
***vlan** 1 **port default** 11*	***vlan** 1 **members linkagg** 11 **untagged***

SPB

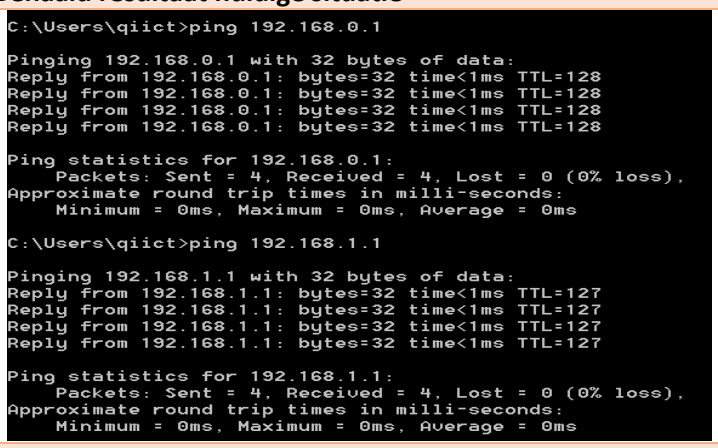
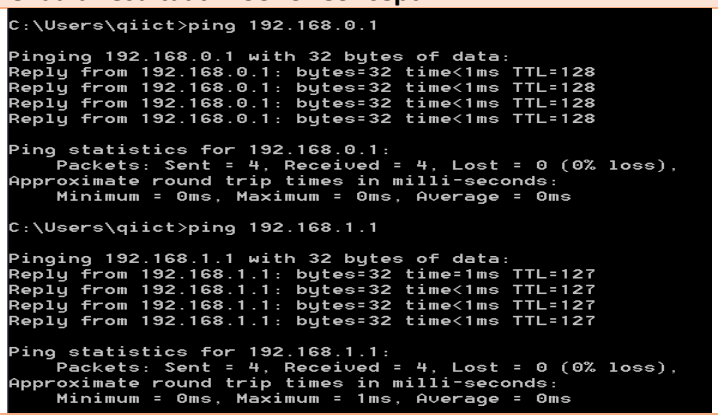
VC1	*Access_Sw3 (OS6860)*	*VC2*
***spb bvlan** 4001*	***spb bvlan** 4001*	***spb bvlan** 4001*
***spb isis control-bvlan** 4001*	***spb isis control-bvlan** 4001*	***spb isis control-bvlan** 4001*
***spb isis interface port** 1/2/3-4*	***spb isis interface port** 1/1/2-3*	***spb isis interface port** 1/1/2-3*
***spb isis interface port** 2/2/5-6*	***spb isis admin-state** enable*	***spb isis interface port** 2/1/2-4*
***spb isis interface port** 2/1/2*	***service access port** 1/1/1*	***spb isis admin-state** enable*
spb isis admin-state enable	***service spb** 1 **isid** 500 **bvlan** 4001 **admin-state** enable*	***spantree vlan** 1 **admin-state** disable*
***spantree vlan** 1 **admin-state** disable*	***service spb** 1 **sap port** 1/1/1:all **admin-state** enable*	***service access linkagg** 11*
***service access linkagg** 10*	***spantree vlan** 1 **admin-state** disable*	***service spb** 1 **isid** 500 **bvlan** 4001 **admin-state** enable*
***service spb** 1 **isid** 500 **bvlan** 4001 **admin-state** enable*		***service spb** 1 **sap linkagg** 11:all **admin-state** enable*
***service spb** 1 **sap linkagg** 10:all **admin-state** enable*		

Overige configuratie

Access_Sw2 (OS6450)
***ip interface** DFGW1 **address** 192.168.0.100/24 **vlan** 1*
***ip interface** DFGW2 **address** 192.168.1.100/24 **vlan** 1*

6.4 Testcases

Allereerst zal er een acceptatie test uitgevoerd worden in de vorm van het kunnen bereiken van beide servers vanaf de PC. Hiermee wordt aangegeven dat beide servers bereikbaar zijn en het netwerk naar behoren werkt.

Testcase M0	**Kan er tussen de PC en de servers gepingd worden?**
Beschrijving	Voordat de metingen uitgevoerd kunnen worden zal eerst gecontroleerd moeten worden of de PC beide servers kan bereiken.
Voorwaarden	• Netwerk ontworpen aan de hand van eerder genoemd ontwerp. • Protocollen geconfigureerd zoals bij het ontwerp is aangegeven
Teststappen	
1	Vanaf de PC worden ICMP-berichten gestuurd naar Server 1 en naar Server 2
2	Er wordt gecontroleerd of er van beide servers een response wordt gekregen
Behaald resultaat huidige situatie	
	In de afbeelding hiernaast is te zien hoe naar beide servers ICMP-berichten worden gestuurd en dat beide servers een response geven op de berichten.
Behaald resultaat Proof of Concept	
	In de afbeelding hiernaast is te zien hoe naar beide servers ICMP-berichten worden gestuurd en dat beide servers een response geven op de berichten.

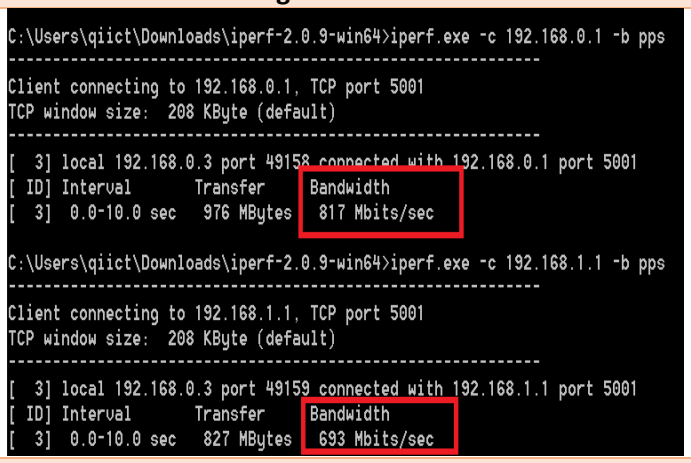
Als bovenstaande testcase geslaagd als resultaat geeft, zullen er verschillende metingen uitgevoerd gaan worden om te kunnen concluderen of het Proof of Concept wenselijker is als de oude situatie. In overleg met de begeleider is er besloten de metingen uit te voeren die betrekking hebben op de volgende gebieden:

- Performance
- Scalability
- Reliability
- Availability
- Maintainability

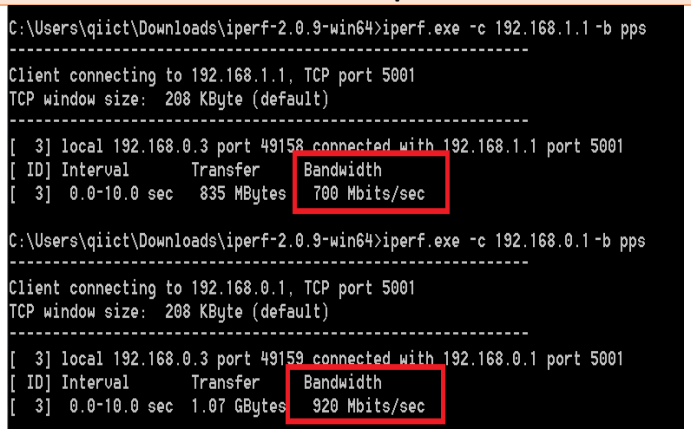
Performance[6]

Met de performance wordt onder andere de snelheid van de bandbreedte bedoeld. Hierbij heeft ook de response tijd ook een groot aandeel. In dit geval zal er voornamelijk gekeken worden hoe snel de bandbreedte is en hoe groot de Latency is van een bericht.

Het controleren van de snelheid kan als volgt worden gedaan: Op de servers wordt een IPERF server opgestart, op de PC wordt een IPERF cliënt opgestart. IPERF kan de bandbreedte meten van een aantal pakketten dat gestuurd wordt via het IPERF applicatie.

<table>
<tr><th>Testcase M1</th><th colspan="2">Bandbreedte meten</th></tr>
<tr><td>Beschrijving</td><td colspan="2">Om de performance vast te stellen zal er een testcase worden gemaakt om te kijken wat de snelheid is van de verbinding.</td></tr>
<tr><td>Voorwaarden</td><td colspan="2">• Netwerk ontworpen aan de hand van eerder genoemd ontwerp.
• Protocollen geconfigureerd zoals bij het ontwerp is aangegeven
• Testcase M0 is geslaagd</td></tr>
<tr><td colspan="3">Teststappen</td></tr>
<tr><td>1</td><td colspan="2">Op de servers wordt de IPERF server opgestart; dit wordt gedaan door het commando “iperf.exe –s” uit te voeren</td></tr>
<tr><td>2</td><td colspan="2">Op de cliënt zullen de commando’s: “iperf.exe –c 192.168.0.1 –b pps” en “iperf.exe –c 192.168.1.1 –b pps” worden uitgevoerd.</td></tr>
<tr><td>3</td><td colspan="2">Controleren wat de bandbreedte is die bereikt wordt tussen de PC en de servers.</td></tr>
<tr><td colspan="3">Behaald resultaat huidige situatie</td></tr>
<tr><td colspan="2"> 
</td><td>Hiernaast is te zien dat eerst de bandbreedte naar Server1 is gemeten.

Hieruit kwam een bandbreedte van 817 Mbits/s.

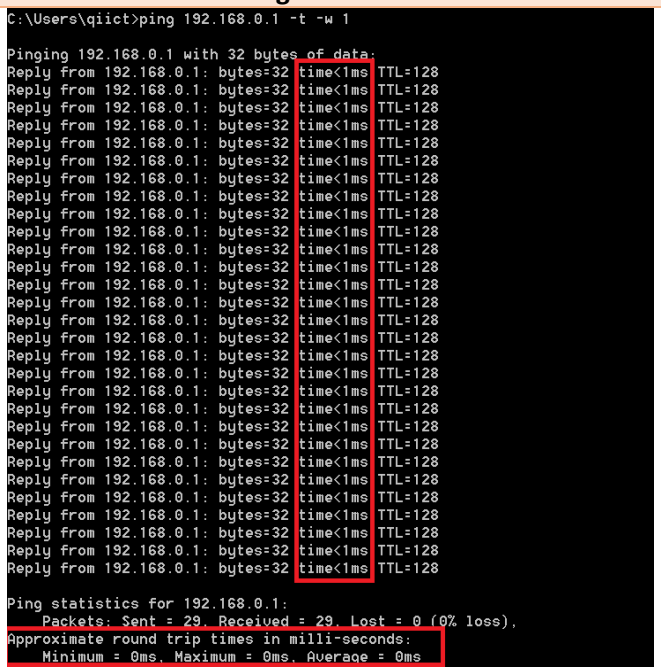
Het meten van de bandbreedte naar Server2 gaf een waarde van 693 Mbit/s</td></tr>
<tr><td colspan="3">Behaald resultaat Proof of Concept</td></tr>
<tr><td colspan="2"> 
</td><td>Hiernaast is te zien dat eerst de bandbreedte naar Server2 is gemeten.

Hieruit kwam een bandbreedte van 700 Mbits/s.

Het meten van de bandbreedte naar Server1 gaf een waarde van 920 Mbit/s</td></tr>
</table>

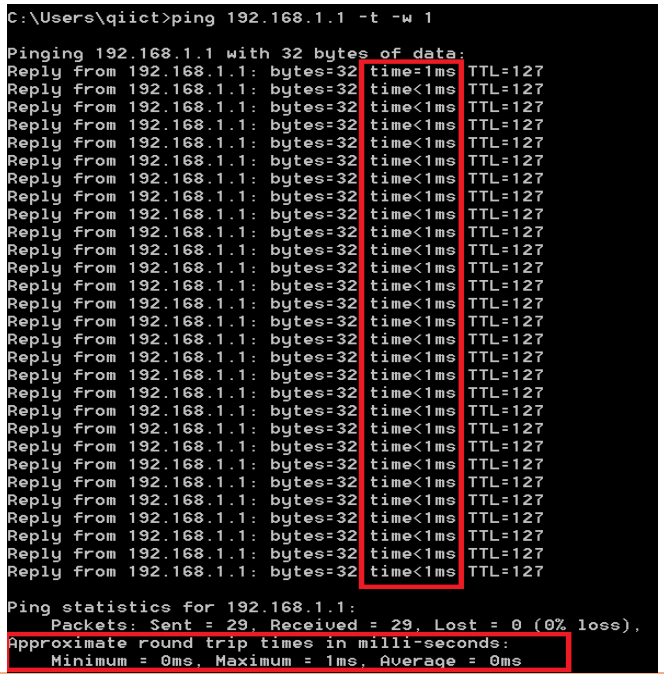
Als tweede wordt de Latency gemeten, hierbij wordt er een ping-bericht gestuurd van de PC naar de servers. Nu wordt er gekeken hoe lang het duurt voordat de PC een response bericht krijgt van de servers. Latency wordt aangeduid in ms.

Testcase M2	Performance; Wat is de latency?
Beschrijving	Om de performance vast te stellen zal er een testcase worden gemaakt om te kijken hoeveel Latency een ping ondervindt.
Voorwaarden	• Netwerk ontworpen aan de hand van eerder genoemd ontwerp. • Protocollen geconfigureerd zoals bij het ontwerp is aangegeven • Testcase M0 is geslaagd
Teststappen	
1	Op de PC worden ICMP-berichten gestuurd naar beide servers met een wait van 1 sec.
2	Er wordt gecontroleerd wat de latency is van de ICMP-berichten uitwisseling
Behaald resultaat huidige situatie	



De tijd die de ICMP-berichten nodig hebben om Server1 te bereiken is <1ms.

Hierbij kan geconcludeerd worden dat de Latency ook <1ms



De tijd die de ICMP-berichten nodig hebben om Server2 te bereiken is <1ms.

Hierbij kan geconcludeerd worden dat de Latency ook <1ms

Behaald resultaat Proof of Concept

```
C:\Users\qiict>ping 192.168.0.1 -t -w 1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 30, Received = 30, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

De tijd die de ICMP-berichten nodig hebben om Server1 te bereiken is <1ms.

Hierbij kan geconcludeerd worden dat de Latency ook <1ms

```
C:\Users\qiict>ping 192.168.1.1 -t -w 1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.1:
    Packets: Sent = 30, Received = 30, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

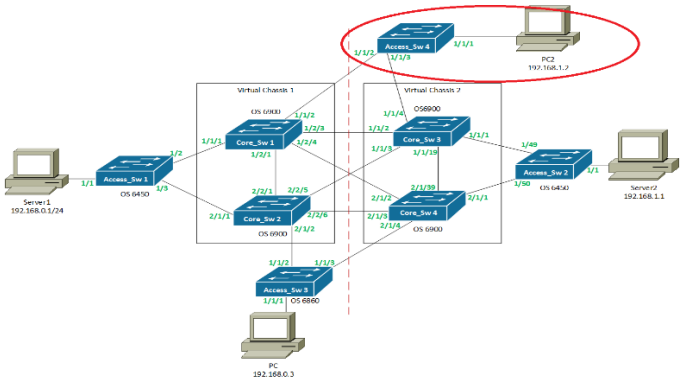
De tijd die de ICMP-berichten nodig hebben om Server2 te bereiken is <1ms.

Hierbij kan geconcludeerd worden dat de Latency ook <1ms

Scalability[6]

De scalability houdt in of het netwerk uitbreidbaar kan worden met meerdere componenten, hierbij kan gedacht worden aan een extra datacenter of een gebruiker. Hierbij mag deze toevoeging geen gevolg hebben op de functionaliteiten van het netwerk. Om dit te testen zal er een gebruiker en switch worden toegevoegd. Dan wordt er gecontroleerd wat voor effect dit heeft op het netwerk.

Voor het testen van Scalability wordt het volgende ontwerp gebruikt, waarbij in de rode cirkel de toegevoegde componenten zich bevinden. Hierbij zal de switch met default instellingen aangesloten worden:



Testcase M3	Scalability; Is het netwerk schaalbaar?
Beschrijving	Om te controleren of het netwerk schaalbaar is zal er een extra gebruiker toegevoegd worden. Als de functionaliteiten van het netwerk geen verandering doormaken tijdens het toevoegen zal dit betekenen dat het netwerk goed schaalbaar is.
Voorwaarden	• Netwerk ontworpen aan de hand van bovenstaand ontwerp. • Protocollen geconfigureerd zoals bij het ontwerp is aangegeven • Testcase M0 is geslaagd
Teststappen	
1	Vanaf PC2 worden ICMP-berichten gestuurd naar beide servers.
2	Er wordt gecontroleerd of er van beide servers een response wordt gekregen
Behaald resultaat huidige situatie	

```
C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.100

Tunnel adapter isatap.{B2E7D4F3-C68B-4F48-A2CA-09D2D429EE9E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\admin>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=15ms TTL=127
Reply from 192.168.0.1: bytes=32 time<1ms TTL=127
Reply from 192.168.0.1: bytes=32 time<1ms TTL=127
Reply from 192.168.0.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 3ms

C:\Users\admin>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Allebei de servers kunnen bereikt worden vanaf PC2.

Hierbij is de switch met default configuratie aangesloten op het netwerk.

Ook is er op de andere switches geen configuratie toegevoegd om het werkend te krijgen.

Behaald resultaat Proof of Concept

```
C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.100

Tunnel adapter isatap.{B2E7D4F3-C68B-4F48-A2CA-09D2D429EE9E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\admin>ping 192.168.0.1 -w 1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=41ms TTL=127
Reply from 192.168.0.1: bytes=32 time<1ms TTL=127
Reply from 192.168.0.1: bytes=32 time<1ms TTL=127
Reply from 192.168.0.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 41ms, Average = 10ms

C:\Users\admin>ping 192.168.1.1 -w 1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Allebei de servers kunnen bereikt worden vanaf PC2

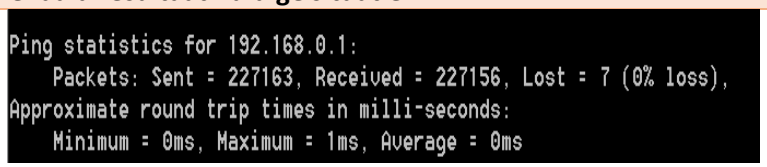
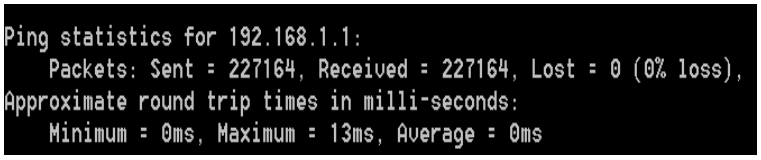
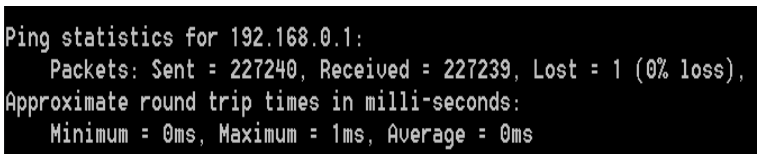
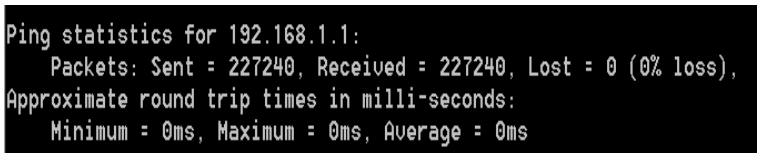
De toegevoegde switch is met de default instellingen aangesloten.

Echter kan er pas gecommuniceerd worden over deze switch nadat er SAP poorten zijn aangemaakt op VC1 en VC2 waar de nieuwe switch op aangesloten is.

Anders is het niet mogelijk om het verkeer door het SPB netwerk te switchen.

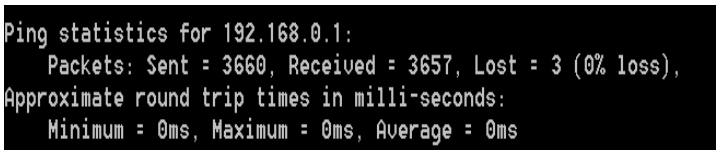
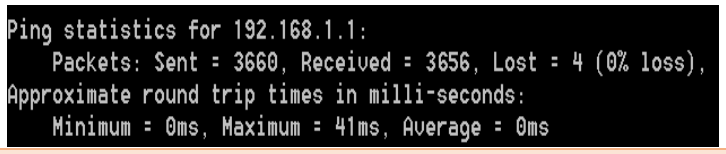
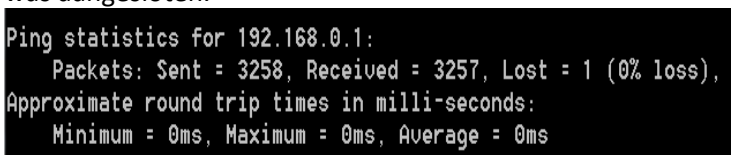
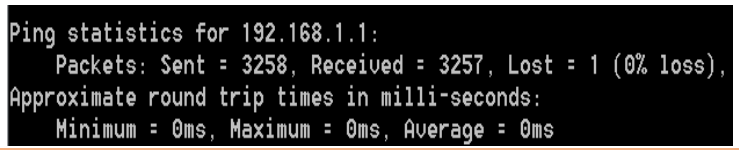
Reliability[6]

Reliability is het consistente gebruik van het netwerk bij verandering. Dit kan zijn dat de datastroom over het netwerk data blijft sturen zonder dat het netwerk enige downtijd ondervindt. Dit kan getest worden door middel van een duurtest. Hierbij worden er ICMP-berichten van de PC naar de servers gestuurd en deze uitwisseling zal ±63 uur lang draaien. Na deze 63 uur zal er gecontroleerd worden of er enige downtijd heeft plaats gevonden.

Testcase M4	**Reliability; Hoeveel downtijd ondervindt het netwerk gedurende 63 uur?**
Beschrijving	Er wordt gecontroleerd of het netwerk enige downtime ondervindt gedurende een 63 uur durende ICMP-berichten uitwisseling. Deze zal opgestart worden en dan zal het netwerk gedurende 63 uur niet gewijzigd worden.
Voorwaarden	• Netwerk ontworpen aan de hand van eerder genoemd ontwerp. • Protocollen geconfigureerd zoals bij het ontwerp is aangegeven • Testcase M0 is geslaagd
Teststappen	
1	Vanaf de PC worden ICMP-berichten gestuurd naar beide servers met een wait van 1 sec.
2	Het netwerk zal de komende 63 uur niet aangepast worden. (± 227000 ICMP-berichten)
3	Na 63 uur wordt de ICMP-uitwisseling gestopt en wordt er gecontroleerd hoeveel downtime er is opgetreden.
Behaald resultaat huidige situatie	
	Op server1 is er na ± 63 uur 7x een request time-out opgetreden. Dit zorgt voor een Reliability van: (7/227163)*100 = 99,997%
	Op server2 is er na ± 63 uur 0x een request time-out opgetreden. Dit zorgt voor een Reliability van: (0/227164)*100 = 100%
Behaald resultaat Proof of Concept	
	Op server1 is er na ± 63 uur 1x een request time-out opgetreden. Dit zorgt voor een Reliability van: (1/227240)*100 = 99,999%
	Op server2 is er na ± 63 uur 0x een request time-out opgetreden. Dit zorgt voor een Reliability van: (0/227240)*100 = 100%

Availability[6]

Bij availability wordt er bijgehouden of de gebruiker de servers kan bereiken. In het geval van dit netwerk moet de gebruiker, de twee servers kunnen bereiken. Ook bij uitval van verbindingen in het netwerk. Dit kan getest worden door het loskoppelen van kabels uit de opstelling, hierbij wordt dan gekeken of de berichten tussen de PC en de servers dan enige down tijd ondervindt.

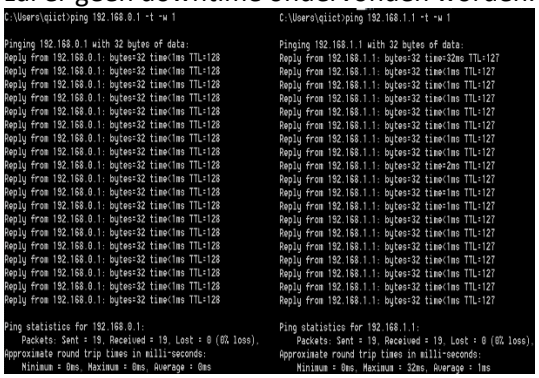
Testcase M5	**Availability; wat is het availability percentage?**
Beschrijving	Om de availability te testen zal er gebruik gemaakt worden van een redundantie test. Hierbij zullen verschillende kabels tussen de switches worden gehaald. Hierna zal gecontroleerd worden of het netwerk hier effect van ondervindt in de vorm van downtime.
Voorwaarden	• Netwerk ontworpen aan de hand van eerder genoemd ontwerp. • Protocollen geconfigureerd zoals bij het ontwerp is aangegeven • Testcase M0 is geslaagd
Teststappen	
1	Vanaf de PC worden ICMP-berichten gestuurd naar beide servers met een wait van 1 sec
2	Een willekeurige verbinding tussen de switches wordt losgekoppeld van beide switches waarmee deze is verbonden.
3	Er wordt gecontroleerd of de ICMP-berichten tussen de PCs nog verzonden worden. Ook wordt er gecontroleerd of de ICMP-berichten onderbroken zijn of dat de latency verhoogd is.
Behaald resultaat huidige situatie	
Tijdens het testen van de Redundantie zijn er verbindingen tussen switches losgekoppeld en wederom aangesloten. Hieruit bleek dat het loskoppelen van sommige verbindingen een time-out gaf van 1 sec. Hiermee wordt duidelijk dat deze verbindingen of de verbinding naar de Root is of Designated routes zijn.	
	Dit zorgt bij Server1 voor een availability van: (3/3660)*100 = 99,918%
	Dit zorgt bij Server2 voor een availability van: (4/3660)*100 = 99,890%
Behaald resultaat Proof of Concept	
Tijdens het testen van de Redundantie zijn er verbindingen tussen switches losgekoppeld en wederom aangesloten. Hieruit bleek dat het loskoppelen van sommige verbindingen een time-out gaf van 1 sec. Dit zijn de routes die gekozen zijn als route naar de destination. Deze test is in een korter tijdsbestek uitgevoerd omdat, de verbindingen tussen de core geen time-out opleverden en hierdoor er niet gewacht moest worden voordat de verbindingen weer was aangesloten.	
	Dit zorgt bij Server1 voor een availability van: (1/3258)*100 = 99,969%
	Dit zorgt bij Server2 voor een availability van: (1/3258)*100 = 99,969%

Maintainability[6]

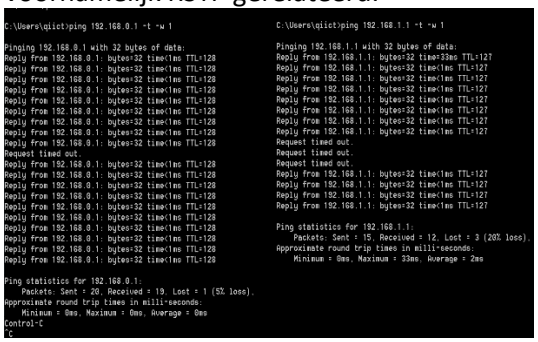
Met Manageability wordt het onderhouden van het netwerk zonder dat de werking daar effect van ondervind bedoeld. Hier wordt voornamelijk het vervangen van een switch bedoeld. Er zal getest worden of het netwerk enige hinder ondervindt als er een switch vervangen moet worden.

Testcase M6	Maintainability
Beschrijving	Om de Maintainability te testen zullen verschillende componenten tussen de van het netwerk worden losgekoppeld en later weer worden aangesloten. Hierna zal gecontroleerd worden of het netwerk hier effect van ondervindt in de vorm van downtime.
Voorwaarden	• Netwerk ontworpen aan de hand van eerder genoemd ontwerp. • Protocollen geconfigureerd zoals bij het ontwerp is aangegeven • Testcase M0 is geslaagd
Teststappen	
1	Vanaf de PC worden ICMP-berichten gestuurd naar beide servers met een wait van 1 sec
2	Een willekeurig component wordt losgekoppeld van de netstroom en na enige tijd weer aangesloten.
3	Er wordt gecontroleerd of de ICMP-berichten tussen de PCs nog verzonden worden. Ook wordt er gecontroleerd of dat de latency verhoogd is.
Behaald resultaat huidige situatie	

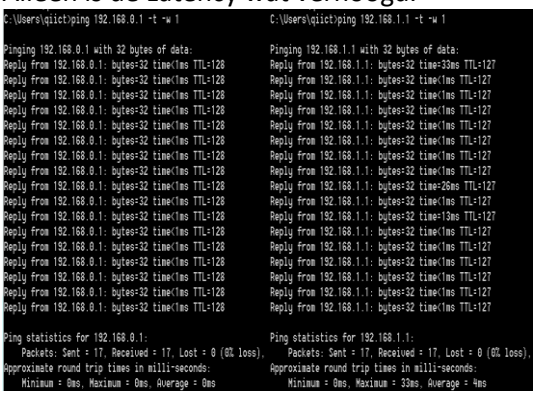
Bij het vervangen van de Master switch van VC1 zal er geen downtime ondervonden worden.



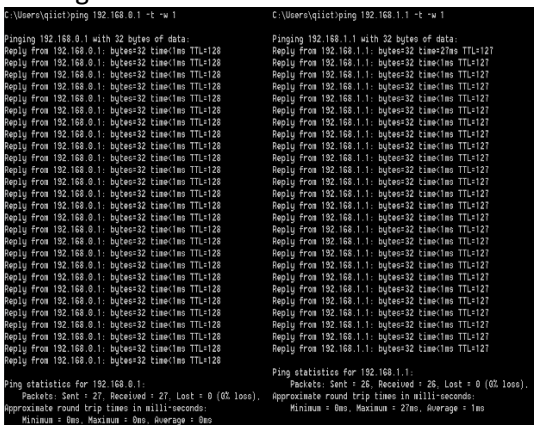
Bij het vervangen van de Slave switch van VC1 wordt enige downtime ondervonden, dit is voornamelijk RSTP gerelateerd.



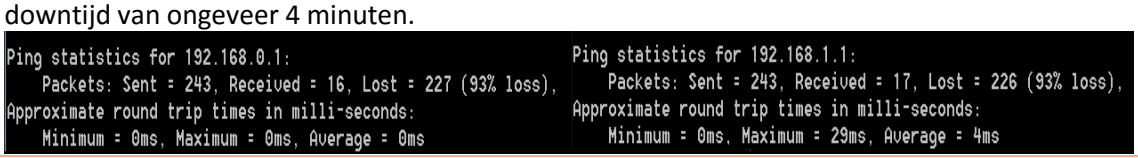
Bij het vervangen van de Master switch van VC2 zal er geen downtime ondervonden worden. Alleen is de Latency wat verhoogd.



Bij het vervangen van de Slave switch van VC2 zal er geen downtime ondervonden worden.

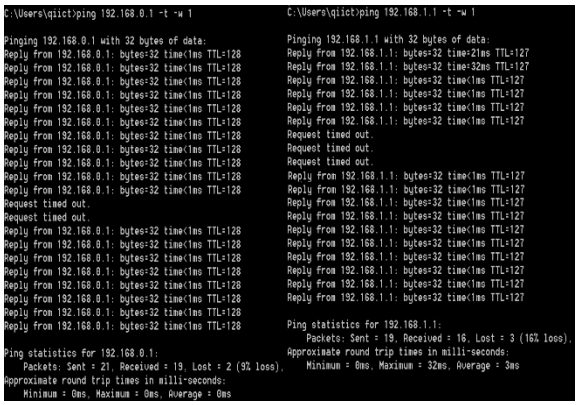


Bij het vervangen van een Acces Switch moet er rekening worden gehouden met een minimale downtijd van ongeveer 4 minuten.

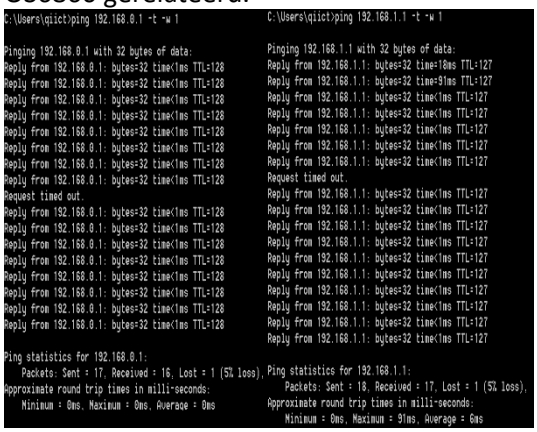


Behaald resultaat Proof of Concept

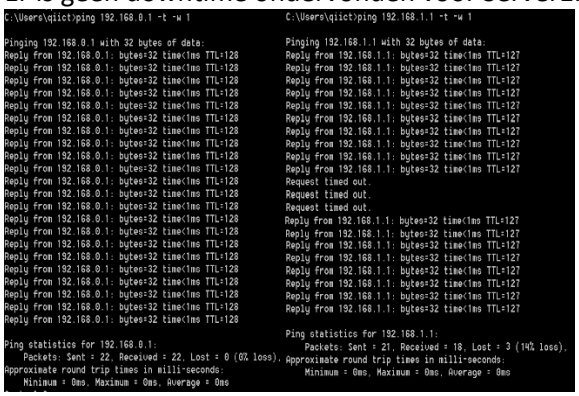
Bij het vervangen van de Master switch van VC1 zal er een downtime ondervonden worden van ongeveer 3 seconden.



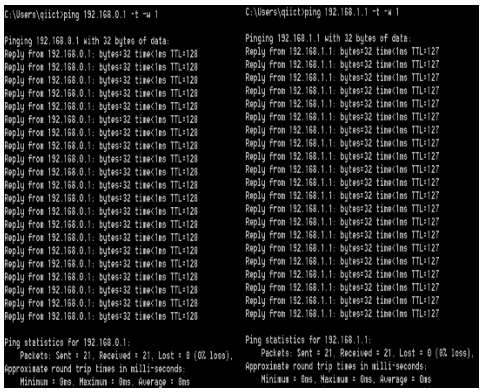
Bij het vervangen van de Slave switch van VC1 wordt enige downtime ondervonden, dit is voornamelijk aan de verbindingen met de OS6860 gerelateerd.



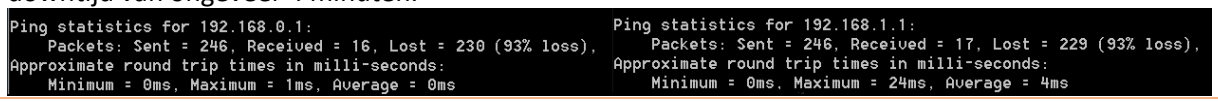
Bij het vervangen van de Master switch van VC2 wordt alleen bij Server2 downtime ondervonden. Er is geen downtime ondervonden voor Server1.



Bij het vervangen van de Slave switch van VC2 zal er geen downtime ondervonden worden.



Bij het vervangen van een Acces Switch moet er rekening worden gehouden met een minimale downtijd van ongeveer 4 minuten.



7. Conclusie resultaten

In het komende hoofdstuk zullen de resultaten van de testcases kort samengevat worden. De resultaten van de testcases om de protocolwerking te verifiëren zullen hier gegeven worden. Hierbij is een verwachting gesteld bij elke testcase en werd er gecontroleerd of deze verwachting is uitgekomen of niet. Als iets afwijkt van de verwachting zal deze afwijking bij de opmerkingen genoteerd worden.

Bij de metingen zullen de waardes van de metingen gegeven worden. Hierbij worden de waardes van de oude en de nieuwe situatie van elkaar gescheiden. Deze waardes zijn op deze manier te vergelijken om een uiteindelijke conclusie te kunnen trekken of één van de twee situaties een wenselijkere werking heeft.

7.1 Resultaten Protocol werking

Resultaten van Virtual Chassis

Test case	Resultaat	Opmerkingen
Testcase P1	✓	
Testcase P2	✓	Het switchen van Slave naar Master duurt langer als dat in de literatuur staat aangegeven. Volgens de literatuur zou de gebruiker geen onderbreking ondervinden, echter is er een downtime van ongeveer 3 seconden
Testcase P3	✓	

Resultaten van VRRP

Test case	Resultaat	Opmerkingen
Testcase P4	✓	
Testcase P5	✓	
Testcase P6	✓	

Resultaten van LACP

Test case	Resultaat	Opmerkingen
Testcase P7	✓	
Testcase P8	✓	

Resultaten van RSTP

Test case	Resultaat	Opmerkingen
Testcase P9	✓	
Testcase P10	✓	
Testcase P11	✓	

Resultaten van SPB

Testcase	Resultaat	Opmerking
Testcase P9	✓	
Testcase P10	✓	
Testcase P11	✓	

7.2 Resultaten metingen

7.2.1 Huidige situatie

Test case	Omschrijving Test case	Resultaat
Testcase M0	Werking situatie	✓
Testcase M1	Performance bandbreedte	Server1: 817 Mbps Server2: 693 Mbps
Testcase M2	Performance latency	Server1: <1 ms Server2: <1 ms
Testcase M3	Scalability	Ja
Testcase M4	Reliability	Server1: 99,997% Server2: 100%
Testcase M5	Availability	Server1: 99,918% Server2: 99,890%
Testcase M6	Maintainability	VC_Master: ±3 seconden VC_Slave: ±1 seconden Access switch: minimaal 4 minuten

7.2.2 Proof of Concept

Test case	Omschrijving Test case	Resultaat
Testcase M0	Werking situatie	✓
Testcase M1	Performance bandbreedte	Server1: 920 Mbps Server2: 700 Mbps
Testcase M2	Performance latency	Server1: <1 ms Server2: <1 ms
Testcase M3	Scalability	Ja; maar er zijn aanpassingen nodig in het netwerk
Testcase M4	Reliability	Server1: 99,999% Server2: 100%
Testcase M5	Availability	Server1: 99,969% Server2:99,969 %
Testcase M6	Maintainability	VC_Master: ±3 seconden VC_Slave: ±1 seconden Access switch: minimaal 4 minuten

Literatuurlijst

[1] Alcatel-Lucent. (jaar onbekend) *"Configuring Virtual Chassis"* http://enterprise.alcatel-lucent.com/assets/documents/userguides/OmniSwitch-AOS-Release-7-Switch-Management-Guide/!SSL!/Multiscreen_HTML5/desktop/os_sw/s_vc/s_vc.htm (geraadpleegd 1 juli 2016)

[2] Alcatel-Lucent. (2015, maart) *"OmniSwitch AOS Release 7 Network CLI Reference Guide".* (geraadpleegd 1 juli 2016)

[3] Alcatel-Lucent. (2013, juni) *"OmniSwitch 6250/6450 Network Configuration Guide".*

[4] Alcatel-Lucent. (2014, mei) *"OmniSwitch AOS Release 8 Network Configuration Guide".*

[5] Alcatel-Lucent. (2015, august) *"OmniSwitch AOS Release 7 Data Center Switching Guide".*

[6] Cade, M., & Roberts, S. (2002, augustus) "*What Is System Architecture?*" http://www.informit.com/articles/article.aspx?p=29030&seqNum=5 (geraadpleegd 1 juli 2016)

Bijlage G

Migratieplan

LIVING UPTIME

Migratieplan

Opdrachtgever: Qi ict bv.
Begeleider: Hans Suttorp
Afstudeerder: Frank van Eijk
Opleiding: Technische Informatica, HHS Delft
Datum: 03-10-2016
Versie: 1.0

Versiebeheer

Versie	Datum	Opmerking
0.1	19-08-2016	Eerste versie
1.0	30-9-2016	Aanpassingen doorgevoerd na feedback van dhr. Hans Suttorp Opmaak consistent gemaakt

Inhoudsopgave

1. Inleiding

Om het onderzoek te ondersteunen zal er een Proof of Concept worden gebouwd op basis van het huidige netwerk. Deze huidige situatie is gebaseerd op één van de vele klanten waar Qi ict bv. haar diensten levert.

Om het onderzoek te ondersteunen zal de migratie van de huidige situatie naar het Proof of Concept uitgevoerd worden. In dit document zullen de onderdelen die betrekking hebben tot de migratie uitgelegd worden. Daarnaast zal elk onderdeel voorwaarden hebben voordat deze gemigreerd kunnen worden in het netwerk. Zodra ook de voorwaarden van de onderdelen bekend zijn zullen de migratiestappen uitgevoerd worden om de migratie van stap 0 (huidige situatie) naar het eindpunt (Proof of Concept) te realiseren. Als laatste zal de conclusie getrokken worden of de migratie geslaagd is.

2. Migratie onderdelen

Als eerste moet er duidelijk worden wat er gewijzigd gaat worden tijdens de migratie. Het onderzoek is gericht op de vervanging van een STP-variant door een TRILL-variant. In deze situatie gaat het om de migratie van RSTP naar SPB. De configuratie voor het realiseren van het Proof of Concept verandert in meerdere opzichten op die van de huidige situatie; Uit eerder onderzoek (zie het experimenteel onderzoeksrapport) is gebleken dat het binnen het SPB netwerk niet gerouteerd kan worden en hierdoor geen VRRP gebruikt kan worden. Hierdoor wordt server2 onbereikbaar in de nieuwe situatie.. Hierdoor is Server2 niet bereikbaar. Dit zou opgelost kunnen worden door het gebruik van een router. Echter is één van de voorwaarden aan de migratie dat de apparatuur niet veranderd mag worden. Dit wordt opgelost doordat je de access switches laat routeren en als default gateway laat functioneren voor de endpoints.

3. Voorwaarden aan de migratie

Voordat er gemigreerd gaat worden moet er wel duidelijk zijn wat de voorwaarden zijn voor de migratie. Deze voorwaarden zijn vooraf opgesteld.

Voorwaarde 1: *"Het netwerk moet dezelfde functionaliteiten behouden"*
Hierbij zal de PC aan het eind van de migratie nog steeds beide servers kunnen bereiken.

Voorwaarde 2: *"RSTP wordt vervangen door SPB"*
RSTP zal tijdens de migratie uitgeschakeld worden op de switches die SPB ondersteunen. Hierbij wordt eerst SPB geconfigureerd voordat RSTP wordt disabled.

Voorwaarde 3: *"De apparatuur zal niet gewijzigd worden"*
Het netwerk zal op deze manier fysiek gezien hetzelfde blijven.

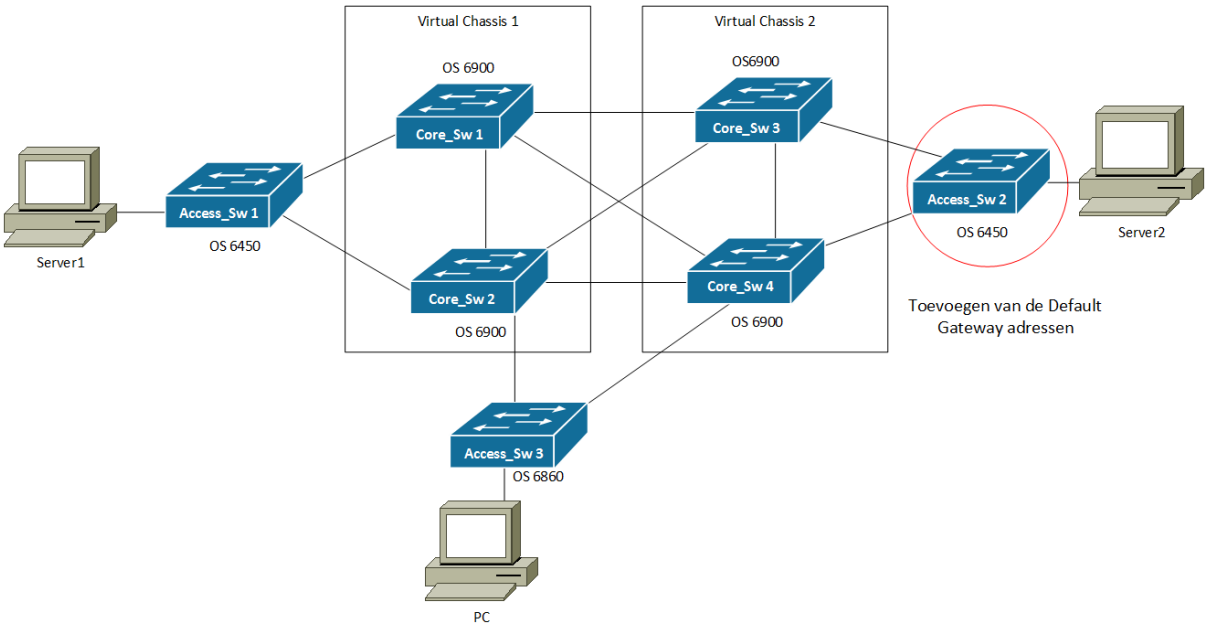
4. Migratiestappen

Nu de onderdelen van de migratie en de voorwaarden vastgesteld staan kan er begonnen worden met de migratie. Hierbij zal de huidige situatie als beginpunt dienen en het Proof of Concept is de gewenste situatie ofwel het eindpunt.

Stap 1

"*Default Gateway adressen op Access_Sw2 instellen.*" Om er voor te zorgen dat er toch nog een default gateway is voor het netwerk zal deze buiten het SPB netwerk ingesteld moeten worden. Hierbij geldt dat in deze situatie alleen op de Access Switches die zich voor de servers begeven. Er is gekozen om de Default Gateways op Access_Sw2 te configureren, omdat als deze switch uitvalt wel Server1 nog te bereiken is. Als de Default Gateways op Access_Sw1 had gestaan, zal bij uitval van de switch geen van beide servers meer te bereiken zijn. Ook zal het verkeer met een omweg switchen. Hier wordt op de switch de volgende configuratie uitgevoerd.

Access_Sw2 (OS6450-48)
***ip interface** DFGW1 **address** 192.168.0.100/24 **vlan** 1*
***ip interface** DFGW2 **address** 192.168.1.100/24 **vlan** 1*



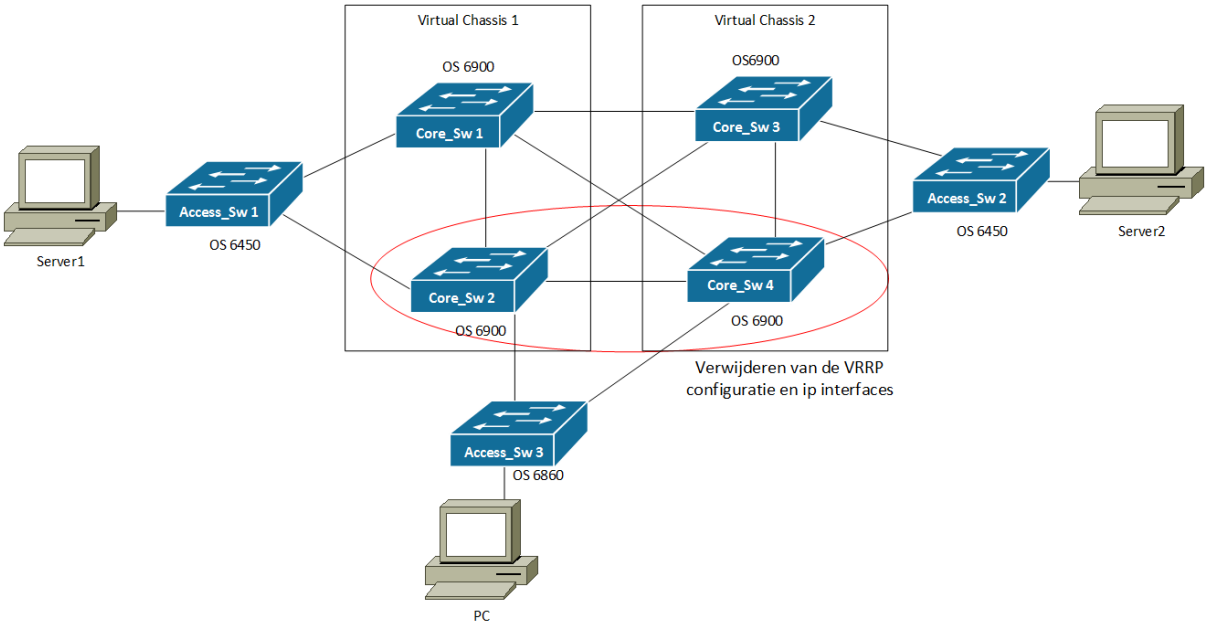
Stap 2

"Het verwijderen van VRRP uit het netwerk." VRRP werkt niet binnen de SPB core en zal daarom ook niet meer van toepassing zijn voor het Proof of Concept. SPB kijkt namelijk niet naar het vlan of IP-adres dat bij het frame binnenkomt. SPB kijkt alleen naar de ISID van het frame en zal deze dan via het bijbehorende BVLAN rondsturen door het netwerk. Het verwijderen van VRRP uit het netwerk wordt gedaan door de volgende configuratie:

VC1	*VC2*
***vrrp** 1 1 **admin-state** disable*	***vrrp** 1 1 **admin-state** disable*
***vrrp** 2 1 **admin-state** disable*	***vrrp** 2 1 **admin-state** disable*
***no vrrp** 1 1*	***no vrrp** 1 1*
***no vrrp** 2 1*	***no vrrp** 2 1*

Ook zullen de interfaces van de switch verwijderd worden:

VC1	*VC2*
***no ip interface** vrrp*	**no ip interface** vrrp
***no ip interface** vrrp2*	**no ip interface** vrrp2

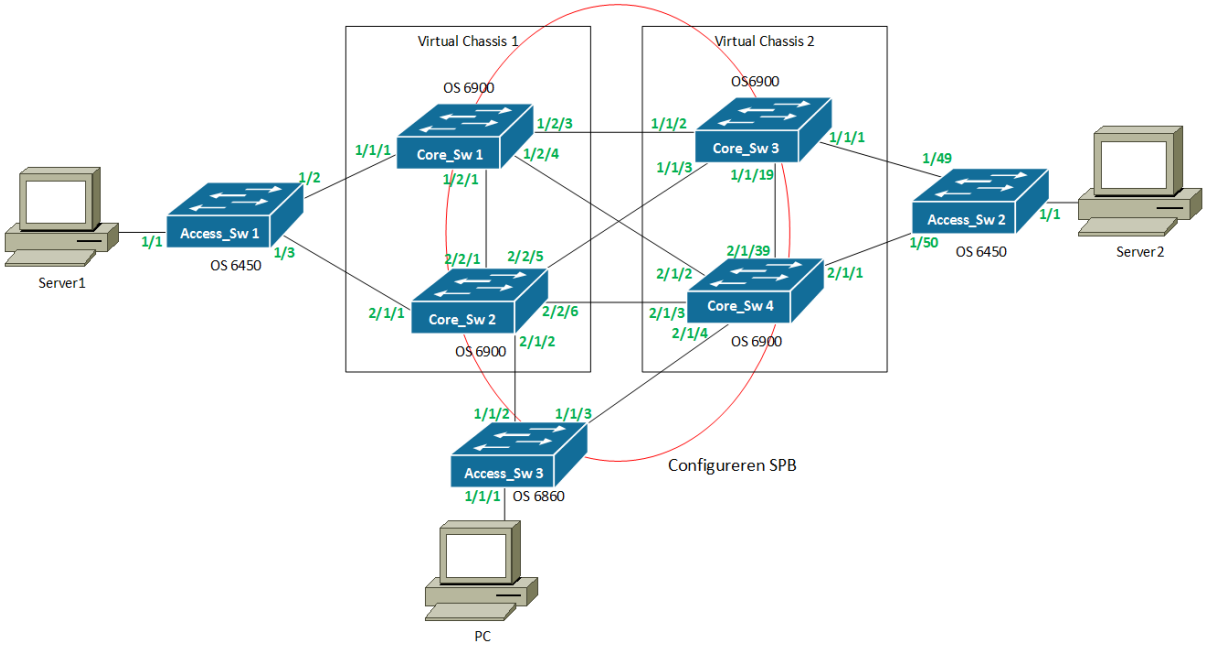


Stap 3

"SPB zal geconfigureerd worden op de switches die de SPB-core vormen"

Omdat RSTP en SPB compatible met elkaar zijn kan SPB geconfigureerd worden terwijl RSTP nog gebruikt wordt. Allereerst moet er een Backbone VLAN aangemaakt worden om het SPB verkeer over te laten switchen. Als dat gedaan is zullen de juiste poorten geconfigureerd worden voor SPB. Dit zijn de poorten die verbonden zijn met de andere switches die SPB ondersteunen. Dit zorgt voor de volgende configuratie op de switches:

VC1	*VC2*	*Access_Sw3 (OS6860)*
***spb bvlan** 4001*	***spb bvlan** 4001*	***spb bvlan** 4001*
***spb isis control-bvlan** 4001*	***spb isis control-bvlan** 4001*	***spb isis control-bvlan** 4001*
***spb isis interface port** 1/2/3-4*	***spb isis interface port** 1/1/2-3*	***spb isis interface port** 1/1/2-3*
***spb isis interface port** 2/2/5-6*	***spb isis interface port** 2/1/2-4*	***spb isis admin-state** enable*
***spb isis interface port** 2/1/3*	***spb isis admin-state** enable*	
spb isis admin-state enable		

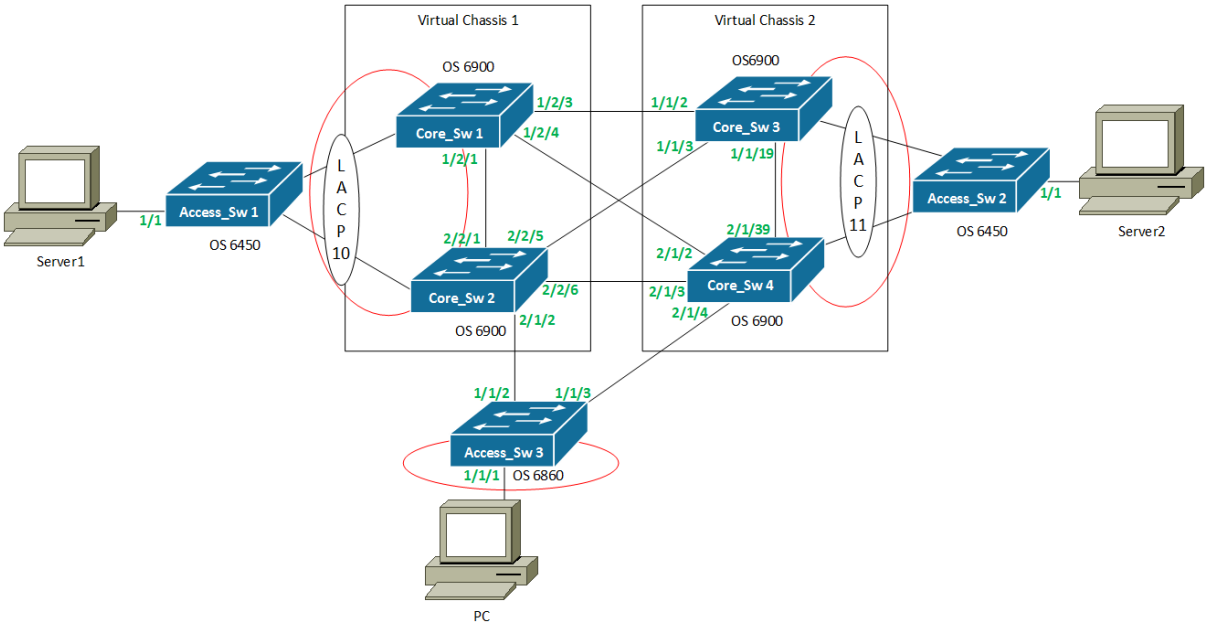


Stap 4

"Service aanmaken om ervoor te zorgen dat het verkeer het SPB netwerk in en uit kan."

Het SPB netwerk kijkt alleen naar de ISID van een frame. Het ISID zorgt ervoor dat het verkeer bij de juiste ontvanger terecht komt. Hierbij zou het gebruik van twee ISID ervoor kunnen zorgen dat het verkeer gescheiden blijft. Dit ISID moet echter wel aan een frame worden toegevoegd voordat deze door het SPB netwerk kan switchen. Hiervoor wordt een service aangemaakt met poorten waarop het verkeer binnenkomt. Dit is volgens de volgende configuratie:

VC1	*VC2*	*Access_Sw3 (OS6860)*
Service access linkagg *10*	***Service access linkagg*** *11*	***Service access port*** *1/1/1*
Service *1* ***spb isid*** *500* ***bvlan*** *4001* ***admin-state*** *enable*	***Service*** *1* ***spb isid*** *500* ***bvlan*** *4001* ***admin-state*** *enable*	***Service*** *1* ***spb isid*** *500* ***bvlan*** *4001* ***admin-state*** *enable*
Service *1* ***sap linkagg*** *10:all* ***admin-state*** *enable*	***Service*** *1* ***sap linkagg*** *11:all* ***admin-state*** *enable*	***Service*** *1* ***sap port*** *1/1/1:all* ***admin-state*** *enable*

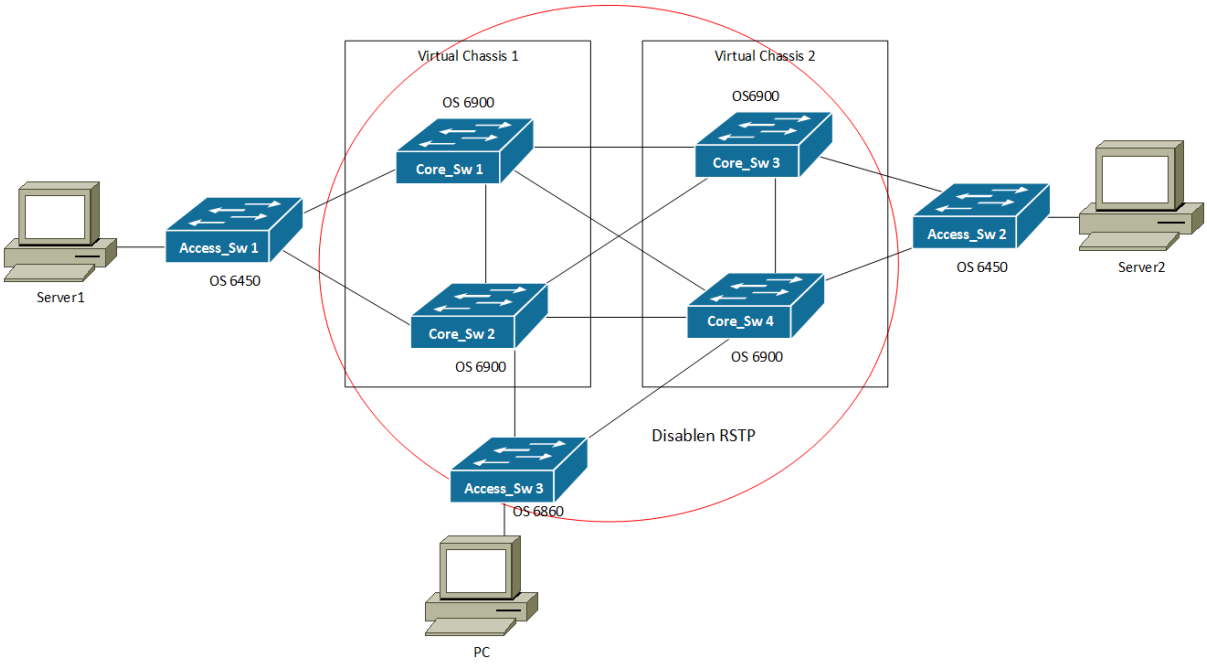


Stap 5

"RSTP zal disabled worden op de switches die SPB gebruiken."

Nu dat alles voor SPB geconfigureerd is zal RSTP op de switches die het SPB netwerk vormen disabled worden. Hierbij gaat het om de switches VC1, VC2 en op de Access_Sw3 (OS6860). Dit zorgt voor de volgende configuratiestap:

VC1	*VC2*	*Access_Sw3 (OS6860)*
***spantree vlan** 1 **admin-state** disable*	***spantree vlan** 1 **admin-state** disable*	***spantree vlan** 1 **admin-state** disable*



5. Resultaat migratie

Om te kunnen concluderen of er voldaan is aan de migratie, moet er aan de vooraf opgestelde voorwaarden zijn voldaan. Dit waren de volgende voorwaarden:

Voorwaarde 1: *"Het netwerk moet dezelfde functionaliteiten behouden"*
Voldaan: Het is nog steeds mogelijk om met de PC de beide servers te bereiken. Dit is getest door middel van het sturen van ICMP-berichten van de PC naar beide servers. . Zie hiervoor ook onderstaande afbeelding:

```
C:\Users\qiict>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\qiict>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Voorwaarde 2: *"RSTP wordt vervangen door SPB"*
Voldaan: Op de switches die SPB ondersteunen kan de configuratie geopend worden en aangetoond worden dat SPB enabled is en dan RSTP disabled is. Ook is het met Wireshark te bewijzen dat er SPB headers zijn toegevoegd aan het Ethernet frame.

```
-> show spb isis info
SPB ISIS Bridge Info:
  System Id             = e8e7.325a.7fb3,
  System Hostname       = VC2,
  SPSourceID            = 0a-7f-b3,
  SPBM System Mode      = auto,
  BridgePriority        = 32768 (0x8000),
  MT ID                 = 0,
  Control BVLAN         = 4001,
  Area Address          = 0
                        0.0.0,
  Level Capability      = L1,
  Admin State           = UP,
  LSDB Overload         = Disabled,
  Last Enabled          = Thu Sep 29 07:42:06 2016,
  Last SPF              = Thu Sep 29 07:54:05 2016,
  SPF Wait              = Max: 1000 ms  Initial: 100 ms  Second: 300 ms,
  LSP Lifetime          = 1200,
  LSP Wait              = Max: 1000 ms, Initial: 0 ms, Second: 300 ms,
  Graceful Restart      = Disabled,
  GR helper-mode        = Disabled,
  # of L1 LSPs          = 3
  Control Address       = 01:80:c2:00:00:14 (AllL1)

-> show spantree
  Spanning Tree Path Cost Mode : AUTO
 Vlan STP Status Protocol Priority
-----+----------+--------+--------------
    1     OFF       RSTP    8192 (0x2000)
 4001     OFF       RSTP   32768 (0x8000)
 4094     OFF       RSTP   32768 (0x8000)
```

```
    48 14.2265760 192.168.0.1      192.168.0.3      ICMP     92 Echo (ping) request  id=0x0001, seq=22/5632, ttl=128 (no response found!)
    49 14.2267150 192.168.0.3      192.168.0.1      ICMP     92 Echo (ping) reply    id=0x0001, seq=22/5632, ttl=128
    50 15.2423530 192.168.0.1      192.168.0.3      ICMP     92 Echo (ping) request  id=0x0001, seq=23/5888, ttl=128 (no response found!)

⊞ Frame 48: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
⊞ Ethernet II, Src: Alcatel-_e6:a0:91 (e8:e7:32:e6:a0:91), Dst: Alcatel-_fa:89:93 (e8:e7:32:fa:89:93)
⊞ IEEE 802.1ah, I-SID: 500, C-Src: Dell_c1:af:6e (a4:ba:db:c1:af:6e), C-Dst: Dell_78:0a:dd (00:21:70:78:0a:dd)
⊞ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.3 (192.168.0.3)
⊞ Internet Control Message Protocol
```

Voorwaarde 3: *"De apparatuur zal niet gewijzigd worden"*
Voldaan: Want er is geen apparatuur vervangen tijdens het migreren. De enige wijziging die tijdens de migratie is uitgevoerd is het wijzigen van de configuratie.

Door de bovenstaande resultaten op de voorwaarden van de migratie kan er geconcludeerd worden dat: Het migreren van RSTP naar SPB mogelijk is. Echter is er wel enige downtime ondervonden bij het verwijderen van VRRP en het in gebruik nemen van de SAP poorten.

Bijlage H

Experimenteel Onderzoeksrapport

Experimenteel onderzoeksrapport

Opdrachtgever: Qi ict bv.
Begeleider: Hans Suttorp
Afstudeerder: Frank van Eijk
Opleiding: Technische Informatica, HHS Delft
Datum: 03-10-2016
Versie: 1.0

Versiebeheer

Versie	Datum	Opmerking
0.1	15-7-2016	Eerste versie
1.0	30-9-2016	Aanpassingen doorgevoerd na feedback van Dhr. Suttorp Opmaak consistent gemaakt.

Gerelateerde documenten

Ref	Auteur	Titel
C1	Frank van Eijk	Literatuur onderzoeksrapport
C2	Frank van Eijk	Testdocument
C3	Frank van Eijk	Migratieplan

Inhoudsopgave

Tabellen

Figuren

1. Inleiding

Het onderzoek is opgedeeld worden in twee aparte onderzoeken, een literatuuronderzoek en een experimenteel onderzoek. Uit beide onderzoeken komt een resultaat en aan de hand van deze resultaten zal een advies gegeven worden of het uit faseren van STP in switched-core netwerken gewenst is.

Om de hoofdvraag te kunnen beantwoorden, zijn er meerdere deelvragen opgesteld. In dit rapport zullen alleen de deelvragen die aan het experimenteel onderzoek zijn gesteld behandeld worden. Voor de beantwoording van de literatuur deelvragen, wordt verwezen naar het Literatuur onderzoeksrapport.

In het volgende hoofdstuk zal de aanleiding tot het onderzoek worden behandeld. Daarna zal het kennisgebied van de afstudeerder worden aangegeven. Als dit is uitgelegd volgt de probleemstelling waarin de deelvragen en eventuele sub-vragen worden uitgelegd en waarom deze vragen relevant zijn voor het onderzoek. Nadat de vragen duidelijk zijn zullen deze in de daarop volgende hoofdstukken behandeld worden. Uiteindelijk zal er een conclusie uit het onderzoek volgen.

2. Aanleiding Experimenteel onderzoek

Qi ict bv. gebruikt op dit moment het Spanning Tree Protocol(STP) voor het gebruik van redundantie in hun switched netwerken, deze keuze is gemaakt toen STP de meest voordehand liggende keuze was, maar is dit tegenwoordig nog steeds de meest logische keuze? De hoofdreden voor dit onderzoek is dat Qi over weinig kennis beschikt wat betreft de mogelijkheden van alternatieven zoals TRILL.

Tijdens het literatuuronderzoek is al enige kennis opgedaan over de werking van de protocollen die in de huidige situatie gebruikt worden. De protocollen die op het huidige netwerk draaien zijn RSTP, VRRP, Virtual Chassis en LACP. Bij de migratie zal RSTP vervangen worden door SPB. Om de werking van deze protocollen te controleren wordt er een experimenteel onderzoek gedaan.

Uiteindelijk kan aan de hand van de resultaten van het experimenteel onderzoek geconcludeerd worden of de gevonden literatuur daadwerkelijk correct is. Ook zal de hoofdvraag door middel van het resultaat van het experimenteel onderzoek beantwoordt worden.

3. Kennisgebied

Het kennisgebied dat betrekking heeft tot het experimenteel onderzoek zijn de protocollen die werken in de huidige situatie of de protocollen die in de nieuwe situatie komen te werken. Dit zijn de volgende protocollen: het Rapid Spanning Tree Protocol (RSTP), Shortest Path Bridging(SPB), Virtual Chassis, Virtual Router Redundancy Protocol (VRRP) en het Link Aggregation Control Protocol(LACP). Hiernaast wordt er ook een switched-core netwerk aangeleverd door Qi ict bv. waarnaar enig onderzoek gedaan moet worden over wat de verwachtingen zijn van het netwerk.

4. Probleemstelling

In dit hoofdstuk zal de hoofdvraag en de deelvragen worden beschreven, deze vragen zullen in de loop van de experimentele onderzoeksfase onderzocht en beantwoordt worden.

4.1 Hoofdvraag

“Is het met TRILL mogelijk om STP uit een door Qi ict bv. gebruikt switched-core netwerk te faseren?”

4.2 Deelvragen

In deze paragraaf zullen de deelvragen en de eventuele sub-vragen die tijdens het experimentele onderzoek beantwoordt worden beschreven.

Deelvraag 5: “Hoe werkt de huidige situatie?”
Reden: Voordat STP uit het huidige netwerk kan worden gefaseerd, moet eerst duidelijk zijn wat de functionaliteiten zijn van de huidige situatie. Zonder beginsituatie is het ook niet mogelijk om de vergelijking met de nieuwe situatie aan het eind van het onderzoek uit te voeren.

Sub-vraag 5.1: “Werken de gebruikte protocollen zoals uit de literatuur naar voren kwam?”
Reden: Hierbij wordt de gevonden literatuur vergeleken met de werkelijkheid op het netwerk. Hierbij kan de literatuur bevestigd worden of ontkracht. Hierbij kan het geval zijn dat de literatuur een andere werking van een protocol weergeeft dan wat het protocol op het netwerk daadwerkelijk doet. De nadruk ligt hierbij op RSTP.

Sub-vraag 5.2: “Wat zijn de waardes van het huidige netwerk?”
Reden: Hierbij wordt een Nulmeting uitgevoerd. Bij een nulmeting worden verschillende waardes van het huidige netwerk achterhaald, om aan het eind van het onderzoek de waardes van het Proof of Concept en de huidige situatie met elkaar te kunnen vergelijken. Voorbeelden van deze waardes zijn: Latency, Reliability en Availability.

Deelvraag 6: “Hoe werkt de nieuwe situatie?”
Reden: Voordat er gemigreerd kan worden naar de nieuwe situatie, moet de nieuwe situatie wel bekend zijn. Op deze manier kan ook de werking van de protocollen op de nieuwe situatie worden getest.

Sub-vraag 6.1: “Werken de gebruikte protocollen zoals uit de literatuur naar voren kwam?”
Reden: Hierbij wordt de gevonden literatuur vergeleken met de werkelijkheid op het netwerk. Hierbij kan de literatuur bevestigd worden of ontkracht. In de nieuwe situatie gaat het vooral om de werking van SPB. De andere protocollen zijn al getest.

Sub-vraag 6.2: “Wat zijn de waardes van het nieuwe netwerk?”
Reden: Hierbij worden verschillende waardes van het nieuwe netwerk achterhaald, om aan het eind van het onderzoek de waardes van de beide situaties met elkaar te kunnen vergelijken. Voorbeelden van deze waardes zijn: Latency, Reliability en Availability.

Deelvraag 7: "Werkt de nieuwe situatie beter als de oude?"
Reden: Om een advies te kunnen geven of het wenselijk is om STP uit de huidige netwerk te faseren, moet wel duidelijk zijn of de nieuwe situatie beter werkt als de oude.

> **Sub-vraag 7.1: "In welk opzicht verschilt de nieuwe situatie met de oude situatie?"**
> *Reden:* Hierbij wordt er gekeken welke verschillen er zijn bij de metingen die bij de oude (huidige) situatie en bij de nieuwe situatie zijn uitgevoerd. Uit deze metingen zullen verschillen komen, echter is het zo dat sommige waardes ook nog hetzelfde kunnen zijn. De gebieden waarnaar gekeken wordt zijn: Scalability, Availability, Manageability, Maintainability en Performance.

Deelvraag 8: "Hoe wordt de oude situatie naar de nieuwe situatie gemigreerd?"
Reden: Om van de oude situatie naar de nieuwe situatie te migreren moeten er een aantal handelingen worden uitgevoerd. Het is noodzakelijk om te weten hoe de migratie gedaan moet worden. Deze stappen zorgen ervoor dat de migratie op een efficiënte manier kan worden uitgevoerd.

> **Sub-vraag 8.1: "Welke stappen moeten hiervoor worden genomen?"**
> *Reden:* Hierbij zijn de stappen van groot belang, als er niet stapsgewijs gewerkt wordt kan het zijn dat er geen overzicht meer is in de migratie. Hierbij is het mogelijk dat er dan iets ontbreekt of niet op de juiste instellingen staat.

> **Sub-vraag 8.2: "Welke voorwaarden zitten er aan de migratie stappen?"**
> *Reden:* Hierbij kan gedacht worden aan de downtijd die het netwerk maximaal mag hebben. Ook moeten de risico's worden gedefinieerd die aanwezig kunnen zijn tijdens het migreren van het netwerk.

5. Werking huidige situatie

In dit hoofdstuk wordt de werking van de huidige situatie weer gegeven. Hierbij wordt de deelvraag: *"Hoe werkt de huidige situatie?"* behandeld. De huidige situatie dient als 'Beginpunt' van de migratie. Door de functionaliteiten van de huidige situatie te weten wordt ook duidelijk welke functionaliteiten er aanwezig moeten zijn op de nieuwe situatie. Bij deze deelvraag zijn nog twee sub-vragen gesteld die hieronder behandeld zullen worden.

5.1 Werking protocollen

Hieronder zal de sub-vraag: *"Werken de gebruikte protocollen zoals uit de literatuur naar voren kwam?"* Deze sub-vraag zal de gevonden literatuur bevestigen of weerleggen. Bij het testen van de werking van de protocollen is er gebruik gemaakt worden van aparte deelontwerpen en van testcases die per protocol zullen verschillen.

In dit hoofdstuk zullen van de protocollen Virtual Chassis, VRRP en LACP alleen de resultaten gegeven worden met eventuele opmerkingen. De testcases worden in het Testdocument besproken. Het Testdocument is te vinden in de bijlagen. Dit wordt gedaan omdat, de werking van de protocollen niet direct effect hebben op het onderzoek. Echter zijn deze wel van belang om ervoor te weten dat de werking van het netwerk overeenkomt met de verwachting.

Tabel 1 Resultaten Virtual Chassis tests

Test case	Resultaat	Opmerkingen
Is de Virtual Chassis correct geconfigureerd?	✓	
Neemt de Slave switch de functionaliteiten over van de Master als deze uitvalt?	✓	Het switchen van Slave naar Master duurt langer als dat in de literatuur staat aangegeven. Volgens de literatuur zou de gebruiker geen onderbreking ondervinden, echter is er een downtime van ongeveer 3 seconden
Blijft het netwerk actief bij het uitvallen van de Slave?	✓	

Tabel 2 Resultaten VRRP tests

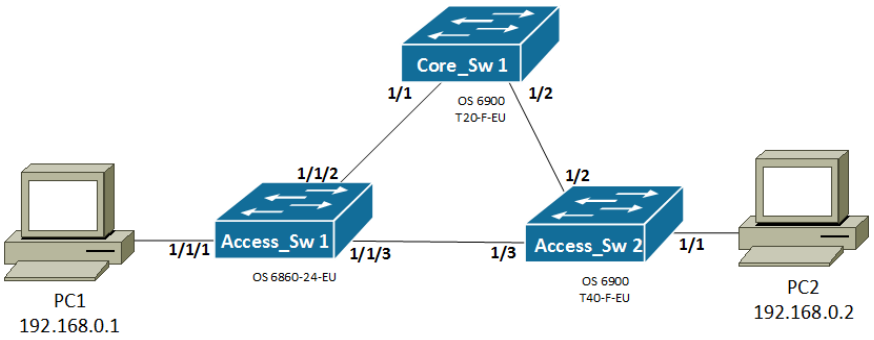
Test case	Resultaat	Opmerkingen
Is VRRP correct geconfigureerd?	✓	
Neemt de Back-up switch de werkzaamheden van de Active switch over?	✓	
Blijft het netwerk actief bij het uitvallen van de Back-up?	✓	

Tabel 3 Resultaten LACP tests

Test case	Resultaat	Opmerkingen
Is LACP correct geconfigureerd?	✓	
Heeft het uitvallen van een verbinding binnen een bundel effect op het netwerk?	✓	

RSTP heeft echter meer betrekking tot het onderzoek omdat, er gekeken moet worden of een variant van TRILL (SPB), RSTP uit het netwerk kan faseren. Hierdoor zal de werking van RSTP wel uitgebreid geverifieerd worden.

Uit het literatuuronderzoek kwam naar voren dat STP gebruikt wordt om loops in een netwerk te voorkomen. Dit wordt gedaan door het blokkeren van verbindingen. Hierbij is het geval dat als een verbinding uitvalt STP ervoor zal zorgen dat de geblokkeerde verbinding weer gebruikt kan worden en zo het netwerk weer data kan versturen. Hieronder zijn de testcases weergegeven die bij horen bij het testen van de werking van het Rapid Spanning Tree Protocol. Hiervoor wordt de volgende testopstelling gebruikt:



Figuur 1 Ontwerp RSTP test

Testcase P9: "Staat RSTP als default ingesteld en is de juiste switch de Rootswitch"
Doel: Uit de literatuur kwam naar voren dat RSTP als default ingesteld staat. Als dit daadwerkelijk het geval is hoeft alleen de prioriteit aangepast te worden om de juiste Root switch te realiseren.

Werkwijze: Op alle switches zal het commando ***show spantree vlan 1*** uitgevoerd om te controleren wat de Spanning Tree instellingen zijn op de switch. Ook wordt er gecontroleerd of de configuratie voor de prioriteit correct is doorgevoerd.

Verwachte resultaat: De OS6900-T20 zal op het commando ***show spantree vlan 1*** aangeven dat deze switch de Root is. De andere switches zullen aangeven welke port het beste is om de Rootswitch te kunnen bereiken.

Behaalde resultaat: Onderstaand zijn een drietal afbeeldingen weergegeven die de uitkomst geven van het commando: ***show spantree vlan 1.*** Uit deze afbeeldingen blijkt dat op alle switches RSTP staat ingesteld. Ook is duidelijk te zien dat alle prioriteiten op de juiste switches staan ingesteld. En hiermee de Rootswitch ook daadwerkelijk de OS6900-T20 is.

OS6860

```
-> show spantree vlan 1
Spanning Tree Parameters for Vlan 1
  Spanning Tree Status :                  ON,
  Protocol             :        IEEE Rapid STP,
  mode                 : Per VLAN (1 STP per Vlan),
  Priority             :         12288 (0x3000),
  Bridge ID            :    3000-e8:e7:32:fa:89:93,
  Designated Root      :    1000-e8:e7:32:e6:a0:91,
  Cost to Root Bridge  :                        4,
  Root Port            :                   1/1/2,
  Next Best Root Cost  :                        8,
  Next Best Root Port  :                   1/1/3,
  TxHoldCount          :                        3,
  Topology Changes     :                        9,
  Topology age         : 2 days and 16:50:54,
    Current Parameters (seconds)
      Max Age             =    20,
      Forward Delay       =    15,
      Hello Time          =     2
    Parameters system uses when attempting to become root
      System Max Age      =    20,
      System Forward Delay =   15,
      System Hello Time   =     2
```

OS6900-T20 (Rootswitch)

```
-> show spantree vlan 1
Spanning Tree Parameters for Vlan 1
  Spanning Tree Status :                  ON,
  Protocol             :        IEEE Rapid STP,
  mode                 : Per VLAN (1 STP per Vlan),
  Priority             :         4096 (0x1000),
  Bridge ID            :    1000-e8:e7:32:e6:a0:91,
  Designated Root      :    1000-e8:e7:32:e6:a0:91,
  Cost to Root Bridge  :                        0,
  Root Port            :                     None,
  Next Best Root Cost  :                        0,
  Next Best Root Port  :                     None,
  TxHoldCount          :                        3,
  Topology Changes     :                        2,
  Topology age         :             00:00:05,
    Current Parameters (seconds)
      Max Age             =    20,
      Forward Delay       =    15,
      Hello Time          =     2
    Parameters system uses when attempting to become root
      System Max Age      =    20,
      System Forward Delay =   15,
      System Hello Time   =     2
```

OS6900-T40

```
-> show spantree vlan 1
Spanning Tree Parameters for Vlan 1
  Spanning Tree Status :                  ON,
  Protocol             :        IEEE Rapid STP,
  mode                 : Per VLAN (1 STP per Vlan),
  Priority             :         8192 (0x2000),
  Bridge ID            :    2000-e8:e7:32:c1:76:29,
  Designated Root      :    1000-e8:e7:32:e6:a0:91,
  Cost to Root Bridge  :                        4,
  Root Port            :                     1/2,
  Next Best Root Cost  :                        0,
  Next Best Root Port  :                     None,
  TxHoldCount          :                        3,
  Topology Changes     :                       14,
  Topology age         :             00:01:32,
    Current Parameters (seconds)
      Max Age             =    20,
      Forward Delay       =    15,
      Hello Time          =     2
    Parameters system uses when attempting to become root
      System Max Age      =    20,
      System Forward Delay =   15,
      System Hello Time   =     2
```

Testcase P10: “Heeft het uitvallen van switch CoreSw1 effect op het netwerk?”
Doel: In het geval van RSTP is CoreSw1 de Rootswitch, hierbij zou het betekenen dat als deze switch uitvalt dat RSTP moet omschakelen naar een andere Root en zal daardoor ook de verbinding op elke switch opnieuw moeten toewijzen. Hierdoor ondervindt het netwerk enige downtijd.

Werkwijze: Er zullen een ICMP-berichten gestuurd worden vanaf PC1 naar PC2 met behulp van de Command prompt. In de Command prompt zal het volgende commando worden uitgevoerd ***ping 192.168.0.2 –t –w 1.*** Hierbij zullen er ICMP-berichten gestuurd worden totdat de gebruiker de berichten onderbreekt. In dit geval zal er een bij een eventuele onderbreking maar 1 seconde gewacht worden in plaats van de default 5 seconden bij het versturen van ICMP-berichten.

Tijdens het versturen van de ICMP-berichten zal de Rootswitch (CoreSw1) van de netstroom losgekoppeld worden. Dit wordt gedaan om er zeker van te zijn dat de switch uit het netwerk verdwijnt. Hierna zal er gecontroleerd worden of de ICMP-berichten onderbroken zijn. Ook wordt er gekeken of er verandering is in het netwerk door middel van de commando’s: ***show spantree ports active*** en ***show spantree vlan 1***.

Verwachte resultaat: CoreSw1 is de Root switch, hierdoor zal RSTP moeten omschakelen naar de switch met de op één na laagste Root prioriteit. De schakel tijd van RSTP bedraagt ± 1 seconden om de nieuwe Rootswitch functionaliteiten over te laten nemen. Hierdoor zal er een downtijd ontstaan van 1 à 2 seconden.

Behaalde resultaat:

```
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Request timed out.
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
```

```
-> show spantree ports active
 Vlan  Port   Oper Status  Path Cost  Role    Note
-----+-------+-------------+---------+-------+---------
    1  1/1/1      FORW             4  DESG
    1  1/1/2      FORW             4  ROOT
    1  1/1/3       BLK             4   ALT

-> show spantree ports active
 Vlan  Port   Oper Status  Path Cost  Role    Note
-----+-------+-------------+---------+-------+---------
    1  1/1/1      FORW             4  DESG
    1  1/1/3      FORW             4  ROOT
```

```
Spanning Tree Parameters for Vlan 1
  Spanning Tree Status :                         ON,
  Protocol             :            IEEE Rapid STP,
  mode                 : Per VLAN (1 STP per Vlan),
  Priority             :             8192 (0x2000),
  Bridge ID            :   2000-e8:e7:32:c1:76:29,
  Designated Root      :   1000-e8:e7:32:e6:a0:91,
  Cost to Root Bridge  :                          2,
  Root Port            :                        1/2,
  Next Best Root Cost  :                          0,
  Next Best Root Port  :                       None,
  TxHoldCount          :                          3,
  Topology Changes     :                         36,
  Topology age         :                 00:33:12,
    Current Parameters (seconds)
      Max Age              =    20,
      Forward Delay        =    15,
      Hello Time           =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
      System Hello Time    =     2

-> show spantree vlan 1
Spanning Tree Parameters for Vlan 1
  Spanning Tree Status :                         ON,
  Protocol             :            IEEE Rapid STP,
  mode                 : Per VLAN (1 STP per Vlan),
  Priority             :             8192 (0x2000),
  Bridge ID            :   2000-e8:e7:32:c1:76:29,
  Designated Root      :   2000-e8:e7:32:c1:76:29,
  Cost to Root Bridge  :                          0,
  Root Port            :                       None,
  Next Best Root Cost  :                          0,
  Next Best Root Port  :                       None,
  TxHoldCount          :                          3,
  Topology Changes     :                         36,
  Topology age         :                 00:33:48,
    Current Parameters (seconds)
      Max Age              =    20,
      Forward Delay        =    15,
      Hello Time           =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
      System Hello Time    =     2
```

Uit de afbeeldingen hierboven blijkt dat bij het uitschakelen van de Rootswitch er een Time-out is opgetreden. In de afbeelding daarnaast is te zien dat de verbinding van OS6860 naar de Rootswitch is verdwenen en dat er een nieuw path is naar de Root.

Op de afbeelding hiernaast is te zien dat toen de Rootswitch nog aan stond de OS6900-T40 niet de Rootswitch had maar alleen een Port naar de Root. Daaronder is de verandering te zien dat OS6900-T40 nu de nieuwe Rootswitch is door zijn lagere prioriteit dan de Root prioriteit van de OS6860.

Testcase P11: “Heeft het uitvallen van een willekeurige verbinding effect op het netwerk?”
Doel: Volgens het literatuuronderzoek schakelt RSTP, net als STP, bij het uitvallen van een niet-Blocking verbinding. Er zal een downtijd van 1 à 2 seconden plaatsvinden, doordat RSTP dit als omschakeltijd nodig heeft.

Werkwijze: Er zullen een ICMP-berichten gestuurd worden vanaf PC1 naar PC2 met behulp van de Command prompt. In de Command prompt zal het volgende commando worden uitgevoerd ***ping 192.168.0.2 –t –w 1.*** Hierbij zullen er ICMP-berichten gestuurd worden totdat de gebruiker de berichten onderbreekt. In dit geval zal er een bij een eventuele onderbreking maar 1 seconde gewacht worden in plaats van de default 5 seconden bij het versturen van ICMP-berichten. Tijdens het versturen van de ICMP-berichten zullen verschillende verbindingen losgekoppeld worden.

Verwachte resultaat: RSTP heeft een schakeltijd van 1 à 2 seconden om het path te wijzigen, tijdens de omschakeling zullen er geen ICMP-berichten gestuurd worden. Dit zal het geval zijn als er een verbinding wordt losgekoppeld die als Root verbinding of Designated verbinding wordt gebruikt. Bij het loskoppelen van een verbinding die in Blocking state staat wordt er geen effect ondervonden.

Behaalde resultaat: Onderstaand geeft weer wanneer welke kabel is losgekoppeld van welke switch en wat voor gevolgen dit heeft gehad voor het versturen van de ICMP-berichten.

```
C:\Users\Rei>ping 192.168.0.2 -t -w 1

Pinging 192.168.0.2 with 32 bytes of data:
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Request timed out.
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Request timed out.
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Request timed out.
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Request timed out.
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
```

➔ *Kabel port 1/1/2 op de OS6860 losgekoppeld*

➔ *Kabel port 1/1/2 op de OS6860 terug geplaatst*

➔ *Kabel port 1/1/3 op de OS6860 losgekoppeld*

➔ *Kabel port 1/1/3 op de OS6860 terug geplaatst*

➔ *Kabel port 1/1 op de OS6900-T20 losgekoppeld*

➔ *Kabel port 1/1 op de OS6900-T20 terug geplaatst*

➔ *Kabel port 1/2 op de OS6900-T20 losgekoppeld*

➔ *Kabel port 1/2 op de OS6900-T20 terug geplaatst*

➔ *Kabel port 1/3 op de OS6900-T40 losgekoppeld*

➔ *Kabel port 1/3 op de OS6900-T40 terug geplaatst*

➔ *Kabel port 1/2 op de OS6900-T40 losgekoppeld*

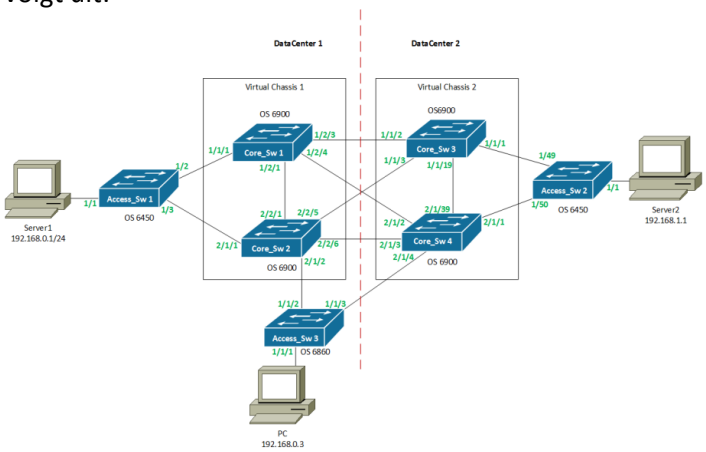
➔ *Kabel port 1/2 op de OS6900-T40 terug geplaatst*

5.2 Nulmeting huidig netwerk

Om uiteindelijk beide situaties met elkaar te kunnen vergelijken zullen er metingen uitgevoerd worden op de volgende gebieden:

- Performance
- Scalability
- Reliability
- Availability
- Maintainability

Bij elk gebied zullen er testcases metingen uitgevoerd worden om de waardes te achterhalen.
Het netwerk voor de testcases is de gehele situatie; de opstelling ziet er daardoor fysiek gezien als volgt uit:



Figuur 2 Fysiek ontwerp huidig netwerk

Testcase M0: "Kan er tussen de PC en de servers gepingd worden?"
Doel: Voordat de metingen uitgevoerd kunnen worden zal eerst gecontroleerd moeten worden of de PC beide servers kan bereiken.

Werkwijze: Er zullen een ICMP-berichten gestuurd worden vanaf PC1 naar Server1 en naar Server2 met behulp van de Command prompt. In de Command prompt zal het volgende commando worden uitgevoerd ***ping 192.168.0.1 –t –w 1*** en ***ping 192.168.1.1 –t –w 1.*** Hierbij zullen er ICMP-berichten gestuurd worden totdat de gebruiker de berichten onderbreekt. In dit geval zal er een bij een eventuele onderbreking maar 1 seconde gewacht worden in plaats van de default 5 seconden bij het versturen van ICMP-berichten.

Behaalde resultaat:

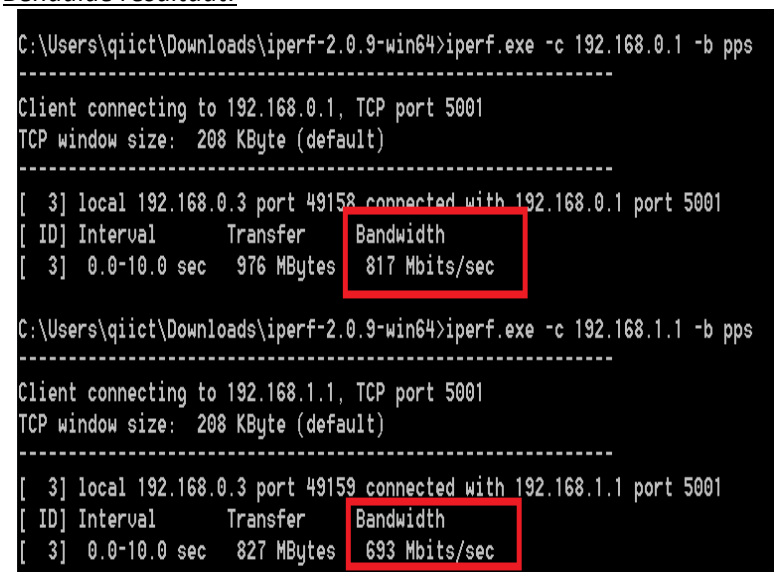
```
C:\Users\qiict>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\qiict>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

In de afbeelding hiernaast is te zien dat beide servers bereikt kunnen worden door de ICMP-berichten.

Testcase M1: “Performance; Wat is de snelheid van het netwerk?”
Doel: Het eerste deel van Performance is de snelheid van de bandbreedte. Hierbij heeft een hogere snelheid het gevolg dat de gebruiker sneller bij de server kan en hierdoor een korte wachttijd heeft als hij iets van de server nodig heeft.

Werkwijze: Er wordt voor deze tets gebruik gemaakt van IPERF. IPERF is een applicatie die de bandbreedte tussen een server en een cliënt kan meten. Hierbij zal op beide servers een IPERF server draaien en zal de PC de cliënt applicatie draaien. Hierna zal op de cliënt gecontroleerd worden wat de bandbreedte is die gehaald wordt.

Behaalde resultaat:



Hiernaast is te zien dat eerst Server1 gemeten is. Hieruit kwam een bandbreedte van 817 Mbits/s.

Het meten van de bandbreedte naar Server2 gaf een waarde van 693 Mbit/s

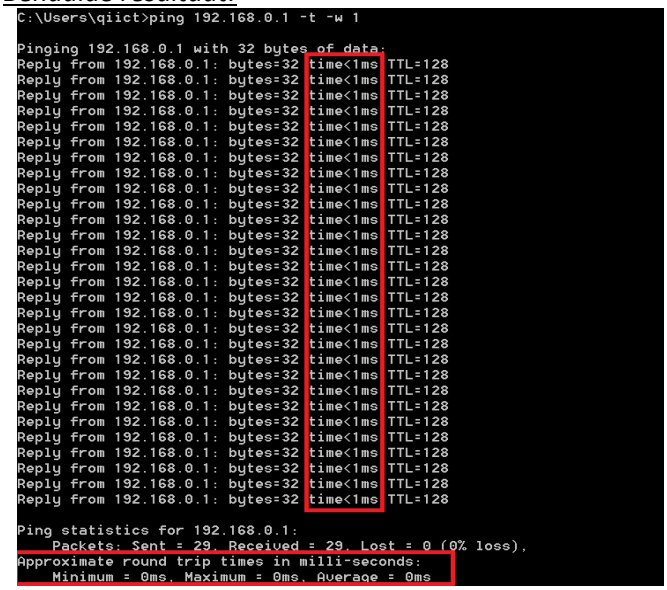
Testcase M2: "Performance; Wat is de latency van het netwerk?"

Doel: Het tweede deel van de performance meting van het netwerk is het meten van de latency bij het uitwisselen van ICMP-berichten tussen de PC en de servers. Hierbij wordt gekeken hoeveel latency een ICMP-bericht bedraagt. Een hoge latency duidt op een vertraging op de verbinding. Hierbij is het gewenste resultaat een zo laag mogelijke latency.

Werkwijze: Er zullen een ICMP-berichten gestuurd worden vanaf PC1 naar Server1 en naar Server2 met behulp van de Command prompt. In de Command prompt zal het volgende commando worden uitgevoerd ***ping 192.168.0.1 –t –w 1*** en ***ping 192.168.1.1 –t –w 1.*** Hierbij zullen er ICMP-berichten gestuurd worden totdat de gebruiker deze uitwisseling onderbreekt. In dit geval zal er een bij een eventuele onderbreking maar 1 seconde gewacht worden in plaats van de default 5 seconden bij het versturen van ICMP-berichten.

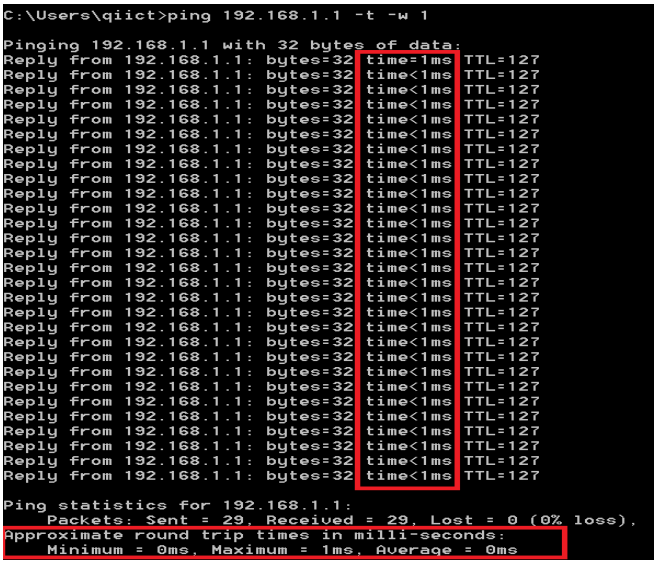
Hierbij wordt er gecontroleerd wat de gemiddelde latency is van de ICMP-berichten uitwisseling; deze uitwisseling zal na een aantal seconde door de gebruiker onderbroken worden. Hierna zal dan de samenvatting van de uitwisseling uitgelezen en gebruikt als resultaat van deze testcase.

Behaalde resultaat:



De tijd die de ICMP-berichten nodig hebben om Server1 te bereiken is <1ms.

Hierbij kan geconcludeerd worden dat de Latency ook <1ms



De tijd die de ICMP-berichten nodig hebben om Server2 te bereiken is <1ms.

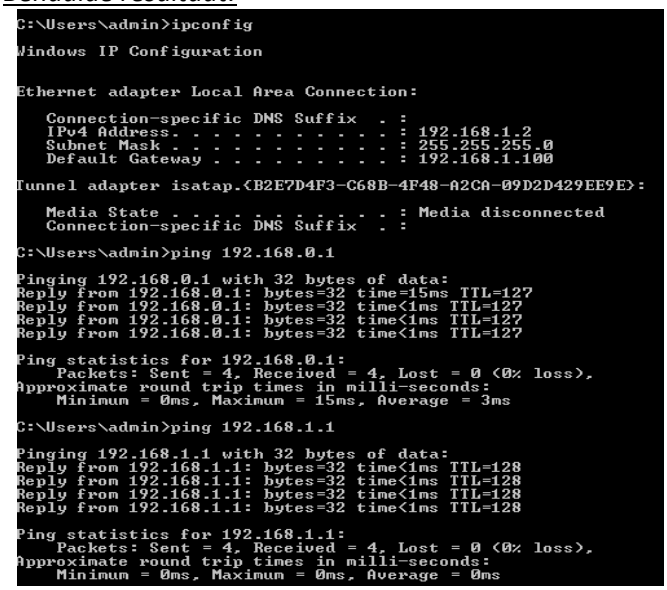
Hierbij kan geconcludeerd worden dat de Latency ook <1ms

Testcase M3: “Scalability; Is het netwerk schaalbaar?”

Doel: Een ander onderdeel van het testen is te controleren of het netwerk schaalbaar is. De scalability van een netwerk houdt in of het netwerk uitbreidbaar kan worden met meerdere componenten, hierbij kan gedacht worden aan een extra datacenter of een gebruiker. Hierbij mag deze toevoeging geen gevolg hebben op de functionaliteiten van het netwerk.

Werkwijze: Er zal een extra switch en gebruiker toegevoegd worden aan het netwerk. Als deze zijn toegevoegd zal er gecontroleerd worden hoe het netwerk hier mee om gaat. Met andere woorden; zal de performance van het netwerk onder de verandering lijden. Er wordt geprobeerd om vanaf de nieuwe gebruiker de servers te bereiken. Dit wordt gecontroleerd door het uitwisselen van ICMP-berichten. Wederom zullen de commando’s in het Command Prompt ***ping 192.168.0.1 –t –w 1*** en ***ping 192.168.1.1 –t –w 1*** zijn. Hier wordt wederom gecontroleerd na een aantal berichten of de latency verhoogd is in vergelijking met de situatie voor de toevoeging van de gebruiker.

Behaalde resultaat:



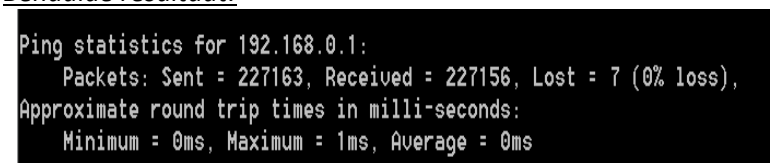
Allebei de servers kunnen worden bereikt vanaf PC2.

Testcase M4: "Reliability; Hoeveel downtijd ondervindt het netwerk gedurende 63 uur?"
Doel: Reliability is het consistente gebruik van het netwerk bij verandering. Dit kan zijn dat de datastroom over het netwerk data blijft sturen zonder dat het netwerk enige downtijd ondervindt. Dit zal getest worden door middel van een duurtest.

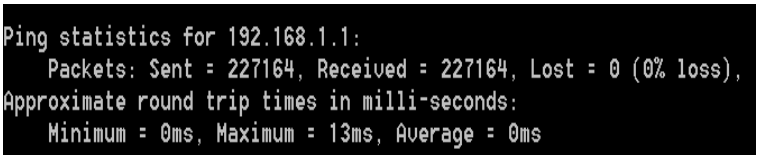
Werkwijze: Er zullen een ICMP-berichten gestuurd worden vanaf PC1 naar Server1 en naar Server2 met behulp van de Command prompt. In de Command prompt zal het volgende commando worden uitgevoerd ***ping 192.168.0.1 –t –w 1*** en ***ping 192.168.1.1 –t –w 1.*** Hierbij zullen er ICMP-berichten gestuurd worden totdat de gebruiker deze uitwisseling onderbreekt. In dit geval zal er een bij een eventuele onderbreking maar 1 seconde gewacht worden in plaats van de default 5 seconden bij het versturen van ICMP-berichten.

Hierbij zal het uitwisselen van de ICMP-berichten ± 63 uur lang uitgevoerd worden. Na deze 63 uur zal er gecontroleerd worden of het netwerk enige downtijd heeft ondervonden.

Behaalde resultaat:



Op server1 is er na ± 63 uur 7x een request time-out opgetreden. Dit zorgt voor een Reliability van:
(7/227163)*100 = 99,997%



Op server2 is er na ± 63 uur 0x een request time-out opgetreden. Dit zorgt voor een Reliability van:
(0/227164)*100 = 100%

Testcase M5: "Availability; wat is het availability percentage?"

Doel: Bij availability wordt er bijgehouden of alle gebruikers/servers te bereiken zijn. In het geval van dit netwerk moet de gebruiker, één van de twee servers te allen tijde kunnen bereiken. Ook bij uitval van switches of verbindingen. Hierbij worden de Access switches buiten beschouwing gelaten. Dit kan getest worden door het loskoppelen van switches en kabels uit de testopstelling, hierbij wordt dan gekeken of de berichten tussen de PC en de servers dan enige down tijd heeft.

Werkwijze: Er zullen een ICMP-berichten gestuurd worden vanaf PC1 naar Server1 en naar Server2 met behulp van de Command prompt. In de Command prompt zal het volgende commando worden uitgevoerd ***ping 192.168.0.1 –t –w 1*** en ***ping 192.168.1.1 –t –w 1.***

Tijdens de uitwisseling van de ICMP-berichten zullen er verschillende kabels losgekoppeld worden om te controleren of deze zorgen voor enige downtime. Ook zullen er switches van het netstroom losgekoppeld worden. Ook hierbij zal de controle op downtime worden uitgevoerd.

Behaalde resultaat:

Tijdens het testen van de Redundantie zijn er verbindingen tussen switches losgekoppeld en wederom aangesloten. Hieruit bleek dat het loskoppelen van sommige verbindingen een time-out gaf van 1 sec. Hiermee wordt duidelijk dat deze verbindingen de Root verbindingen zijn.

```
Ping statistics for 192.168.0.1:
    Packets: Sent = 5260, Received = 5257, Lost = 3 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Dit zorgt bij Server1 voor een availability van:
(3/5260)*100 = 99,943%

```
Ping statistics for 192.168.1.1:
    Packets: Sent = 5260, Received = 5256, Lost = 4 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 41ms, Average = 0ms
```

Dit zorgt bij Server2 voor een availability van:
(3/5257)*100 = 99,923%

Testcase M6: “Maintainability; upgraden/vervangen componenten?”

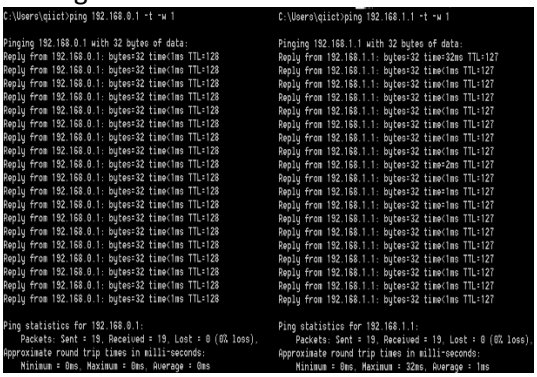
Doel: Met Manageability wordt het onderhouden van het netwerk zonder dat de werking daar effect van ondervind bedoeld. Dit zou kunnen gaan over het updaten van een protocol versie of het updaten van de algemene software versie van de switch. Ook kan hier het vervangen van een switch bedoeld worden.

Werkwijze: Er zullen een ICMP-berichten gestuurd worden vanaf PC1 naar Server1 en naar Server2 met behulp van de Command prompt. In de Command prompt zal het volgende commando worden uitgevoerd ***ping 192.168.0.1 –t –w 1*** en ***ping 192.168.1.1 –t –w 1.***

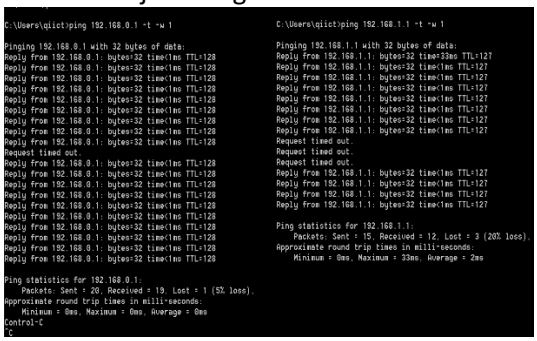
Tijdens de uitwisseling van de ICMP-berichten zal er een switch van de Core van het netstroom worden losgekoppeld en na enige tijd weer worden aangesloten. Hierbij wordt getest of het netwerk enige hinder ondervindt bij het vervangen van een component in het netwerk. Hierna zal wederom gecontroleerd worden of deze vervanging van een component gevolgen heeft voor de uitwisseling van de ICMP-berichten.

Behaalde resultaat:

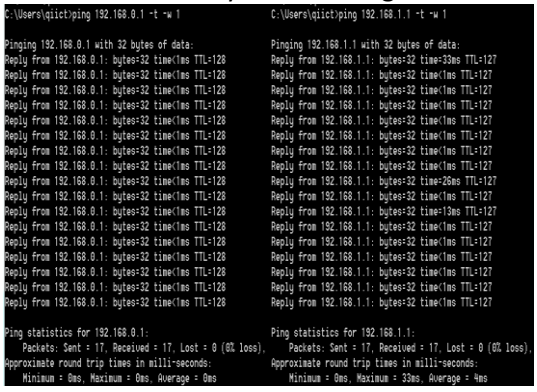
Bij het vervangen van de Master switch van VC1 zal er geen downtime ondervonden worden:



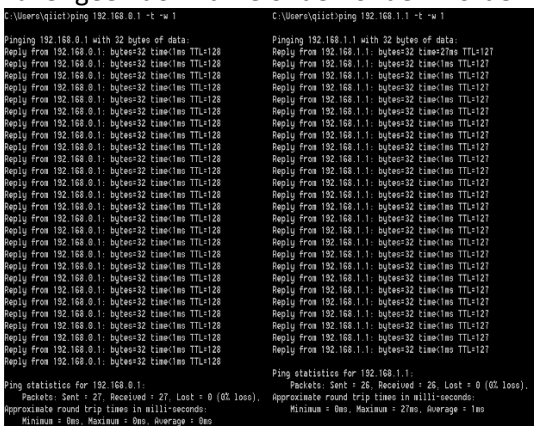
Bij het vervangen van de Slave switch van VC1 wordt enige downtime ondervonden, dit is voornamelijk RSTP gerelateerd:



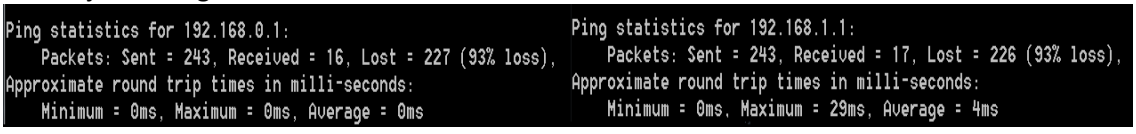
Bij het vervangen van de Master switch van VC2 zal er geen downtime ondervonden worden. Alleen is de Latency wat verhoogd:



Bij het vervangen van de Slave switch van VC2 zal er geen downtime ondervonden worden:



Bij het vervangen van een Acces Switch moet er rekening worden gehouden met een minimale downtijd van ongeveer 4 minuten.



6. Werking nieuwe situatie

In dit hoofdstuk wordt de werking van de nieuwe situatie weer gegeven. Hierbij wordt de deelvraag: *"Hoe werkt de nieuwe situatie?"* behandeld. De nieuwe situatie is het eindpunt van de latere migratie. Bij deze deelvraag zijn nog twee sub-vragen gesteld die hieronder behandeld zullen worden.

6.1 Werking protocollen

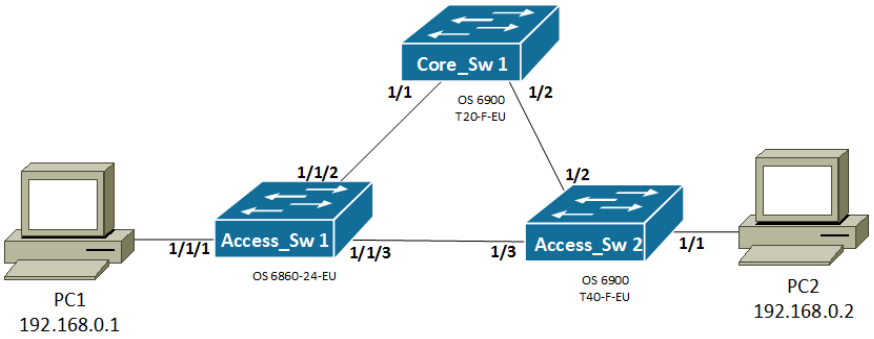
In dit sub-hoofdstuk zal de sub-vraag: *"Werken de gebruikte protocollen zoals uit de literatuur naar voren kwam?"* Deze sub-vraag zal de gevonden literatuur bevestigen of weerleggen. Bij het testen van de werking van de protocollen is er gebruik gemaakt worden van aparte deelontwerpen en van testcases die per protocol zullen verschillen.

In dit hoofdstuk zullen niet wederom de resultaten van de protocollen Virtual Chassis, VRRP en LACP resultaten gegeven worden. De resultaten zijn al eerder weergegeven in hoofdstuk 5.1 *"Werking protocollen".* De overige resultaten en testcases zijn in het Testdocument uitgebreider besproken.

De tests die wel besproken worden, zijn de tests die hetzelfde uitgevoerd zijn als de tests die uitgevoerd zijn op de huidige situatie. Het enige verschil is dat er nu gebruik gemaakt zal worden van SPB op de core in plaats van RSTP. Hierdoor zal de werking van SPB nog getest moeten worden.

Uit de literatuur kwam naar voren dat SPB bijna hetzelfde werkt als TRILL. Zo wordt er bij beide gebruik gemaakt van het IS-IS algoritme en wordt er gebruik gemaakt van het ECMP protocol om het verkeer over meerdere verbindingen te kunnen sturen.

Voor SPB zal hetzelfde deelontwerp gebruikt worden als die van RSTP, dit komt doordat beide protocollen dezelfde functionaliteit hebben in dit netwerk. Namelijk het voorkomen van loops in het netwerk. Voor het testen van SPB zullen dezelfde testcases gebruikt worden. Ook wordt hetzelfde testopstelling gebruikt:



Figuur 3 Ontwerp SPB tests

Testcase P9.1: “Is SPB correct geconfigureerd?”

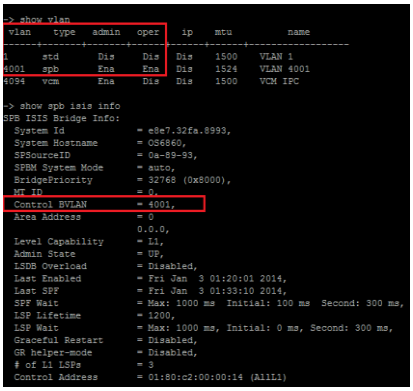
Doel: Er moet gecontroleerd worden of de SPB configuratie in de switch is doorgevoerd. Dit wordt gedaan door te controleren op de switches of SPB als type spantree is geselecteerd.

Werkwijze: Op alle switches zal het commando ***show vlan*** en ***show spb isis info*** uitgevoerd om te controleren of de SPB configuratie correct is doorgevoerd.

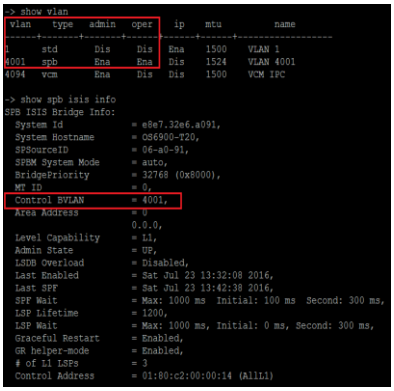
Gewenste resultaat: VLAN 1 met RSTP is disabled en VLAN 4001 met type SPB is enabled. VLAN 4001 is eigenlijk BVLAN 4001 en is het eerste VLAN dat bij het SPB protocol hoort.

Behaalde resultaat: Uit deze afbeeldingen blijkt dat SPB op alle drie de switches is enabled en werkt op BVLAN 4001. Het vlan met RSTP is disabled om er zeker van te zijn dat er geen conflict ontstaat tussen het RSTP en SPB protocol.

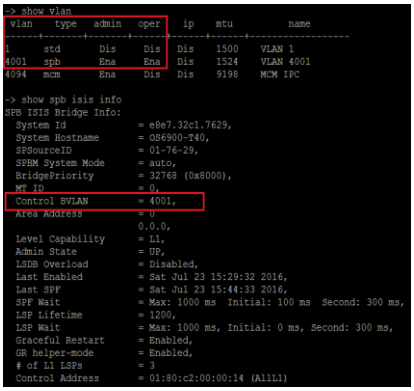
OS6860



OS6900-T20



OS6900-T40



Testcase P10.1: “Heeft het uitvallen van switch CoreSw1 effect op het netwerk?”
Doel: Als in het netwerk switch CoreSw1 uitvalt, mag dit bij SPB niet voor problemen zorgen. SPB blokkeert namelijk geen verbindingen zoals RSTP dit doet. Ook is uit de literatuur gebleken dat het omschakelen van verbinding bij SPB maar enkele milliseconden duurt. Hierdoor zal het netwerk niet tot nauwelijks effect ondervinden van de verandering.

Werkwijze: Er zullen een ICMP-berichten gestuurd worden vanaf PC1 naar PC2 met behulp van de Command prompt. In de Command prompt zal het volgende commando worden uitgevoerd ***ping 192.168.0.2 –t –w 1.*** Hierbij zullen er ICMP-berichten gestuurd worden totdat de gebruiker de berichten onderbreekt. In dit geval zal er een bij een eventuele onderbreking maar 1 seconde gewacht worden in plaats van de default 5 seconden bij het versturen van ICMP-berichten.

Tijdens het versturen van de ICMP-berichten zal de Rootswitch (CoreSw1) van de netstroom losgekoppeld worden. Dit wordt gedaan om er zeker van te zijn dat de switch uit het netwerk verdwijnt. Hierna zal er gecontroleerd worden of de ICMP-berichten onderbroken zijn.

Gewenste resultaat: Het versturen van de ICMP-berichten zal geen onderbreking ondervinden van de uitgevallen verbinding. Op de OS6860 is te zien dat CoreSw1 (OS6900-T20) verdwijnt uit de SPB omgeving.

Behaalde resultaat:

```
-> show spb isis adjacency
SPB ISIS Adjacency:
 System
 (Name : SystemId)                     Type   State   Hold  Interface
-------------------------------------+------+-------+------+----------
 OS6900-T20          : e8e7.32e6.a091  L1     UP        24       1/1/2
 OS6900-T40          : e8e7.32c1.7629  L1     UP        20       1/1/3

Adjacencies : 2
```

Op de afbeeldingen is te zien dat op de OS6860 het commando “*show spb isis adjacency*” is uitgevoerd. Dit commando laat de switches zien die in de topology ook SPB draaien.

🡐 *Voor het uitschakelen van CoreSw1*

```
-> show spb isis adjacency
SPB ISIS Adjacency:
 System
 (Name : SystemId)                     Type   State   Hold  Interface
-------------------------------------+------+-------+------+----------
 OS6900-T40          : e8e7.32c1.7629  L1     UP        25       1/1/3

Adjacencies : 1
```

Hierbij is te zien dat bij het uitschakelen van CoreSw1 (OS6900-T20) deze niet langer te zien is in de tabel.

🡐 *Na het uitschakelen van CoreSw1*

```
Pinging 192.168.0.2 with 32 bytes of data:
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
```

In de afbeelding is het uitwisselen van ICMP-berichten weergegeven tussen de PCs. Hierbij is te zien dat het uitvallen van CoreSw1 geen effect heeft op deze uitwisseling.

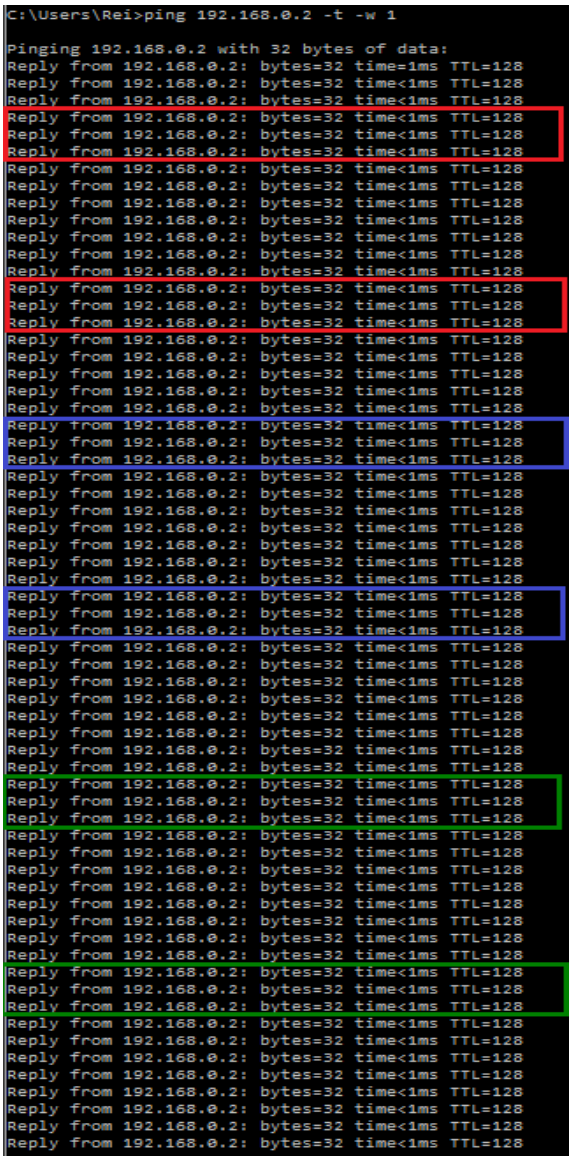
🡐 *Het gevolg van het loskoppelen van CoreSw1*

Testcase P11.1: "Heeft het uitvallen van een willekeurige verbinding effect op het netwerk?"
Doel: Volgens het literatuuronderzoek gebruikt SPB alle verbindingen. Dit zorgt ervoor dat het netwerk een minimale downtijd ondervindt. SPB heeft maar een aantal milliseconden nodig en zal hierdoor alleen een hogere latency hebben.

Werkwijze: Er zullen een ICMP-berichten gestuurd worden vanaf PC1 naar PC2 met behulp van de Command prompt. In de Command prompt zal het volgende commando worden uitgevoerd ***ping 192.168.0.2 –t –w 1.*** Hierbij zullen er ICMP-berichten gestuurd worden totdat de gebruiker de berichten onderbreekt. In dit geval zal er een bij een eventuele onderbreking maar 1 seconde gewacht worden in plaats van de default 5 seconden bij het versturen van ICMP-berichten. Tijdens het versturen van de ICMP-berichten zullen verschillende verbindingen losgekoppeld worden.

Gewenste resultaat: Het netwerk zal geen effect ondervinden van de uitgevallen verbinding. Er zal hoogstens een verhoging zijn in de latency.

Behaalde resultaat: Onderstaand geeft weer wanneer welke kabel is losgekoppeld van welke switch en wat voor gevolgen dit heeft gehad voor het versturen van de ICMP-berichten.



➔ *Kabel port 1/1/2 op de OS6860 losgekoppeld*

➔ *Kabel port 1/1/2 op de OS6860 terug geplaatst*

➔ *Kabel port 1/1/3 op de OS6860 losgekoppeld*

➔ *Kabel port 1/1/3 op de OS6860 terug geplaatst*

➔ *Kabel port 1/1 op de OS6900-T20 losgekoppeld*

➔ *Kabel port 1/1 op de OS6900-T20 terug geplaatst*

➔ *Kabel port 1/2 op de OS6900-T20 losgekoppeld*

➔ *Kabel port 1/2 op de OS6900-T20 terug geplaatst*

➔ *Kabel port 1/3 op de OS6900-T40 losgekoppeld*

➔ *Kabel port 1/3 op de OS6900-T40 terug geplaatst*

➔ *Kabel port 1/2 op de OS6900-T40 losgekoppeld*

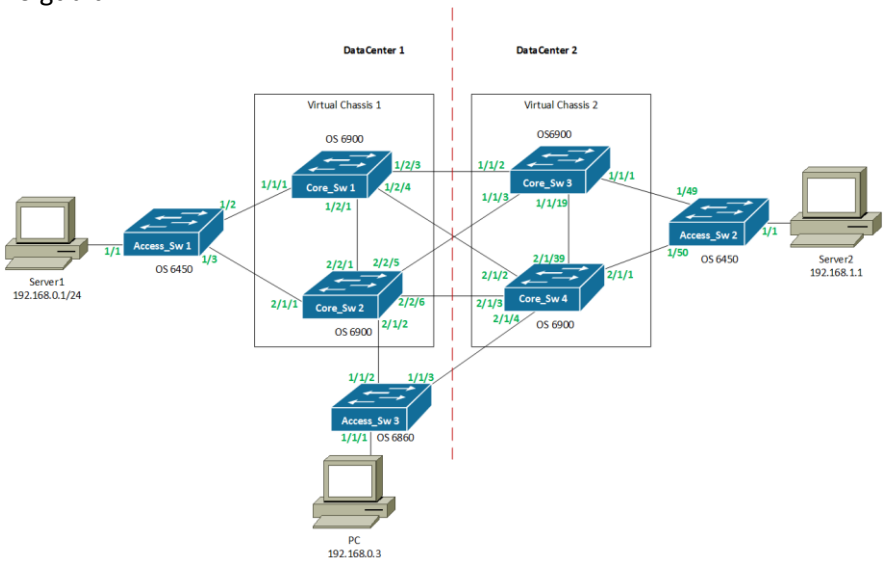
➔ *Kabel port 1/2 op de OS6900-T40 terug geplaatst*

6.2 Meting nieuw netwerk

Om uiteindelijk beide situaties met elkaar te kunnen vergelijken zullen er metingen uitgevoerd worden op de volgende gebieden:

- Performance
- Scalability
- Reliability
- Availability
- Maintainability

Hierbij zullen dezelfde metingen gedaan worden als bij de meting van de oude situatie.
Het netwerk voor de testcases is de gehele situatie; de opstelling ziet er daardoor fysiek gezien als volgt uit:



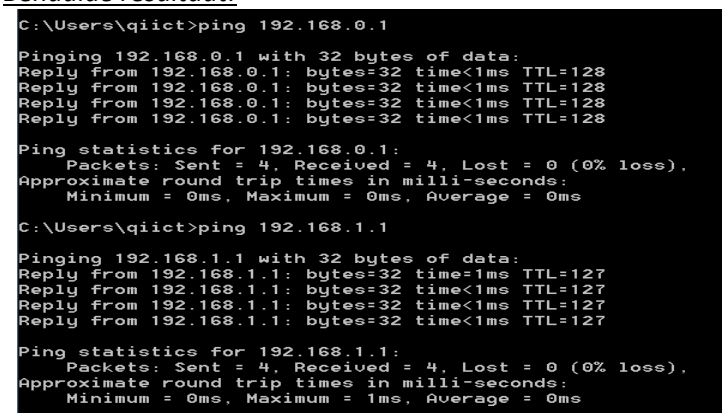
Figuur 4 Fysiek ontwerp Proof of Concept

Echter werd bij het configureren van het Proof of Concept duidelijk dat VRRP niet werkt binnen een SPB omgeving. Dit komt doordat SPB geen IP-adressen leest binnen zijn inkomende frame. SPB gebruikt namelijk een extra tag in de frames die binnenkomen op de SAP port. Hierin wordt het VLAN aan een ISID gekoppeld. Het ISID is door middel van een SPB service aan een BVLAN gekoppeld binnen het SPB netwerk. Het ISID wordt uiteindelijk gebruikt voor het switchen binnen het SPB netwerk over het aangegeven BVLAN. Hierdoor is het gebruik van VRRP of iedere andere vorm van routeren binnen het SPB netwerk niet mogelijk. Dit wordt nu opgelost door een Access switches beide ip interfaces te geven om beide servers te kunnen bereiken.

Testcase M0: "Kan er tussen de PC en de servers gepingd worden?"
Doel: Voordat de metingen uitgevoerd kunnen worden zal eerst gecontroleerd moeten worden of de PC beide servers kan bereiken.

Werkwijze: Er zullen een ICMP-berichten gestuurd worden vanaf PC1 naar Server1 en naar Server2 met behulp van de Command prompt. In de Command prompt zal het volgende commando worden uitgevoerd ***ping 192.168.0.1 –t –w 1*** en ***ping 192.168.1.1 –t –w 1.*** Hierbij zullen er ICMP-berichten gestuurd worden totdat de gebruiker de berichten onderbreekt. In dit geval zal er een bij een eventuele onderbreking maar 1 seconde gewacht worden in plaats van de default 5 seconden bij het versturen van ICMP-berichten.

Behaalde resultaat:

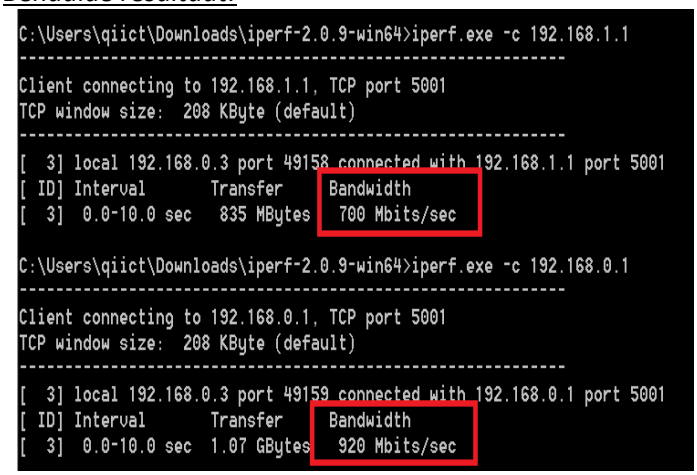


In de afbeelding hiernaast is te zien hoe naar beide servers ICMP-berichten worden gestuurd en dat beide servers een response geven op de berichten.

Testcase M1: “Performance; Wat is de snelheid van het netwerk?”
Doel: Het eerste deel van Performance is de snelheid van de bandbreedte. Hierbij heeft een hogere snelheid het gevolg dat de gebruiker sneller bij de server kan en hierdoor een korte wachttijd heeft als hij iets van de server nodig heeft.

Werkwijze: Er wordt voor deze tets gebruik gemaakt van IPERF. IPERF is een applicatie die de bandbreedte tussen een server en een cliënt kan meten. Hierbij zal op beide servers een IPERF server draaien en zal de PC de cliënt applicatie draaien. Hierna zal op de cliënt gecontroleerd worden wat de bandbreedte is die gehaald wordt.

Behaalde resultaat:



Hiernaast is te zien dat eerst de bandbreedte naar Server2 is gemeten. Hieruit kwam een bandbreedte van 700 Mbits/s.

Het meten van de bandbreedte naar Server1 gaf een waarde van 920 bit/s

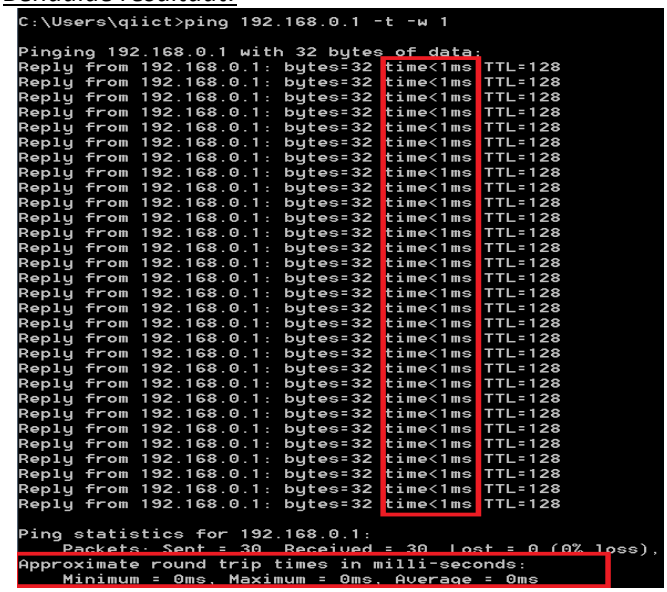
Testcase M2: "Performance; Wat is de latency van het netwerk?"

Doel: Het tweede deel van de performance meting van het netwerk is het meten van de latency bij het uitwisselen van ICMP-berichten tussen de PC en de servers. Hierbij wordt gekeken hoeveel latency een ICMP-bericht bedraagt. Een hoge latency duidt op een vertraging op de verbinding. Hierbij is het gewenste resultaat een zo laag mogelijke latency.

Werkwijze: Er zullen een ICMP-berichten gestuurd worden vanaf PC1 naar Server1 en naar Server2 met behulp van de Command prompt. In de Command prompt zal het volgende commando worden uitgevoerd ***ping 192.168.0.1 –t –w 1*** en ***ping 192.168.1.1 –t –w 1.*** Hierbij zullen er ICMP-berichten gestuurd worden totdat de gebruiker deze uitwisseling onderbreekt. In dit geval zal er een bij een eventuele onderbreking maar 1 seconde gewacht worden in plaats van de default 5 seconden bij het versturen van ICMP-berichten.

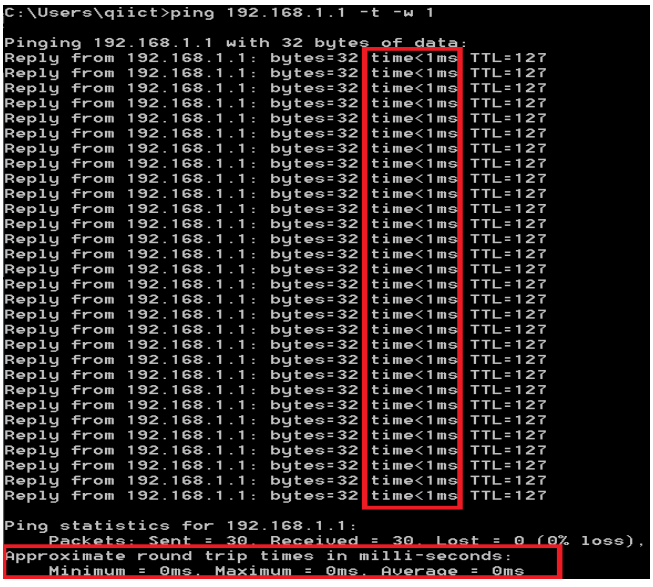
Hierbij wordt er gecontroleerd wat de gemiddelde latency is van de ICMP-berichten uitwisseling; deze uitwisseling zal na een aantal seconde door de gebruiker onderbroken worden. Hierna zal dan de samenvatting van de uitwisseling uitgelezen en gebruikt als resultaat van deze testcase.

Behaalde resultaat:



De tijd die de ICMP-berichten nodig hebben om Server1 te bereiken is <1ms.

Hierbij kan geconcludeerd worden dat de Latency ook <1ms



De tijd die de ICMP-berichten nodig hebben om Server2 te bereiken is <1ms.

Hierbij kan geconcludeerd worden dat de Latency ook <1ms

Testcase M3: "Scalability; Is het netwerk schaalbaar?"

Doel: Een ander onderdeel van het testen is te controleren of het netwerk schaalbaar is. De scalability van een netwerk houdt in of het netwerk uitbreidbaar kan worden met meerdere componenten, hierbij kan gedacht worden aan een extra datacenter of een gebruiker. Hierbij mag deze toevoeging geen gevolg hebben op de functionaliteiten van het netwerk.

Werkwijze: Er zal een extra switch en gebruiker toegevoegd worden aan het netwerk. Als deze zijn toegevoegd zal er gecontroleerd worden hoe het netwerk hier mee om gaat. Met andere woorden; zal de performance van het netwerk onder de verandering lijden. Er wordt geprobeerd om vanaf de nieuwe gebruiker de servers te bereiken. Dit wordt gecontroleerd door het uitwisselen van ICMP-berichten. Wederom zullen de commando's in het Command Prompt ***ping 192.168.0.1 –t –w 1*** en ***ping 192.168.1.1 –t –w 1*** zijn. Hier wordt wederom gecontroleerd na een aantal berichten of de latency verhoogd is in vergelijking met de situatie voor de toevoeging van de gebruiker.

Behaalde resultaat:

```
C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.100

Tunnel adapter isatap.{B2E7D4F3-C68B-4F48-A2CA-09D2D429EE9E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\admin>ping 192.168.0.1 -w 1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=41ms TTL=127
Reply from 192.168.0.1: bytes=32 time<1ms TTL=127
Reply from 192.168.0.1: bytes=32 time<1ms TTL=127
Reply from 192.168.0.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 41ms, Average = 10ms

C:\Users\admin>ping 192.168.1.1 -w 1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Allebei de servers kunnen bereikt worden vanaf PC2

Dit is echter pas het geval nadat er SAP poorten zijn aangemaakt op VC1 en VC2 waar de nieuwe switch op aangesloten is.

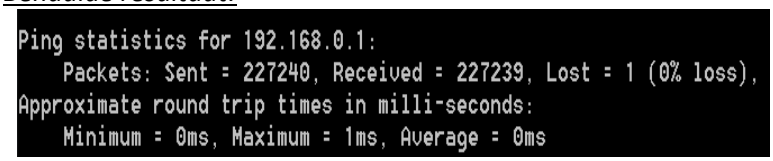
Anders is het niet mogelijk om het verkeer door het SPB netwerk te sturen.

Testcase M4: "Reliability; Hoeveel downtijd ondervindt het netwerk gedurende 63 uur?"
Doel: Reliability is het consistente gebruik van het netwerk bij verandering. Dit kan zijn dat de datastroom over het netwerk data blijft sturen zonder dat het netwerk enige downtijd ondervindt. Dit zal getest worden door middel van een duurtest.

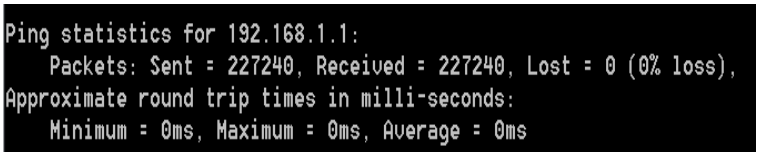
Werkwijze: Er zullen een ICMP-berichten gestuurd worden vanaf PC1 naar Server1 en naar Server2 met behulp van de Command prompt. In de Command prompt zal het volgende commando worden uitgevoerd ***ping 192.168.0.1 –t –w 1*** en ***ping 192.168.1.1 –t –w 1.*** Hierbij zullen er ICMP-berichten gestuurd worden totdat de gebruiker deze uitwisseling onderbreekt. In dit geval zal er een bij een eventuele onderbreking maar 1 seconde gewacht worden in plaats van de default 5 seconden bij het versturen van ICMP-berichten.

Hierbij zal het uitwisselen van de ICMP-berichten 24 uur lang uitgevoerd worden. Na deze 63 uur zal er gecontroleerd worden of het netwerk enige downtijd heeft ondervonden.

Behaalde resultaat:



Op server1 is er na ± 63 uur 1x een request time-out opgetreden. Dit zorgt voor een Reliability van:
(1/227240)*100 = 99,999%



Op server2 is er na ± 63 uur 0x een request time-out opgetreden. Dit zorgt voor een Reliability van:
(0/227240)*100 = 100%

Testcase M5: "Availability; wat is het availability percentage?"
Doel: Bij availability wordt er bijgehouden of alle gebruikers/servers te bereiken zijn. In het geval van dit netwerk moet de gebruiker, één van de twee servers te allen tijde kunnen bereiken. Ook bij uitval van switches of verbindingen. Hierbij worden de Access switches buiten beschouwing gelaten. Dit kan getest worden door het loskoppelen van switches en kabels uit de testopstelling, hierbij wordt dan gekeken of de berichten tussen de PC en de servers dan enige down tijd heeft.

Werkwijze: Er zullen een ICMP-berichten gestuurd worden vanaf PC1 naar Server1 en naar Server2 met behulp van de Command prompt. In de Command prompt zal het volgende commando worden uitgevoerd ***ping 192.168.0.1 –t –w 1*** en ***ping 192.168.1.1 –t –w 1.***

Tijdens de uitwisseling van de ICMP-berichten zullen er verschillende kabels losgekoppeld worden om te controleren of deze zorgen voor enige downtime. Ook zullen er switches van het netstroom losgekoppeld worden. Ook hierbij zal de controle op downtime worden uitgevoerd.

Behaalde resultaat:
Tijdens het testen van de Redundantie zijn er verbindingen tussen switches losgekoppeld en wederom aangesloten. Hieruit bleek dat het loskoppelen van sommige verbindingen een time-out gaf van 1 sec. Dit zijn de routes die gekozen zijn als route naar de destination. Deze test is in een korter tijdsbestek uitgevoerd omdat, de verbindingen tussen de core geen time-out opleverden en hierdoor er niet gewacht moest worden voordat de verbindingen weer was aangesloten.

```
Ping statistics for 192.168.0.1:
    Packets: Sent = 3258, Received = 3257, Lost = 1 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Dit zorgt bij Server1 voor een availability van:
(1/3258)*100 = 99,969%

```
Ping statistics for 192.168.1.1:
    Packets: Sent = 3258, Received = 3257, Lost = 1 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Dit zorgt bij Server2 voor een availability van:
(1/3258)*100 = 99,969%

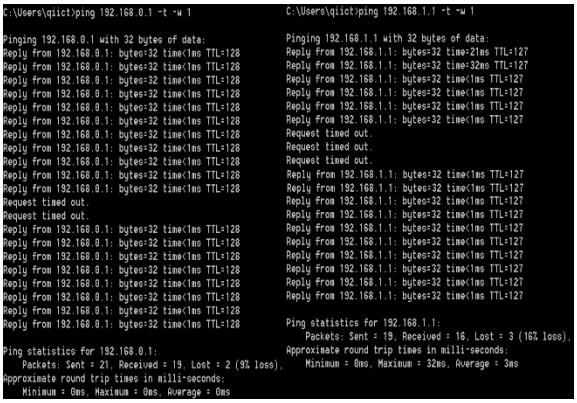
Testcase M6: "Maintainability; wat is de downtime bij het vervangen van componenten?"
Doel: Met Manageability wordt het onderhouden van het netwerk zonder dat de werking daar effect van ondervind bedoeld. Dit zou kunnen gaan over het updaten van een protocol versie of het updaten van de algemene software versie van de switch. Ook kan hier het vervangen van een switch bedoeld worden.

Werkwijze: Er zullen een ICMP-berichten gestuurd worden vanaf PC1 naar Server1 en naar Server2 met behulp van de Command prompt. In de Command prompt zal het volgende commando worden uitgevoerd ***ping 192.168.0.1 –t –w 1*** en ***ping 192.168.1.1 –t –w 1.***

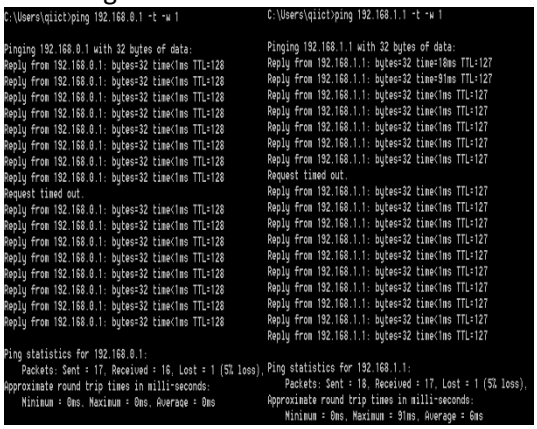
Tijdens de uitwisseling van de ICMP-berichten zal er een switch van de Core van het netstroom worden losgekoppeld en na enige tijd weer worden aangesloten. Hierbij wordt getest of het netwerk enige hinder ondervindt bij het vervangen van een component in het netwerk. Hierna zal wederom gecontroleerd worden of deze vervanging van een component gevolgen heeft voor de uitwisseling van de ICMP-berichten.

Behaalde resultaat:

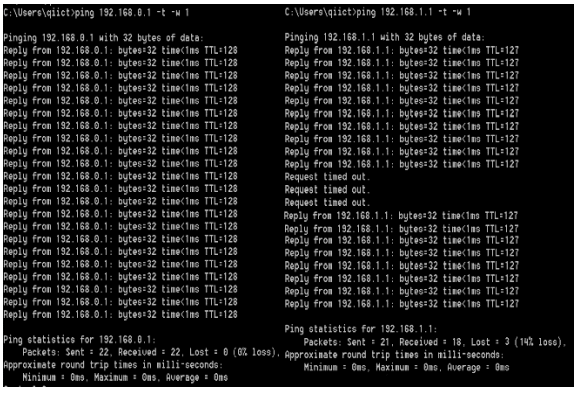
Bij het vervangen van de Master switch van VC1 zal er een downtime ondervonden worden van ongeveer 3 seconden.



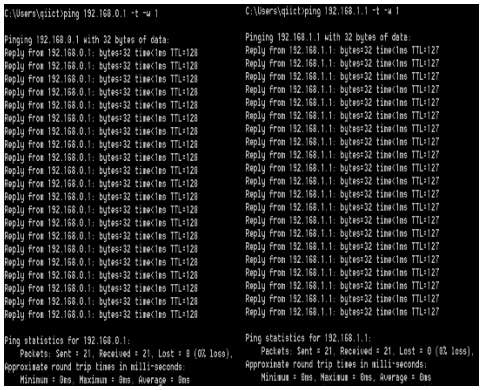
Bij het vervangen van de Slave switch van VC1 wordt enige downtime ondervonden, dit is voornamelijk aan de verbindingen met de OS6860 gerelateerd.



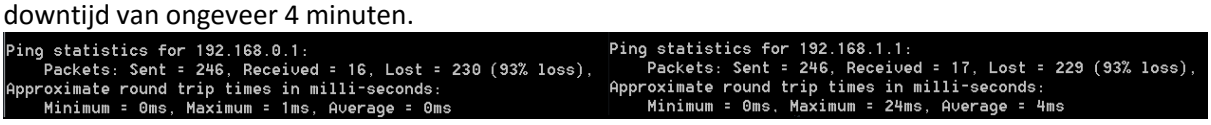
Bij het vervangen van de Master switch van VC2 wordt alleen bij Server2 downtime ondervonden. Er is geen downtime ondervonden voor Server1.



Bij het vervangen van de Slave switch van VC2 zal er geen downtime ondervonden worden.



Bij het vervangen van een Acces Switch moet er rekening worden gehouden met een minimale downtijd van ongeveer 4 minuten.



7. Vergelijking huidige situatie met Proof of Concept

Aan de hand van de metingen die uitgevoerd zijn op zowel de oude situatie als op het Proof of Concept kan er een vergelijkend onderzoek uitgevoerd worden. Hierbij worden de waardes van de beide situaties naast elkaar gelegd en zal er gekeken worden welke situatie een wenselijkere werking heeft.

Tabel 4 Resultaten huidige situatie

Test case	Omschrijving Test case	Resultaat
Testcase M1	Performance bandbreedte	Server1: 817 Mbps Server2: 693 Mbps
Testcase M2	Performance latency	Server1: <1 ms Server2: <1 ms
Testcase M3	Scalability	Ja
Testcase M4	Reliability	Server1: 99,997% Server2: 100%
Testcase M5	Availability	Server1: 99,918% Server2: 99,890%
Testcase M6	Maintainability	VC_Master: ±3 seconden VC_Slave: ±1 seconden Access switch: minimaal 4 minuten

Tabel 5 Resultaten Proof of Concept

Test case	Omschrijving Test case	Resultaat
Testcase M1	Performance bandbreedte	Server1: 920 Mbps Server2: 700 Mbps
Testcase M2	Performance latency	Server1: <1 ms Server2: <1 ms
Testcase M3	Scalability	Ja; maar er zijn aanpassingen nodig in het netwerk
Testcase M4	Reliability	Server1: 99,999% Server2: 100%
Testcase M5	Availability	Server1: 99,969% Server2:99,969 %
Testcase M6	Maintainability	VC_Master: ±3 seconden VC_Slave: ±1 seconden Access switch: minimaal 4 minuten

Uit bovenstaande resultaten kan geconcludeerd worden dat het Proof of Concept een sneller (Performance) en betrouwbaarder (Reliability & Availability) netwerk is als de huidige situatie.

Echter is er wel configuratie nodig als het netwerk uitgebreid wordt met niet-SPB ondersteunende switches. Ook als deze switch wel SPB zou ondersteunen, is het afhankelijk of aan de switch een End point hangt. Dan is er namelijk nog configuratie van de SAP-poorten nodig.

8. Migratie huidige situatie naar Proof of Concept

Als laatste stap voor het experimenteel onderzoek zal er gekeken worden of het mogelijk is om van de huidige situatie te migreren naar het Proof of Concept. Hier zal nagedacht moeten worden over welke stappen er uitgevoerd moeten worden om deze migratie zo efficiënt mogelijk te laten verlopen. Ook zal er aan de migratie een aantal voorwaarden zitten.

8.1 Migratie onderdelen

Als eerste moet er duidelijk worden wat er vervangen gaat worden tijdens de migratie. Het onderzoek is gericht op de vervanging van een STP-variant door een TRILL-variant. In het geval van deze situatie is het de vervanging van RSTP naar SPB. De configuratie voor het realiseren van het Proof of Concept verandert in meerdere opzichten op die van de huidige situatie; zo is VRRP in de core niet mogelijk als de core SPB gebruikt. SPB gebruikt namelijk een extra tag in de frames die binnenkomen op de SAP port. Hierin wordt het VLAN aan een ISID gekoppeld. Het ISID wordt uiteindelijk gebruikt voor het switchen binnen het SPB netwerk. Hierdoor is het gebruik van VRRP of iedere andere vorm van routeren binnen het SPB netwerk niet mogelijk. Dit wordt nu opgelost door de Access switches beide interfaces te geven om beide servers te kunnen bereiken.

8.2 Voorwaarden aan de migratie

Voordat er gemigreerd gaat worden moet er wel duidelijk zijn wat de voorwaarden zijn voor de migratie. Deze voorwaarden zijn vooraf opgesteld.

Voorwaarde 1: *“Het netwerk moet dezelfde functionaliteiten behouden”*
Hierbij zal de PC aan het eind van de migratie nog steeds beide servers kunnen bereiken.

Voorwaarde 2: *“RSTP wordt vervangen door SPB”*
RSTP zal tijdens de migratie uitgeschakeld worden op de switches die SPB ondersteunen. Hierbij wordt eerst SPB geconfigureerd voordat RSTP wordt disabled.

Voorwaarde 3: *“De apparatuur zal niet gewijzigd worden”*
Het netwerk zal op deze manier fysiek gezien hetzelfde blijven. Deze eis was al gesteld bij het ontwerpen van het Proof of Concept. Deze eis geldt daardoor ook voor de migratie.

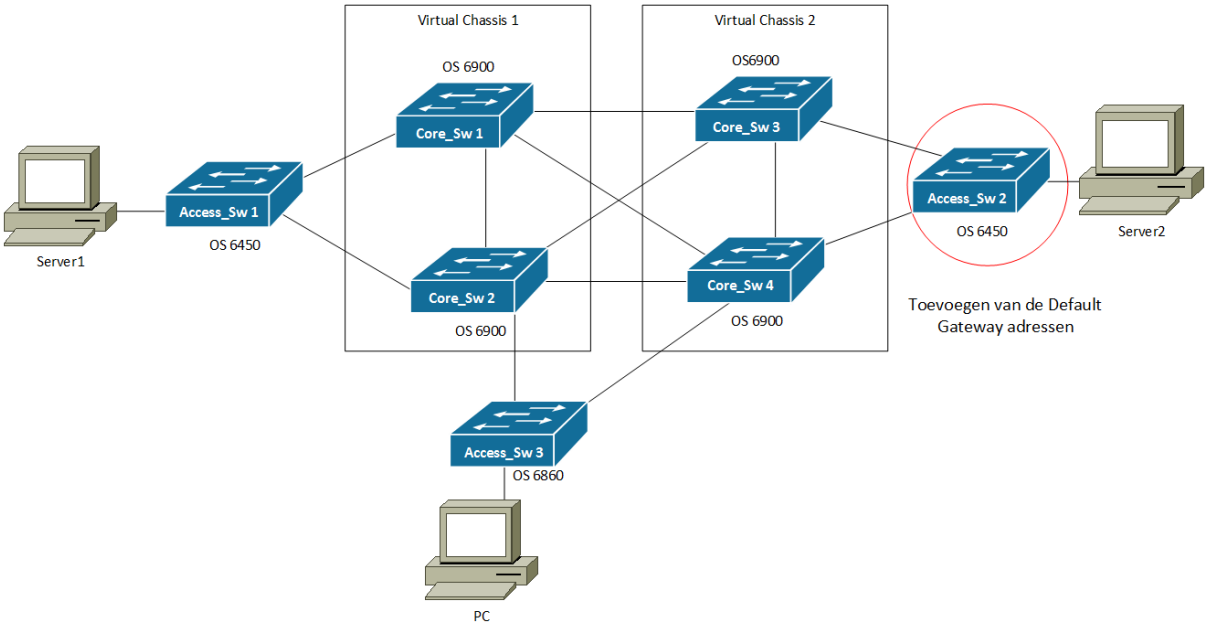
8.3 Migratiestappen

Nu de onderdelen van de migratie en de voorwaarden vastgesteld staan kan er begonnen worden met de migratie. Hierbij zal de huidige situatie als beginpunt dienen en het Proof of Concept is de gewenste situatie ofwel het eindpunt.

Stap 1

"*Default Gateway adressen op Access_Sw2 instellen.*" Om er voor te zorgen dat er toch nog een default gateway is voor het netwerk zal deze buiten het SPB netwerk ingesteld moeten worden. Hierbij geldt dat in deze situatie alleen op de Access Switches die zich voor de servers begeven. Er is gekozen om de Default Gateways op Access_Sw2 te configureren, omdat als deze switch uitvalt wel Server1 nog te bereiken is. Als de Default Gateways op Access_Sw1 had gestaan, zal bij uitval van de switch geen van beide servers meer te bereiken zijn. Ook zal het verkeer met een omweg switchen. Hier wordt op de switch de volgende configuratie uitgevoerd.

Access_Sw2 (OS6450-48)
***ip interface** DFGW1 **address** 192.168.0.100/24 **vlan** 1*
***ip interface** DFGW2 **address** 192.168.1.100/24 **vlan** 1*



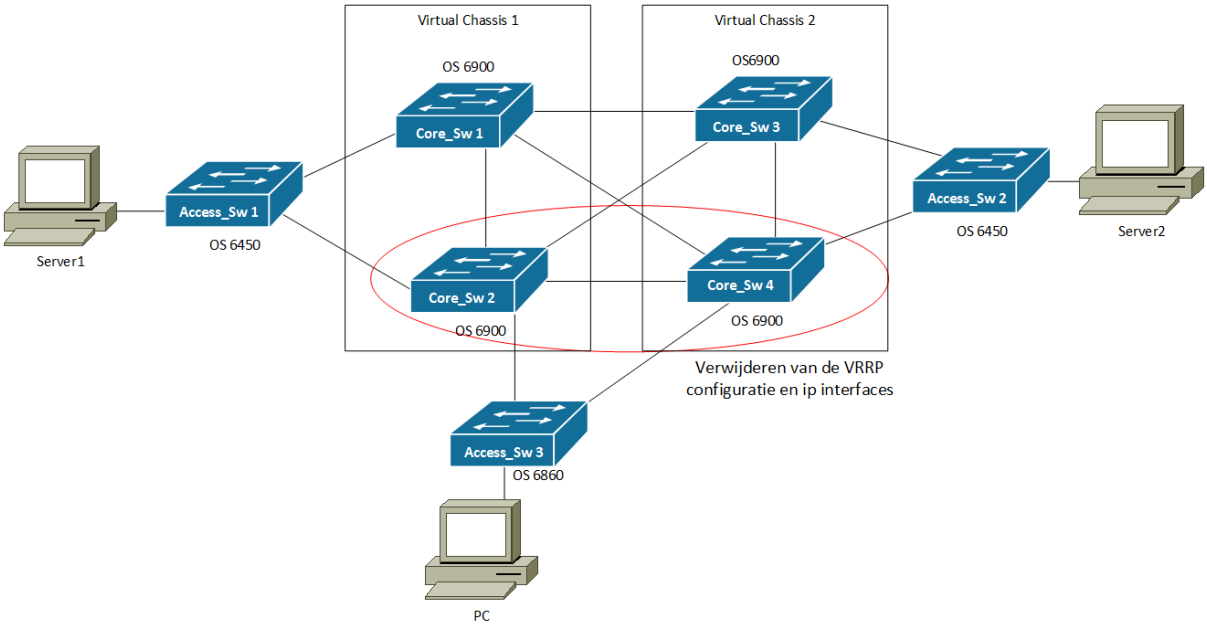
Stap 2

"Het verwijderen van VRRP uit het netwerk." VRRP werkt niet binnen de SPB core en zal daarom ook niet meer van toepassing zijn voor het Proof of Concept. SPB kijkt namelijk niet naar het vlan of IP-adres dat bij het frame binnenkomt. SPB kijkt alleen naar de ISID van het frame en zal deze dan via het bijbehorende BVLAN rondsturen door het netwerk. Het verwijderen van VRRP uit het netwerk wordt gedaan door de volgende configuratie:

VC1	*VC2*
***vrrp** 1 1 **admin-state** disable*	***vrrp** 1 1 **admin-state** disable*
***vrrp** 2 1 **admin-state** disable*	***vrrp** 2 1 **admin-state** disable*
***no vrrp** 1 1*	***no vrrp** 1 1*
***no vrrp** 2 1*	***no vrrp** 2 1*

Ook zullen de interfaces van de switch verwijderd worden:

VC1	*VC2*
***no ip interface** vrrp*	**no ip interface** vrrp
***no ip interface** vrrp2*	**no ip interface** vrrp2

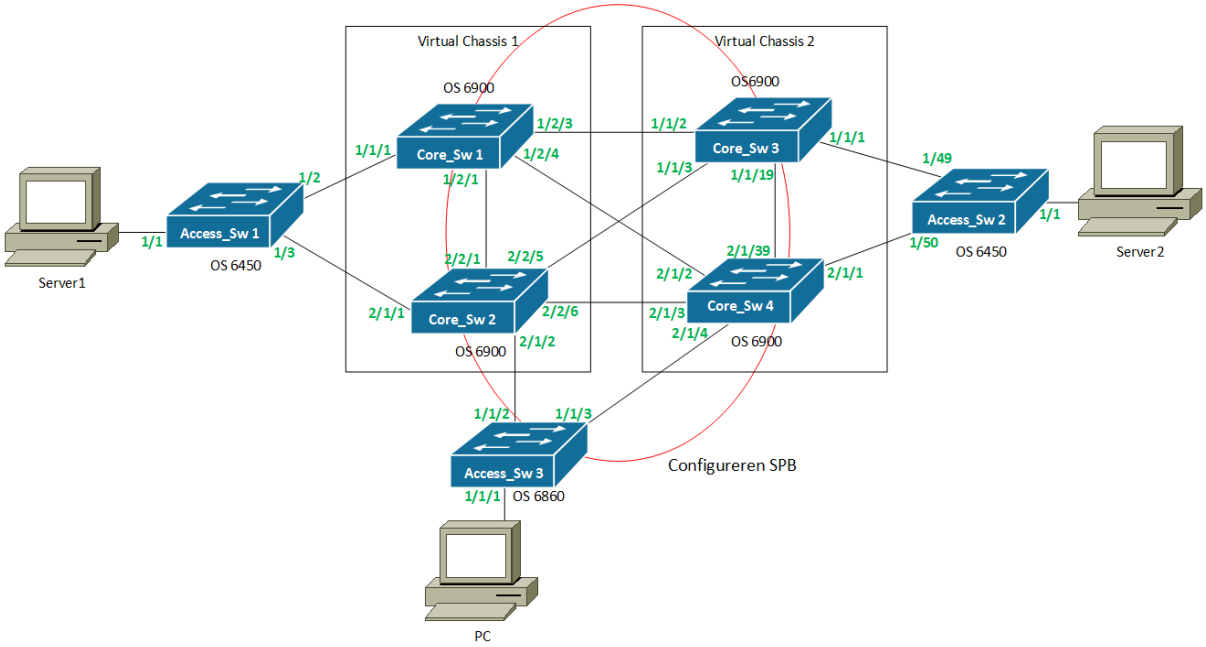


Stap 3

"SPB zal geconfigureerd worden op de switches die de SPB-core vormen"

Omdat RSTP en SPB compatible met elkaar zijn kan SPB geconfigureerd worden terwijl RSTP nog gebruikt wordt. Allereerst moet er een Backbone VLAN aangemaakt worden om het SPB verkeer over te laten switchen. Als dat gedaan is zullen de juiste poorten geconfigureerd worden voor SPB. Dit zijn de poorten die verbonden zijn met de andere switches die SPB ondersteunen. Dit zorgt voor de volgende configuratie op de switches:

VC1	*VC2*	*Access_Sw3 (OS6860)*
***spb bvlan** 4001*	***spb bvlan** 4001*	***spb bvlan** 4001*
***spb isis control-bvlan** 4001*	***spb isis control-bvlan** 4001*	***spb isis control-bvlan** 4001*
***spb isis interface port** 1/2/3-4*	***spb isis interface port** 1/1/2-3*	***spb isis interface port** 1/1/2-3*
***spb isis interface port** 2/2/5-6*	***spb isis interface port** 2/1/2-4*	***spb isis admin-state** enable*
***spb isis interface port** 2/1/3*	***spb isis admin-state** enable*	
spb isis admin-state enable		

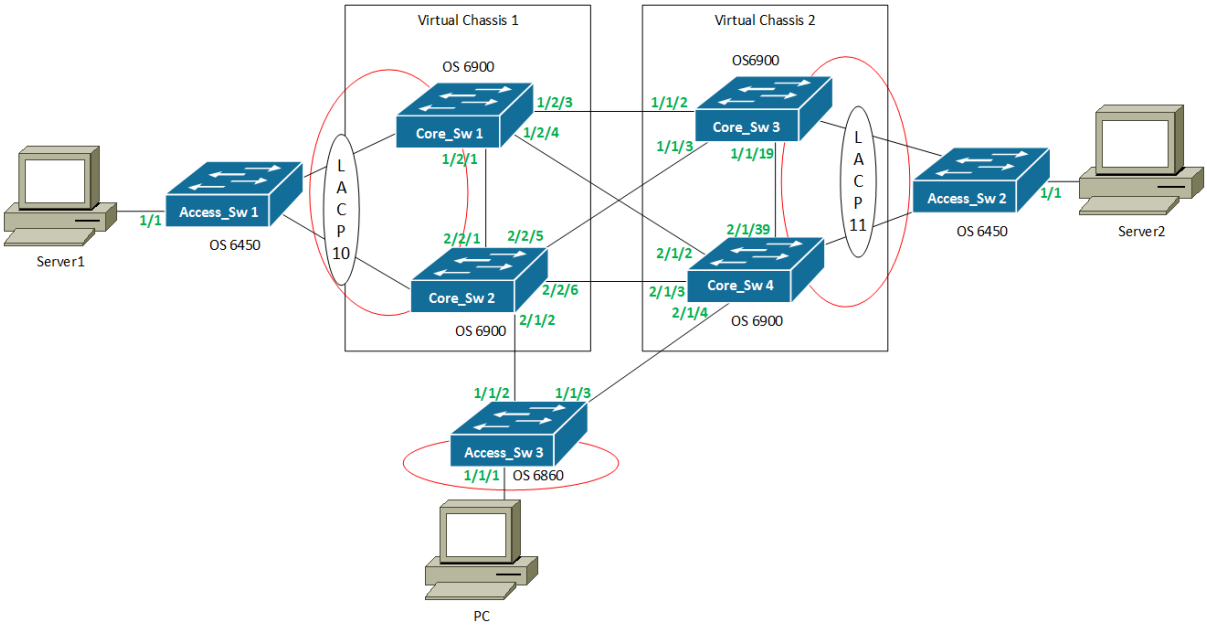


Stap 4

"Service aanmaken om ervoor te zorgen dat het verkeer het SPB netwerk in en uit kan."

Het SPB netwerk kijkt alleen naar de ISID van een frame. Het ISID zorgt ervoor dat het verkeer bij de juiste ontvanger terecht komt. Hierbij zou het gebruik van twee ISID ervoor kunnen zorgen dat het verkeer gescheiden blijft. Dit ISID moet echter wel aan een frame worden toegevoegd voordat deze door het SPB netwerk kan switchen. Hiervoor wordt een service aangemaakt met poorten waarop het verkeer binnenkomt. Dit is volgens de volgende configuratie:

VC1	*VC2*	*Access_Sw3 (OS6860)*
Service access linkagg *10*	***Service access linkagg*** *11*	***Service access port*** *1/1/1*
Service *1* ***spb isid*** *500* ***bvlan*** *4001* ***admin-state*** *enable*	***Service*** *1* ***spb isid*** *500* ***bvlan*** *4001* ***admin-state*** *enable*	***Service*** *1* ***spb isid*** *500* ***bvlan*** *4001* ***admin-state*** *enable*
Service *1* ***sap linkagg*** *10:all* ***admin-state*** *enable*	***Service*** *1* ***sap linkagg*** *11:all* ***admin-state*** *enable*	***Service*** *1* ***sap port*** *1/1/1:all* ***admin-state*** *enable*

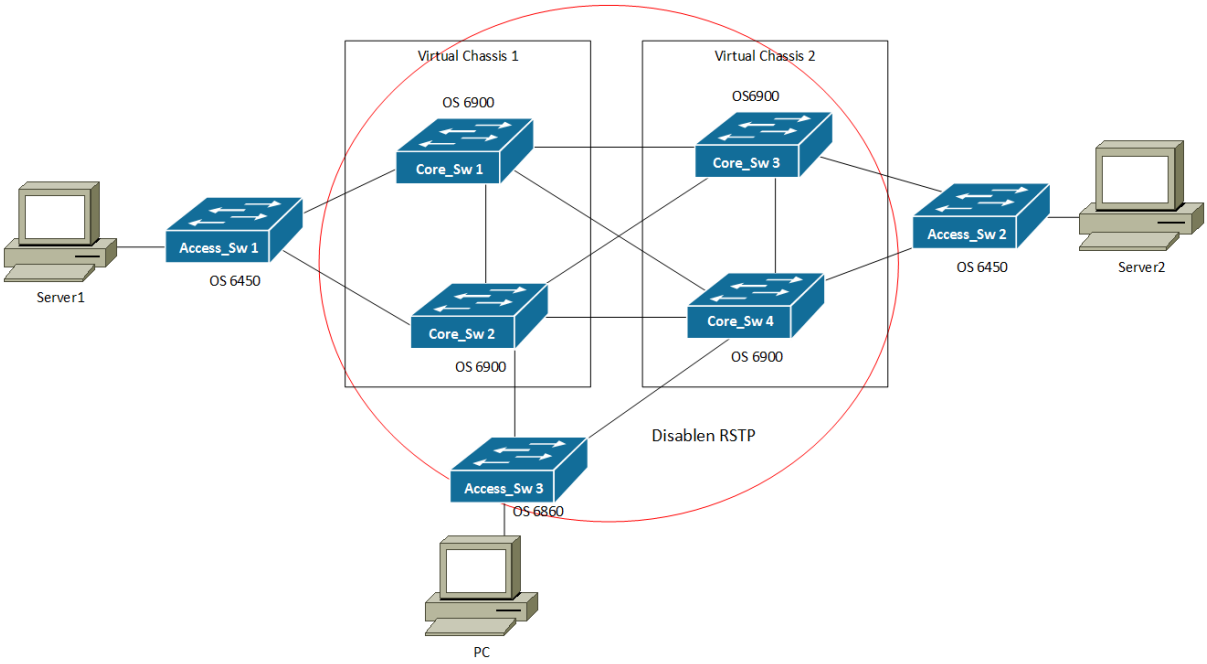


Stap 5

"RSTP zal disabled worden op de switches die SPB gebruiken."

Nu dat alles voor SPB geconfigureerd is zal RSTP op de switches die het SPB netwerk vormen disabled worden. Hierbij gaat het om de switches VC1, VC2 en op de Access_Sw3 (OS6860). Dit zorgt voor de volgende configuratiestap:

VC1	*VC2*	*Access_Sw3 (OS6860)*
***spantree vlan** 1 **admin-state** disable*	***spantree vlan** 1 **admin-state** disable*	***spantree vlan** 1 **admin-state** disable*



8.4 Resultaat migratie

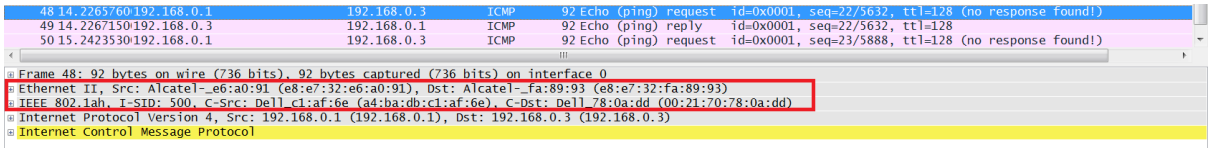
Om te kunnen concluderen of er voldaan is aan de migratie, moet er aan de vooraf opgestelde voorwaarden zijn voldaan. Dit waren de volgende voorwaarden:

Voorwaarde 1: *"Het netwerk moet dezelfde functionaliteiten behouden"*
Voldaan: Het is nog steeds mogelijk om met de PC de beide servers te bereiken. Dit is getest door middel van het sturen van ICMP-berichten van de PC naar beide servers. . Zie hiervoor ook onderstaande afbeelding:

```
C:\Users\qiict>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\qiict>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127
Reply from 192.168.1.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Voorwaarde 2: *"RSTP wordt vervangen door SPB"*
Voldaan: Op de switches die SPB ondersteunen kan de configuratie geopend worden en aangetoond worden dat SPB enabled is en dan RSTP disabled is. Ook is het met Wireshark te bewijzen dat er SPB headers zijn toegevoegd aan het Ethernet frame.

```
-> show spb isis info
SPB ISIS Bridge Info:
  System Id              = e8e7.325a.7fb3,
  System Hostname        = VC2,
  SPSourceID             = 0a-7f-b3,
  SPBM System Mode       = auto,
  BridgePriority         = 32768 (0x8000),
  MT ID                  = 0,
  Control BVLAN          = 4001,
  Area Address           = 0
                         0.0.0,
  Level Capability       = L1,
  Admin State            = UP,
  LSDB Overload          = Disabled,
  Last Enabled           = Thu Sep 29 07:42:06 2016,
  Last SPF               = Thu Sep 29 07:54:05 2016,
  SPF Wait               = Max: 1000 ms  Initial: 100 ms  Second: 300 ms,
  LSP Lifetime           = 1200,
  LSP Wait               = Max: 1000 ms, Initial: 0 ms, Second: 300 ms,
  Graceful Restart       = Disabled,
  GR helper-mode         = Disabled,
  # of L1 LSPs           = 3
  Control Address        = 01:80:c2:00:00:14 (AllL1)

-> show spantree
  Spanning Tree Path Cost Mode : AUTO
 Vlan STP Status Protocol Priority
-----+----------+--------+--------------
    1     OFF       RSTP    8192 (0x2000)
 4001     OFF       RSTP   32768 (0x8000)
 4094     OFF       RSTP   32768 (0x8000)
```



Voorwaarde 3: *"De apparatuur zal niet gewijzigd worden"*
Voldaan: Want er is geen apparatuur vervangen tijdens het migreren. De enige wijziging die tijdens de migratie is uitgevoerd is het wijzigen van de configuratie.

Door de bovenstaande resultaten op de voorwaarden van de migratie kan er geconcludeerd worden dat: Het migreren van RSTP naar SPB mogelijk is. Echter is er wel enige downtime ondervonden bij het verwijderen van VRRP en het in gebruik nemen van de SAP poorten.

9. Conclusie experimenteel onderzoek

Uit het Experimentele onderzoek kan geconcludeerd worden dat het (deels)mogelijk is om RSTP uit het gebruikte netwerk te faseren.

Als eerste zijn de gebruikte protocollen getest op de huidige situatie. Dit is gedaan om meer inzicht te krijgen over wat het protocol toevoegt aan het netwerk. Hierbij wordt ook getest of het protocol ook reageert zoals uit het literatuuronderzoek naar voren kwam. Dit bleek in bijna alle gevallen het geval te zijn. Echter werd er een drietal Time-outs gegenereerd bij de uitschakeling van de Master switch in het geval van het Virtual-Chassis. Volgens de literatuur zou de Slave switch zonder Time-out de rol van de Master overnemen.

Ook werd bij het configureren van het Proof of Concept duidelijk dat VRRP niet werkt binnen een SPB omgeving. Dit komt doordat SPB geen IP-adressen leest op zijn inkomende frame. SPB gebruikt namelijk een extra tag in de frames die binnenkomen op de SAP port. Hierin wordt het VLAN aan een ISID gekoppeld. Het ISID is door middel van een SPB service aan een BVLAN gekoppeld binnen het SPB netwerk. Het ISID wordt uiteindelijk gebruikt voor het switchen binnen het SPB netwerk over het aangegeven BVLAN. Hierdoor is het gebruik van VRRP of iedere andere vorm van routeren binnen het SPB netwerk niet mogelijk. Dit wordt nu opgelost door een Access switches beide ip interfaces te geven om beide servers te kunnen bereiken.

Ook werd duidelijk dat het maar deels mogelijk was om SPB in het netwerk te gebruiken. Dit komt doordat de OS6450 switches geen SPB ondersteunen. Hierdoor is het niet mogelijk om RSTP in zijn geheel uit het netwerk te faseren. Moet dit toch gedaan worden, zullen er vervangende switches gekocht moeten worden die SPB wel ondersteunen. Bijvoorbeeld de OS6860 of de OS6900.

Er zijn verschillende metingen uitgevoerd op de huidige situatie. Dezelfde metingen zijn ook uitgevoerd op het Proof of Concept. Dit is gedaan om van de resultaten een vergelijking te kunnen maken. Uit deze vergelijking is te concluderen dat het Proof of Concept betere resultaten oplevert op het gebied van Performance, Reliability en Availability. Echter werd ook duidelijk dat als het netwerk uitgebreid wordt door een switch die SPB niet ondersteund dat er dan extra configuratie nodig is. Ook als het een switch is die SPB ondersteunt is het nog mogelijk dat er configuratie moet worden toegevoegd. Een voorbeeld hiervan is het toevoegen van een OS6900 switch met een endpoint. Hiervoor zal dan een SAP-poort worden aangemaakt omdat anders het endpoint niet bereikbaar is door het SPB netwerk.

Als laatste werd het migreren van RSTP naar SPB uitgevoerd. De migratie is gedaan aan de hand van een aantal migratie stappen. Dit draaiboek is uitgevoerd en hieruit is het resultaat geconcludeerd. Het resultaat van de migratie was positief. De migratie verliep echter niet zonder downtime. De downtime werd ondervonden bij het verwijderen van VRRP en het in gebruik nemen van de SAP poorten. Voordat het verkeer alle end points kan bereiken moeten op alle switches de SAP-poorten geconfigureerd zijn met hetzelfde ISID en BVLAN. Als de SAP-poort maar op één switch is geconfigureerd zal het verkeer binnen het SPB netwerk blijven loopen.

Terminologielijst

Term	Definitie
STP	Spanning Tree Protocol; protocol gebruikt in switched netwerken om loops te voorkomen
TRILL	Transparent Interconnection of Lots of Links (TRILL), de IETF standard om STP te vervangen
SPB	Shortest Path Bridging; de IEEE standard als vervanger van STP
RSTP	Rapid Spanning Tree Protocol; STP variant, wordt gebruikt vanwege de snellere omschakelingstijd in vergelijking met STP
LACP	Link Aggregation Control Protocol; het bundelen van meerdere fysieke verbindingen en wordt gezien als één logische verbinding
VRRP	Virtual Router Redundancy Protocol; het aanmaken van een Default gateway op een virtuele router die uit twee switches bestaat
VC	Virtual Chassis; het stacken van twee switches om als één logische switch te beheren

Bijlage I

Adviesrapport

LIVING UPTIME

Adviesrapport

Opdrachtgever: Qi ict bv.
Begeleider: Hans Suttorp
Afstudeerder: Frank van Eijk
Opleiding: Technische Informatica, HHS Delft

Datum: 03-10-2016
Versie: 1.0

Versiebeheer

Versie	Datum	Opmerking
0.1	13-9-2016	Eerste versie
1.0	30-9-2016	Aanpassingen doorgevoerd na feedback van Dhr. Suttorp Opmaak consistent gemaakt.

Gerelateerde documenten

Ref	Auteur	Titel
D1	Frank van Eijk	Literatuur onderzoeksrapport
D2	Frank van Eijk	Experimenteel onderzoeksrapport
D3	Frank van Eijk	Testdocument
D4	Frank van Eijk	Migratieplan

Management samenvatting

Qi ict bv. maakt op dit moment veelal gebruik van het spanning tree protocol(STP) voor het gebruik van redundantie in hun switched core netwerken, deze keuze is gemaakt toen STP de meest voordehand liggende keuze was, maar is dit tegenwoordig nog steeds de beste keuze? De hoofdreden voor dit onderzoek is dat Qi over weinig kennis beschikt wat betreft de mogelijkheden van alternatieven zoals TRILL. Hierbij kan de vraag worden gesteld;

"Onder welke voorwaarden Is het met TRILL mogelijk om STP uit een door Qi ict bv. gebruikt switched core netwerk te faseren?"

Aan de hand van bovenstaande hoofdvraag zijn meerdere deelvragen opgesteld. Deze worden verderop besproken en uitgelegd waarom deze deelvragen van belang zijn. Om de hoofdvraag te kunnen beantwoorden zijn er vier verschillende onderzoeksmethoden gebruikt: literatuur onderzoek, experimenteel onderzoek, vergelijkend onderzoek en een toegepast onderzoek

Uit het Literatuuronderzoek kon geconcludeerd worden dat het mogelijk is om STP uit een switched core netwerk van Qi ict bv. te faseren. Eén van de voorwaarden is wel dat TRILL gebruik maakt van Rbridges in plaats van standaard switches. Hierdoor moet de hardware die in het netwerk gebruik wordt wel TRILL 'ready' zijn. Als dit niet het geval is zouden deze nog vervangen kunnen worden, echter kost dit wel meer tijd en geld. Een eis bij het uit faseren van STP was, dat de apparatuur hetzelfde zou blijven. De apparatuur die gebruikt gaat worden is van Alcatel. Hierdoor zullen de TRILL varianten FabricPath en VCS afvallen, omdat dit TRILL proprietary varianten van Cisco en van Brocade zijn. SPB daarentegen wordt wel ondersteund door Alcatel. Hierdoor is de keuze gevallen op SPB om STP uit het huidige netwerk te faseren.

Uit het Experimentele onderzoek kon ook geconcludeerd worden dat het (deels)mogelijk is om RSTP uit het gebruikte netwerk te faseren. Maar ook dat het wenselijk is. Dit komt doordat er verschillende metingen zijn uitgevoerd op de huidige situatie. Dezelfde metingen zijn ook uitgevoerd op het Proof of Concept. Dit is gedaan om van de resultaten een vergelijking te kunnen maken. Uit deze vergelijking is te concluderen dat het Proof of Concept betere resultaten oplevert op het gebied van Performance, Reliability en Availability. Echter werd ook duidelijk dat als het netwerk uitgebreid wordt door een switch die SPB niet ondersteund dat er dan extra configuratie nodig is. Ook als het een switch is die SPB ondersteunt is het nog mogelijk dat er configuratie moet worden toegevoegd. Als laatste werd het migreren van RSTP naar SPB uitgevoerd. De migratie is gedaan aan de hand van een aantal migratie stappen. Dit draaiboek is uitgevoerd en hieruit is het resultaat geconcludeerd. Het resultaat van de migratie was positief. De migratie verliep echter niet zonder downtime.

Op basis van de resultaten van het vergelijkend onderzoek is het zeker wenselijk om te migreren naar een SPB netwerk. Uit het vergelijkende onderzoek is te concluderen dat het Proof of Concept betere resultaten oplevert op het gebied van Performance, Reliability en Availability. Echter werd ook duidelijk dat als het netwerk uitgebreid wordt er bij SPB nog configuratie nodig is.

Uit het literatuuronderzoek werd ook duidelijk dat het wordt aangeraden om het hele netwerk te migreren naar een 'TRILL' omgeving. Dit zorgt namelijk voor meer mogelijkheden in het geval van best path. Echter is in dit onderzoek gefocust op een Layer 2 netwerk. Bij Layer 3 netwerken is niet duidelijk of het gebruik van SPB wenselijker is als RSTP. Hierdoor blijven er nog wel wat vragen over. Deze vragen leiden tot de volgende aanbevelingen:

- *Het uitzoeken van routering over SPB op Layer 3*
- *Het uitzoeken van werking compleet SPB netwerk*

Inhoudsopgave

Tabellen

Figuren

1. Inleiding

In opdracht van Qi ict bv. is er onderzoek gedaan naar onder welke voorwaarden het mogelijk is om met TRILL STP uit een door Qi ict bv. gebruikt switched core netwerk te faseren.

1.1 Aanleiding

Qi ict bv. maakt op dit moment veelal gebruik van het spanning tree protocol(STP) voor het gebruik van redundantie in hun switched core netwerken, deze keuze is gemaakt toen STP de meest voordehand liggende keuze was, maar is dit tegenwoordig nog steeds de beste keuze?

De reden dat er een literatuuronderzoek wordt gedaan is: er moet kennis worden opgedaan over de protocollen die voor het experimentele onderzoek nodig zijn. Het literatuuronderzoek wordt uitgevoerd omdat het van essentieel belang is dat de protocollen al enigszins bekend zijn als zij geconfigureerd moeten worden.

De reden van het experimentele onderzoek is het bevestigen of ontkrachten van de theorieën die uit het literatuuronderzoek voortkomen. Ook wordt er geëxperimenteerd of het mogelijk is om STP uit een switched-core netwerk te migreren. Hieruit zullen een aantal stappen volgen die tot het uiteindelijke resultaat zullen leiden.

De resultaten van beide onderzoeken zullen ervoor zorgen dat de hoofdvraag beantwoordt kan worden en dat er een advies kan worden gegeven aan de hand van dit resultaat.

1.2 Probleemstelling

De hoofdreden voor dit onderzoek is dat Qi over weinig kennis beschikt wat betreft de alternatieve mogelijkheden van STP zoals TRILL.

De huidige opdracht is voor Qi niet echt een probleem, maar omdat Qi ict bv. uiteraard de beste kwaliteit wil leveren, zal deze opdracht wel degelijk toegevoegde waarde hebben voor het bedrijf. Maar niet alleen Qi ict bv. zal hier profijt van hebben, ook de klanten zullen hier van mee profiteren. En dat de beste kwaliteit leveren houdt onder andere in; het netwerk zo efficiënt mogelijk inrichten en onderhouden.

1.3 Doelstelling

Het doel van de opdracht is het onderzoeken onder welke voorwaarden het mogelijk is om met TRILL, STP uit de huidig gebruikte switched core netwerken te kunnen faseren. Hierbij wordt de mogelijkheid bedoeld of TRILL zonder grote veranderingen kan worden doorgevoerd in een bestaand netwerk. Door middel van een literatuuronderzoek en een experimenteel onderzoek zal deze doelstelling behaald moeten worden. Beide onderzoeken zullen een resultaat geven over de mogelijkheid of TRILL daadwerkelijk STP uit een switched core netwerk kan faseren dan wel migreren. Deze resultaten zullen een bijdrage leveren aan de adviezen die Qi ict bv. haar klanten geeft omtrent de keuze voor redundantie oplossingen en de engineers helpen om deze oplossing goed te kunnen implementeren.

1.4 Hoofdvraag

"Onder welke voorwaarden Is het met TRILL mogelijk om STP uit een door Qi ict bv. gebruikt switched-core netwerk te faseren?"

1.5 Deelvragen

In deze paragraaf zullen de deelvragen en de eventuele sub-vragen ervan beschreven worden. Hierbij worden de vragen voor het literatuuronderzoek en het experimentele onderzoek gescheiden.

Literatuur onderzoek

Deelvraag 1: "Wat is STP?"

Reden: Voordat gezegd kan worden of STP uit de huidige switched core netwerken gefaseerd wordt, moet er wel duidelijk zijn wat STP precies inhoudt. Denk hierbij aan waarom is STP ooit ontworpen en waarom is er op dit moment zoveel vraag naar alternatieven.

> **Sub-vraag1.1: "Hoe werkt STP in een switched core netwerk?"**
> *Reden:* De grootste vraag bij STP is "wat doet STP?" Bij deze vraag wordt onderzocht wat STP aan een netwerk toevoegt, maar ook wat er gebeurt als STP uitgeschakeld staat en er geen alternatief op het netwerk actief is.
>
> **Sub-vraag1.2: "Wat zijn nadelen van het Spanning Tree Protocol"**
> *Reden:* Om de kwestie omtrent de vraag naar alternatieven van STP, moet er wel duidelijk zijn waarom deze vraag er is. Dit zal voornamelijk te maken hebben met het feit dat STP bepaalde keuzes maakt waarbij een aantal nadelen aan deze keuzes hangen.

Deelvraag 2: "Wat is TRILL?"

Reden: Bij deze deelvraag geldt hetzelfde als bij de deelvraag "Wat is STP?". Voordat er een conclusie kan worden getrokken uit de hoofdvraag moet niet alleen het oude protocol (STP) bekend zijn, maar ook de eventuele vervanger (TRILL).

> **Sub-vraag2.1: "Hoe werkt TRILL in een switched core netwerk?"**
> *Reden:* Net als STP, is het logisch dat duidelijk moet zijn hoe TRILL werkt in een switched core netwerk.
>
> **Sub-vraag 2.2: "Welke varianten van TRILL zijn er?"**
> *Reden:* Uit het onderzoek blijkt dat TRILL een open standaard is en door verschillende bedrijven gebruikt is om hun eigen versie van TRILL te creëren. Hierbij wordt gekeken welke varianten eventueel relevant zijn voor Qi ict bv.
>
> **Sub-vraag 2.3: "Wat zijn de verschillen tussen de varianten en TRILL?"**
> *Reden:* Om een duidelijk overzicht te krijgen wat er precies verschilt tussen de varianten van TRILL en TRILL zelf. Hierbij kan gedacht worden aan de werking en toepassing van de protocollen.
>
> **Sub-vraag 2.4: "Welke randvoorwaarden zijn er om TRILL te implementeren?"**
> *Reden:* Bij de deelvraag kan de vraag worden gesteld, aan welke randvoorwaarden moet er worden voldaan om TRILL of een variant te implementeren. Hierbij kan gedacht worden aan apparatuur en welke configuratie.

Sub-vraag 2.5: "Waar kunnen TRILL en de varianten het beste worden toegepast in een netwerk?"
Reden: Deze deelvraag is ontstaan uit het deel van de hoofdvraag of TRILL STP uit de huidig gebruikte switched core netwerken faseert. Hierbij wordt gekeken waar TRILL het best in een netwerk kan worden geïmplementeerd.

Deelvraag 3: "Wat zijn de verschillen tussen STP en TRILL?"
Reden: Nu alle protocollen (die behandeld worden) duidelijk zijn, kan de vergelijking opgemaakt worden. Hierbij worden een aantal kenmerken van de protocollen naast elkaar gezet Hierbij kan gedacht worden aan de manier van loops voorkomen en de schaalbaarheid van de netwerken waar de protocollen worden toegepast. Met deze deelvraag kan al een groot deel van de hoofdvraag beantwoordt worden.

Deelvraag 4: "Kan TRILL in de reeds bestaande infrastructuren worden geïmplementeerd?"
Reden: Als laatste wordt er onderzocht of TRILL direct zonder aanpassingen aan de huidige netwerken kan worden toegevoegd. Denk hierbij dat alleen de configuratie aangepast hoeft te worden. Geen verandering van de infrastructuur of apparatuur.

Sub-vraag 4.1: "Hoe ziet deze infrastructuur eruit?"
Reden: Om deze deelvraag te beantwoorden moet wel eerst duidelijk worden om wat voor soort infrastructuur het hier gaat. Hoe ziet de infrastructuur eruit en welke apparatuur wordt er gebruikt; "Is deze apparatuur wel TRILL compatible?"

Sub-vraag4.2: "Wat zijn de huidig gebruikte protocollen?"
Reden: Naast de vraag hoe de infrastructuur eruit ziet, moet er ook duidelijk worden hoe de infrastructuur werkt. Met welke protocollen wordt het huidige netwerk draaiend gehouden.

Sub-vraag 4.3: "Is er compatibiliteit mogelijk met de huidig gebruikte protocollen?"
Reden: Ook moet duidelijk zijn of TRILL of de varianten compatible zijn met de huidig gebruikte protocollen. Met andere woorden, is het bijvoorbeeld mogelijk om een TRILL-core te hebben met een STP-access? Of moet de hele infrastructuur aangepast worden?

Experimenteel onderzoek
Deelvraag 5: "Hoe werkt de huidige situatie?"
Reden: Voordat STP uit het huidige netwerk kan worden gefaseerd, moet eerst duidelijk zijn wat de functionaliteiten zijn van de huidige situatie. Zonder beginsituatie is het ook niet mogelijk om de vergelijking met de nieuwe situatie aan het eind van het onderzoek uit te voeren.

Sub-vraag 5.1: "Werken de gebruikte protocollen zoals uit de literatuur naar voren kwam?"
Reden: Hierbij wordt de gevonden literatuur vergeleken met de werkelijkheid op het netwerk. Hierbij kan de literatuur bevestigd worden of ontkracht. Hierbij kan het geval zijn dat de literatuur een andere werking van een protocol weergeeft dan wat het protocol op het netwerk daadwerkelijk doet. De nadruk ligt hierbij op RSTP.

Sub-vraag 5.2: "Wat zijn de waardes van het huidige netwerk?"
Reden: Hierbij wordt een Nulmeting uitgevoerd. Bij een nulmeting worden verschillende waardes van het huidige netwerk achterhaald, om aan het eind van het onderzoek de waardes van de nieuwe en oude situatie met elkaar te kunnen vergelijken. Voorbeelden van deze waardes zijn: Latency, Reliability en Down time.

Deelvraag 6: "Hoe werkt de nieuwe situatie?"
Reden: Voordat er gemigreerd kan worden naar de nieuwe situatie, moet de nieuwe situatie wel bekend zijn. Op deze manier kan ook de werking van de protocollen op de nieuwe situatie worden getest.

> **Sub-vraag 6.1: "Werken de gebruikte protocollen zoals uit de literatuur naar voren kwam?"**
> *Reden:* Hierbij wordt de gevonden literatuur vergeleken met de werkelijkheid op het netwerk. Hierbij kan de literatuur bevestigd worden of ontkracht. In de nieuwe situatie gaat het vooral om de werking van SPB. De andere protocollen zijn al getest.
>
> **Sub-vraag 6.2: "Wat zijn de waardes van het nieuwe netwerk?"**
> *Reden:* Hierbij worden verschillende waardes van het nieuwe netwerk achterhaald, om aan het eind van het onderzoek de waardes van de beide situaties met elkaar te kunnen vergelijken. Voorbeelden van deze waardes zijn: Latency, Reliability en Down time.

Deelvraag 7: "Werkt de nieuwe situatie beter als de oude?"
Rede: Om een advies te kunnen geven of het wenselijk is om STP uit de huidige netwerk te faseren, moet wel duidelijk zijn of deze situatie beter werkt.

> **Sub-vraag 7.1: "In welk opzicht verschilt de nieuwe situatie met de oude situatie?"**
> *Reden:* Hierbij wordt er gekeken welke verschillen er zijn bij de metingen die bij de oude situatie en bij de nieuwe situatie zijn uitgevoerd. Uit deze metingen zullen verschillen komen, echter is het zo dat sommige waardes ook nog hetzelfde kunnen zijn. De gebieden waarnaar gekeken wordt zijn: Scalability, Availability, Manageability, Maintainability en Performance.

Deelvraag 8: "Hoe wordt de oude situatie naar de nieuwe situatie gemigreerd?"
Reden: Om van de oude situatie naar de nieuwe situatie te migreren moeten er een aantal handelingen worden uitgevoerd. Het is noodzakelijk om te weten hoe de migratie gedaan moet worden. Deze stappen zorgen ervoor dat de migratie op een efficiënte manier kan worden uitgevoerd.

> **Sub-vraag 8.1: "Welke stappen moeten hiervoor worden genomen?"**
> *Reden:* Hierbij zijn de stappen van groot belang, als er niet stapsgewijs gewerkt wordt kan het zijn dat er geen overzicht meer is in de migratie. Hierbij is het mogelijk dat er dan iets ontbreekt of niet op de juiste instellingen staat.
>
> **Sub-vraag 8.2: "Welke voorwaarden zitten er aan de migratie stappen?"**
> *Reden:* Hierbij kan gedacht worden aan de downtijd die het netwerk maximaal mag hebben. Ook moeten de risico's worden gedefinieerd die aanwezig kunnen zijn tijdens het migreren van het netwerk.

2. Aanpak onderzoek

Om de hoofdvraag te kunnen beantwoorden zijn er vier verschillende onderzoeksmethoden gebruikt:

Literatuuronderzoek
Het schrijven van een onderzoek of advies begint vaak met een literatuuronderzoek. Literatuuronderzoek is een methode om bestaande kennis over een onderwerp of probleemstelling te verzamelen. Deze kennis kan gevonden worden in verschillende bronnen, zoals wetenschappelijke tijdschriftartikelen, boeken, papers, scripties en archiefmateriaal. Dit onderzoek wordt uitgevoerd tijdens de Onderzoeksfase. Dit wordt gedaan om ervoor te zorgen dat er geen onduidelijkheden zijn tijdens de experimentele fase. Ook wordt hier een verwachting gesteld over hoe de protocollen reageren op een bepaalde situatie.

Experimenteel onderzoek
Bij een experimenteel onderzoek wordt een bepaalde omstandigheid gemanipuleerd om hiervan het effect te zien. Hierbij gaat het om het bouwen van een bepaalde testopstelling met een gewenst resultaat. Dit onderzoek wordt uitgevoerd in de Experimentele fase. Het experimenteel onderzoek is vooral gebruikt voor het testen van de protocollen en het uitvoeren van de metingen.

Vergelijkend onderzoek
Het testen van de vooraf gestelde testopstellingen en de vooraf bepaalde protocollen zijn een voorbeeld van zowel een vergelijkend onderzoek als een experimenteel onderzoek. Bij een vergelijkend onderzoek wordt het effect van verschillende omstandigheden op bepaalde variabelen gemeten. Ook dit onderzoek wordt uitgevoerd in de Experimentele fase. Dit onderzoek is gedaan om te kunnen adviseren of het migreren naar het Proof of Concept naast mogelijk ook daadwerkelijk wenselijk is.

Toegepast onderzoek
De resultaten van bovenstaande onderzoeken leiden uiteindelijk tot conclusies en aanbevelingen die direct toepasbaar zijn voor in de praktijk. Deze onderzoekmethode wordt veelal gebruikt bij onderzoeken die worden gedaan bij het schrijven van een scriptie bij een bedrijf. Dit onderzoek zal gebruikt worden in de adviseerfase.

2.1 Onderzoeksresultaten

In dit hoofdstuk zullen de resultaten van de hierboven genoemde onderzoeksmethoden samengevat beschreven worden. De gedetailleerde resultaten zijn te vinden in het Literatuur-, Experimentele onderzoeksrapport en Testdocument.

2.1.1 Literatuur onderzoek

Deelvraag 1: "Wat is STP?"

Sub-vraag1.1: "Hoe werkt STP in een switched core netwerk?"

Als resultaat uit het onderzoek naar het Spanning Tree Protocol blijkt dat zonder STP er loops ontstaan in een switched netwerk en dat er broadcast storms kunnen ontstaan. Hierdoor kan een netwerk vastlopen en zal het netwerk frames rond blijven sturen over het netwerk totdat er een switch crasht.

Ook werd duidelijk dat STP loops voorkomt door het blokkeren van de redundante verbindingen. Hierbij wordt een Root-switch gekozen waarlangs al het verkeer gaat. Nadat de Root-switch bepaalt is, kiest elke niet Root-Switch een path naar de Root-switch. Hierbij worden afwegingen gemaakt om te kijken welk path het efficiënts is. Als laatste worden de overgebleven paths vanaf één kant geblokkeerd door een switch. Hierbij wordt hetzelfde selectieproces uitgevoerd als voor het vinden van het beste path naar Root-switch.

Sub-vraag1.2: "Wat zijn nadelen van het Spanning Tree Protocol"

STP maakt door het blokkeren van de redundante verbinding niet optimaal gebruikt van de bandbreedte. Ook de omschakelingstijd als er een verbinding uitvalt, is langzaam bij STP. Hier zijn daarentegen wel het RSTP en MSTP ontwikkelt, dit zijn snellere vormen van STP. Als laatste is STP slecht schaalbaar(als het gehele netwerk moet veranderen), zal bij uitbreiding van het netwerk moeten de switches handmatig geconfigureerd worden.

Deelvraag 2: "Wat is TRILL?"

Sub-vraag2.1: "Hoe werkt TRILL in een switched core netwerk?"

Als resultaat uit het onderzoek naar TRILL blijkt dat TRILL geen verbindingen blokkeert om loops te voorkomen. TRILL maakt gebruik van het IS-IS routing protocol. Hierbij wordt het verkeer tussen de switches gerouteerd. Ook blijkt dat TRILL niet gebruik maakt van de standaard switches maar van switches die TRILL implementatie ondersteunen. Deze switches worden ook wel Rbridges genoemd.

Uit het onderzoek bleek ook dat Rbridges gebruik maken van een Hello conversatie om te achterhalen wie zijn neighbor is en waar deze zich bevindt. Bij TRILL wordt er een verzendende Rbridge gekozen deze staat ook wel bekend als een Designated Rbridge. De DRB zal een VLAN kiezen waarin de Rbridges onderling met elkaar communiceren. Hiernaast kiest de DRB ook een Appointed Forwarder(AF). Een AF zorgt ervoor dat een fysieke loop niet zorgt voor een broadcast storm. Een AF zal als enige Rbridge nog verkeer van een bepaald VLAN ontvangen en doorsturen. De andere Rbridges zullen niets met het frame doen.

Sub-vraag 2.2: "Welke varianten van TRILL zijn er?"

Naast de werking van TRILL op de Rbridges is er ook onderzoek gedaan naar relevante varianten van TRILL. Hieruit kwamen drie resultaten. FabricPath van Cisco, VCS van Brocade en SPB van Alcatel. Deze varianten zijn gekozen omdat Qi ict bv. veelal gebruik maakt van apparatuur van deze fabrikanten. Naast meerdere overeenkomsten tussen TRILL en de varianten zijn er ook nog een aantal verschillen.

Sub-vraag 2.3: "Wat zijn de verschillen tussen de varianten en TRILL?"
Cisco FabricPath vs. TRILL

- FabricPath is Cisco proprietary oplossing
- FabricPath heeft geen outer header
- STP en IGMP snooping is nodig op de edge om loops te voorkomen
- FabricPath leert niet alle remote node MAC-adressen
- FabricPath maakt geen gebruik van ESADI protocol

Brocade VCS vs. TRILL

- VCS is Brocade proprietary oplossing.
- VCS maakt gebruik van Fabric Shortest Path First (FSPF) routing protocol
- Ethernet Name Service(eNS) wordt er gebruikt voor MAC learning i.p.v. ESADI

SPB vs. TRILL

- SPB maakt de hele topologie bekend bij de edge switches.
- SPB gebruikt geen Rootswitch bij Multi-destination verkeer
- SPB gebruikt een andere Header
- SPB gebruikt een andere OAM
- SPB gebruikt voor unicast een andere loop prevention

Sub-vraag 2.4: "Welke randvoorwaarden zijn er om TRILL te implementeren?"
Sub-vraag 2.5: "Waar kunnen TRILL en de varianten het beste worden toegepast in een netwerk?"
Als laatste werd bij het onderzoek naar TRILL gekeken welke randvoorwaarden er zijn om TRILL te kunnen implementeren. Hierbij werd al duidelijk dat net als bij alle varianten er gebruik moet worden gemaakt van aparte switches. In het geval van de standaard TRILL, zal er gebruik worden gemaakt van Rbridges. Hierbij moet er gekeken worden welke switch fabrikanten TRILL 'ready' apparatuur leveren. Naast de apparatuur is er ook nog configuratie, echter is het zo dat TRILL gebruik maakt van een Plug&Play configuratie. Ook kan er nog gedacht worden aan waar TRILL geïmplementeerd wordt. Zo kan TRILL in alleen de Core worden geïmplementeerd of voor een efficiëntere manier van routeren in het hele netwerk.

Deelvraag 3: "Wat zijn de verschillen tussen STP en TRILL?"
Uit het onderzoek van STP kwam naar voren dat er gebruikt wordt gemaakt van het blokkeren van verbindingen om loops te voorkomen. Hierbij wordt niet de hele bandbreedte gebruikt. TRILL daarentegen maakt wel gebruik van de gehele bandbreedte.

Bij TRILL is het door het gebruik van alle verbindingen ook mogelijk om verkeer te loadbalancen over meerdere verbindingen. Dit wordt gedaan door het Equal Cost Multipath algoritme. Dit is bij STP niet mogelijk omdat er gebruik wordt gemaakt van het blokkeren van verbindingen.

Het blokkeren van verbindingen om loops voorkomen brengt bij STP een nadeel met zich mee. STP zal na het uitvallen van een verbinding 50 seconden verder zijn voordat het hele netwerk weer werkt. Hiervoor is al een ander protocol bedacht, het Rapid Spanning Tree Protocol (RSTP). RSTP werkt net als STP nog steeds met het blokkeren van verbindingen, maar de omschakelingstijd is vele malen sneller dan die van STP. RSTP doet er maar een aantal seconden over in plaats van de 50 seconden die STP nodig heeft. Nu is het wel het geval dat TRILL er maar een aantal milliseconden over doet in plaats van seconden.

Als laatste kwam er uit het onderzoek naar de protocollen dat STP slecht schaalbaar is. Als het netwerk uitgebreid moet worden, maar de huidige netwerkconfiguratie hetzelfde moet blijven, dan zal de nieuwe switch helemaal geconfigureerd worden. Hiervoor is ook een protocol bedacht door de IEEE groep, namelijk Multi Spanning Tree Protocol (MSTP). MSTP wordt vooral gebruikt als het netwerk met meerdere VLANs werkt, maar niet voor elk VLAN een aparte Distribution Tree moet

worden gecreëerd. MSTP maakt Distribution Trees per “instance” en aan een “instance” kunnen VLANs worden toegevoegd. Ook omdat er geen verbindingen geblokkeerd worden, is er minder configuratie nodig om TRILL te implementeren. De Rbridge zal zijn gegevens aan zijn neighbors laten weten door middel van Hello uitwisseling en daarna met het synchroniseren van de Link State Database (LSDB). Hierdoor weet de nieuwe Rbridge hoe hij de andere Rbridges kan bereiken en welk path de laagste Path Cost heeft.

Deelvraag 4: “Kan TRILL in de reeds bestaande infrastructuren worden geïmplementeerd?”

Sub-vraag 4.1: “Hoe ziet deze infrastructuur eruit?”

De topologie van de huidige infrastructuur is gebaseerd op één van de klanten waar Qi ict bv. het netwerk heeft aangelegd en beheerd. Hierbij gaat het om een netwerk dat de redundantie van de verbindingen beheert door middel van het Rapid Spanning Tree Protocol.

Uit de fysieke topologie werd duidelijk dat het netwerk in twee aparte datacenters kon worden opgedeeld. De apparatuur die gebruikt wordt zijn Alcatel Omniswitches. De beide datacenters hebben ieder een eigen Virtual Chassis dat de core vormt voor dat datacenter. Beide Virtual Chassis zijn full-mesh verbonden en vormen samen een collapsed core voor het gehele netwerk. Uit de logische tekening werd duidelijk dat VRRP wordt gebruikt om een Single point-of-Failure uit de core te voorkomen. Ook wordt duidelijk dat Access_Sw2 gebruik maakt van een Link Aggregation voor de verbindingen naar de Virtual Chassis.

Sub-vraag 4.2: “Wat zijn de huidig gebruikte protocollen?”

Virtual Chassis(VC) is een technologie die gebruik maakt van stack switches, hierbij worden meerdere switches met elkaar verbonden en worde de switches logische wijs gezien als 1 switch. De switches hebben samen 1 switch Fabric, 1 Control Plane, 1 Configuratie bestand en 1 Operating System. Virtual Chassis wordt gebruikt vanwege een aantal voordelen:

- Zorgt voor redundantie door meerdere switches te ‘stacken;
- Beter beheerbaar doordat alle switches 1 Config file gebruikt;
- Beter schaalbaard door de mogelijkheid om meerdere switches toe te voegen aan het VC.
- Efficiënter kabelbeheer.
- Lagere kosten, het aanschaffen van meerdere kleine switches, die onderdeel worden van een virtual chassis, zorgt voor de spreiding van kosten.

Virtual Router Redundancy Protocol(VRRP) is lid van de First-Hop Redundancy Protocol familie en is de IETF standaard. VRRP is een layer 3 redundantie protocol dat meerdere routers/switches voorziet van redundante routing services naar gebruikers. Virtual Router Redundancy Protocol wordt gebruikt voor het elimineren van het ‘single point of failure’ mede door het handmatig configureren van een default gateway adres op elke host in het netwerk.

Een Link Aggregation is het bundelen van meerdere parallelle verbindingen tot een enkele (logische) verbinding om de doorvoer van het netwerk verkeer te verhogen. Voor het samenvoegen van Ethernet verbindingen is het LACP protocol de standaard. LACP is de IEEE standaard, terwijl Link Aggregation meer als overkoepelende term wordt gebruikt. LACP wordt vanwege twee hoofdredenen gebruikt:

- Het verhogen van de capaciteit;
- Redundantie;

Het Rapid Spanning Tree Protocol is de snellere versie van de standaard Spanning Tree Protocol. Hierbij heeft STP het grote nadeel dat de omschakelingstijd bij het uitvallen van een verbinding hoog is. Dit is dan ook de reden waarom RSTP de voorkeur krijgt boven STP.

Sub-vraag 4.3: “Is er compatibiliteit mogelijk met de huidig gebruikte protocollen?”
Alle protocollen die hierboven zijn besproken zijn compatible met het Shortest Path Bridging protocol. Hierbij is het geval dat Virtual Chassis en VRRP niets met SPB te maken hebben. Deze protocollen draaien apart van elkaar. Het Link Aggregation Control Protocol (LACP) ziet niet welk protocol er over een verbinding loopt. LACP bundelt alleen verbindingen en is daarmee dus compatible met SPB. Als SPB in het netwerk alleen in bijvoorbeeld de core wordt geplaatst en RSTP blijft op de Access switches werken, dan moet er compatibiliteit zijn tussen de protocollen. Nu is het zo dat beide protocollen bedacht zijn door de groep van IEEE. Ook vallen beide protocollen onder de categorie van 802.1 protocollen. Zo is SPB 802.1aq en is RSTP 802.1w.

2.1.2 Experimenteel onderzoek

Deelvraag 5: "Hoe werkt de huidige situatie?"
Deelvraag 6: "Hoe werkt de nieuwe situatie?"

Om de deelvragen 5 en 6 te beantwoorden zijn twee sub-vragen gesteld. Bij de eerste sub-vraag wordt er gekeken naar de werking van de protocollen in het netwerk. Bij de tweede sub-vraag wordt er gekeken wat de resultaten zijn van de gehele netwerken op een aantal gebieden.

Sub-vraag 5.1: "Werken de gebruikte protocollen zoals uit de literatuur naar voren kwam?"
Sub-vraag 6.1: "Werken de gebruikte protocollen zoals uit de literatuur naar voren kwam?"

Voor het beantwoorden van sub-vraag 5.1 en 6.1 zijn de protocollen die in het netwerk draaien getest aan de hand van de achterhaalde informatie uit het Literatuur onderzoek. Het verschil in de testen is dat bij de huidige situatie RSTP is getest en bij de nieuwe situatie SPB. De verschillende tests zijn uitgevoerd om te achterhalen of de literatuur overeenkomt met de praktijk. Voor de uitgebreidere informatie zie het Testdocument. Uit de protocol tests kwam het volgende resultaat:

Tabel 1 Resultaten Virtual Chassis tests

Test case	Resultaat	Opmerkingen
Testcase P1	✓	
Testcase P2	✓	Het switchen van Slave naar Master duurt langer als dat in de literatuur staat aangegeven. Volgens de literatuur zou de gebruiker geen onderbreking ondervinden, echter is er een downtime van ongeveer 3 seconden
Testcase P3	✓	

Tabel 2 Resultaten VRRP tests

Test case	Resultaat	Opmerkingen
Testcase P4	✓	
Testcase P5	✓	
Testcase P6	✓	

Tabel 3 Resultaten LACP tests

Test case	Resultaat	Opmerkingen
Testcase P7	✓	
Testcase P8	✓	

Tabel 4 Resultaten RSTP tests

Test case	Resultaat	Opmerkingen
Testcase P9	✓	
Testcase P10	✓	
Testcase P11	✓	

Tabel 5 Resultaten SPB tests

Testcase	Resultaat	Opmerking
Testcase P9	✓	
Testcase P10	✓	
Testcase P11	✓	

Sub-vraag 5.2: "Wat zijn de waardes van het huidige netwerk?"
Sub-vraag 6.2: "Wat zijn de waardes van het nieuwe netwerk?"
Voor het beantwoorden van sub-vraag 5.2 en 6.2 zijn op zowel de huidige situatie als op het Proof of Concept (nieuwe situatie) verschillende test uitgevoerd. In overleg met de begeleider is er besloten de metingen uit te voeren die betrekking hebben op de volgende gebieden:

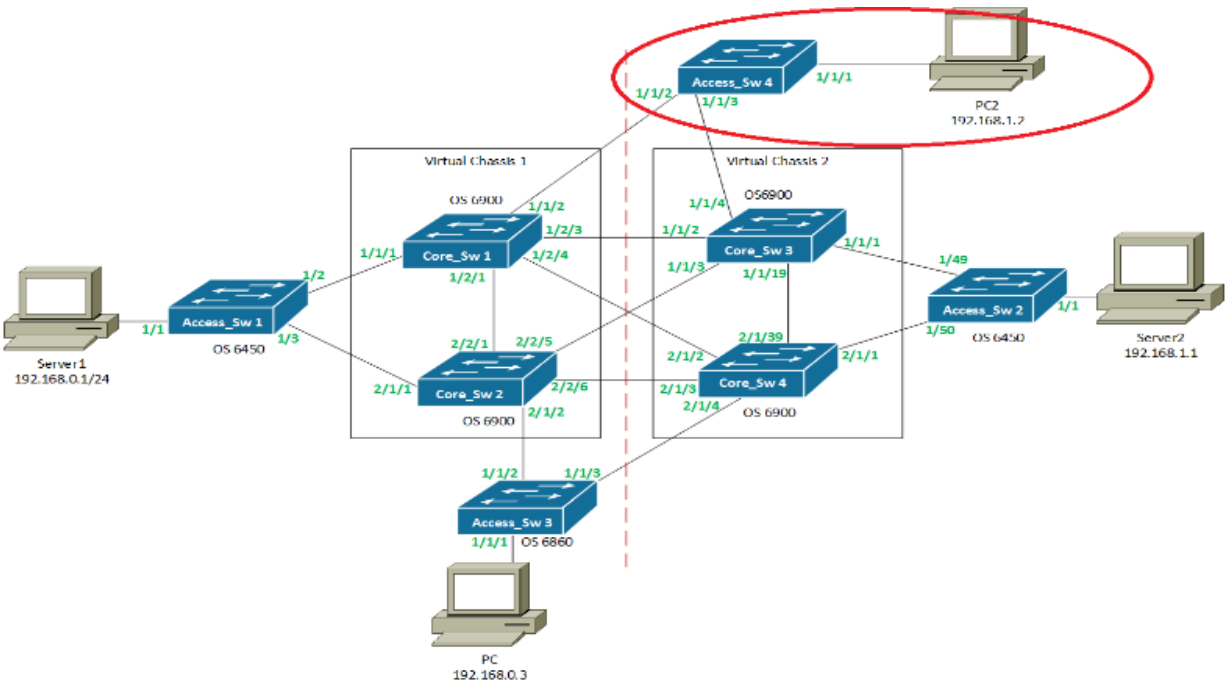
- Performance
- Scalability
- Reliability
- Availability
- Maintainability

Performance[1]
Met de performance wordt onder andere de snelheid van de bandbreedte bedoeld. Hierbij heeft ook de response tijd ook een groot aandeel. In dit geval zal er voornamelijk gekeken worden hoe snel de bandbreedte is en hoe groot de Latency is van een bericht.

Het controleren van de snelheid kan als volgt worden gedaan: Op de servers wordt een IPERF server opgestart, op de PC wordt een IPERF cliënt opgestart. IPERF kan de bandbreedte meten van een aantal pakketten dat gestuurd wordt via het IPERF applicatie. Ook wordt de Latency gemeten, hierbij wordt er een ping-bericht gestuurd van de PC naar de servers. Nu wordt er gekeken hoe lang het duurt voordat de PC een response bericht krijgt van de servers. Latency wordt aangeduid in ms.

Scalability[1]
De scalability houdt in of het netwerk uitbreidbaar kan worden met meerdere componenten, hierbij kan gedacht worden aan een extra datacenter of een gebruiker. Hierbij mag deze toevoeging geen gevolg hebben op de functionaliteiten van het netwerk. Om dit te testen zal er een gebruiker en switch worden toegevoegd. Dan wordt er gecontroleerd wat voor effect dit heeft op het netwerk.

Voor het testen van Scalability is het volgende ontwerp gebruikt, waarbij in de rode cirkel de toegevoegde componenten zich bevinden. Hierbij zal de switch met default instellingen aangesloten worden:



Figuur 1 Scalability ontwerp

Reliability[1]
Reliability is het consistente gebruik van het netwerk bij verandering. Dit kan zijn dat de datastroom over het netwerk data blijft sturen zonder dat het netwerk enige downtijd ondervindt. Dit kan getest worden door middel van een duurtest. Hierbij worden er ICMP-berichten van de PC naar de servers gestuurd en deze uitwisseling zal ±63 uur lang draaien. Na deze 63 uur zal er gecontroleerd worden of er enige downtijd heeft plaats gevonden.

Availability[1]
Bij availability wordt er bijgehouden of de gebruiker de servers kan bereiken. In het geval van dit netwerk moet de gebruiker, de twee servers kunnen bereiken. Ook bij uitval van verbindingen in het netwerk. Dit kan getest worden door het loskoppelen van kabels uit de opstelling, hierbij wordt dan gekeken of de berichten tussen de PC en de servers dan enige down tijd ondervindt.

Maintainability[1]
Met Manageability wordt het onderhouden van het netwerk zonder dat de werking daar effect van ondervind bedoeld. Hier wordt voornamelijk het vervangen van een switch bedoeld. Er zal getest worden of het netwerk enige hinder ondervindt als er een switch vervangen moet worden.

Tabel 6 Resultaten huidige situatie

Test case	Omschrijving Test case	Resultaat
Testcase M0	Werking situatie	✓
Testcase M1	Performance bandbreedte	Server1: 817 Mbps Server2: 693 Mbps
Testcase M2	Performance latency	Server1: <1 ms Server2: <1 ms
Testcase M3	Scalability	Ja
Testcase M4	Reliability	Server1: 99,997% Server2: 100%
Testcase M5	Availability	Server1: 99,918% Server2: 99,890%
Testcase M6	Maintainability	VC_Master: ±3 seconden VC_Slave: ±1 seconden Access switch: minimaal 4 minuten

Tabel 7 Resultaten Proof of Concept

Test case	Omschrijving Test case	Resultaat
Testcase M0	Werking situatie	✓
Testcase M1	Performance bandbreedte	Server1: 920 Mbps Server2: 700 Mbps
Testcase M2	Performance latency	Server1: <1 ms Server2: <1 ms
Testcase M3	Scalability	Ja; maar er zijn aanpassingen nodig in het netwerk
Testcase M4	Reliability	Server1: 99,999% Server2: 100%
Testcase M5	Availability	Server1: 99,969% Server2:99,969 %
Testcase M6	Maintainability	VC_Master: ±3 seconden VC_Slave: ±1 seconden Access switch: minimaal 4 minuten

Deelvraag 8: "Hoe wordt de oude situatie naar de nieuwe situatie gemigreerd?"

Sub-vraag 8.1: "Welke stappen moeten hiervoor worden genomen?"

Voor het beantwoorden van deelvraag 8 en sub-vraag 8.1 is er nagedacht over wat er gemigreerd moet worden en welke stappen er hiervoor worden genomen.

Stap 1 "*Default Gateway adressen op Access_Sw2 instellen.*"
Om er voor te zorgen dat er toch nog een default gateway is voor het netwerk zal deze buiten het SPB netwerk ingesteld moeten worden. Hierbij geldt dat in deze situatie alleen op de Access Switches die zich voor de servers begeven.

Stap 2 *"Het verwijderen van VRRP uit het netwerk."*
VRRP werkt niet binnen de SPB core en zal daarom ook niet meer van toepassing zijn voor het Proof of Concept. SPB kijkt namelijk niet naar het vlan of IP-adres dat bij het frame binnenkomt. SPB kijkt alleen naar de ISID van het frame en zal deze dan via het bijbehorende BVLAN rondsturen door het netwerk.

Stap 3 *"SPB zal geconfigureerd worden op de switches die de SPB-core vormen"*
Omdat RSTP en SPB compatible met elkaar zijn kan SPB geconfigureerd worden terwijl RSTP nog gebruikt wordt. Allereerst moet er een Backbone VLAN aangemaakt worden om het SPB verkeer over te laten switchen. Als dat gedaan is zullen de juiste poorten geconfigureerd worden voor SPB. Dit zijn de poorten die verbonden zijn met de andere switches die SPB ondersteunen.

Stap 4 *"Service aanmaken om ervoor te zorgen dat het verkeer het SPB netwerk in en uit kan."*
Het SPB netwerk kijkt alleen naar de ISID van een frame. Dit ISID moet echter wel aan een frame worden toegevoegd voordat deze door het SPB netwerk kan switchen. Hiervoor wordt een service aangemaakt met poorten waarop het verkeer binnenkomt.

Stap 5 *"RSTP zal disabled worden op de switches die SPB gebruiken."*
Nu dat alles voor SPB geconfigureerd is zal RSTP op de switches die het SPB netwerk vormen disabled worden. Hierbij gaat het om de switches VC1, VC2 en op de Access_Sw3 (OS6860).

Sub-vraag 8.2: "Welke voorwaarden zitten er aan de migratie stappen?"
Voordat er gemigreerd gaat worden moet er wel duidelijk zijn wat de voorwaarden zijn voor de migratie. Deze voorwaarden zijn vooraf opgesteld.

Voorwaarde 1: *"Het netwerk moet dezelfde functionaliteiten behouden"*
Hierbij zal de PC aan het eind van de migratie nog steeds beide servers kunnen bereiken.

Voorwaarde 2: *"RSTP wordt vervangen door SPB"*
RSTP zal tijdens de migratie uitgeschakeld worden op de switches die SPB ondersteunen. Hierbij wordt eerst SPB geconfigureerd voordat RSTP wordt disabled.

Voorwaarde 3: *"De apparatuur zal niet gewijzigd worden"*
Het netwerk zal op deze manier fysiek gezien hetzelfde blijven. Deze eis was al gesteld bij het ontwerpen van het Proof of Concept. Deze eis geldt daardoor ook voor de migratie.

2.1.3 Vergelijkend onderzoek

Deelvraag 7: "Werkt de nieuwe situatie beter als de oude?"

Sub-vraag 7.1: "In welk opzicht verschilt de nieuwe situatie met de oude situatie?"

Om deelvraag 7 en sub-vraag 7.1 te beantwoorden zullen de tests van het experimentele onderzoek met elkaar vergeleken worden om te concluderen welke situatie beter is en op welk opzicht de situaties van elkaar verschillen.

Tabel 8 Vergelijking test resultaten

Test case	Omschrijving Test case	Resultaat Huidige situatie	Resultaat Proof of Concept
Testcase M1	Performance (bandbreedte)	Server1: 817 Mbps Server2: 693 Mbps	Server1: 920 Mbps Server2: 700 Mbps
Testcase M2	Performance (latency)	Server1: <1 ms Server2: <1 ms	Server1: <1 ms Server2: <1 ms
Testcase M3	Scalability	Ja	Ja; maar er zijn aanpassingen nodig in het netwerk
Testcase M4	Reliability	Server1: 99,997% Server2: 100%	Server1: 99,999% Server2: 100%
Testcase M5	Availability	Server1: 99,918% Server2: 99,890%	Server1: 99,969% Server2:99,969 %
Testcase M6	Maintainability	VC_Master: ±3 seconden VC_Slave: ±1 seconden Access switch: minimaal 4 minuten	VC_Master: ±3 seconden VC_Slave: ±1 seconden Access switch: minimaal 4 minuten

Uit dit onderzoek valt te concluderen dat het Proof of Concept een betere Performance heeft qua bandbreedte; Een hogere Reliability heeft en een betere Availability. Echter is er ook configuratie nodig bij het uitbreiden van het netwerk. Hierdoor is het Proof of Concept minder schaalbaar als de huidige situatie.

De Latency en Maintainability zijn de enige twee tests waarbij de resultaten niet verschillen. Dit zal mede te maken hebben dat het gaat om dezelfde apparatuur en dat daardoor de tijd van het omschakelen van de switches bij het uitvallen van de VC_Master hetzelfde blijft.

3. Alternatieven

Om te kunnen concluderen of er voldaan is aan de migratie, moet er aan de vooraf opgestelde voorwaarden zijn voldaan. Dit waren de volgende voorwaarden:

Voorwaarde 1: *"Het netwerk moet dezelfde functionaliteiten behouden"*
Voorwaarde 2: *"RSTP wordt vervangen door SPB"*
Voorwaarde 3: *"De apparatuur zal niet gewijzigd worden"*

Om aan deze voorwaarden te voldoen blijven er na het onderzoek maar twee mogelijkheden over:

- Het deels migreren naar de SPB omgeving (zoals het Proof of Concept)
    - Het migreren van de Core en Access_Sw3
- Het niet migreren van de huidige situatie

Andere mogelijkheden zijn niet onderzocht en zullen onder het kopje Aanbevelingen gemeld worden. Hieronder wordt aangegeven wat de voor- en nadelen zijn van de wel onderzochte mogelijkheden.

Tabel 9 Voor- en nadelen migratiemogelijkheden

Huidige situatie	Proof of Concept
Voordelen Schaalbaar zonder dat er extra configuratie nodig is	**Voordelen:** Hogere bandbreedte Hogere Reliability Hogere Availability
Nadelen Lagere bandbreedte Lagere Reliability Lagere Availability	**Nadelen** SAP-poorten configuratie nodig als het netwerk uitgebreid wordt met niet-SPB ondersteunende switches. Ook als deze switch wel SPB zou ondersteunen, is het afhankelijk of aan de switch een End point hangt.

In onderstaande tabel zijn de verschillen nog duidelijk aangegeven met de bijbehorende cijfers:

Tabel 10 Resultaat verschillen migratiemogelijkheden

Gebied	Waardes Huidige situatie	Waardes Proof of Concept
Performance (bandbreedte)	Server1: 817 Mbps Server2: 693 Mbps	Server1: 920 Mbps Server2: 700 Mbps
Scalability	Ja	Ja; maar er zijn eventueel aanpassingen nodig in het netwerk
Reliability	Server1: 99,997% Server2: 100%	Server1: 99,999% Server2: 100%
Availability	Server1: 99,918% Server2: 99,890%	Server1: 99,969% Server2:99,969 %

4. Aanbevelingen

Op basis van de resultaten van het vergelijkend onderzoek is het zeker wenselijk om te migreren naar een SPB netwerk. Uit het vergelijkende onderzoek is te concluderen dat het Proof of Concept betere resultaten oplevert op het gebied van Performance, Reliability en Availability. Echter werd ook duidelijk dat als het netwerk uitgebreid wordt door een switch die SPB niet ondersteund, dat er dan extra configuratie nodig is. Ook als het een switch is die SPB ondersteunt is het nog mogelijk dat er configuratie moet worden toegevoegd. Een voorbeeld hiervan is het toevoegen van een OS6900 switch met een endpoint. Op de port waar het endpoint aan vast zit, zal dan als SAP-poort worden aangemaakt op de nieuwe OS6900, omdat anders het endpoint niet bereikbaar is door het SPB netwerk.

Uit het literatuuronderzoek werd ook duidelijk dat het wordt aangeraden om het hele netwerk te migreren naar een 'TRILL' omgeving. Dit zorgt namelijk voor meer mogelijkheden in het geval van best path. Echter is in dit onderzoek gefocust op een Layer 2 netwerk. Bij Layer 3 netwerken is niet duidelijk of het gebruik van SPB wenselijker is als RSTP. Hierdoor blijven er nog wel wat vragen over. Deze vragen leiden tot de volgende aanbevelingen:

Het uitzoeken werking SPB met een routed core
Tijdens dit onderzoek is er gefocust op het migreren van SPB in een Layer 2 netwerk. Hierbij is de werking van SPB met een routed core buiten beschouwing gelaten. Hierdoor is het niet duidelijk hoe SPB omgaat met de werking van een routed core.

Het uitzoeken van werking compleet SPB netwerk
In het onderzoek was één van de eisen dat de apparatuur in het netwerk niet zou veranderen. Hierdoor is er niet onderzocht wat de resultaten zijn als het gehele netwerk gemigreerd zou worden naar een SPB omgeving. Ook is niet duidelijk of hier dan nog extra configuratie nodig is door het verschil in subnetten van Server1 en Server2.

Literatuurlijst

[1] Cade, M., & Roberts, S. (2002, augustus) "*What Is System Architecture?*" http://www.informit.com/articles/article.aspx?p=29030&seqNum=5 (geraadpleegd 1 juli 2016)