Externe Bijlagen

Locator/ID Separation Protocol (LISP)

Shaun Smit

Gegevens afstuderen	
Student	Shaun Smit
Studentnummer	11086785
Bedrijfsmentor	Dhr. Prins
Bedrijf	Qi ict
1e examinator	Dhr. Maris
2e examinator	Dhr. Burghouwt
Versie	1.0

INHOUDSOPGAVE

I. AFSTUDEERPLAN

Informatie afstudeerder en gastbedrijf (*structuur niet wijzigen*)

Afstudeerblok: 2014-2.2 (start uiterlijk 17 november 2014)
Startdatum uitvoering afstudeeropdracht: 17 november 2014
Inleverdatum afstudeerdossier volgens jaarrooster: 23 maart 2015

Studentnummer: 11086785
Achternaam: dhr. Smit (*) *weghalen niet van toepassing*
Voorletters: S
Roepnaam: Shaun
Adres: Hendrik Tollensstraat 142
Postcode: 2624BK
Woonplaats: Delft
Telefoonnummer: 0639449018
Mobiel nummer: 0639449018
Privé emailadres: smit_shaun@hotmail.com

Opleiding: Technische informatica
Locatie: Delft (*) *weghalen niet van toepassing*
Variant: voltijd

Naam studieloopbaanbegeleider: S. van Peski
Naam begeleidend examinator: Dhr. Maris
Naam tweede examinator: Dhr. Burghouwt

Naam bedrijf: Qi ict
Afdeling bedrijf: Lan backbone
Bezoekadres bedrijf: Delftechpark 35-37
Postcode bezoekadres: 2628 XJ
Postbusnummer: 402
Postcode postbusnummer: 2600 AK
Plaats: Delft
Telefoon bedrijf: 015 888 04 44
Telefax bedrijf: 015 888 04 45

Internetsite bedrijf: https://www.qi.nl

Achternaam opdrachtgever: dhr. Ebben (*) *weghalen niet van toepassing*
Voorletters opdrachtgever: M.
Titulatuur opdrachtgever:
Functie opdrachtgever: Supervisor Remote Control
Doorkiesnummer opdrachtgever:
Email opdrachtgever: martijn.ebben@qi.nl

Achternaam bedrijfsmentor: dhr. Prins (*) *weghalen niet van toepassing*
Voorletters bedrijfsmentor: W.
Titulatuur bedrijfsmentor:
Functie bedrijfsmentor: Senior Netwerk Engineer
Doorkiesnummer bedrijfsmentor:
Email bedrijfsmentor: wouter.prins@qi.nl
NB: bedrijfsmentor mag dezelfde zijn als de opdrachtgever

Doorkiesnummer afstudeerder:
Functie afstudeerder (deeltijd/duaal):

Titel afstudeeropdracht:

Uitvoeren van een onderzoek naar de mogelijkheden en implementatie van het LISP protocol bij Qi ict te Delft.

Opdrachtomschrijving *(toelichtende tekst verwijderen)*

1. Bedrijf

Qi ict is een gespecialiseerd leverancier van hoogwaardige ict infrastructuurproducten en diensten. De missie van QI kan worden omschreven met de woorden "living uptime". Qi streeft ernaar om voor de ict infrastructuur van hun klanten een zo hoog mogelijke beschikbaarheid te realiseren. Tevens wordt deze beschikbaarheid door QI zo hoog mogelijk gehouden door hun grote voorraad reserve onderdelen en testlab voor nabootsing van klantsituaties. Verder worden de primaire werkzaamheden die voor de hoge beschikbaarheid zorgen dagelijks uitgevoerd door een team van ruim 100 werknemers die gezamenlijk al ruim 30 jaar Qi ict financieel gezond houden.

2. Probleemstelling

In de jaren tachtig werd het IPv4 protocol geïntroduceerd om connectiviteit tussen apparatuur te verkrijgen op de manier waarop wij tegenwoordig gewend zijn. Hierbij is het principe simpelweg dat een IP-adres bepaalt wat de identiteit (EID) is van het apparaat en het IP-adres beschrijft daarnaast ook de manier waarop het apparaat is verbonden aan het netwerk (RLOC). Er zijn echter meningen dat dit principe kan worden verbeterd, door de EID en RLOC parameters te scheiden om zo schaalbaarheid- en snelheidswinst te behalen in een netwerk. Een voorbeeld hiervan is het LISP protocol van Cisco. Dit protocol is echter nog experimenteel en zelden geïmplementeerd. Bij Qi ict is interesse in het gebruik van dit protocol en daarbij vooral de manier waarop het geïntegreerd kan worden in bestaande netwerken en in hoeverre het bestaande protocollen vervangt.

3. Doelstelling van de afstudeeropdracht

Het doel is om voor 23 maart 2015 een onderzoek te hebben uitgevoerd dat Qi ict inzicht geeft in het gebruik en de implementatie van het LISP protocol in het bestaande internet model. Het onderzoek dient een rapport en een testopstelling op te leveren die als basis gaat fungeren voor het beter adviseren van klanten die geïnteresseerd zijn in deze techniek.

4. Resultaat

Op het moment van succesvol voltooien van de opdracht beschikt Qi ict over een rapport dat inzicht geeft in het gebruik en de implementatie van LISP. In dit rapport zal de focus vooral liggen op implementatie van LISP in bestaande netwerken en in hoeverre het bestaande protocollen kan vervangen. Vervolgens kan Qi ict deze kennis gebruiken om nieuwe oplossingen te verkopen aan geïnteresseerde klanten.

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

Het afstuderen zal beginnen met het schrijven van een plan van aanpak. Hierin zal ik enkele zaken aankaarten die voor elk onderzoek van belang zijn, zoals de risico's, randvoorwaarden en de keuze van een aanpak methode. Wanneer dit is goedgekeurd door zowel mijn begeleiders van school als die van Qi ict zal ik met mijn begeleider van Qi ict verder in gesprek gaan over het probleemdomein. Het is de bedoeling om in dit gesprek te inventariseren in hoeverre er al onderzoek is gedaan naar LISP en de onderwerpen in kaart brengen die Qi ict minimaal onderzocht wilt hebben. Hieruit zullen ook enkele hoofd- en deelvragen naar voren komen voor het onderzoek.

Het volgende onderdeel is het onderzoek zelf. Hierbij zal ik aan de hand van literatuuronderzoek, antwoorden gaan zoeken op de eerder opgestelde vragen. Hieruit zal een onderzoekrapport komen naar de mogelijkheden van LISP. Deze mogelijkheden zullen in het

volgende deel van het afstuderen worden uitgewerkt en geïmplementeerd in een testopstelling, voor zo ver mogelijk.

Verder dient er natuurlijk een rapport te worden opgesteld die alle informatie samenvoegt en vervolgens gebruikt kan worden voor het geven van een advies aan Qi ict.

Kort samengevat komen de volgende werkzaamheden aan bod bij deze opdracht:

- *Schrijven plan van aanpak*
- *Analyseren probleemdomein*
- *Literatuur onderzoek LISP*
- *Ontwikkel- en implementatietraject testopstelling*
- *Schrijven adviesrapport*

De verschillende mijlpalen zijn:

- *Onderzoeksrapport naar LISP*
- *Een (werkende) testopstelling*
- *Adviesrapport*

6. Op te leveren (tussen)producten

De volgende documenten zullen worden opgeleverd:

- *Plan van aanpak*
- *Kort rapport over gesprek probleemdomein*
- *Onderzoekrapport naar LISP*
- *(Werkende) testopstelling met testplannen*
- *Adviesrapport*
- *(Eventueel) Presentatie voor collega engineers*

7. Te demonstreren competenties en wijze waarop

A1: Analyse van het probleemdomein

- *Door middel van gesprekken met Qi ict, zal ik de verschillende problemen inventariseren en bepalen wat de nodige veranderingen zijn. Met deze gegevens zal ik het probleemdomein opstellen.*

A3: Achterhalen van behoeften van belanghebbenden

- *Nadat de problemen zijn geïnventariseerd in competentie A1 zal ik deze gaan omzetten tot eisen en wensen. Hieruit zal een overzicht komen van werkzaamheden die minimaal uitgevoerd moeten worden om de opdrachtgever tevreden de stellen.*

C9: Ontwerpen van een infrastructuur

- *Wanneer het literatuuronderzoek is afgerond en de mogelijkheden van LISP op papier staan, dient er een infrastructuur te worden opgebouwd die de mogelijkheden in een praktijkomgeving nabootst.*

D18: Testen van een infrastructuur

- *De hierboven beschreven ontwikkelde testomgeving dient ook getest te worden om een goed beeld te krijgen hoe LISP reageert in de praktijk. Hiervoor zal ik een testplan uitwerken en uitvoeren.*

H5: Professioneel werken: Zelfstandig werken

- *Initiatief tonen, werkzaamheden snel oppakken en niet in paniek raken wanneer zaken in de problemen lijken te lopen.*

II. PLAN VAN AANPAK

INHOUDSOPGAVE

1. INLEIDING

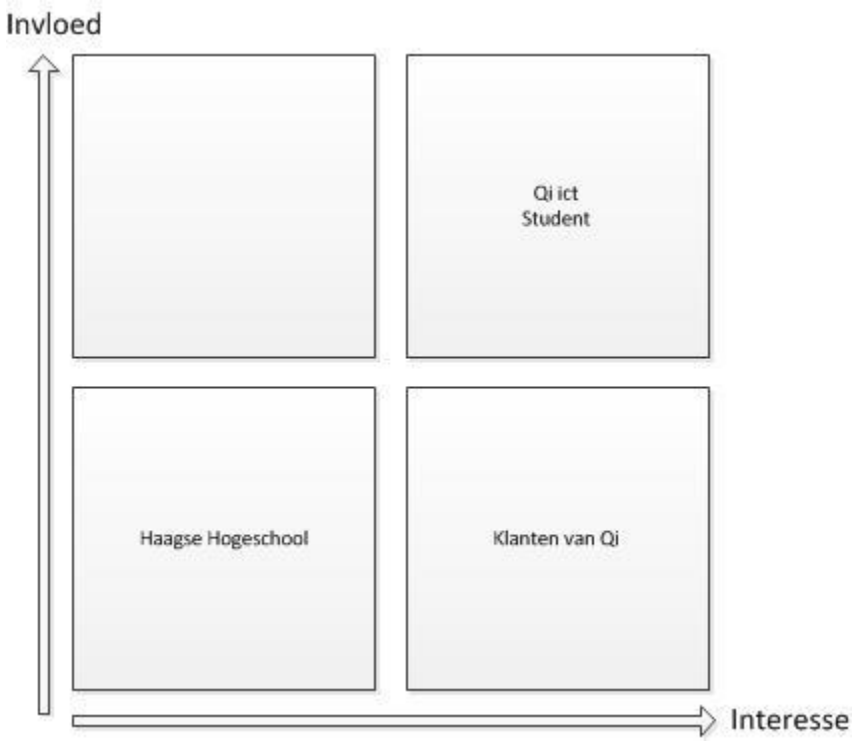
Als bedrijf dat ICT-oplossingen levert in verschillende sectoren is het belangrijk om het kennisniveau hoog te houden en te blijven innoveren. Om dit te doen is constant kennis nodig van de nieuwste technieken. Hiermee kan je tenslotte blijven voldoen aan de wensen van klanten. Dit document bevat de plan van aanpak om zo'n nieuwe techniek te onderzoeken; Cisco LISP. Dit protocol is ontwikkelend om de huidige vorm van IP-routing te vernieuwen op gebied van schaalbaarheid en simpliciteit. Het idee erachter is om het bestaande IP-adres van apparatuur op te delen in twee adressen waarbij de één bepaald wat de identiteit is van het apparaat en het tweede adres bepaald hoe de verbinding met het netwerk loopt. Hierdoor zouden bestaande problemen van schaalbaarheid in het huidige internetmodel opgelost kunnen worden, plus dat er ook voordelen tevoorschijn komen op het gebied van IP-mobility, IPv4-IPv6 transitie en multihoming.

Allereerst zal er inzicht worden gegeven in de achtergrond van het onderzoek en de betrokken partijen. Ten tweede wordt de projectopdracht verder uitwerkt met de aanleiding, probleemstelling, doelstelling en verwachte resultaten. Als derde worden de projectactiviteiten besproken door middel van de gekozen methodiek en fasering. Het volgende hoofdstuk omvat de eisen en wensen van het project met daarna de projectgrenzen om het onderwerp af te bakenen. Het zesde hoofdstuk geeft een overzicht van de op te leveren producten weer. Het zevende hoofdstuk geeft een overzicht van de organisatie waarin het project wordt uitgevoerd. Het achtste hoofdstuk geeft een overzicht van de planning en als laatste komen de risico's nog aan bod.

2. ACHTERGROND

Het onderzoek van deze afstudeerstage zal worden uitgevoerd bij Qi ict in Delft. Qi ict is een specialistisch bedrijf dat zich inmiddels al dertig jaar bezig houdt met ICT-oplossingen in de network-, security-, datacom-, en storage-sector en voert daarbij de motto “Living uptime”. Met deze motto in gedachte en de drijfveer om de beschikbaarheid van alle klanten zo hoog mogelijk te houden, zijn elke dag ruim honderd werknemers bezig met de dagelijkse werkzaamheden. Het onderhouden van deze netwerken is echter maar één kant van het verhaal. De werknemers van Qi moeten ook constant nieuwe technieken onderzoeken om aan de wensen van klanten te kunnen blijven voldoen. Het onderzoek naar de mogelijkheden van LISP vallen hier ook onder.

Hieronder bevindt zich een diagram die de stakeholders van het onderzoek aangeven. Hiermee wordt geïnventariseerd welke partijen in welke mate invloed en interesse in het onderzoek hebben.



Figuur 2.1 – Stakeholders onderzoek

De student die het onderzoek uitvoert en Qi ict zelf vallen rechtsboven in de categorie met veel interesse en invloed. Zij zullen samen in overleg bepalen welke richting wordt gekozen in het onderzoek en welke informatie precies bruikbaar is. De klanten van Qi ict, een daarbij een select aantal, heeft interesse in de mogelijkheden van LISP, maar zullen verder geen invloed uitoefenen. Als laatste is er nog de Haagse Hogeschool die vooral geïnteresseerd is in de voortgang van de student, niet zozeer in het onderzoek zelf.

3. PROJECTOPDRACHT

Dit hoofdstuk omvat informatie over de projectopdracht zoals die door Qi ict is omschreven. Hierin worden de aanleiding, probleemstelling, doelstelling en verwachte resultaten besproken.

3.1 AANLEIDING

Qi ict werkt inmiddels al dertig jaar aan ICT-oplossingen binnen verschillende sectoren om de beschikbaarheid van klantennetwerken zo hoog mogelijk te houden. Om dit te doen is het nodig om te blijven innoveren en op de hoogte te zijn van de nieuwe technieken. Het LISP protocol van Cisco (Cisco, 2012) is één van die technieken waar interesse in is en om die reden is er een onderzoek gestart naar de mogelijkheden.

3.2 PROBLEEMSTELLING

In de jaren tachtig werd het IPv4 protocol geïntroduceerd om connectiviteit tussen apparatuur te verkrijgen op de manier waarop wij tegenwoordig gewend zijn. Hierbij is het principe simpelweg dat een IP-adres bepaalt wat de identiteit (EID) is van het apparaat en het IP-adres beschrijft daarnaast ook de manier waarop het apparaat is verbonden aan het netwerk (RLOC). Er zijn echter meningen dat dit principe kan worden verbeterd, door de EID en RLOC parameters te scheiden om zo schaalbaarheid- en snelheidswinst te behalen in een netwerk. Een voorbeeld hiervan is het LISP protocol van Cisco. Dit protocol is echter nog experimenteel en zelden geïmplementeerd. Bij Qi ict is interesse in het gebruik van dit protocol en daarbij vooral de manier waarop het geïntegreerd kan worden in bestaande netwerken en in hoeverre het bestaande protocollen vervangt.

3.3 DOELSTELLING

Het doel is om voor 23 maart 2015 een onderzoek te hebben uitgevoerd dat Qi ict inzicht geeft in het gebruik en de implementatie van het LISP protocol in het bestaande internet model. Het onderzoek dient een rapport en een testopstelling op te leveren die als basis gaat fungeren voor het beter adviseren van klanten die geïnteresseerd zijn in deze techniek.

3.4 VERWACHTE RESULTATEN

Op het moment van succesvol voltooien van de opdracht beschikt Qi ict over een rapport dat inzicht geeft in het gebruik en de implementatie van LISP. In dit rapport zal de focus vooral liggen op implementatie van LISP in bestaande netwerken en in hoeverre het bestaande protocollen kan vervangen. Vervolgens kan Qi ict deze kennis gebruiken om nieuwe oplossingen te verkopen aan geïnteresseerde klanten.

4. PROJECTACTIVITEITEN

Dit hoofdstuk omvat de verschillende activiteiten die moeten worden uitgevoerd aan de hand van de gekozen methodiek. Verder zullen er ook verschillende beslismomenten en bijbehorende taken worden vermeld.

4.1 METHODIEK

Het onderzoek dat besproken wordt in dit plan van aanpak bestaat uit twee hoofdonderdelen. Allereerst dient er een literatuuronderzoek uitgevoerd te worden die inzicht biedt in de werking, voor- en nadelen van LISP en ten tweede dienen verschillende demo-opstellingen ontwikkeld te worden waarmee getest kan worden of de eerder gevonden theorie ook daadwerkelijk in de praktijk zich zo uit. Om deze twee hoofdonderdelen samen te voegen en beheersbaar te houden dient er een geschikte methode gevonden te worden. De volgende speerpunten zijn opgesteld om een selectie te maken uit de grote hoeveelheid bestaande methoden.

- **Beheersbaarheid voor een individu**. Het onderzoek wordt uitgevoerd door één afstudeerder wat betekent dat alle processen simpel en beheersbaar moeten zijn. Grote onderzoeksmethoden zoals Prince2 die normaal door complete teams worden gehanteerd om alle processen te beheersen vallen voor dit onderzoek buiten de boot.
- **Ruimte voor uitgebreide literatuur onderzoek**. Het literatuuronderzoek dat van toepassing is op dit project is niet een korte fase van bronnen zoeken om uiteindelijk een product op te leveren. Het literatuuronderzoek van dit project is al een groot deel van het product. Qi ict wilt namelijk graag een onderzoeks- en advies rapport over de werking en geschiktheid van LISP.
- **Weinig extra documentatie**. Vanuit de Haagse Hogeschool worden al meerdere eisen gesteld aan de literatuur die verplicht opgeleverd moet worden en daarnaast heeft Qi ict alleen behoefde aan het onderzoeks- en advies rapport. Elk document dat erbij komt is van weinig interesse voor zowel de hogeschool als het bedrijf, wat betekent dat het simpelweg extra overbodig werk is voor de student. Een methode die weinig extra documentatie genereerd is gewenst.

Met deze speerpunten in gedachte is besloten verder te kijken naar de mogelijk vormen van onderzoek. Voor het eerste gedeelte van het onderzoek waarbij informatie gezocht en geïnventariseerd wordt zijn kwalitatief en kwantitatief onderzoek het meest bekend. Kwalitatief onderzoek richt zich vooral op de diepgang van de informatie terwijl kwantitatief onderzoek zich vooral richt op de hoeveelheid.

Kwalitatief	Kwantitatief
Observatieonderzoek - Hier wordt alleen gelet op gedragingen die interessant zijn voor het onderzoek - Kleine groepen	**Surveyonderzoek** - Voor het bijhouden van opinies, meningen of kennis van grote groepen - Informatie wordt verzameld door het uitvoeren van enquêtes en vragenlijsten
Open Interview - Gebruikt voor het bijhouden van belevingen en motieven in een kleine groep	**Secundaire analyse** - Een analyse uitvoeren op basis van eerder verzameld werk. Dit kan informatie zijn van een andere onderzoeksgroep
Literatuuronderzoek - Algemene technieken waarbij literatuur wordt gebruikt voor het zoeken van informatie over een onderwerp	**Experimenteel onderzoek** - Onderzoek op basis van hypothesen en experimenten. - Gebruikt om effecten te meten

Een keuze maken tussen kwalitatief en kwantitatief onderzoek is in dit geval lastig. Voor het zoeken van informatie om de vragen van de opdrachtgever te beantwoorden lijkt kwalitatief onderzoek de enige optie, maar met het feit dat dit onderzoek ook testresultaten oplevert met demo-opstellingen dat gaat helpen bij het advies leveren geeft aan dat kwantitatief onderzoek ook een optie is. In dit geval lijkt de enige optie een combinatie tussen kwalitatieve literatuur onderzoek en kwantitatieve experimenteel onderzoek.

Het uitvoeren van literatuuronderzoek zelf is een redelijk eenvoudig proces en is vaak geen onderzoeksmethode op zichzelf, maar juist een onderdeel van een grotere methode. Dat idee wordt in dit onderzoek ook toegepast, wat betekent dat er een methode gezocht moet worden die aan de ene kant kwalitatieve literatuuronderzoek toelaat en anderzijds ruimte houdt voor het ontwikkelen van een product met daarbij kwantitatieve onderzoek voor het advies. De verschillende vormen van methoden voor productontwikkeling zijn als volgt.

Iteratief	Incrementeel	Waterval
Iteratieve ontwikkeling bestaat uit het ontwikkelen van een voorlopige versie, vervolgens feedback vragen en dat verwerken in een nieuwe versie	Incrementeel ontwikkelen omvat het uitbrengen van verschillende releases waarbij steeds meer functionaliteit wordt bijgevoegd	Bij de watervalmethode verloopt het ontwikkelen in meerdere fasen, waarbij de ene fase pas mag worden aangeroepen als de voorgaande fase helemaal af is. Aan het eind van alle fasen is er een volledige product afgeleverd
Voorbeelden: - RUP - Spiraalmodel - Test-Driven Development		Voorbeelden: - Model van Royce - Sashimi model - AORTA - SDM

Om de afweging te maken tussen de bovenstaande methoden is gekeken naar de wensen van de opdrachtgever. Die heeft geen behoefte halve producten of een voorlopige versie die steeds vernieuwd wordt. De opdrachtgever heeft behoefte aan kennis in een hapklare vorm, die vervolgens aan de hand van demo-opstellingen kan worden gepresenteerd aan collega engineers en klanten. Met dit in gedacht is besloten de iteratieve en incrementele methoden te laten vallen en verder te focussen op de watervalmethode.

Binnen de watervalmethode zijn er ook nog een tal van methoden te onderscheiden die elk op hun beurt weer voor- en nadelen hebben. Met de reden dat de opstellingen puur als demo zullen fungeren en geen productienetwerken zullen zijn, is er gekozen voor een generieke watervalmethode. Deze methode is gemakkelijk beheersbaar, fouten kunnen gemakkelijk worden herstelt en er kan gebruik worden gemaakt van mijlpalen om de voortgang te meten. Verder is er binnen de analysefase van de methode ruimte om literatuuronderzoek te doen.

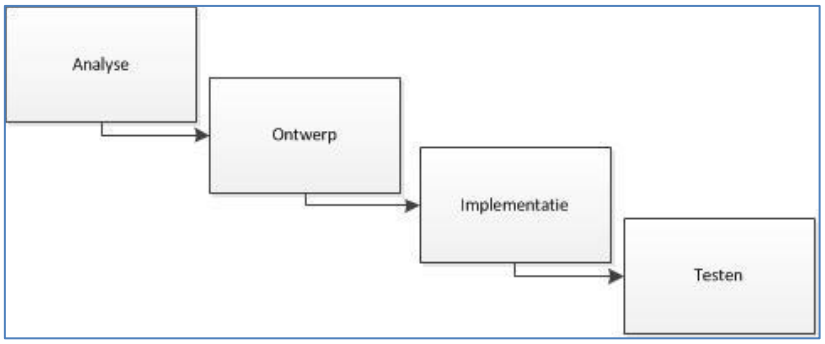
Als laatste rest zich nog de manier waarop het literatuuronderzoek gedaan wordt. Hoewel het wellicht niet nodig is om een specifieke methode te kiezen voor bronnenonderzoek is er toch gekozen om aan de hand van systematisch literatuur zoeken (Groningen, 2012) van de universiteit van Groningen te werken. Via deze methode kan gegarandeerd worden dat relevante bronnen niet overgeslagen worden, omdat je begint met wetenschappelijk bronnen en vervolgens van elk artikel de referenties gaat volgen. Dit wordt ook wel de sneeuwballenmethode genoemd.

4.2 Fasering en besluitmomenten

De watervalmethode die in het vorige hoofdstuk is beschreven bestaat uit verschillende fasen, namelijk de analyse-, ontwerp-, implementatie-, test- en onderhoudsfase. Hoewel de onderhoudsfase in dit geval geschrapt mag worden, omdat het niet om productienetwerken gaat zijn de andere fasen wel belangrijk. Verder bevatten alle fasen een bepaald moment waarbij er doorgezet mag worden naar de volgende fase. Deze fasen en beslismomenten worden toegelicht in het volgende overzicht.

Fase	Werkzaamheden	Besluitmomenten
Analyse: - Oriëntatie en afbakeningen - Systematisch zoeken - Proces en opbrengst evalueren	- Programma van eisen opstellen - Opstellen onderzoeksvragen - Literatuur onderzoek uitvoeren - Schrijven onderzoeksrapport - Testcases analyseren	Wanneer er voldoende informatie is verzameld en de opdrachtgever tevreden is met de antwoorden op alle vragen zal worden doorgegaan met het opzetten van demo-opstellingen.
Ontwerp:	- Ontwerprapport schrijven - Testplannen schrijven	Wanneer het ontwerprapport in voldoende mate beschrijft welke testopstellingen gebouwd gaan worden en de opdrachtgever akkoord geeft mag worden voortgezet naar de volgende fasen van implementatie.
Implementatie:	- Opbouwen en uitwerken van de opstellingen die bepaald zijn in de testcases	Aan de hand van de beschikbare apparatuur zal besloten worden of de implementatie en testfase samen worden uitgevoerd of na elkaar. Er is gekozen om een demo-opstelling volledige uit te werken en wanneer deze volledig operationeel is door te gaan naar de volgende fase om deze te testen.
Test:	- Testen van de opstellingen - Schrijven adviesrapport	n.v.t

Een visuele weergave van deze fasen is hieronder weergeven:



Figuur 4.1 – Fasen overzicht

5. WENSEN

Het protocol dat onderzocht gaat worden is experimenteel en zelden geïmplementeerd wat het opstellen van eisen en wensen lastig maakt. In overleg met de opdrachtgever zijn de onderstaande wensen opgesteld die in een later stadium zullen worden omgezet tot eisen. Hiervoor zal een programma van eisen worden geschreven. Deze eisen zullen later de basis vormen van de onderzoeksvragen die vervolgens beantwoordt en beoordeelt worden op volledigheid. De volgende lijst is opgesteld:

Gedurende het onderzoek dient een rapport te worden opgeleverd met de volgende elementen:

- Er dient achtergrond informatie gegeven te worden over het LISP protocol, zoals het ontstaan ervan, op welke protocollen het is gebaseerd en welke problemen uit het huidige internetmodel dat het mogelijk oplost.
- Er dient informatie gegeven te worden over de werking van LISP en wat er minimaal nodig is om het protocol te gebruiken in een netwerkomgeving. Hierbij kan gedacht worden aan zaken als apparatuur en topologie.
- Er dient een overzicht gemaakt te worden van de voor- en nadelen van LISP.
- Er dient een vergelijking aanwezig te zijn waarbij huidige IP-routing, tunnel- en overlay technieken worden vergeleken met LISP. De volgende protocollen dienen minimaal vergeleken te worden.
    - BGP
    - OSPF
    - IS-IS
    - MPLS
- Er dient een overzicht gemaakt te worden van de meest interessante technieken die LISP beschikbaar maakt of vernieuwd. Belangrijk hier is dat er ook een betogend wordt omschreven in welk opzicht LISP vernieuwend en/of beter werkt dan huidige protocollen.
- Er dient een afweging gemaakt te worden in welke mate LISP geschikt is voor klanten van Qi ict. Voorbeelden zijn datacenters, Service Providers en Enterprise klanten.

Het onderzoek zal in de tweede fase een aantal demo-opstellingen opleveren die aan het volgende moeten voldoen op basis van het LISP protocol:

- Een opstelling die multi-homing toelaat zonder het BGP protocol
- Een opstelling met IPv4 en IPv6 transitie actief
- Een opstelling met VM mobility

Na voldoende informatie over de werking van LISP in theorie en de praktijk dient een adviesrapport te worden opgeleverd over de mate waarin LISP aantrekkelijk is voor Qi. Dit rapport bevat de volgende onderdelen:

- In hoeverre het LISP protocol aantrekkelijk is voor internet netwerken van ISP’s
- In hoeverre het LISP protocol aantrekkelijk is voor internet netwerken van Enterprises
- In welke mate er oplossingen worden geboden voor omgevingen die LISP adopteren

In het kader van kwaliteitsbeheersing van het onderzoek en om te garanderen dat deze wensen voldoende worden uitgewerkt zal om de twee weken een voortgangsgesprek plaatsvinden met de opdrachtgever.

6. PROJECTGRENZEN

In dit hoofdstuk worden de verschillende projectgrenzen bepaald voor het onderzoek. Dit met de reden dat Cisco LISP op verschillende manieren ingezet kan worden en daarbij zijn niet alle aspecten interessant voor Qi ict. Verder is het belangrijk dat er door beperkte tijd goed afgebakend wordt er onderzocht moet worden, zodat er in een later stadium niet allerlei onderdelen half werk wordt afgeleverd. Allereerst zullen hieronder verschillende zaken worden opgesomd die bij het onderzoek betrokken zouden kunnen worden en daarna zal worden aangegeven wat minimaal gebruikt moet gaan worden om Qi ict tevreden te stellen aan het eind van het onderzoek.

Mogelijke protocollen die LISP zou kunnen vervangen en die in het onderzoek vergelijken zouden kunnen worden:

- BGP
- EIGRP
- IS-IS
- OSPF
- RIPv2
- MPLS
- GRE
- IPIP

Technieken die door Cisco worden aangegeven als ideaal voor LISP en welk gebruikt zouden kunnen worden als demo-opstelling en vergelijkingsmateriaal in het onderzoek:

- Multi-homing
- IPv6 Transition Support
- VM Mobility
- Network Virtualization

Mogelijke partijen om onderzoek op af te stemmen:

- Datacenters
- Enterprise
- Small Business
- ISP netwerken
- Intern netwerk Qi

Met de bovenstaande protocollen, technieken en partijen opgesomd is het duidelijk dat er genoeg elementen zijn om een rapport mee te vullen. Het is echter ook duidelijk dat het ene element belangrijker is dan de ander en dat er wellicht teveel is om in achttien weken te onderzoeken. Om die reden is er na een gesprek met de opdrachtgever besloten om eerst de volgende zaken te onderzoeken en bij voldoende tijd de andere onderdelen aan te roepen.

Protocollen: BGP, MPLS, OSPF, IS-IS

Technieken: Multi-homing, IPv6 Transition, IP Mobility

Partijen: Enterprise, ISP netwerken

De reden voor de bovenstaande keuzes zal in het afstudeerdossier verder worden toegelicht. Kort samengevat bevatten deze protocollen en technieken in combinatie Enterprise en ISP netwerken de meest voorkomende situaties waar Qi ict haar geld aan verdiend. Deze zijn om die reden het meest interessant.

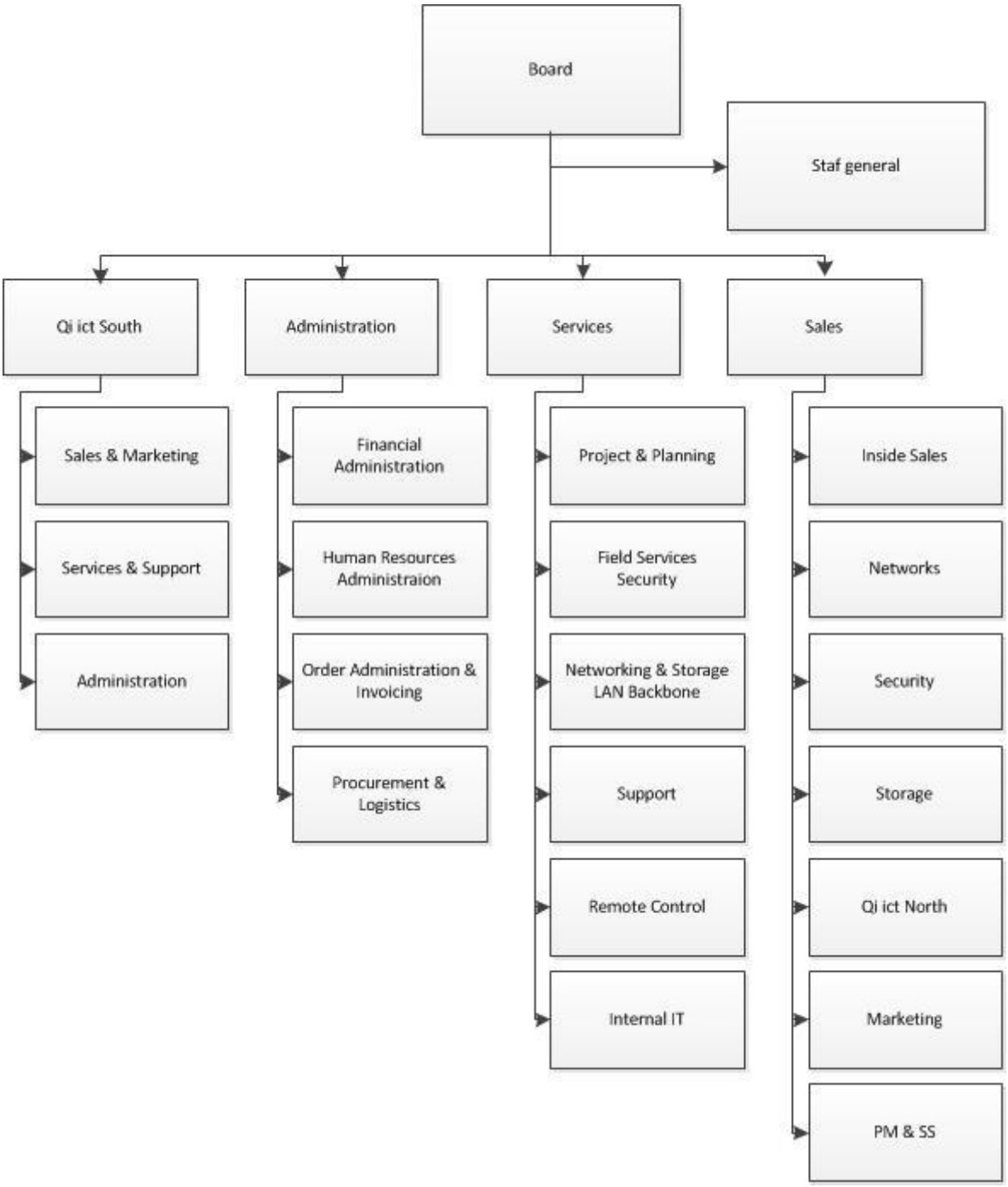
7. PRODUCTEN

Tijdens het onderzoek zullen in alle fasen verschillende producten worden geproduceerd en opgeleverd. De volgende lijst is daar een overzicht van.

- **Plan van aanpak.** Dit is het huidige document.
- **Programma van eisen.** De wensen uit het huidige document zullen verder worden omgezet tot eisen. Die worden in het programma van eisen verwerkt wat vervolgens door de opdrachtgever wordt goedgekeurd en ondertekend.
- **Onderzoekrapport naar LISP**. Dit document bevat achtergrond informatie over de werking van LISP, welke protocollen het vervangt, wat er nodig is voor de werken en mogelijke partijen voor wie het aantrekkelijk is.
- **Ontwerprapport**. Dit document bevat de uitwerkingen van de testcases die gekozen zijn naar aanleiding van het onderzoeksrapport.
- **Testopstellingen met testplannen.** De opstellingen uit het ontwerprapport die met hardware zijn gebouwd en vervolgens getest aan de hand van testplannen.
- **Adviesrapport.** Dit rapport zal informatie bevatten over de voor- en nadelen van LISP van klanten en in hoeverre het geschikt is om LISP te adopteren.
- **(Eventueel) Presentatie voor collega engineers**

8. PROJECTORGANISATIE

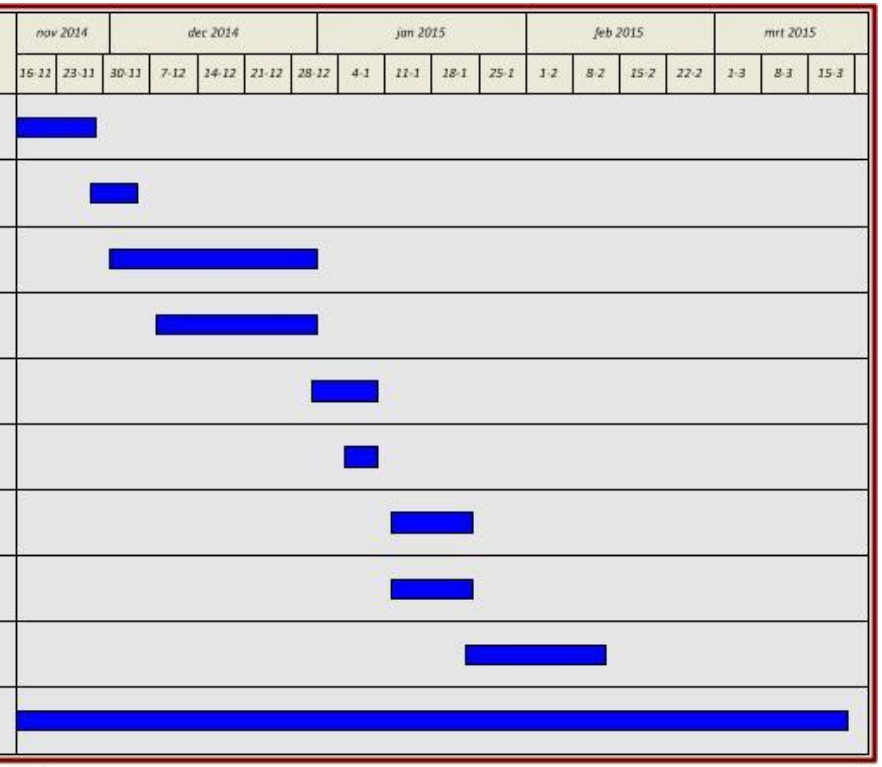
Hieronder bevindt zich een overzicht van de organisatie waarin het onderzoek plaatsvindt. De afdeling waar vanuit het onderzoek wordt uitgevoerd en begeleid is “Networking & Storage”. Op deze afdeling houden zij zich vooral bezig met de onderste lagen van het OSI-model en daar past het LISP protocol goed tussen. De begeleiding vanuit deze afdeling wordt geregeld door “Senior network engineer” Wouter Prins.



9. PLANNING

De eerder benoemde onderdelen in de activiteitenlijst zijn hierin omgezet tot een planning. Het is echter wel een ruime schatting. Voor het onderzoek staat in principe maximaal achttien weken, maar in hoeverre de verschillende onderdelen tijd gaan kosten is bijzonder lastig in te schatten.

Id	Taaknaam	Begindatum	Einddatum	Duur
1	Orientatie en afbakening Product: Plan van aanpak/Onderzoeksvragen	17-11-2014	28-11-2014	2w
2	Eisen opstellen Product: Programma van Eisen	28-11-2014	4-12-2014	1w
3	Systematisch zoeken	1-12-2014	31-12-2014	4,6w
4	Proces en opbrengst evaluren Product: Onderzoeksrapport	8-12-2014	31-12-2014	3,6w
5	Ontwerpen kiezen en uitwerken Product: Ontwerprapport	31-12-2014	9-1-2015	1,6w
6	Testplannen schrijven	5-1-2015	9-1-2015	1w
7	Opbouwen en uitwerken van opstellingen	12-1-2015	23-1-2015	2w
8	Testen van de opstellingen	12-1-2015	23-1-2015	2w
9	Schrijven adviesrapport	23-1-2015	12-2-2015	3w
10	Afstudeerddossier bijhouden	17-11-2014	20-3-2015	18w



Analysefase

Ontwerpfase

Implementatiefase

Testfase

Mijlpalen onderzoek:

- Plan van aanpak	(28/11/2014)
- Programma van eisen	(04/12/2014)
- Onderzoeksrapport	(31/12/2014)
- Ontwerprapport	(09/01/2015)
- Testopstellingen	(23/01/2015)
- Adviesrapport	(12/02/2015)

Mijlpalen School:

- Plan van aanpak	(28/11/2014)
- Voortgangsverslag	(12/01/2015)
- Dossier v1	(02/02/2015)
- Dossier v2	(23/02/2015)
- Dossier vDef	(23/03/2015)

10. RISICO'S

In elk onderzoek zijn risico's die het succes kunnen beïnvloeden. Deze zijn hieronder geïnventariseerd met bijbehorende maatregelen voor wanneer deze voorkomen.

Risico	Kans	Maatregel
Tijdnood door verkeerde inschatting van werkzaamheden	Middel	Zorgen voor een ruime planning met ruimte voor fouten en een constante beheersing van de tijd. Ook erkenning van problemen is belangrijk. Hoe eerder een probleem bekend is bij de begeleiding, hoe eerder er hulp ingeschakeld kan worden.
Geen beschikking over de nodige hardware om een testopstelling te ontwikkelen	Klein	Qi beschikt over een zeer grote voorraad apparatuur dus de kans is klein. Echter mocht het voorkomen dat er geen apparatuur is zal er moeten worden gekeken of er direct iets met Cisco kan worden geregeld.
Afwezigheid begeleiding wat tot oponthoud zorgt	Middel	De engineers van Qi ict doen veel werk buiten de deur. Dat geldt ook voor de begeleiders van studenten. Door te zorgen voor een goede planning die rekening houdt met afwezigheid van de begeleider moet het niet voor teveel problemen zorgen. Verder kan door communicatie via telefoon en e-mail al zeer veel geregeld worden. Ook is er tweewekelijks een vaste tijd ingesteld waarbij de begeleider tijd maakt voor de student om de voortgang te bespreken.
LISP is een experimentele techniek dus de kans bestaat dat het niet werkt, ondanks alle documentatie	Klein	Het adviesrapport zal omgevormd moeten worden naar een negatief advies. Het antwoord "Nee, het werkt niet" is ook een antwoord voor een onderzoek, maar het brengt de planning wel in de war.

11. LITERATUURLIJST

Cisco. (2012, 02 01). *Cisco Locator/ID Separation Protocol.* Opgeroepen op 11 26, 2014, van www.cisco.com: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/locator-id-separation-protocol-lisp/datasheet_c78-576698.pdf

Groningen, R. (2012, 10 30). *Systematisch literatuur zoeken*. Opgeroepen op 11 26, 2014, van www.rug.nl: http://www.rug.nl/education/other-study-opportunities/hcv/schriftelijke-vaardigheden/voor-studenten/bronnen-literatuur/systematisch-literatuur-zoeken

III. PROGRAMMA VAN EISEN

Het onderzoek bestaat uit drie delen. Allereerst wordt er informatie verzameld over het protocol. Hiermee kunnen verschillende vragen worden beantwoord die door de opdrachtgever zijn gesteld. Dit levert uiteindelijk een onderzoeksrapport op. Aan dit document worden enkele eisen gesteld aan de inhoud welk hieronder zullen worden benoemd. Het tweede deel is het ontwerpen van testopstellingen. De eisen hieraan kunnen slechts globaal worden bepaald aangezien er informatie nodig is uit de literatuurstudie om definitieve eisen te bepalen. De laatste fasen omvat het testen en schrijven van een adviesrapport. Ook hier kunnen wel enkele globale eisen worden opgesteld, maar ook hier zijn het eisen die gegarandeerd gaan evolueren in de toekomst.

ONDERZOEKSRAPPORT

- Het rapport dient algemene informatie te bevatten over het LISP protocol. Elementen die hierin moeten voorkomen zijn als volgt:
    - Globale werking van het huidige netwerkmodel met de nadruk op IP-routing en de huidige problemen met het model
    - Ontstaan van LISP
    - Op welke mechanismen en/of protocollen het is gebaseerd
    - Welke problemen mogelijk door LISP opgelost kunnen worden
- Het rapport bevat informatie over de werking van LISP met hierin de volgende elementen:
    - De werking van LISP op protocol laag.
        - Control- en data plane
        - Mapping system technieken
        - LISP encapsulation
    - De minimale topologie vereisten die nodig zijn om LISP te implementeren in een netwerk
        - LISP – to – LISP
        - LISP – to – Non-LISP
        - Non-LISP – to - LISP
    - In welke mate apparatuur en/of software nodig is om LISP te kunnen gebruiken
- Het rapport bevat informatie van LISP in vergelijking met andere routingprotocollen. Hierin minimaal te verstaan, de protocollen BGP, OSPF, IS-IS en MPLS. Verder dient in de vergelijking opgenomen te worden:
    - De globale werking van het te vergelijken protocol in het huidige internet model
    - Minimale topologie en apparatuur dat nodig is om het protocol te laten werken
    - Toepassingen van het protocol
    - Welke werkzaamheden LISP zou kunnen overnemen
- Het rapport bevat informatie over technieken die LISP mogelijk vervangt of vernieuwd. Technieken die minimaal omschreven dienen te worden zijn:
    - Multi-homing
    - IPv6 Transition Support
    - VM Mobility
- Vergelijken van deze technieken ten opzichte van huidige oplossingen dient beoordeelt te worden op basis van:
    - Minimale topologie en apparatuur vereisten (voor zo ver dat relevant is)
    - Voor- en nadelen
    - Mogelijke problemen die verdwijnen na het inzetten van LISP
- Het rapport bevat een afweging op het LISP protocol in theorie een interessante oplossing is voor ISP en Enterprise netwerken.

ONTWERPRAPPORT

- Het ontwerprapport bevat informatie over de opstellingen die gebouwd worden om LISP in de praktijk te demonstreren en de manier waarop deze worden getest. Hierin staan drie opstellingen beschreven.
    - Een opstelling op basis van een LISP-ISP, in dit geval het bèta-netwerk, om te bepalen welke gevolgen het adopteren van LISP heeft op de bereikbaarheid van een omgeving.
    - Een "standalone" omgeving waarin de technieken IPv6 transitie, multihoming en VM/IP mobility werken en alle netwerkelementen van een LISP omgeving aanwezig zijn (xTR, PxTR, MS, MR). Dit lab is bedoeld om technieken te demonsteren en meten.
    - Een veelvoorkomend topologie van een QI ict klantnetwerk dat gecombineerd is met LISP functionaliteit om te bepalen waar mogelijke breek- en knelpunten zitten wanneer LISP wordt geadopteerd.
- Voor alle drie de opstellingen dienen de volgende elementen beschreven te worden:
    - Het doel van de opstelling
    - De topologie van de opstelling, zonder specifieke gegevens zoals IP-adressen.
    - De benodigde hard- en software van de opstelling
    - Het testplan van de opstelling

DEMO-OPSTELLINGEN

- Van alle opstellingen dienen verschillende gegevens opgeslagen te worden. De gegevens worden in de laatste fase van het onderzoek gebruikt als bron om het adviesrapport te schrijven. Per opstellingen dienen de volgende gegevens aanwezig te zijn:
    - Configuratie van netwerkelementen en de definitieve topologie
    - Metingen/resultaten van het testplan
    - Eventuele bevindingen die niet tijdens het literatuuronderzoek naar voren zijn gekomen
    - Korte conclusie over de werking

ADVIESRAPPORT

- Het adviesrapport bevat een algemene beschouwing van LISP op basis van de testresultaten en bevindingen uit het testresultatenrapport. De beschouwing bevat:
    - Een analyse van de netwerkcomponenten (xTr, PxTR, MS, MR) die nodig zijn voor het opzetten van een LISP omgeving. Relevante informatie is:
        - Moeilijkheidsgraad van het opzetten (configuratie)
        - Hard- en software vereisten
    - Een analyse van de technieken multihoming, IPv6 transitie en VM/IP mobility. Hierbij dient te worden vergeleken hoe de technieken zich in de praktijk hebben geuit in vergelijking met de theorie uit het onderzoekrapport.
- Het adviesrapport bevat een overzicht van LISP-technologie dat tijdens het onderzoek niet aan bod is gekomen. Dit kunnen technieken zijn waarvoor geen tijd en/of middelen beschikbaar waren, of technologie dat nog in ontwikkeling is.
- Op basis van de resultaten uit het onderzoeksrapport en testresultatenrapport dient een advies te worden opgesteld over de geschiktheid van LISP voor klanten van Qi ict. De partijen wier netwerk hiervoor bekeken dienen te worden zijn:
    - Enterprises (met meerdere vestigingen)
    - Internet Service Providers
- De geschiktheid van LISP voor een onderneming dient bepaald te worden aan de hand van:
    - De voordelen van LISP adoptie
    - De nadelen van LISP adoptie

- Een grove schatting wat de adoptie zou kosten

IV. ONDERZOEKSRAPPORT

SAMENVATTING

Het internetmodel zoals wij dat kennen heeft problemen. Het grootste probleem waar het op dit moment mee worstelt, is het feit dat de BGP-routers in het DFZ overlopen met routes die voor een groot deel onnodig zijn. Dit komt doordat de huidige statische vorm van het internet, waarbij een IP-adres bepaalt wie en waar je bent niet goed overweg kan met het steeds dynamischer worden van werkzaamheden. Veel partijen werken nu virtueel of via laptoppen en mobiele telefoons, waardoor we per definitie mobiel zijn geworden.

In 2006 is op het *Amsterdam Routing and Addressing Workshop* gesproken over dit probleem en de mogelijke oplossingen. Het Location/ID Separation Protocol (LISP) was één van de mogelijkheden en ook de oplossing die door veel partijen, bijvoorbeeld Cisco, werd gezien als het meest haalbaar. Het is inmiddels acht jaar geleden dat LISP is bedacht en is gedurende die jaren ontwikkeld als open standaard.

LISP werkt op basis van een scheiding tussen identiteit en locatie. Aan ieder eindsysteem wordt een identiteit-adres toegekend (EID) en een locatie-adres (RLOC). De koppeling tussen deze twee adressen wordt opgeslagen in een database. Wanneer het ene eindsysteem de ander zoekt doet hij een verzoek om de koppeling uit de database. Bij de gezochte EID wordt een RLOC geretourneerd, waardoor de LISP-router weet waar het verkeer naar toe moet.

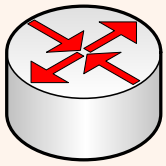
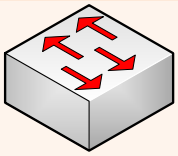
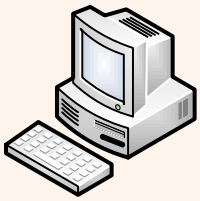
Omdat LISP helpt bij het routeren van verkeer wordt het vaak gezien als een routeringsprotocol. Dit is niet het geval. LISP beschikt slechts over de informatie en is nog steeds afhankelijk van onderliggende protocollen als BGP en OSPF om het verkeer te verplaatsen. Toch kan LISP wel protocollen vervangen onder bepaalde omstandigheden. LISP kan BGP en NAT vervangen bij multihomed omgevingen, tunneling en translatie bij IPv6 transitie en verschillende protocollen bij IP/VM Mobility.

LISP zorgt in zijn eenvoud voor flexibiliteit en schaalbaarheid van het internet. Toch kleven er ook nadelen aan LISP. Het grootste nadeel is de experimentele status. De informatie die beschikbaar is over LISP bespreekt vooral de voordelen en er is weinig informatie bekend over de nadelen, omdat het protocol nog maar weinig wordt geïmplementeerd. De nadelen zullen ongetwijfeld tijdens de volgende fase van het onderzoek naar voren komen als de lab opstellingen worden opgebouwd en getest.

VERKLARENDE WOORDENLIJST

Woord	Betekenis
Decapsulation	Data dat tijdens het encapsulationproces is bijgevoegd verwijderen.
EID	Endpoint ID. Een 32- of 128 bits IP-adres van een eindsysteem dat gebruikt wordt voor de afzender- of bestemmingsadres in de LISP-header.
EID-Prefix	Een blok EID's dat door een autoreiteit wordt uitgegeven. Deze blok van EID's wordt aan een RLOC gekoppeld in het mapping-system database.
Encapsulation	Het "inpakken" van verkeer en tijdens het proces het pakket voorzien van nieuwe data, zoals het bijvoegen van een LISP header.
ETR	Egress tunnel router. Een router die op de grens tussen EID en RLOC omgevingen werkt en zorgt dat encapsulated verkeer van de ITR wordt decapsulated en doorgestuurd naar de gezochte EID.
ITR	Ingress tunnel router. Een router die op de grens tussen EID en RLOC omgevingen werkt en zorgt voor de encapsulation van LISP-verkeer.
Mapping System	Overkoepelende term voor de map-server, map-resolver en de mapping-system-database.
Mapping-system database	Omschrijf een database techniek die gebruikt wordt voor het opzoeken van de koppeling tussen EID en RLOC.
PITR	Proxy ITR. Zorgt voor een koppeling tussen wel- en niet LISP omgevingen door bekende LISP routes te distribueren in het traditionele internetmodel via BGP.
PETR	Proxy ETR. Een ETR dat verkeer kan decapsulaten dat niet voor een LISP omgevingen bestemt is. Dit kan nodig zijn bij het overbruggen van een netwerk met een ander type IP protocol.
RLOC	Routing locator. Een IPv4 of IPv6 adres van een xTR aan de zijde dat in verbinding staat met het DFZ. Tevens het resultaat van zoekopdracht in de database.
xTR	Router dat de functionaliteit kan hebben van een ITR, ETR, PITR of PETR

SYMBOLENLIJST

Symbool	Betekenis
	**Router** - Verantwoordelijk voor het verbinden van twee computernetwerken. - Vaak ook te zien als xTR in een topologie. Een xTR is een router met LISP functionaliteit.
	**Switch** - Verbinden van eindsystemen op laag twee.
	**Eindsysteem** - Eindpunt in een netwerk. Kan een desktop, laptop, telefoon etc. zijn.
	**Server** - Eindsysteem dat gebruikt wordt om informatie op te slaan, zoals databases met mapping-data.
	**Wolk** - Computernetwerk waarvan de interne werking niet relevant is. Bestaat uit een tal van routers en switches.

INHOUDSOPGAVE

1. INLEIDING

Op de website van het Classless Inter-Domain Routing (CIDR) wordt het aantal actieve routes van de BGP tabellen uit het DFZ gerapporteerd. Eind 2014 stond de teller op ongeveer 530.000 routes voor IPv4 en ongeveer twintig duizend voor IPv6 (APNIC, 2014). Hoewel de grootste reden van het snelle groeien van het aantal routes valt te wijten aan de explosieve groei van het internet is er nog een reden. Aggregatie van routes in de tabellen wordt zeer moeilijk gemaakt doordat eindsystemen steeds verplaatsen. Door het vele gebruik van laptoppen, mobiele telefoon en virtuele machines zijn werkzaamheden in de huidige tijd per definitie mobiel. Het originele idee dat een IP-adres bepaald wie een eindsysteem is en waar hij is bevindt zich in de kern van het probleem. Voor het optimaal aggregeren van routes zouden IP-adressen binnen een vast subnet moeten blijven zitten, terwijl je voor het verplaatsen zou willen dat je IP-adres onafhankelijk is van een topologie en hetzelfde blijft om sessies beschikbaar te houden.

Het Location/ID Separation Protocol (LISP) is in 2006 in ontworpen als bestrijding van de overtollige routes in de routetabellen van het DFZ. Inmiddels is het LISP bèta-netwerk in gang en worden steeds meer toepassingen ontdekt, zoals multihoming, IPv6 transitie en IP mobility. Qi ict heeft interesse in dit protocol en heeft daarvoor een afstudeeropdracht opgezet. Dit document is het resultaat van het literatuuronderzoek.

In dit document komt de werking van LISP aan bod op basis van het huidige DDT-netwerk. De onderwerpen die worden toegelicht zijn de control- en dataplane, de mapping-system, werken tussen wel- en niet-LISP omgeving, encapsulation en beveiliging. In het volgende hoofdstuk wordt LISP vergeleken met de protocollen BGP, MPLS, OSPF en IS-IS. Het laatste hoofdstuk beschrijft technieken waarvoor LISP kan worden toegepast.

2. PROBLEEMSTELLING

Elk onderzoek begint met een probleem en het doel om voor dat probleem een oplossing te vinden. Het probleem in deze kwestie is dat Qi ict niet over de nodige kennis beschikt om klanten te informeren over het LISP protocol. Het probleem zal hieronder worden toegelicht met daarbij ook de doelstelling van het onderzoek.

2.1 PROBLEEM

In de jaren tachtig werd het IPv4 protocol geïntroduceerd om connectiviteit tussen apparatuur te verkrijgen op de manier waarop wij tegenwoordig gewend zijn. Het principe van het protocol is dat een IP-adres bepaalt wat de identiteit (EID) is van het apparaat en daarnaast ook de manier waarop het apparaat is verbonden aan het netwerk (RLOC). Er zijn meningen dat dit principe kan worden verbeterd, door de EID en RLOC parameters te scheiden om zo schaalbaarheid- en snelheidswinst te behalen in een netwerk. Het LISP protocol is naar aanleiding van een discussie op het Amsterdam Routing and Addressing Workshop geopperd door Cisco. Het protocol is sinds 2006 als open standaard in ontwikkeling en bevindt zich nu in bèta fase. Bij Qi ict is interesse in het gebruik en positionering van dit protocol en daarbij vooral de manier waarop het geïntegreerd kan worden in bestaande netwerken en in hoeverre het bestaande protocollen vervangt of verrijkt.

2.2 DOELSTELLING

Het doel is om voor 23 maart 2015 een onderzoek te hebben uitgevoerd dat Qi ict inzicht geeft in het gebruik en de implementatie van het LISP protocol in het bestaande internet model. Het onderzoek dient een rapport en een testopstelling op te leveren die als basis gaat fungeren voor het beter adviseren van klanten die geïnteresseerd zijn in deze techniek.

3. AANPAK

In het plan van aanpak is duidelijk gemaakt dat in de analysefase van de watervalmethode er op basis van systematisch literatuur zoeken informatie zal worden gezocht en geëvalueerd. Deze manier van zoeken bestaat uit drie fasen. Deze zullen in dit hoofdstuk worden toegelicht.

3.1 METHODIEK

De systematisch literatuur zoek methode is ontwikkeld aan de Rijksuniversiteit van Groningen en bestaat uit drie fasen. Allereerst de oriëntatie- en afbaken fase. Hierin wordt de (voorlopige) probleemstelling geformuleerd, het zoekdomein afgebakend en de algemene eisen geformuleerd. In het geval van dit onderzoek worden die voorlopige eisen omgezet in een set van hoofd- en deelvragen die uiteindelijk na het uitvoeren van deze methodiek beantwoord zullen zijn. De tweede fase is de systematische zoek fase. Hierin wordt het onderzoek definitief gepland, wordt er literatuur gezocht en uiteindelijk geïnventariseerd. De laatste fase omvat het beoordelen van de informatie en logischerwijs beantwoorden van alle onderzoeksvragen.

Tabel 3.1 – Fasen en stappen van slz-methode. Bron: (Groningen, 2012)

Fasen	Stappen
Oriënteren en afbakenen	- Probleemstelling en algemene eisen formuleren - Oriënteren op het onderwerp van het onderzoek - Zoekterrein afbakenen - Begrippenkader vaststellen - Onderwerp specifieke publicaties zoeken en globaal bestuderen - Vakgenoten inventariseren
Systematisch zoeken	- Onderzoek definitief plannen - Literatuur zoeken en beoordelen - Sneeuwbalmethode toepassen - (Eventueel) vakgenoten raadplegen
Proces en opbrengst evalueren	- De waarde van gevonden publicaties beoordelen - Proces evalueren

De universiteit achter deze methode stelt dat elke zoekactie uniek is en om die reden niet altijd alle stappen toegepast dienen te worden. De methode is bedoeld als stok achter de deur om belangrijke en relevante bronnen niet over te slaan.

3.2 TOEPASSING

Het toepassen van deze methode is reeds begonnen met het schrijven van het plan van aanpak. In dit document is de probleemstelling bepaald met daarbij ook de wensen en grenzen aan het project die de opdrachtgever stelt. De volgende stap zal het zoeken naar informatie zijn die nodig is om de vragen te beantwoorden die uit de eisen en wensen zijn voortgekomen. Wanneer deze informatie is gevonden zullen de onderzoeksvragen uit het volgende hoofdstuk beantwoord worden.

4. ONDERZOEKSVRAGEN

De eisen en wensen die in het plan van aanpak naar voren zijn gekomen zijn elementen die uiteindelijk in dit rapport zijn uitgewerkt. Met dit in gedachte is besloten deze eisen en wensen om te vormen naar onderzoeksvragen. Wanneer deze vragen voldoende beantwoord zijn, is er ook logischerwijs voldaan aan de eisen van de opdrachtgever. De volgende vragen zijn opgesteld voor dit onderzoek.

Hoofdvraag:

- In hoeverre is het LISP protocol een verrijking voor het bestaande internetmodel en is het protocol interessant voor Qi ict en haar klanten?

Deelvragen:

- Wat is het LISP protocol en welke problemen lost het op?
- Hoe werkt LISP en wat is nodig om het te kunnen implementeren in een netwerk?
- Wat is het verschil met bestaande routingprotocollen en bestaande overlay- en tunneling methoden?
- Op welke manier vervangt LISP andere protocollen/mechanismen in bestaande technieken?
- Wat zijn de voor- en nadelen van LISP?
- Voor welke omgevingen is LISP een geschikt protocol?

De deelvragen zullen aan de hand van de informatie die tijdens het literatuuronderzoek wordt gevonden voor zover mogelijk worden beantwoord. Volledige beantwoording van de deelvragen en hoofdvraag komt later in het onderzoek aan bod, omdat hier ook praktijkgegevens voor nodig zijn.

5. WAT IS LISP?

De huidige vorm van het internet die bij ons allen thuis uit de kabel komt lijkt op het eerste gezicht naar behoren te werken. Onder de motorkap zijn er problemen met onder andere de schaalbaarheid. Onlangs zijn de IPv4-adressen opgeraakt en lijken de routeringstabellen van de routers in de Default Free Zone (DFZ) over te lopen. Er is in de afgelopen jaren op verschillende momenten nagedacht over oplossingen voor deze schaalbaarheidsproblemen. Het LISP protocol is hiervoor één van de mogelijkheden. In dit hoofdstuk wordt achtergrond informatie weergegeven over het huidige internetmodel en de problemen die het heeft. Tevens zal het LISP protocol worden toegelicht.

5.1 BESTAAND INTERNETMODEL

Eind jaren zestig is er vanuit de Amerikaanse defensie het idee geopperd om een op basis van het TCP/IP model een netwerk te creëren dat verschillende instanties met elkaar zou verbinden (Barry M, 2012). Uiteindelijk werd na een periode van negen maanden het eerste werkende model van het internet opgeleverd door het toenmalige Bolt, Beranek and Newman Technologies (BBN). Hoewel het netwerk destijds voor driekwart werd gebruikt voor het sturen van e-mail tussen leden van de Advanced Research Projects Agency (ARPA), de toenmalige defensie afdeling, is het internet inmiddels uitgegroeid tot een onmisbaar fenomeen in onze samenleving.

De kern van het internet werkt op basis van een 32-bits IP-adres voor IPv4 en een 128-bits IP-adres voor IPv6. Dit IP-adres wordt door een eindsysteem gebruikt om zichzelf kenbaar te maken op het internet. Er kan dus worden gezegd dat het IP-adres de identiteit is van het eindsysteem binnen het internetmodel. Dit IP-adres is niet alleen de identiteit, maar bepaald ook de manier waarop het eindsysteem is verbonden aan het internet. Verschillende routeringsprotocollen bepalen op basis van het IP-adres de locatie van het eindsysteem. Om dit te realiseren worden routeringstabellen bijgehouden die gebruikt worden om het juiste pad te vinden om het verkeer langs te sturen.

Dit internetmodel heeft de afgelopen veertig jaar gedraaid zonder dat er aan de oppervlakte veel problemen te merken waren, maar de laatste jaren zijn er problemen naar voren gekomen die niet langer ontkent kunnen worden. Allereerst is er het probleem dat de IP-adressen opraken voor IPv4. Veertig jaar geleden werd er bepaald dat met het 32-bits adres ongeveer 4,3 miljard adressen toegewezen konden worden. Deze hoeveelheid leek op het eerste gezicht ruim voldoende voor de destijds bedachte toepassing van het internet, maar door de bijzonder snelle groei en gebruik van IP-adressen in ontzettend veel apparaten is er een eind gekomen aan de voorraad. Het tweede probleem is de slechte schaalbaarheid van routeringstabellen in de DFZ. In de DFZ bevinden zich alle autonomous systems (AS), die prefixes bevatten voor alle IP-routing netwerken op de wereld. De routers in de DFZ beschikken niet over een default gateway wat betekent dat ze een totale verzameling routes nodig hebben om het verkeer te kunnen doorsturen. Dit wordt geregeld door routes te aggregeren om zo de grootte van tabellen te beperken. Het aggregeren wordt bijzonder lastig gemaakt doordat de verdeling van IP-adressen over de wereld vanaf het begin al slecht is geregeld door het Internet Assigned Numbers Authority (IANA). Dit komt doordat vroeger IP-adressen classfull werden verdeeld in klasse A, B of C wat overeenkomt met een 8-, 16-, of 24-bit prefix. Subnetting van prefixes was niet toegestaan, waardoor veel partijen veel te veel IP-adressen toegewezen kregen. Toen het classfull systeem later werd vervangen met een classless systeem dat subnetting toestond is er door Internet Service Providers (ISP) steeds kleinere blokken van adressen verkocht wat voor extra routes zorgt binnen de DFZ.

Deze problemen komen in de kern voort uit het feit dat IP-adressen zowel de identiteit als locatie van een eindsysteem moeten weergeven en vormen daarbij ook de basis van het ontstaan van LISP. Dit wordt in de volgende paragraaf toegelicht.

5.2 ONTSTAAN VAN LISP

Gedurende een debat op het *Amsterdam Routing and Addressing Workshop* in 2006 werd het volgende gezegd: *"routing scalability is the most important problem facing the internet today and must be solved* (D. Meyer, 2007). Sindsdien is gewerkt aan oplossingen om dit probleem te verhelpen. Het location/ID separation protocol (LISP) wordt door Cisco aangedragen als de meest haalbare optie.

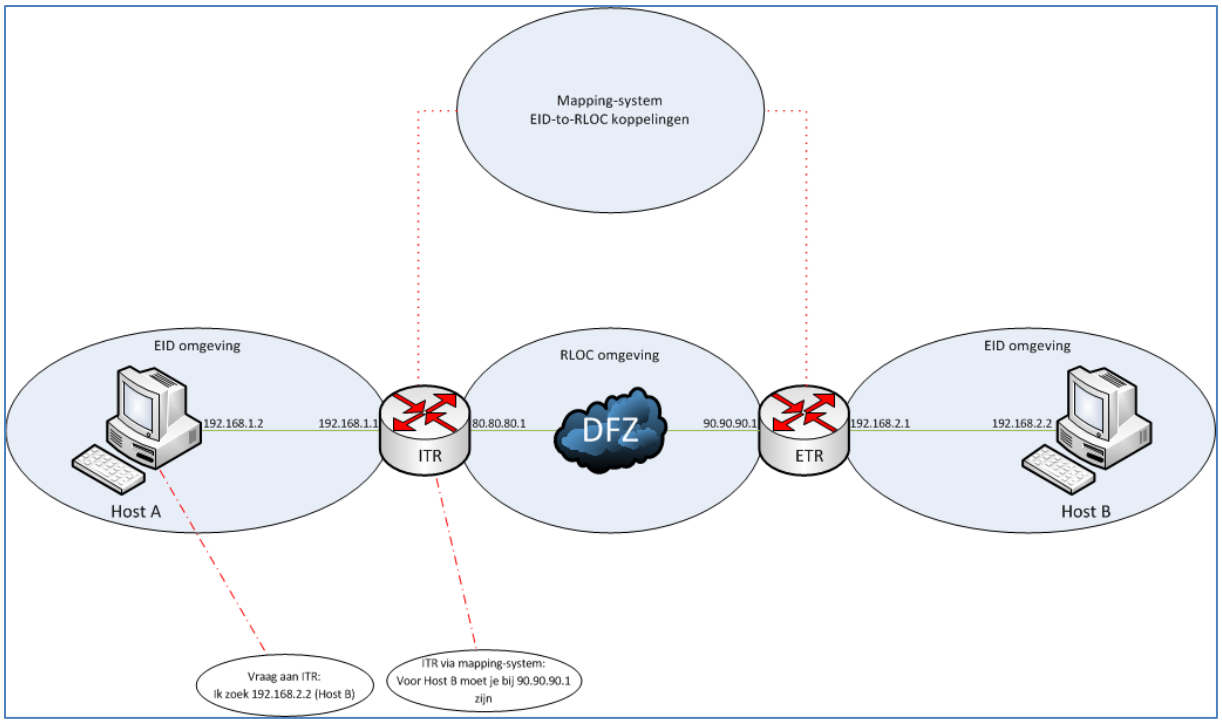
In de vorige paragraaf is toegelicht dat het IP-adres bepaald wat de identiteit is van het eindsysteem en daarnaast ook de manier waarop het eindsysteem is verbonden aan het netwerk. Dit kan worden vertaald in wie je bent als eindsysteem en waar je bent. Het feit dat deze samenstelling voor problemen zorgt komt door een conflict van twee principes in de kern van het internet model (D. Farinacci, 2013). Het eerste principe is die van identiteit. De definitie van identiteit is *"De kenmerken en omstandigheden van een ding, persoon of groep, die hetzelfde blijven gedurende een verandering"* (Slot Webcommerce BV., 2014). Ondanks het feit dat het IP-adres wordt gebruikt om de identiteit van een eindsysteem te bepalen, veranderd dit adres bij het wisselen van netwerken. Dit komt doordat het IP-adres van een eindsysteem gekoppeld zit aan de topologie van het netwerk. Iedereen heeft tegenwoordig een mobiele telefoon of laptop waar overal en altijd mee gebeld en gewerkt wordt. Mensen en hun apparatuur zijn per definitie mobiel en dat lijkt alleen maar groter te worden met thuis- en flexwerken. Dit brengt het effectief managen van eindsystemen in de problemen, omdat IP-adressen constant wijzigen. Het is om die reden voor identiteit gewenst om niet afhankelijk te zijn van een topologie. Het tweede principe is die van locatie. Om effectief te bepalen waar een eindsysteem is en daar verkeer naar toe te sturen is aggregeren van routes gewenst. De hoeveelheid routes in de routers van de Default Free Zone (DFZ) zijn van directe impact op de snelheid waarmee verkeer een eindpunt bereikt. Om effectieve aggregatie te bereiken is een IP-adres dat afhankelijk is van de topologie wel gewenst. Op deze manier krijg je het conflict tussen identiteit en locatie van een eindsysteem waar LISP uit is ontstaan.

5.3 LISP ALS PROTOCOL

Hoewel Cisco bijzonder veel tijd stopt in het promoten van LISP als oplossing voor de eerder omschreven problemen, wordt LISP ontwikkeld als open standaard zonder enige vorm van copyright voor Cisco. Het protocol is geïmplementeerd in de laatste versies van Cisco IOS, IOS-XE en NXOS en is het daarnaast ook te vinden als het open source project LISPMob voor ondersteuning op Linux, Android en OpenWRT.

De naam van het protocol "location/ID separation protocol" verklaard voor een groot deel wat het protocol inhoudt. Het scheidt de locatie en identiteit van het IP-adres in twee aparte onderdelen. Allereerst de RLOC parameter voor het bepalen van de locatie en als tweede de EID parameter voor het bepalen van de identiteit. In essentie komt de EID overeen met het IP-adres van het eindsysteem zoals je computer tegenwoordig ook een IP-adres heeft. De RLOC parameter is het IP-adres aan de buitenkant van de router die voor de EID staat en is het resultaat van een koppeling die opgezocht wordt in de database.

In de onderstaande afbeelding komt het EID van host A overeen met het IP-adres 192.168.1.2 en het RLOC adres van host A komt overeen met 80.80.80.1, omdat host A zich op het moment van zoeken achter die router bevindt. Stel dat host A zich zou verplaatsen naar het netwerk van host B, dan zou de EID van host A nog steeds 192.168.1.2 zijn, maar de RLOC zou veranderen naar 90.90.90.1. In de mapping system wordt de koppeling tussen EID en RLOC, de EID-to-RLOC mapping, bijgehouden.



Figuur 5.1 – LISP Topologie

LISP werkt op basis van een client-server model. Een client kan een verzoek doen om een koppeling uit een hiërarchisch server model door het mapping-system te gebruiken voor het zoeken van de juiste RLOC bij een EID. Dit model is geïnspireerd door de werking van het Domain Name System (DNS). LISP zorgt zelf nog niet voor het volledig versturen van een pakket van A naar B. Het LISP protocol zorgt voor de juiste eindbestemming en is afhankelijk van onderliggende routingprotocollen om het pakket van A naar B te krijgen.

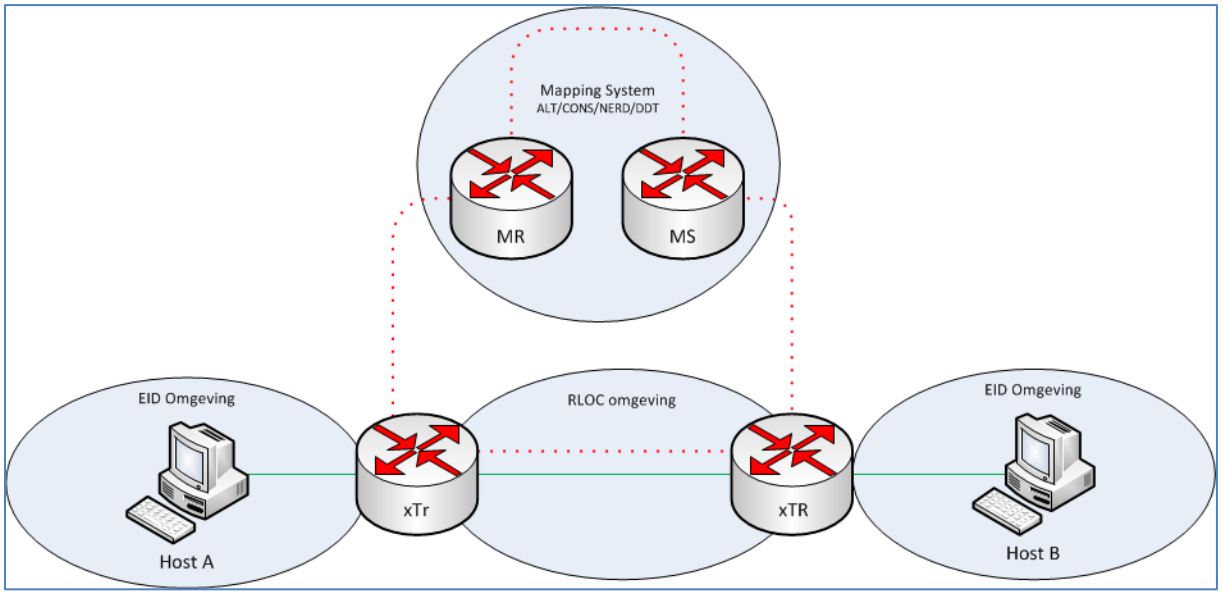
Hoewel LISP ontwikkeld is als oplossing voor de schaalbaarheidsproblemen in de routers van het DFZ is het protocol ook voor andere zaken toepasbaar. Technieken als IP/VM mobility in datacenters, IPv4 naar IPv6 transitie en multi-homing zonder BGP zijn mogelijkheden die op het moment sterk gepromote worden (Hill, 2011).

6. WERKING VAN LISP

In dit hoofdstuk wordt de werking van LISP toegelicht. Allereerst zal de basiswerking van LISP worden toegelicht met de control- en data plane als onderdelen. Vervolgens komt het mapping-system aan bod om de database achter LISP te verduidelijken. In de volgende paragraaf worden verschillende topologievormen van LISP uitgewerkt, waarbij verkeer van wel- en niet-LISP omgevingen worden verstuurd. Als laatste wordt er informatie gegeven over de LISP-header, de beveiliging van het LISP protocol en de systemen die LISP ondersteunen.

6.1 CONTROL- EN DATA PLANE

De werking van LISP is gebaseerd op een verdeling van twee lagen. De eerste laag is de “control plane” die zorgt voor het bijhouden van de mapping-database en de tweede laag is “data plane” die zorgt voor het uiteindelijk sturen van LISP pakketten (Moreno, 2014).



Figuur 6.1 – Basis topologie LISP

In de bovenstaande afbeelding is de basistopologie van een LISP omgeving weergeven. Hierin geven de groene lijnen de activiteiten van de data plane weer en de rode gestippelde lijnen de activiteiten van de control plane.

Data plane
Het doel van de data plane is het zorgen dat het pakket van host A naar host B komt. Dit wordt gedaan aan de hand van de informatie uit de control plane. De data plane bestaat uit twee onderdelen:

- **Ingress tunnel router (ITR)**. De ITR bevindt zich op de grens van de LISP omgeving tussen de EID en RLOC adressen. De verantwoordelijkheid van de ITR is het ontvangen van IP-pakketten van een host en daarna te bepalen of deze door middel van LISP verstuurd moet worden, of via het traditionele internetmodel. Dit doet de ITR op basis van een map-request die gestuurd wordt naar het mapping-system.
- **Egress tunnel router (ETR)**. De ETR bevindt zich net als de ITR op de grens van een LISP omgeving tussen de EID en RLOC adressen. De verantwoordelijkheid van de ETR bestaat uit twee onderdelen**.** Allereerst het registreren van de EID’s uit het lokale netwerk achter zich bij de mapping-server en als tweede het analyseren of de opgevraagde EID adres uit de map-request inderdaad in zijn achterliggende EID-omgeving actief is om dit vervolgens te melden aan ITR.

In topologietekeningen worden de ITR en ETR vaak weergegeven als xTR, omdat de functionaliteit van beide systemen op één netwerkcomponent geconfigureerd kan worden. Op deze manier is LISP ook geschikt voor partijen met minder middelen, zoals consumenten met één router. Dit is geen verplichte handeling. De functionaliteit van de ITR en ETR kan gescheiden worden over twee of meer systemen uit bijvoorbeeld redundantie overwegingen.

Control plane
De control plane heeft als doel het bijhouden van de juiste koppelingen tussen EID-adressen en RLOC-adressen. De control plane zorgt er voor dat de data plane over de juiste informatie beschikt om het LISP-pakket van host A naar host B te krijgen. De control plane bestaat uit vijf onderdelen:

- **Map-Resolver (MR)**. De MR is een netwerkcomponent dat verzoeken ontvangt van de ITR, waarbij de ITR wil weten of er bij een opgevraagd EID een RLOC bekend is. Deze verzoeken worden door de MR doorgestuurd naar de map-server via het mapping-system. Tevens is de MR verantwoordelijk voor het versturen van negatieve mapping-berichten, wanneer de EID niet bekend is en het verkeer zonder LISP encapsulation via de default gateway het traditionele internet op moet gaan.
- **Map-Server (MS)**. De MS is een netwerkcomponent die registraties ontvangt van een ETR en deze verwerkt in de mapping-system-database. De MS stuurt ook map-requests door naar de verantwoordelijke ETR wanneer deze bekend is in zijn database.
- **Map-Cache (MC)**. De MC is een tijdelijk geheugen op de ITR die routes opslaat die op basis van map-replies van de ETR zijn aangemaakt. Deze routes worden aan de hand van een time-to-live (TTL) voor een bepaalde tijd vastgehouden.
- **Site Mapping-Database (MD)**. De MD is een lokale database op de ETR die alle EID-to-RLOC koppelingen bijhoudt voor een lokale LISP-omgeving.
- **Mapping-System-Database (MSD)**. De MSD wordt omschreven als een database, maar is een techniek voor het distribueren van routes tussen de MR en MS. Op het moment wordt in het LISP bèta-netwerk gebruik gemaakt van hiërarchisch boomstructuur waarbij EID-to-RLOC koppelingen worden gedelegeerd.

De data- en control plane werken samen door verschillende berichten te sturen naar de map-onderdelen en LISP-routers. Het gaat hier om de volgende berichten:

- **Map-Register**. Dit bericht wordt door de ETR naar de MS gestuurd met informatie over de EID's die zich in zijn lokale LISP-omgeving bevinden. De MS koppelt vervolgens deze EID-prefixes aan de gewenste RLOC, zodat bij een verzoek van de ITR de juiste eindbestemming wordt gekozen.
- **Map-Request**. Dit bericht wordt door de ITR naar de MR gestuurd om te controleren of een IP-pakket in aanmerking komt voor LISP encapsulation. Het bericht is een verzoek om een koppeling tussen EID en RLOC. Het bericht wordt ook gebruikt voor het controleren of het doel nog te bereiken is.
- **Map-Reply**. Dit bericht wordt door de ETR teruggestuurd naar de ITR wanneer de EID van het eerder genoemde map-request is bevestigd in zijn lokale omgeving. De ITR gebruikt dit bericht voor het toevoegen van de router aan de mapping-cache op de ITR.
- **Map-Notify**. Dit bericht wordt door de MS naar de ETR gestuurd om te bevestigen dat registratie van een koppeling succesvol heeft plaatsgevonden. Dit is een optioneel bericht en wordt alleen gestuurd wanneer er een bepaalde flag is gezet in de header.

De berichten worden door het mapping-system en routers verstuurd via UDP poort 4341 en 4342. De reden dat er gekozen is voor UDP komt doordat oudere legacy routers de berichten dan wel accepteren en doorsturen, ondanks dat ze LISP niet begrijpen.

6.2 MAPPING-SYSTEM

Het mapping-system is een overkoepelende term voor de MR, MS en de manier waarop de MR en MS communiceren voor het vinden van de juiste koppeling tussen een EID- en RLOC-adres. Het doel van het mapping-system is de druk op de routeringstabellen van de DFZ te verlichten door extern gegevens over identiteit en locatie op te slaan. Door middel van deze gegevens kan het rap stijgende aantal routes worden teruggedrongen, omdat er bijvoorbeeld geen extra routes meer nodig zijn voor eindsystemen die verplaatsen. In deze paragraaf wordt de werking van het mapping-system toegelicht.

6.2.1 MAPPING RESOLVER

De MR is een netwerkcomponent, vaak een router, dat LISP-encapsulated map-requests ontvangt van een ITR en deze verwerkt. Het proces dat de MR volgt begint met het decapsulaten van het eerder ontvangen map-request. Uit dit bericht komt een IP-adres van een EID. Aan de hand van dit adres zal de MR beoordelen of het bericht met LISP encapsulation verstuurd moet worden, of dat het traditionele internet gebruikt wordt.

Om te bepalen welke situatie het geval is wordt het gevonden IP-adres vergeleken met een lokale set mapping-entries. Deze kunnen zowel statisch ingevoerd zijn als opgehaald uit een map-server als de functionaliteit van de MR en MS in één systeem geïmplementeerd zijn. Wanneer er lokaal geen koppeling gevonden kan worden en de MS ook niets oplevert wordt er een negatief bericht teruggestuurd naar de ITR die initieel het verzoek verstuurde. In dit bericht, de “Negative map-reply”, staat de actiecode “Natively-foward” waardoor de ITR weet dat het bericht via de default gateway van het traditionele internet verstuurd moet worden, zonder daar encapsulation op toe te passen. Om dit te realiseren wordt er een tijdelijk pad in de cache gezet met een TTL van vijftien minuten. De ITR gebruikt vervolgens deze route om het bericht te versturen.

De reden dat de TTL kort is heeft te maken met het feit dat een negatief map-reply ook kan voorkomen wanneer de MS tijdelijk niet bereikbaar is voor de MR. Door een tijdelijke route op te nemen kan verkeer evengoed verstuurd worden, maar wordt de optimale LISP route ook weer na vijftien minuten hersteld als de verbinding naar de MS terug is.

Als de MR wel een route vindt in de lokale entries of via de gegevens van de MS wordt het bericht via de MS doorgestuurd aan de ETR die verantwoordelijk is voor het opgevraagde EID.

6.2.2 MAPPING SERVER

De MS is een netwerkcomponent, vaak een router, dat map-requests die doorgestuurd zijn door de MR verder stuurt naar de verantwoordelijke ETR die het gezochte EID in zijn lokale netwerk heeft. Om dit te realiseren ontvangt de MS EID-prefixes, aggregaties van EID-adressen, van ETR’s en adverteert deze in de database van het mapping-system. Het proces dat hiervoor nodig is bestaat uit twee onderdelen.

Het eerste gedeelte van het proces is het registreren van EID’s bij de MS. Dit wordt gedaan door vanaf de ETR map-register berichten te sturen die verschillende EID-prefixes bevatten die aanwezig zijn in het lokale LISP-netwerk van de ETR. Voordat dit geregeld kan worden dient er een shared secret afgesproken te worden tussen de MS en ETR, met daarbij ook een lijst van prefixes waar de ETR autoriteit over heeft. Dit is geïmplementeerd om te voorkomen dat derde partijen valse EID’s in het systeem plaatsen. Na het registreren van de EID-prefixes worden aan de hand van een ingevoerde interval de geregistreerde EID’s bijgehouden op bereikbaarheid. Standaard stuurt de ETR elke minuut een update van zijn EID’s via map-register berichten en wordt na drie minuten een EID verwijderd als er geen update plaatsvindt.

Het tweede gedeelte van het proces is het adverteren van deze EID-prefixes in de database van het mapping-systemen. Hiervoor zijn verschillende technieken bekend die in de volgende paragraaf worden toegelicht.

Andere functionaliteiten van de MS zijn het sturen van map-notify berichten om te bevestigen dat een registratie heeft plaatsgevonden als de ETR daarom vraagt en het uitvoeren van een “quick registration” als

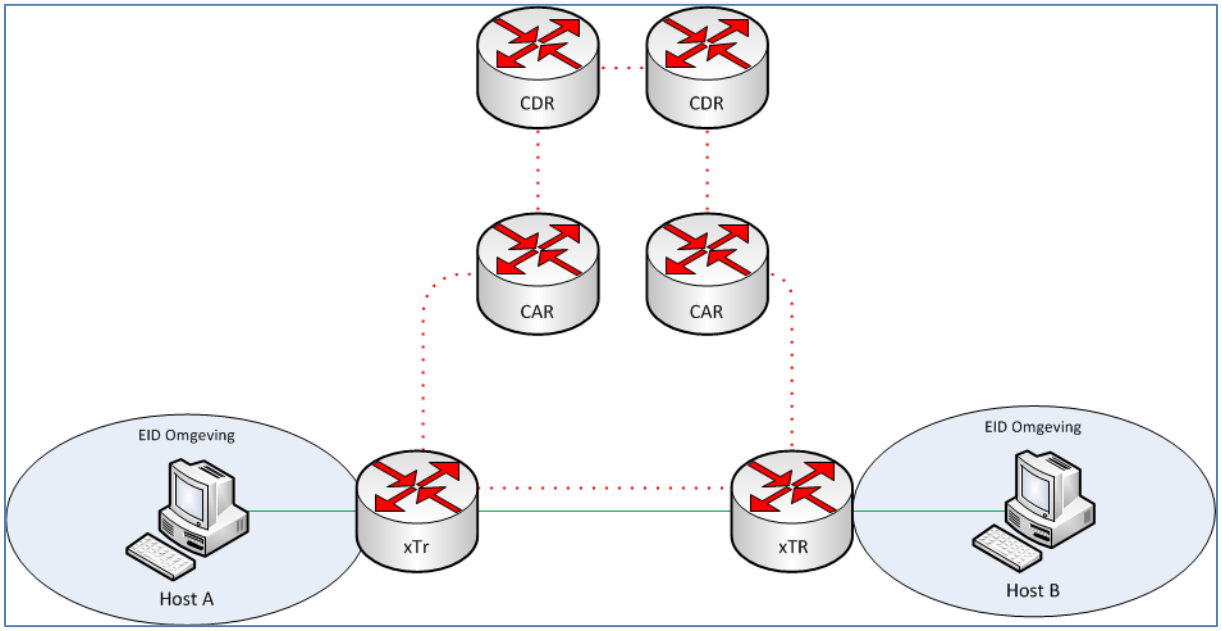
een MS zijn mapping is verloren door bijvoorbeeld stroomuitval. Quick registration houdt het verlagen van de registreerinterval in om snel alle registreerberichten binnen te krijgen.

6.2.3 MAPPING-SYSTEM DATABASE

De koppeling tussen de MR en MS wordt normaliter beschreven als een database waarin alle EID-to-RLOC koppelingen zijn opgenomen. Deze beschrijving is niet altijd geldig. De database is namelijk meer een gedistribueerd netwerk die de map-requests routeert dan een statische database met koppelingen in de vorm van records. Hiermee is de database geen vervanger van het DFZ. De database is afhankelijk van het onderliggende netwerk, om de map-requests ook daadwerkelijk te verplaatsen. Sinds het moment dat LISP ontstond zijn er verschillende technieken geweest om deze database invulling te geven. Deze vier technieken worden in deze paragraaf beschreven. De huidige standaard, LISP-DDT, zal in de volgende paragraaf uitgebreid worden toegelicht aan de hand van topologievoorbeelden.

LISP CONS

De eerste techniek die ontwikkeld is om een database te implementeren in het LISP model is LISP-CONS (S. Brim, 2008). CONS staat voor “Content Distribution Overlay Network Service” en omschrijft een techniek waarbij een hiërarchisch model op basis van push- en pull-berichten de EID-to-RLOC koppeling van begint tot eind transporteert door middel van een overlay-netwerk.



Figuur 6.2 – LISP CONS Technologie

Het CONS netwerk dat nodig is voor het vinden van de juiste router bestaat uit vier componenten:

1. ITR
2. ETR
3. Content Access Resource (CAR).
4. Content Distribution Resource (CDR)

De CAR in de topologie vervangt de functionaliteit van de MR en MS en kan fungeren als twee systemen. De answering CAR (aCAR) werkt als een soortgelijk MS en heeft de autoriteit om te antwoorden op map-requests. Om dit te realiseren registreert de aCAR ook EID-prefixes die afkomstig zijn van een LISP-router en stuurt deze door naar de CDR. De tweede functie die een CAR kan hebben is een querying CAR (qCAR). De qCAR vervangt de MR die voor de ITR een map-request kan sturen in de richting van een CDR.

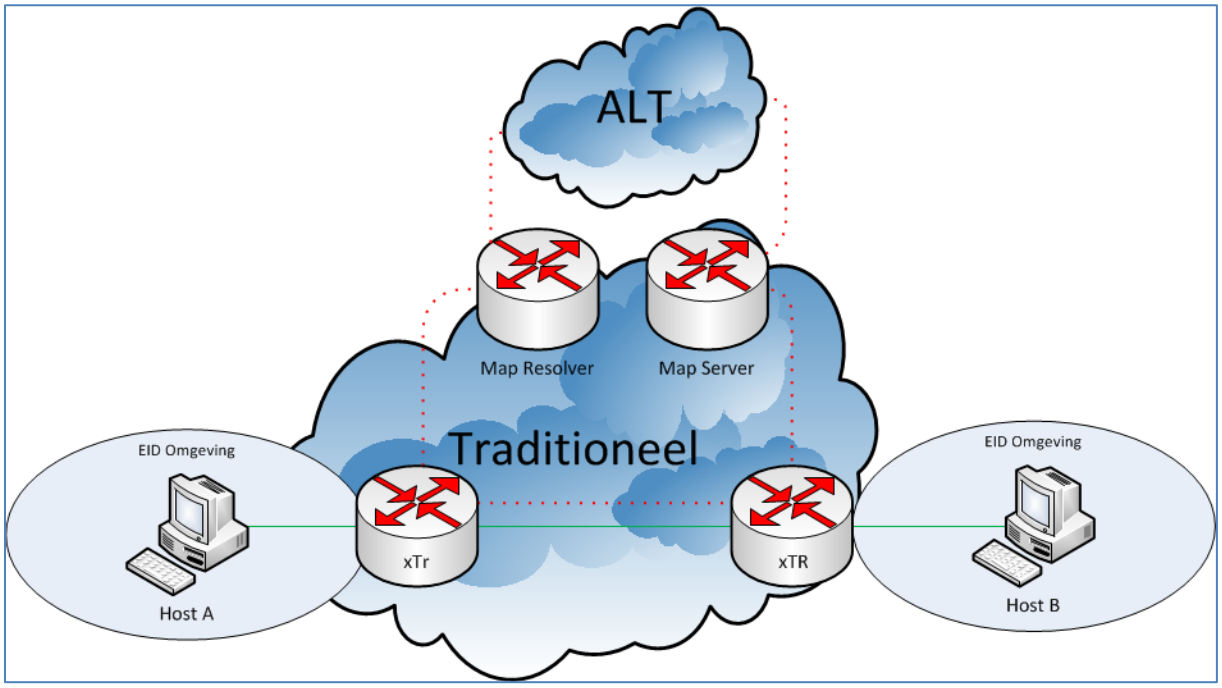
De CDR's vormen de kern van de database. De CDR's bevatten ieder sterk geaggregeerde clusters van EID-prefixes. Wanneer een verzoek verstuurt wordt vanaf een qCAR wordt dit bericht verstuurt naar verschillende CDR's die zich ieder op een andere laag van het hiërarchische model bevinden. Elke laag in het model beschikt over een iets minder geaggregeerde cluster, waardoor het verzoek uiteindelijk aankomt bij een aCAR die informatie heeft over de precieze locatie van de EID. Deze aCAR retourneert een map-reply aan de qCAR die initieel het verzoek verstuurde die de informatie doorgeeft aan de ITR. Met deze informatie kan de ITR vervolgens direct informatie versturen naar de ETR die de EID in zijn lokale netwerk heeft.

Voor het distribueren van informatie tussen de CAR's en CDR's worden er push- en pull berichten verstuurd. Wanneer een aCAR informatie heeft over een set EID-prefixes worden deze samengevat tot een aggregatie die vervolgens wordt "gepushed" naar een verbonden CDR. Deze set wordt met andere bekende sets van die CDR ook samengevat tot een kleinere aggregatie en verder gepushed naar een CDR die zich op een hogere laag bevindt. Wanneer er informatie nodig is wordt deze door ITR's "gepulled" uit de laagste lagen van het model.

De IETF working group die aan de ontwikkeling van CONS werkte is sinds oktober 2008 niet langer actief, waardoor de internet draft waarin de specificaties werden omschreven het nooit tot een RFC hebben gehaald. Vermoedelijk heeft dit te maken met het feit dat een groot deel van de functionaliteit overgenomen is door een nieuwe database techniek genaamd LISP+ALT.

LISP+ALT

De tweede mogelijkheid om een database te implementeren in het mapping-system is LISP+ALT (V. Fuller, 2013). Het "ALT" gedeelte in de naam beschrijft een alternatieve topologie dat als overlay-netwerk fungeert voor het distribueren van routes op basis van BGP en een gekozen tunnelprotocol. Standaard werd er gebruik gemaakt van Generic Routing Encapsulation (GRE) als tunnelprotocol.



Figuur 6.3 – LISP+ALT Topologie

De LISP+ALT architectuur is net als het eerder beschreven CONS een push/pull model waarbij EID-prefixes het alternatieve netwerk ingeduwd worden en weer door de ITR's uit het netwerk getrokken worden. Ook hier is de mapping-system-database geen echte database, maar juist een netwerk die de map-request routeert. Dit alternatieve netwerk is in het leven geroepen, omdat het IP-adres dat aanwezig is op de hosts (EID's) niet globaal routeerbaar zijn. Om die reden worden ze via en overlay-netwerk verstuurd dat bestaat uit tunnels die de adressen wel kan routeren. De MR en MS bevinden zich aan de grens van dit alternatieve netwerk en

fungeren als first- en last hop routers die door middel van BGP aggregaties van EID's het alternatieve netwerk in sturen.

Het tunnelprotocol dat gebruikt wordt in LISP+ALT is standaard het GRE-protocol, maar kan vervangen worden door elk ander tunnelprotocol. Zo zou het netwerk beveiligd kunnen worden met een protocol als IPSEC. Het LISP bèta-netwerk heeft voor een aantal jaar gedraaid op basis van LISP+ALT en is eind 2012 vervangen voor het huidige DDT-model. Het feit dat het architectuur afhankelijk was van BGP en een tunnelprotocol maakt het onhandig en lastig te troubleshooten, waardoor het niet langer in gebruik is (Heimlich, 2014).

LISP NERD

Een derde mogelijkheid om een database te implementeren in LISP is met LISP NERD (E. Lear, 2013). NERD is een architectuur dat in dezelfde periode is ontwikkeld als LISP+ALT, maar heeft niet veel bekendheid gehad, omdat de focus van ontwikkelaars vooral bij LISP+ALT lag.

Waar LISP ALT en CONS zich focussen op een gedistribueerd overlay-netwerk die gebruikt wordt voor het routeren van map-requests, is NERD gebaseerd op een techniek waar gebruik wordt gemaakt van een database. Het proces achter NERD begint met een hoge instantie, zoals het IANA, dat een database creëert met alle bekende EID's. Deze database dient gedistribueerd te worden naar verschillende servers. ITR's kunnen gebruik maken van deze servers om een kopie van de NERD-database binnen te halen. Na een positieve verificatie van de database door een PKI-systeem wordt de kopie lokaal opgeslagen op de ITR. Bij het opslaan wordt een database versienummer bijgevoegd die in een later stadium gebruikt kan worden voor het controleren van wijzigingen in de database.

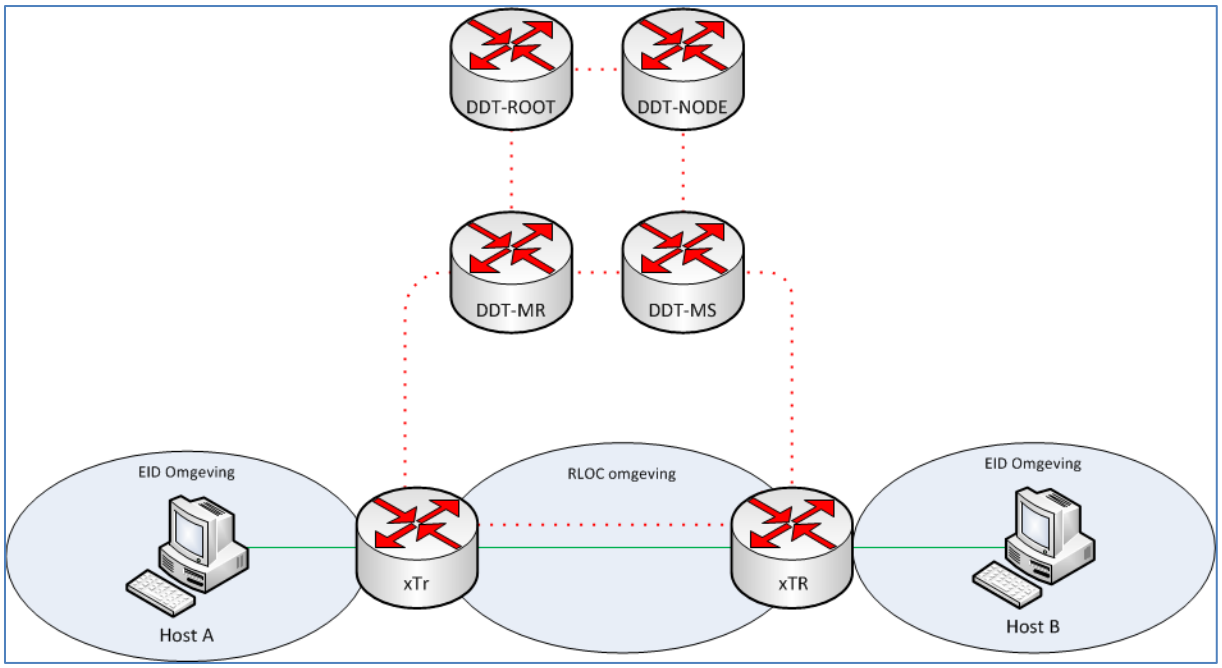
De RFC's die betrekking hebben op NERD beschrijven het model als een database format voor het opslaan van EID-to-RLOC koppelingen, maar laat het versturen van data over aan de verbeelding. In theorie zou de lokale database voldoende zijn voor het bereiken van de ETR, maar hierbij wordt er vanuit gegaan dat het pad waarvoor de map-request wordt verstuurt geen obstakels bevat. Er wordt om die reden ook een idee geopperd om een soortgelijke techniek als LISP+ALT te gebruiken voor het controleren van de verbinding. Dit is speculatief, omdat net als LISP+ALT, de LISP NERD techniek sinds 2012 niet verder wordt ontwikkeld.

LISP DDT

Het LISP bèta-netwerk dat gebruikt wordt voor het testen van LISP op globaal niveau is sinds 2012 overgegaan op huidige standaard LISP-DDT. LISP-DDT oftewel "Delegated Database Tree", is een combinatie van alle voorgaande technieken. Het is een hiërarchisch gedistribueerd database waarbij alle EID's door middel van verwijzingen naar routers op lagere lagen de juiste MS zoeken (Cisco Systems, 2013).

LISP-DDT is sterk geïnspireerd door de werking van DNS. Voor de ontwikkeling van DDT is geprobeerd de functionaliteit van DNS zelf aan te passen, maar de modificaties aan het protocol werden te agressief bevonden voor een protocol dat zo fundamenteel is voor het internet.

Om de werking van DNS te imiteren is de DDT-Node ontworpen. De DDT-Node beschikt over een aantal EID-prefixes waar de DDT-Node autoriteit over heeft en waarvan hij de verbonden MS-DDT kent. Tevens beschikt de DDT-Node over een aantal prefixes die wijzen naar andere DDT-Nodes. Wanneer een MR-DDT een map-request verstuurd zal deze door de DDT-Root, de DDT-Node op het hoogste niveau, worden gedelegeerd naar een DDT-node op een lagere laag in het model, tot dat het bij een DDT-MS aankomt die het verzoek kan beantwoorden. Eenmaal beantwoord kan de ITR die initieel het verzoek deed het verkeer sturen in de richting van de ETR die verantwoordelijk is voor de EID in zijn lokale netwerk.



Figuur 6.4 – LISP DDT Technologie

Voor het vinden van de juiste DDT-Node is er een nieuw bericht nodig op de control plane genaamd “map-referral”. Dit bericht kan op twee manieren worden gebruikt. Allereest als NODE-REFERRAL om map-reqeusts te refereren naar andere DDT-Nodes en ten tweede als MS-REFERRAL om te refereren aan een MS die over de informatie beschikt te gezocht wordt. De resterende informatie over de werking van LISP-DDT zal in het volgende hoofdstuk worden toegelicht.

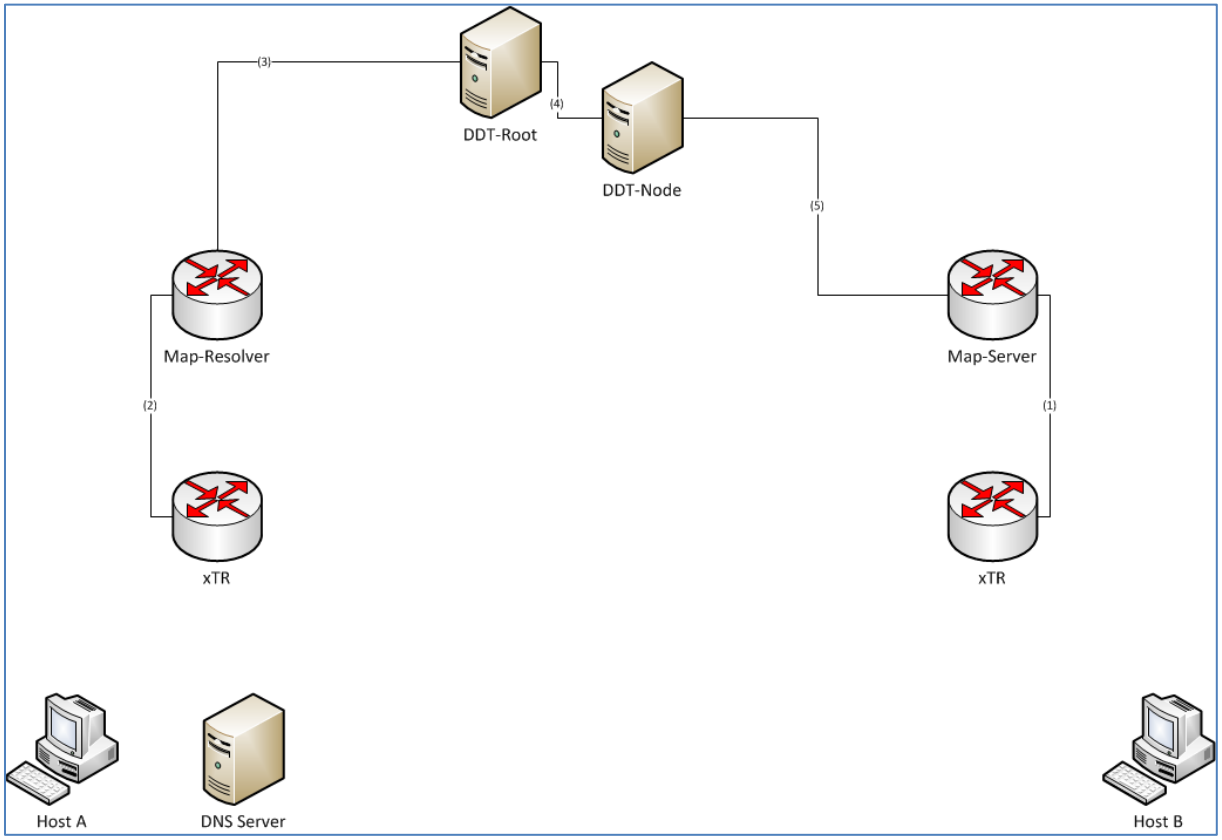
6.3 LISP TOPOLOGIËN

Het LISP protocol is op het moment inzetbaar, maar blijft een experimenteel protocol. Het feit dat niet alle netwerkomgevingen LISP ondersteunen brengt een nieuwe uitdaging met zich mee. Er moet worden gezorgd voor een verbinding tussen netwerkomgevingen die wel en niet LISP ondersteunen. Het kan tenslotte voorkomen dat verkeer van een niet-LISP omgeving wordt verstuurd naar een LISP omgeving en andersom. In deze paragraaf zal de werking van LISP op basis van het DDT model worden uitgewerkt, omdat DDT op het moment de standaard is van het bèta-netwerk.

6.3.1 LISP-TO-LISP

Wanneer verkeer wordt gestuurd naar een LISP omgeving en andersom zijn er grote verschillen in het proces. Toch begint het altijd op dezelfde manier met het vullen van de database van het mapping-system. Dat gaat aan de hand van het volgende stappenplan:

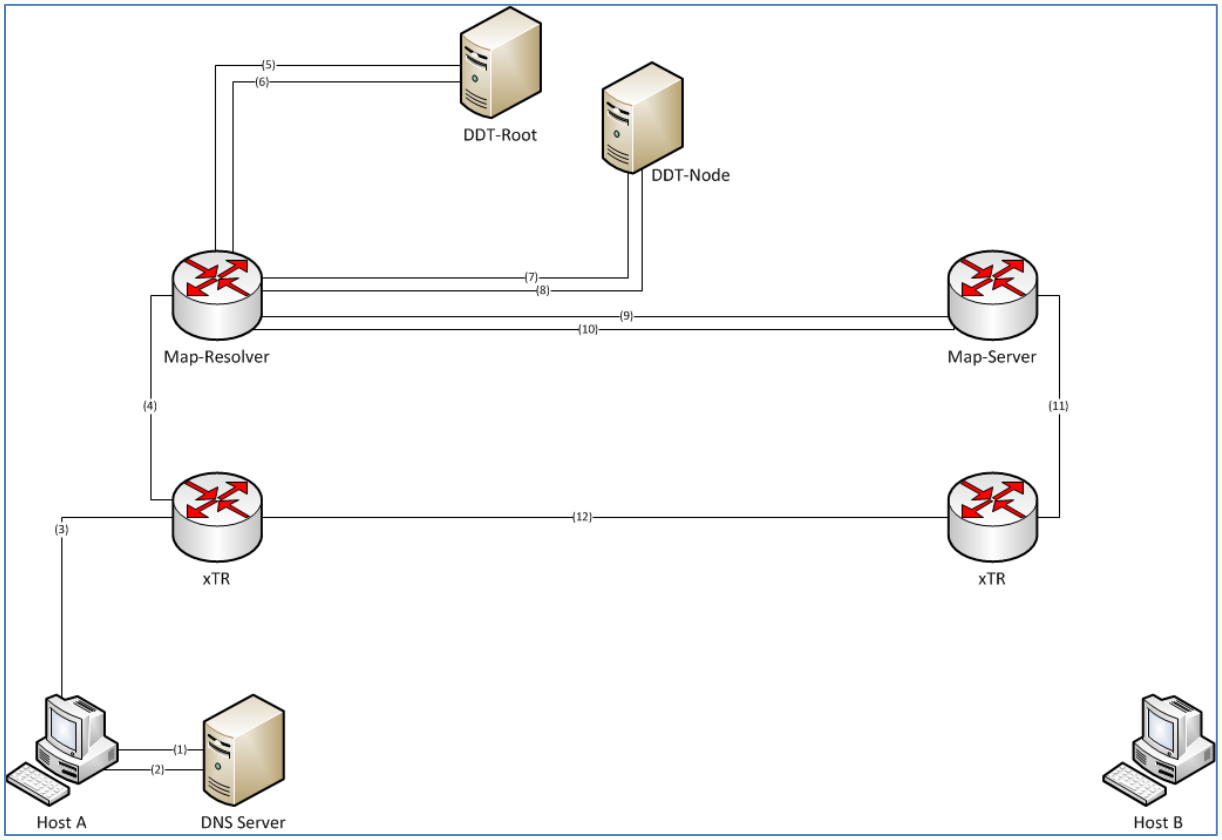
1. De ETR zet statisch aan de hand van commando's een EID-prefix dat in zijn lokale netwerk aanwezig is. De ETR geeft in het commando ook aan welke RLOC zich voor de EID's bevindt. Dit kan in een geval van multihoming ook meerdere RLOC's zijn, waarbij de prioriteit en verdeling van verkeer over de lijnen aangegeven kunnen worden. De ETR geeft met een commando aan wie zijn verantwoordelijke MS wordt met daarbij een afgesproken shared secret. Door middel van map-register berichten wordt de mapping doorgegeven aan de MS. Die kan eventueel een map-notify bericht retourneren om aan te geven dat een registratie gelukt is als de notify-flag gezet is in de LISP-header.
2. De ITR geeft aan welke MR verantwoordelijk zal zijn voor het afhandelen van zijn map-requests.
3. De MR geeft aan welke DDT-Root(s) verantwoordelijk is/zijn voor het afhandelen van zijn map-requests.



Figuur 6.5 – DDT Database invulling

4. De DDT-Root neemt alle delegaties op in zijn configuratie. In deze delegaties wordt aangegeven welke DDT-Nodes verantwoordelijk zijn voor bepaalde EID-prefixes. De DDT-Root moet in principe een delegatie bevatten voor elk mogelijke prefix.
5. De DDT-Node configureert twee lijsten. De ene lijst bevat gegevens van XEID-prefixes de DDT-MS bekend is en de tweede lijst bevat gegevens van DDT-Nodes aan wie hij kan delegeren wanneer dat niet het geval is.

De XEID-prefixes zijn vergelijkbaar met de eerder genoemde EID-prefixes. Aan deze adressen is een optionele voorvoegsel toegevoegd, de instance ID, voor het geval dat de EID-adressen die gebruikt worden niet uniek zijn in de netwerkomgeving. Dit kan bijvoorbeeld voorkomen in een Enterprise netwerk waarbij verschillende vestigingen dezelfde private adressen gebruiken.



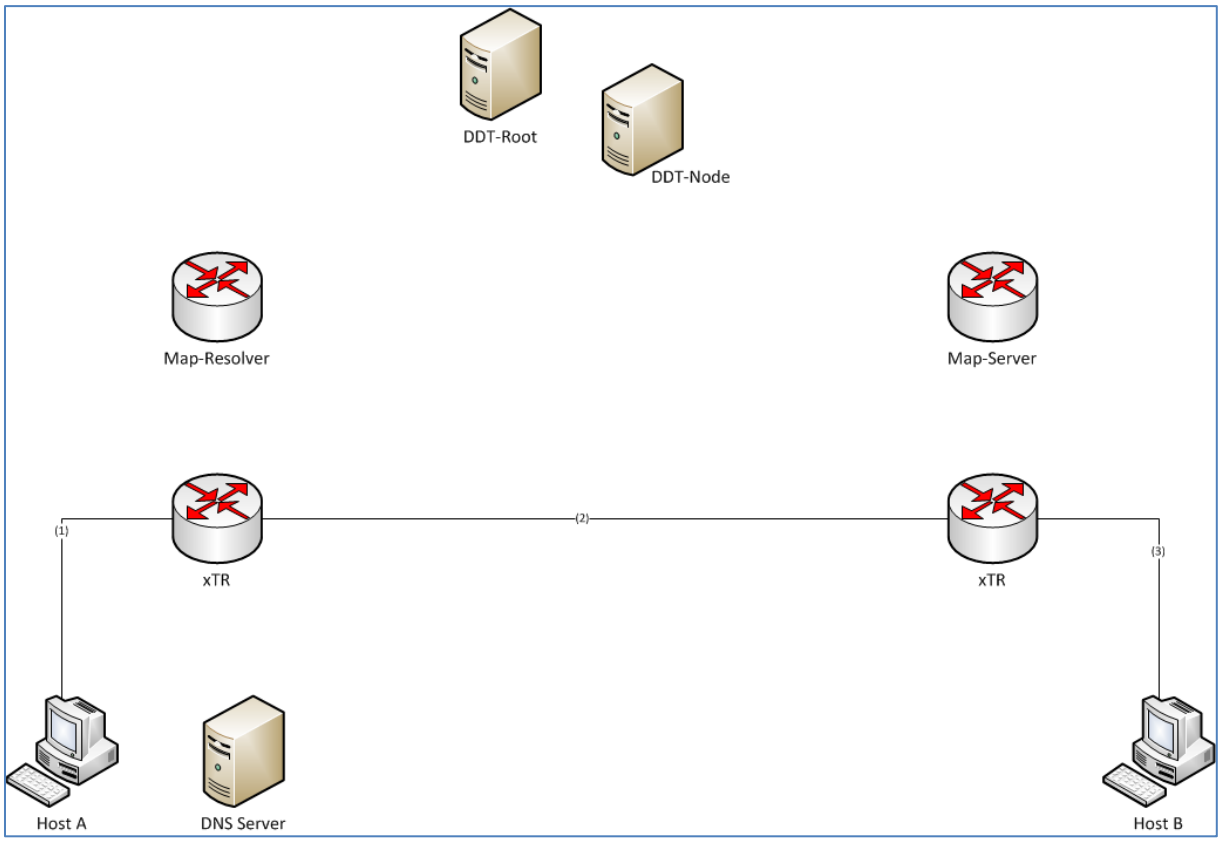
Figuur 6.6 – DDT zoek proces

Met een database dat over de informatie beschikt om map-request bij een MS te krijgen kan het proces om verkeer te sturen van host A naar host B gestart worden.

1. Host A verstuurt een DNS-query naar de DNS-server. Hierbij wordt een verzoek gedaan om de IP-adres achter een hostname. Bijvoorbeeld ‘lisp.cisco.com’ resolved naar het IP-adres ‘153.16.5.30’.
2. De DNS-server retourneert het gevonden IP-adres naar host A.
3. Host A maakt een IP-pakket aan en stuurt dat op basis van zijn routetabel naar zijn default gateway. De default gateway komt in dit voorbeeld overeen met een LISP-router (ITR).
4. Wanneer het pakket aankomt bij de ITR wordt er gekeken of het pakket kandidaat is voor LISP-encapsulation. Hiervoor moet het pakket voldoen aan één van de onderstaande vier criteria. In dit voorbeeld gaat het om verkeer van een LISP omgeving naar een andere LISP omgeving. Er wordt dus voldaan aan de eisen. De ITR maakt een map-request aan en stuurt deze naar zijn MR.
    - Het verzoek komt van een bekende EID-host
    - Er is een map-entry bekend in de cache tabel

- Er is een route aanwezig naar een legitieme (LISP) next-hop
- Er is geen route aanwezig

5. In de queue van de MR wordt een “pending request” aangemaakt, wat betekent dat er wordt gewacht op een antwoord die aangeeft in welke richting het pakket gestuurd moet worden. Als er geen oude informatie bekend is bij de MR die antwoord biedt op de locatie wordt de map-request doorgestuurd naar de DDT-Root.
6. De DDT-ROOT raadpleegt zijn delegaties en reageert op de map-request met een NODE-REFERAL. Die geeft aan welke DDT-Node autoriteit heeft over de prefix die gezocht wordt.
7. De MR slaat deze NODE-REFERAL op in zijn referral-cache en stuurt een nieuwe map-request naar de aangegeven DDT-Node.
8. De DDT-Node raadpleegt zijn twee lijsten. Als er geen MS bekend is wordt er gedelegeerd naar een andere DDT-Node door middel van een NODE-REFERRAL. In dit geval is er wel een MS bekend en reageert de DDT-Node met een MS-REFERAL die aangeeft welke MS verantwoordelijk is voor de prefix.
9. De MR maakt een laatste map-request aan en stuurt deze naar aangegeven MS.
10. De MS reageert naar de MR met een map-referral bericht met actiecode “MS-ACK” om te bevestigen dat hij inderdaad verantwoordelijk is voor de gezochte prefix. De MR ontvangt dat bericht en gebruikt het om de eerder aangemaakte pending-request uit de queue te halen. Tevens stuurt de MS de map-request door naar de ETR.
11. Na controle of de EID zich inderdaad in het lokale netwerk van de ETR bevindt stuurt de ETR een map-reply naar de ITR die het verzoek initieerde. Aan de hand van dit bericht kan de ITR een route plaatsen in zijn mapping-cache, zodat er een route bestaat om het verkeer langs te sturen.

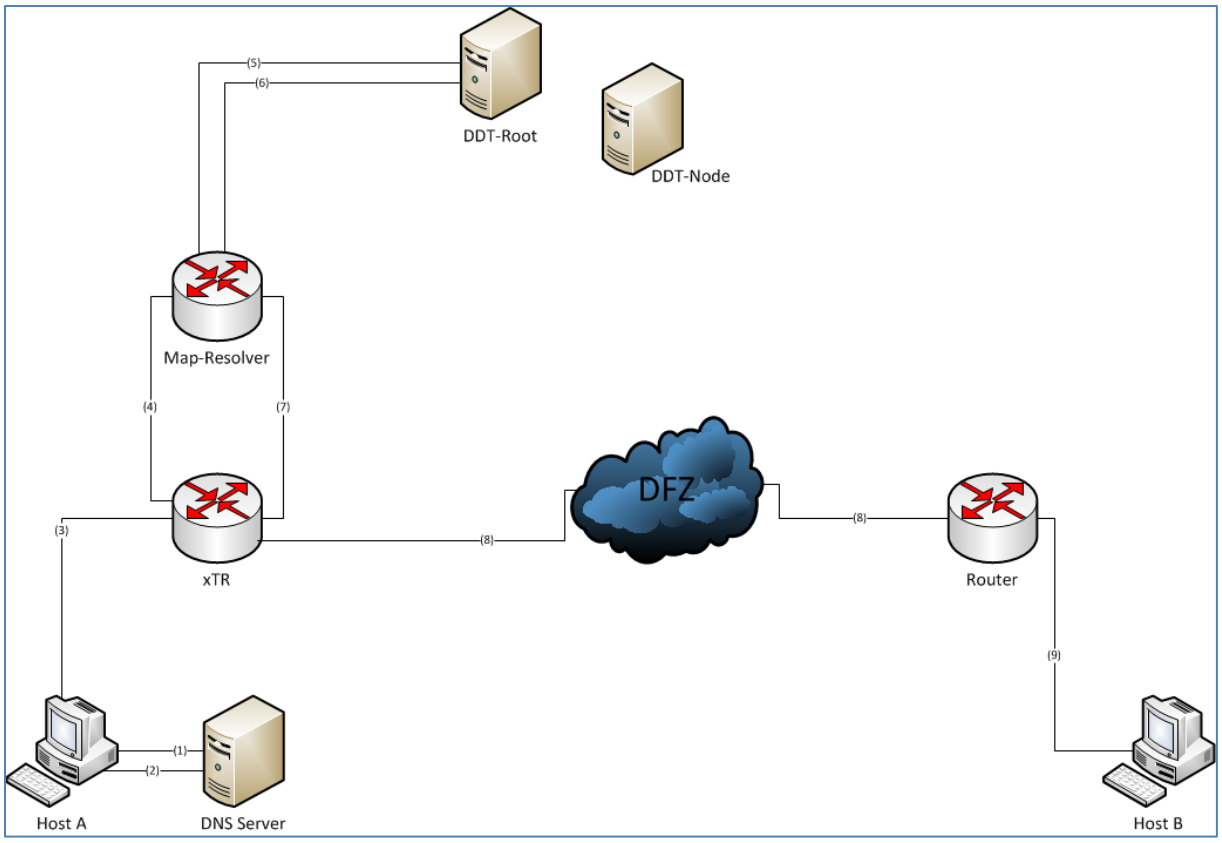


Figuur 6.7 – Verkeer sturen EID

Met de route aanwezig in de mapping-cache van de ITR kan verkeer voortaan worden verstuurt zonder dat daar een DDT-database voor nodig is. Er dient slechts op de ITR LISP-encapsulation toegepast te worden, die op de ETR wordt verwijdert. Aan de hand van het IP-adres wat tijdens het decapsulation proces naar voren komt, weet de ETR voor welke host het pakket is bedoeld.

6.3.2 LISP-TO-NON-LISP

De tweede topologie die besproken wordt is het versturen van verkeer van een bekende LISP omgeving naar een omgeving zonder LISP ondersteuning. Hierbij wordt er vanuit gegaan dat het vullen van de database al heeft plaatsgevonden.



Figuur 6.8 – LISP – to – Non-LISP

Het proces start met stap één, twee en drie dat door middel van DNS in een IP-pakket resulteert bij de ITR. De ITR bepaald aan de hand van de criteria dat het pakket in aanmerking komt voor LISP-encapsulation en stuurt een map-request (4) naar de MR die een pending-request in de queue zet. Hierna wordt het een nieuwe map-request naar de DDT-Root gestuurd (5). Vanaf hier wordt het proces anders.

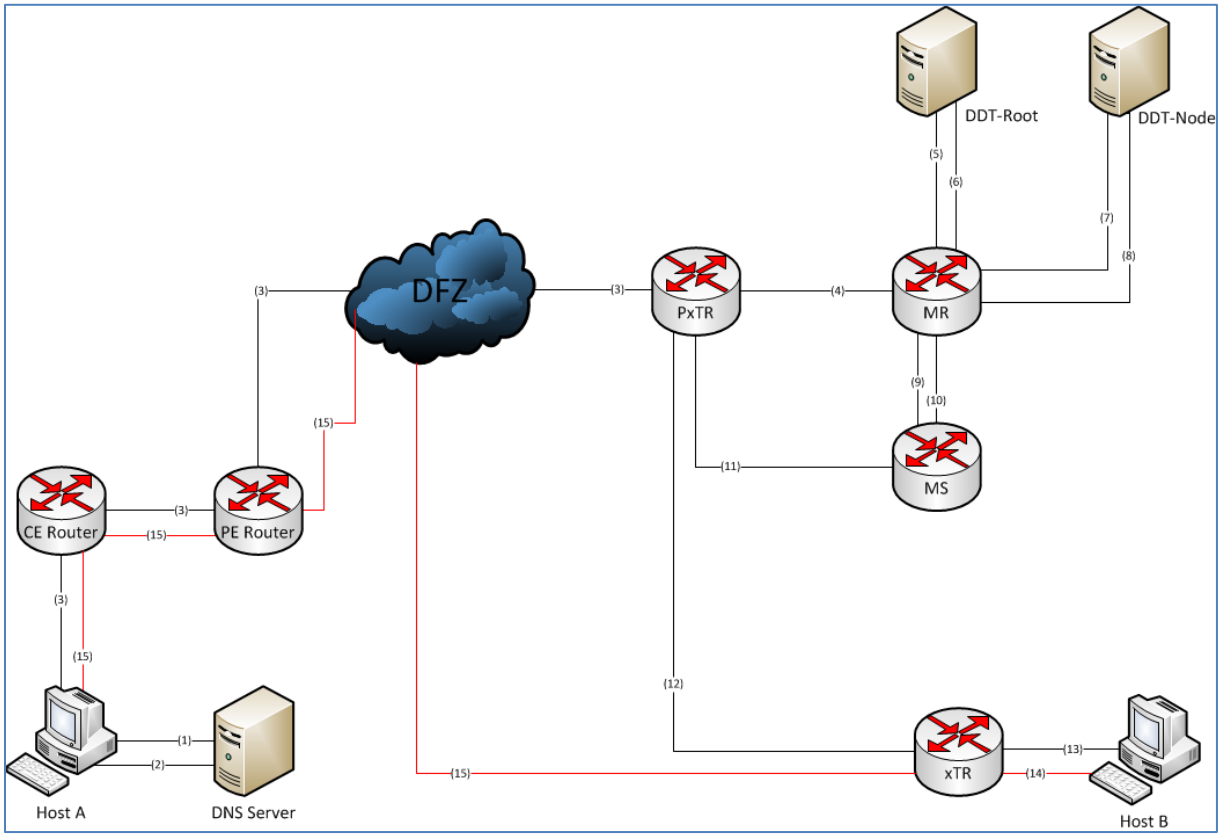
6. Omdat de eindbestemming geen LISP-EID is kan de DDT-Root geen bestaande koppeling vinden in zijn delegaties. Er wordt door de DDT-ROOT een map-referral bericht aangemaakt en teruggestuurd met actiecode “Delegatie-hole”. Dit houdt in dat een aggregatie meegestuurd waar geen delegatie voor bekend is, maar waar de gezochte IP-adres wel onder valt.
7. De MR interpreteert dit bericht als een niet bekend EID en maakt daar een negatief map-reply voor aan met de melding “Natively-Foward” die geretourneerd wordt aan de ITR. De MR verwijdert ook de pending-request uit de queue.
8. Aan de hand van de negatieve map-reply wordt een route in de mapping-cache gezet met en een TTL van 15 minuten. Deze route wordt gebruikt om verkeer te sturen via de DFZ, zonder dat daar LISP encapsulation aan wordt toegevoegd.

Er kunnen situaties voorkomen waarbij een ITR is geconfigureerd om verkeer wel te voorzien van een LISP-encapsulation, terwijl het bestemd is voor een niet-LISP omgeving. Dit verkeer wordt dan doorgestuurd naar een zogeheten “Proxy-ETR (PETR)”. De PETR is logisch gezien geplaatst tussen de ITR en DFZ (8) en zal de encapsulation verwijderen voordat het verkeer wordt doorgestuurd naar zijn eindbestemming. De reden voor zo’n PETR kan het overbruggen van een IPv4/IPv6 transitie zijn.

6.3.3 NON-LISP-TO-LISP

Veruit de moeilijkste topologie is het versturen van verkeer van een niet-LISP omgeving naar een wel-LISP omgeving. De grootste uitdaging bevindt zich in het feit dat er standaard geen routes aanwezig zijn naar de LISP omgevingen (D. Lewis, 2013). Om deze uitdaging te overwinnen is er een nieuw onderdeel nodig, de Proxy Ingress Tunnel Router (PITR).

De PITR bevindt zich op de grens tussen de DFZ en LISP omgeving en houdt zich bezig met het distribueren van routes, zodat eindsystemen buiten LISP omgevingen toch een mogelijkheid hebben om EID's te bereiken. Om het distribueren van LISP-routes te realiseren in het DFZ wordt op het moment in het bèta-netwerk gebruikt gemaakt van statische null0 routes om aggregaties te adverteren naar BGP routers. Tevens zijn er op het moment ontwikkelingen aan de gang om dit statische model te vervangen met een EID-route-server model die dynamisch de juiste routes kan adverteren.



Figuur 6.9 – Non-LISP to LISP

Het proces begint bij host A met een DNS-request (1) en DNS-reply (2) om het IP-adres van host B te vinden. Aan de hand van dit IP-adres wordt een IP-pakket opgezet die vervolgens richting het DFZ wordt gestuurd via de klant router (CE) en ISP router (PE) tot dat het bij een PxTR aankomt die de route voor het gezochte IP-adres heeft geadverteerd. De PxTR gaat volgens de bekende DDT-manier van opzoeken een EID-to-RLOC mapping opvragen (4-11) tot dat de PxTR een RLOC adres terug krijgt van een ETR die verantwoordelijk is voor host B.

De PxTR voorziet het originele IP-pakket van encapsulation en stuurt het bericht door naar de gevonden ETR. De ETR decapsulate het bericht en stuurt het door naar host B. Om te reageren op het bericht stelt host B ook een IP-pakket op en stuurt deze door naar zijn ITR. De ITR zal in dit geval het bericht niet voorzien van encapsulation, omdat er na het raadplegen van de DDT-database bekend zal worden dat het eindsysteem geen bekende EID is. Vervolgens zal het bericht natively worden doorgestuurd naar de DFZ waarna het bericht later wordt afgeleverd bij host A via normale routing procedures.

6.4 UITZONDERINGEN

In de vorige paragrafen zijn verschillende voorbeelden uitgewerkt van de manier waarop LISP werkt. In deze voorbeelden is er vanuit gegaan dat alle processen zonder problemen verlopen. Er zijn een aantal uitzonderingen mogelijk binnen deze situaties die hieronder worden uitgewerkt.

Autoriteit
Als beveiliging tegen ongeldige invoer in de mapping-database dient er in de configuratie van LISP netwerkelementen aangegeven te worden voor welke prefixes een element autoriteit heeft. Het kan voorkomen dat wanneer een map-request aankomt bij een MS of DDT-Node hij niet de juiste autoriteit heeft om op het bericht te reageren. Op deze map-requests wordt gereageerd met map-referral berichten met actiecode “NOT-AUTHORITATIVE”. Wanneer dit bericht aankomt bij de MR die de map-request verstuurde kan de MR proberen het verzoek opnieuw in te dienen bij de DDT-ROOT. Dit met de reden dat een autoriteitsprobleem ook kan voorkomen door een slechte synchronisatie van de database. Als dit ook niet werkt dan zal de MR het bericht verwijderen zonder terugkoppeling naar de ITR.

Registratie
Wanneer een MS een map-request ontvangt dient hij dit verzoek te koppelen aan een geregistreerd ETR die verantwoordelijk is voor de gezochte prefix. Het kan door misconfiguratie voorkomen dat er geen ETR bekend is. De MS zal reageren met een negatief map-referral bericht met actiecode “MS-NOT-REGISTERED” die naar de verstuurder van de map-request wordt geretourneerd. De MR die het bericht verstuurde zal als het mogelijk is de map-request versturen naar andere verbonden MS’en. Als er geen andere mogelijkheden zijn om het verzoek naar te sturen zal de MR een negatief map-reply bericht retourneren naar de ITR die een negatief mapping-cache entry maakt met een TTL van één minuut. Aan de hand van de negatieve mapping kan de ITR proberen het gezochte EID te bereiken via het traditionele internet.

Loop Detection
Bij het raadplegen van de DDT-database worden constant map-referral berichten geretourneerd die meer specifieke informatie over een EID-prefix bevatten. Het kan voorkomen door misconfiguratie dat een oneindige keten van map-referrals ontstaat. Om dit te voorkomen wordt er door de MR in zijn cache-referral berichten bijgehouden om te controleren of de prefix die de DDT-Nodes retourneren ook daadwerkelijk specifieker wordt. Als dit niet het geval is worden deze berichten verwijderd. Dit kan als resultaat hebben dat een map-request nooit beantwoord wordt. De manier waarop hiermee moet worden omgegaan is bij LISP nog in ontwikkeling, maar om het tijdelijk op te vangen wordt het proces afgerond met een negatief map-reply bericht. Hierdoor kan er geprobeerd worden om het pakket natively te versturen.

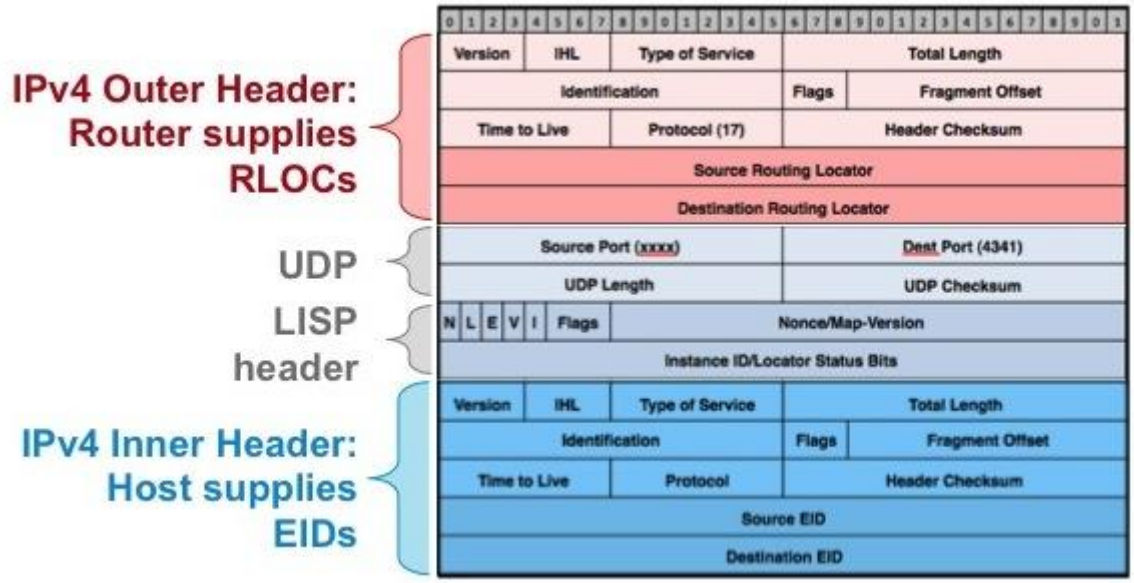
LISP NAT
Om connectiviteit tussen LISP en niet-LISP omgevingen te realiseren dienen de adressen globaal routeerbaar over het internet te zijn. Als oplossing voor dit probleem is het mogelijk om op de xTR’s een uitgeklede vorm van NAT te implementeren genaamd LISP-NAT. Het proces van LISP-NAT werkt hetzelfde als het normale NAT protocol en zorgt ervoor dat interne EID’s worden verschuilt achter een publiek IP dat wel globaal routeerbaar is. De koppeling tussen de originele en nieuwe IP-adres worden bijgehouden in een tabel om terugkerend verkeer in de goede richting te wijzen.

6.5 LISP HEADER

In deze paragraaf zal de LISP header worden toegelicht die nodig is voor het sturen van verkeer van- en naar eindsystemen die zich in LISP omgevingen bevinden.

6.5.1 TOELICHTING HEADER

Wanneer een host verkeer wil sturen naar een andere host terwijl er gebruik wordt gemaakt van LISP dient er encapsulation toegepast te worden door een ITR. Hierbij wordt een IPv4- of IPv6 pakket voorzien van een LISP-header en word RLOC informatie bijgevoegd. De volgende afbeelding is het resultaat van encapsulation



Figuur 6.10 – LISP Encapsulation

Het pakket bestaat uit vier componenten. Het eerste component is de inner header (IH). De IH is afkomstig van een datagram die door de originele host is verzonden. Dit onderdeel bevat de afzender- en bestemmingsadres van de EID's die contact willen. Het tweede onderdeel is de outer header (OH). Dit onderdeel wordt door een ITR geplaatst en bevat informatie over RLOC die zich voor de EID's bevindt. Het derde deel is de UDP header en bevat de poorten die door de ITR zijn geselecteerd. Normaliter gaat het hier om poort 4341 en 4342.

Als laatste is er de LISP header. Die bestaat op zichzelf ook uit een aantal componenten. Allereerst zijn er de flag bits:

- **Nounce-present-bit (N)**. Wanneer dit bit wordt aangezet bevat de "nonce/map-version" gedeelte van de header een 24-bit getal, de nonce. Deze bit mag niet tegelijk actief zijn met de V-bit.
- **Locator-status-bits (L).** Wanneer dit bit wordt aangezet worden de 32-bits van de locator status bits actief in de LISP-header.
- **Echo-nonce-bit (E).** Wanneer dit bit wordt aangezet in combinatie met het N-bit wordt de nonce terug "ge-echoed" in encapsulated berichten. Dit is nodig wanneer een router zowel ITR als ETR is.
- **Map-Version-bit (V).** Wanneer dit bit actief is, mag de N-bit dat niet zijn. Door dit bit te activeren wordt het "nonce/map-version" gedeelte ingericht met een source- en destination map-version.
- **Instance-ID-bit (I).** Wanneer dit bit actief is worden de locator-status-bits gereduceerd naar 8-bits en worden de overige 24-bits gebruikt als instance ID.
- **Flags.** De overige 3 bits zijn gereserveerd voor toekomstige veranderingen aan het LISP protocol.

De overige gedeelten worden actief wanneer bepaalde bits aangezet zijn. Het gaat om de volgende onderdelen:

- **Nonce**. Een 24-bits getal dat random wordt gegenereerd en gebruikt wordt voor het beschermen van verkeer tegen bijvoorbeeld replay attacks. Tevens wordt de nonce in combinatie met het E-bit gebruikt om bereikbaarheid van routes te bevestigen.
- **Map-version**. Wanneer dit gedeelte actief is wordt het ingericht met source- en destination map-version getallen. Wanneer een ETR map-reply berichten verstuurt voorziet hij de destination map-version met een versienummer. Wanneer een ITR verkeer stuurt naar een ETR voorziet hij het verkeer ook van een versienummer. In dit geval in de source map-version. Deze versienummers worden gebruikt om oudere versies te herkennen waarbij een hoger getal wordt gezien als een recentere versie.
- **Instance ID**. Dit ID-nummer wordt gebruik om EID's om te zetten naar XEID's. Dit voorvoegsel wordt gebruikt op IP-adressen waarvan niet gegarandeerd kan worden dat ze uniek zijn in een omgeving. Bijvoorbeeld een Enterprise met meerdere locaties die dezelfde private adressen gebruiken of het LISP bèta-netwerk waar meerdere EID-omgevingen dezelfde private adressen gebruiken.
- **Locator status bits**. Deze bits worden gebruikt om bereikbaarheid tussen ITR en ETR's te controleren. Elk RLOC in een map-reply krijgt een getal toegewezen. Wanneer het bit dat overeenkomt met dat getal op één wordt gezet geeft de ITR daarmee aan voor de ETR dat de RLOC bereikbaar is.

6.5.2 MTU PROBLEMEN

De LISP header die wordt toegevoegd aan IP-pakketten zorgt voor een extra 36 bytes bij IPv4 en 56 bytes bij IPv6 die meegestuurd moeten worden. Dit kan voor problemen zorgen bij netwerkcomponenten die een maximale MTU-size toestaan van 1500 bytes, de standaard maximale grootte van een ethernetframe. Om dit probleem te verhelpen zijn er twee oplossingen bedacht.

Stateless oplossing

De eerste oplossing is een stateless oplossing, wat wil zeggen dat alle pakketten die verstuurd worden onafhankelijk zijn van elkaar en zelf de versturing en afhandeling regelen, zonder dat een voorgaand pakket daar invloed op heeft. Het idee achter deze stateless oplossing is het definiëren van een maximale MTU grootte die niet overschreden mag worden. Wanneer dit wel gebeurt, zoals bij het plaatsen van een LISP-header, dient het pakket opgedeeld te worden in twee stukken van gelijke grote. Beide fragmenten worden vervolgens encapsulated en doorgestuurd naar een ETR, die bij ontvangst de fragmenten decapsulate en doorstuurt naar de eindbestemming. Daar worden de pakketten weer samengevoegd tot het originele IP-pakket.

Om deze techniek toe te passen is het nodig om het "Don't Fragment" bit van de IPv4-header op 0 te zetten. Wanneer dit niet gebeurt en het DF-bit op 1 wordt gezet zal het pakket worden gedropt bij de ITR, omdat het pakket de maximale MTU-grootte overschrijdt.

Statefull oplossing

De tweede oplossing is een statefull oplossing wat betekent dat de versturing van een set pakketten afhankelijk is van de afhandeling van voorgaande pakketten. De statefull oplossing is het bijhouden van de maximale MTU-grootte tussen ITR en ETR in de map-cache. Wanneer een pakket wordt verstuurd en deze te groot blijkt te zijn wordt aan de hand van een ICMP "Packet Too Big Message" aan de ITR bekend gemaakt dat het pakket niet kan worden verstuurd. De ITR verwerkt dit bericht en past de maximale MTU in de map-cache aan van de router die het bericht niet kon verwerken.

Wanneer de ITR een pakket ontvangt die verstuurt moet gaan worden wordt eerst de MTU gecontroleerd aan de hand van de gegevens in de map-cache. Wanneer de grootte van het pakket te groot blijkt te zijn wordt er een ICMP "Packet Too Big Message" geretourneerd naar aan de afzender van het pakket, met daarin de

maximale MTU grootte die afkomstig is uit de map-cache. De afzender kan het bericht nu opnieuw proberen met een kleinere MTU grootte.

Het is aan de persoon die het netwerk opzet om te bepalen welke oplossing wordt gebruikt. De voorkeur gaat uit naar een stateless oplossing, omdat de werking van de statefull oplossing niet gegarandeerd kan worden. Veel netwerken blokkeren ICMP verkeer in de firewall, waardoor de statefull oplossing niet zal werken.

6.6 MOGELIJKHEDEN VAN LISP

Hoewel de verschillende mogelijkheden en technieken die LISP met zich mee brengt in een later hoofdstuk uitgebreid worden toegelicht, zal in deze paragraaf kort worden omschreven in welke omstandigheden LISP een verrijking kan zijn voor een netwerk.

Multihoming
Om de beschikbaarheid van een netwerk hoog te houden wordt vaak gebruik gemaakt van technieken als multihoming. Hierbij wordt een lokaal netwerk verbonden met één of meer externe locaties. Normaliter zijn die externe locaties verschillende ISP's. Om die verbindingen te realiseren wordt vaak gebruikt gemaakt van het BGP protocol. BGP brengt de nodige problemen met zich mee, omdat het een zwaar protocol is met directe impact op het internet.

Doordat LISP gebruik maakt van een scheiding tussen locatie en identiteit en deze koppelingen opslaat in een database, kan er gemakkelijk en goedkoop voor multihoming gezorgd worden in een netwerk. Doordat er eerst een pad naar de gezochte locatie wordt opgezocht in de database, kan de ETR aangeven over welke link hij verkeer wilt ontvangen door middel van zijn priority- en weight parameters. Met deze oplossing is BGP niet meer nodig om de lijnen te beheren en kan er multihoming worden ingericht met routers die over minder kracht beschikken.

IP Mobility
Door de scheiding tussen locatie en identiteit is het mogelijk om eindsystemen te verplaatsen in een netwerk, zonder dat er aanpassingen nodig zijn om connectie te herstellen. Het is mogelijk om een eindsysteem te verplaatsen naar een andere vestiging waar de xTR die de veranderingen detecteert een wijzigingen doorvoert in de database. Dit gebeurd binnen enkele seconden, waarna de verbinding hersteld is. Dit werkt in theorie beter dan huidige technieken waarbij je gedwongen bent veranderingen door te voeren, omdat je IP-adres bepaald wie jij bent en waar je bent.

IPv4 – IPv6 transitie
Doordat LISP routers gebruik maken van encapsulation is het mogelijk om zowel IPv4 als IPv6 adressen aan te geven in de header. Hierdoor is het mogelijk voor een IP-pakket om door middel van encapsulation een IPv6 netwerk te overbruggen om vervolgens door een PxTR te worden decapsulated en doorgestuurd worden over een IPv4 netwerk. Deze techniek werkt ook van wanneer een IPv4 netwerk moet worden overbrugt om vervolgens over te gaan in IPv6.

De bovenstaande technieken zijn op het moment de grootste voordelen van LISP naast het feit dat LISP helpt bij het terugdringen van de overgelopen routetabellen in de DFZ. Tevens zijn er ook ontwikkelingen in gang voor het regelen van fast mobility voor mobiele telefoons, open source LISP voor linux en segmentatie van netwerkverkeer door verschillende VPN's op basis van instance id's.

6.7 BEVEILIGING

In de huidige tijd waarin het internet zich bevindt is er steeds meer vraag naar goede beveiliging van protocollen. Dit is bij het LISP protocol ook zeer belangrijk aangezien je met routering van verkeer te maken hebt. Aantasting van de tabellen in de routers en mapping-servers zouden tot verkeer in de verkeerde richting kunnen leiden met man-in-the-middle-attacks als gevolg.

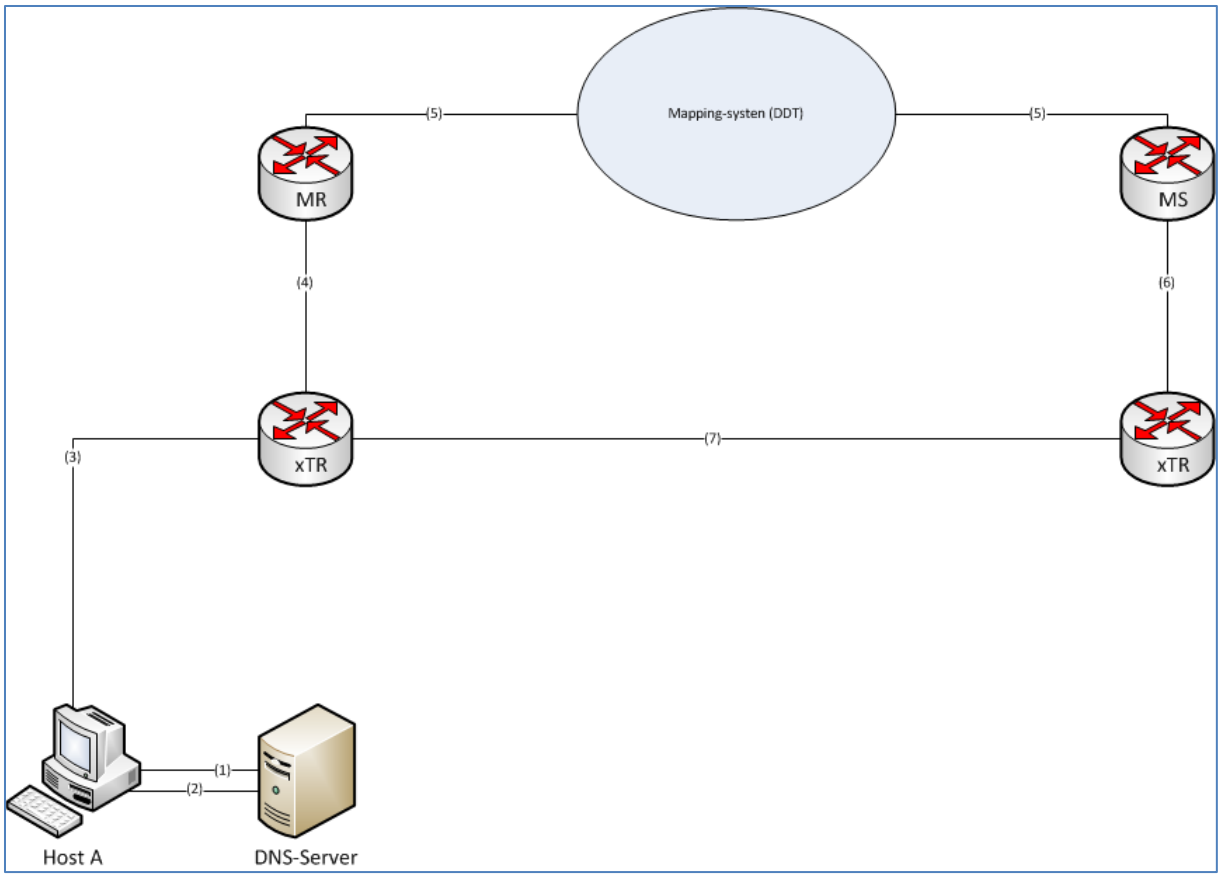
Onderzoekers hebben reeds een threat-analysis uitgevoerd op het LISP protocol (D. Saucez, 2014). Daarbij zijn verschillende vormen van aanvallen gecategoriseerd. Het gaat hierbij om het volgende:

- **On-path & off-path attacks**. De focus van deze aanvallen ligt op het onderscheppen en veranderen van pakketten of het injecteren van zelfgemaakte pakketten.
- **Internal & External attacks**. Hierbij gaat het om een aanval lanceren vanuit een legitiem LISP omgeving of bij external attacks van buitenaf een aanval lanceren op een LISP omgeving.
- **Live attacks & Time-shifted attacks**. Bij live attacks duurt de aanval zolang er verbinding is. Bij Time-shifted aanvallen gaat de aanval nog door nadat de verbinding verbroken is.
- **Control-plane & Data-plane attacks**. Bij control-plane aanvallen worden controleberichten onderschept om het mapping-system aan te vallen. Bij data-plane aanvallen worden aanvallen gepleegd op de routes zelf. Er is geen fysieke scheideing tussen de twee lagen, wat betekent dat aanvallen vaak gecombineerd worden.
- **Cross mode attacks**. Een aanval waarbij verschillende van de bovenstaande aanvallen worden gecombineerd.

Voorbeelden van aanvallen die onder deze categorieën vallen zijn replay aanvallen, pakket manipulatie, adres spoofing en denial of service. Met deze analyse als achtergrondinformatie zijn verschillende beveiligingsopties toegevoegd in het LISP-model.

- **Nonce**. Het ontwikkelteam van LISP verwacht dat de meeste aanvallen uitgevoerd zullen worden op het mapping-system van de control plane om EID-to-RLOC mappings te bemachtigen en beïnvloeden. Om deze reden is er een 24-bit getal toegevoegd aan de LISP-header en een 64-bit getal in de LISP controle berichten. Dit getal is door zijn grote omvang nagenoeg niet te raden, waardoor aanvallers geen eigen berichten kunnen injecteren. Mocht dit toch geprobeerd worden werkt de nonce als een verificatie dat er niet met de inhoud geknoeid is.
- **Rate-limiting**. Aanvallers kunnen proberen grootte hoeveelheden mappings te injecteren om de juiste nonce te raden of om een denial-of-service aanval te lanceren. Door een limiet aan te geven van de hoeveelheid map-replies gestuurd mogen worden kan zo'n aanval worden afgeweerd.
- **EID-Verification**. Spoofing van een EID-adres is altijd mogelijk, maar het gevolg kan worden voorkomen doordat de ETR's altijd in hun eigen mapping-database controleren of een EID daadwerkelijk actief is in het lokale LISP netwerk.

Hoewel deze standaard implementaties al een goede bescherming leveren tegen veel aanvallen is er op het moment en ontwikkeling aan de gang voor een extra laag bescherming voor LISP in de vorm van LISP-SEC (F. Maino, 2014). Het LISP-SEC model werkt op basis van one-time-keys (OTK). Bij elk proces dat gestart wordt voor het opzoeken van een EID-to-RLOC koppeling wordt het volgende uitgevoerd.



Figuur 6.11 – LISP-SEC

Het LISP-SEC systeem start standaard met stap één, twee en drie, waarbij een DNS-query resulteert in een IP-pakket dat bij de ITR aankomt. Eenmaal beoordeelt dat het pakket voor een LISP-EID bestemt is wordt het OTK-systeem gestart.

4. De ITR genereert een ITR-OTK en slaat deze lokaal op. Er wordt een map-request aangemaakt waar de ITR-OTK ook in meegestuurd wordt en verstuurt naar de MR.
5. De MR maakt een nieuwe map-request aan met diezelfde ITR-OTK erin en stuurt deze door middel van de DDT mapping-system richting de MS.
6. De MS bepaalt met zijn mapping de juiste EID-prefix die nodig is en voorziet deze van een hash based message authentication code (HMAC) op basis van de ITR-OTK. Tevens genereert de MS een nieuwe OTK (MS-OTK). Zowel de gehashde prefix als de nieuwe OTK worden in een nieuwe map-request in de richting van de ETR gestuurd.
7. De ETR neemt de informatie over uit het vorige bericht en plaatst deze in een map-reply die ook voorzien wordt van een HMAC op basis van de MS-OTK. Daarna wordt het bericht naar de initiële ITR gestuurd.
8. De ITR controleert de EID-to-RLOC koppeling door middel van de lokaal opgeslagen OTK-ITR. De ITR genereert ook dezelfde MS-OTK om de map-reply te controleren. Als één van de twee onderdelen niet door de controle komt wordt het bericht verwijderd.

Op basis van de functionaliteit die LISP-SEC levert is het mogelijk om LISP verkeer te voorzien van afzender authenticatie en integriteit met daarnaast ook goed beveiliging tegen replay-aanvallen. Wat niet standaard in LISP of LISP-SEC aanwezig is, maar wel dient te worden geïmplementeerd is een shared secret tussen de ITR en MR zoals deze ook aanwezig is tussen de ETR en MS. Hiermee kan het transporteren van de OTK's ook veilig gebeuren.

6.8 LISP ONDERSTEUNING

Hoewel LISP als open standaard wordt ontwikkeld en gepubliceerd is betekent het niet dat LISP aanwezig is op alle fabrikanten van netwerkapparatuur. Het is op het moment vooral nog Cisco routers die ondersteuning aanbieden. In deze paragraaf worden de verschillende vormen van toepassingen opgesomd die LISP ondersteunen (LISP Feature Support by Operating System, 2014).

Cisco
Het is bekend dat Cisco de meeste ondersteuning biedt bij het implementeren van LISP. Zo is LISP in grote mate ondersteund door IOS, IOS-XE, NX-OS, IOS-XR en CatOS operating systems van Cisco. Deze operating systems zijn breed verspreid over zeer veel versies van Cisco apparatuur.

Tabel 6.1 – Overzicht Cisco Apparatuur met LISP – Bron: (Cisco Systems, 2014)

IOS	IOS-XE	NX-OS	IOS-XR	CatOS
ISRG1	**ASR1K**	**Nexus 7000**	ASR 9000	Catalyst 6K
1800 series	ASR 1001, -X	7000 series	9000 series	6500 series
2800 series	ASR 1002. –X	7700 series		6800 series
3800 series	ASR 1004			
7200 series	ASR 1006			
	ASR 1013			
	ISR 4451-X			
ISRG2	**CSR1KV**			
800 series	CSR1KV			
900 series				
1900 series				
2900 series				
3900 series				

LISPmob
In het kader van open standaard is er ook een opensource project gestart voor de ontwikkeling en distributie van LISP. Het project werkt onder de naam LISPmob. Door middel van dit project is LISP nu beschikbaar voor alle Linux, Android en OpenWRT systemen. Het LISPMob project loopt qua ondersteuning iets achter op implementaties zoals die van Cisco, maar het bevat wel de meest belangrijke zaken. Zo is het mogelijk om te verbinden met het DDT bèta-netwerk en worden technieken als multihoming ook ondersteund.

Fritz!Box
De klanten van XS4ALL ontvangen bij het afsluiten van een abonnement een fritzbox voor het aansluiten van het internet. Sinds fritzbox versie zes wordt ook LISP ondersteund. Dit is wel een beperkte versie.

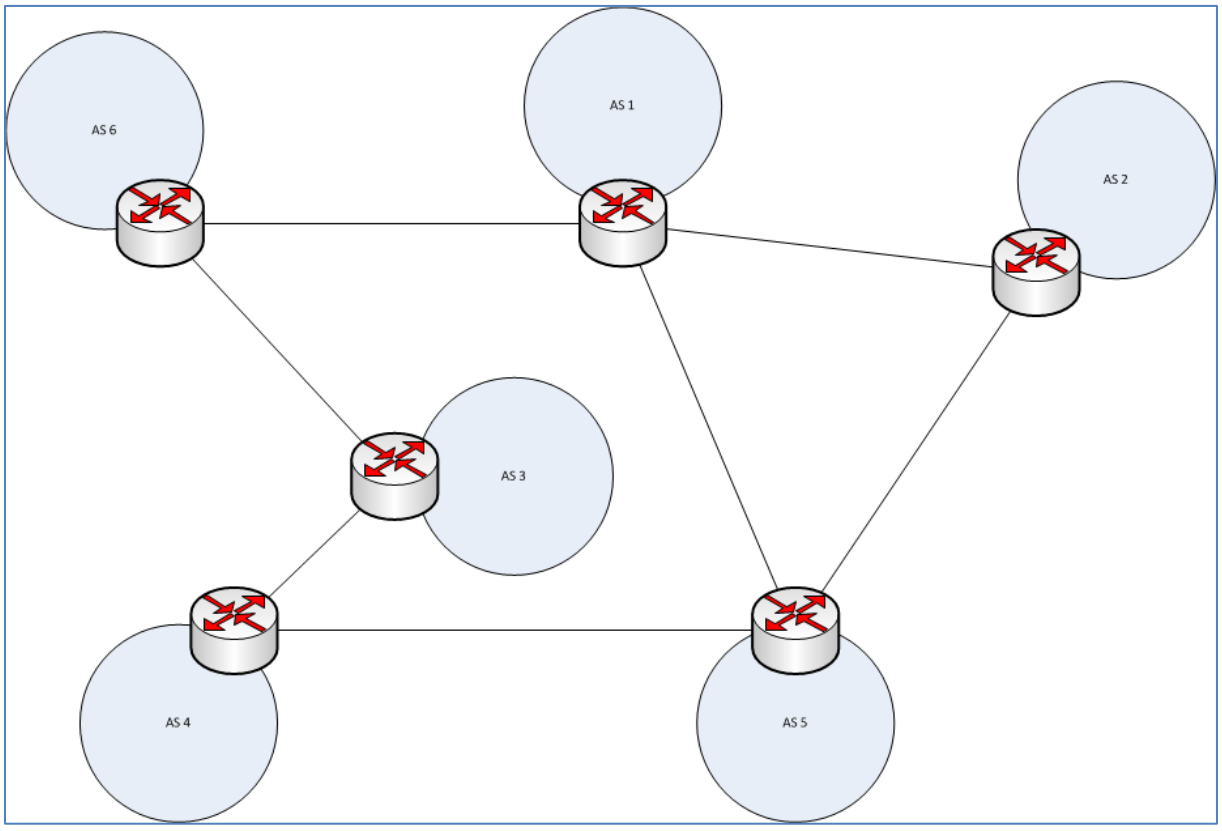
7. LISP VS ANDERE PROTOCOLLEN

Het LISP protocol is op verschillende momenten verward als routeringsprotocol, omdat het op meerdere momenten aangedragen is als vervanger van protocollen als BGP en MPLS. In dit hoofdstuk zal LISP worden vergeleken met verschillende protocollen om te bepalen in hoeverre het een vervanger is.

7.1 BGP

Het Border Gateway Protocol (BGP) is het meest belangrijke routeringsprotocol dat actief is in het huidige internetmodel en is verantwoordelijk voor het transporteren van routeringsinformatie tussen autonomous systems (AS) in het DFZ. Een AS is een verzameling van routers dat onder één technische administratie valt, zoals een ISP of Enterprise. De routers die door middel van BGP de routering in het DFZ regelen, beschikken niet over een default gateway wat betekent dat ze in theorie moeten beschikken over een volledig routetabel van het totale internet. Eind 2014 is er door de Asian Pacific Network Information Centre (APNIC) bekend gemaakt dat BGP routers op het moment voor IPv4 over een routetabel beschikken met 530.000 routes.

BGP is een path vector protocol wat inhoudt dat het protocol het bijhouden van informatie dynamisch verzorgt (Halabi, 1997). BGP houdt bij welke AS'en zijn gepasseerd tijdens het verplaatsen naar de eindbestemming. Met deze informatie kan worden ontdekt of er loops aanwezig zijn in het netwerk en deze onklaar maken. Het transporteren van de routeringsinformatie doet BGP op basis van het Transmission Control Protocol (TCP) op poort 179. Door gebruikt de maken van TCP is het niet meer nodig om het protocol te voorzien van zaken als foutcontrole, omdat TCP dit standaard al verzorgt.



Figuur 7.1 – BGP autonomous systems topologie

Het verspreiden van informatie door het DFZ gebeurt op basis van een TCP-sessie die tussen twee BGP-routers wordt opgezet. Na het opzetten van zo'n sessie worden de twee routers bestempeld als 'peers' of 'neighbours'. De berichten die nodig zijn voor het verspreiden van informatie zijn tussen de 19 en 4096 bytes groot en bestaan uit de volgende vier opties:

- OPEN
- UPDATE
- NOTIFICATION
- KEEPALIVE

Het OPEN-bericht is het eerste bericht dat gestuurd wordt na het voltooien van de three-way-handshake van TCP. In dit bericht staat informatie vermeld over parameters die gecontroleerd en afgesproken dienen te worden, zoals BGP versienummer en AS gegevens. Wanneer dit bericht is geaccepteerd wordt een KEEPALIVE bericht verzonden ter bevestiging. Dit KEEPALIVE bericht is het kleinste bericht van 19 bytes dat verstuurd kan worden tussen peers en heeft als doel het beschikbaar houden van de sessie. Het sturen van KEEPALIVE berichten wordt elke dertig seconden herhaald.

Het UPDATE-bericht wordt gebruikt voor het transporteren van routeringsinformatie. In dit bericht wordt informatie vermeld over routes die toegevoegd of verwijderd moeten worden. In dit bericht kan ook informatie worden toegevoegd over bepaalde route-attributen. Voorbeelden van deze attributen zijn NEXT_HOP voor de eerstvolgende router die geraadpleegd moet worden en AS_PATH dat bestaat uit een sequentie van AS nummers die gebruikt wordt voor het detecteren van loops. Het laatste bericht, NOTIFICATION, wordt verstuurd wanneer er fouten zijn gedetecteerd. Als dit het geval is wordt de BGP sessies direct gesloten.

Toepassingen
De hoofdtoepassing van BGP is het zorgen voor de verspreiding van routeringsinformatie in het DFZ. De manier waarop BGP dit doet via TCP is uniek en onmisbaar. BGP kan ook voor andere toepassingen worden gebruikt, namelijk omstandigheden waar de beschikbaarheid van een netwerk zo hoog mogelijk moet zijn. BGP is één van de mogelijkheden voor het creëren van een multihomed netwerk. Multihoming kan gebruikt worden voor het realiseren van redundantie en load balancing.

- **Redundantie.** Voor het redundant uitvoeren van internetlijnen van één of meer ISP's is NAT of BGP nodig. NAT vaak wordt gezien als een slordige oplossing, omdat je snel te maken hebt met overgelopen sessietabellen en afhankelijk bent van scripts die connectieverlies detecteren. Bij BGP worden beide routes geadverteerd en bepaald het BGP protocol welke route er gekozen worden. Een oplossing met NAT kan voldoende zijn voor consumenten, maar voor grote bedrijven gaat de voorkeur uit naar BGP.
- **Load Balancing.** Wanneer je als bedrijf beschikt over meerdere internetlijnen kan het gewenst zijn om inkomend en uitgaand verkeer te verdelen over de lijnen. Door middel van de vele parameters die meewegen in het proces voor het kiezen van de juiste route kan BGP voor load balancing worden gebruikt. Een perfecte balans zal het nooit worden, omdat het aantal parameters dat meeweegt in het keuzeproces het verdelen ingewikkeld maakt. Daarnaast heeft elke AS zijn eigen policy, waardoor verdeling nooit gelijk is.

Benodigdheden
Om BGP te configureren en toe te passen in een netwerk zijn de volgende elementen minimaal nodig:

- **AS nummer.** BGP zorgt voor de connectie tussen AS'en. Om aan het DFZ deel te mogen nemen moet het netwerk over een AS nummer beschikken. Deze is op te vragen bij instanties zoals de IANA tegen een kleine vergoeding.
- **Apparatuur met BGP ondersteuning.** Om BGP te kunnen gebruiken is het nodig om (een deel van) de internet routetabel over te nemen in jouw eigen BGP router. Aangezien de connecties steeds meer toenemen is het nodig om apparatuur te hebben met genoeg rekenkracht voor de opname en beheer van alle routes.

- **Provider Independent Address.** Een blok IP-addressen die niet afhankelijk is van een ISP. Dit is nodig wanneer er gebruik wordt gemaakt van BGP multihoming met twee of meer lijnen van verschillende ISP's.

Vergelijking met LISP

BGP is onmisbaar in het huidige internetmodel door connectie te realiseren tussen AS'en in het DFZ. Daarmee is BGP een routingprotocol in hart en nieren. LISP is dat niet. LISP zorgt voor een architectuur waarmee de eindbestemming opgezocht kan worden in een database, maar is nog steeds afhankelijk van onderliggende protocollen voor het verplaatsen van het verkeer.

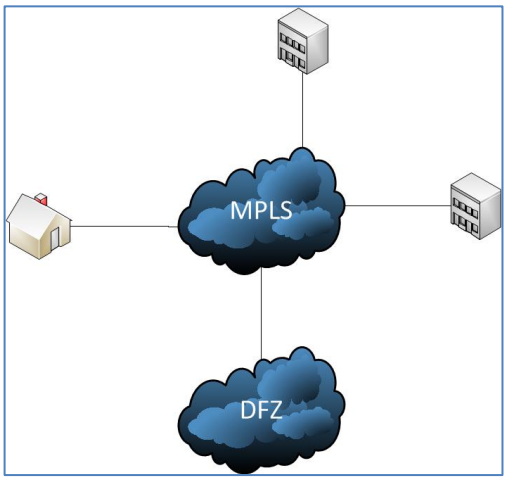
Wat LISP wel kan doen is de informatie die BGP moet opslaan verkleinen. Door de functies van het IP-adres, identiteit en locatie, te scheiden kan aggregatie in de routetabellen sterk worden verbeterd. Voor eindsystemen die verplaatsen hoeven ten slotte geen extra routes meer opgenomen te worden. Alleen de locatie is nog afhankelijk van de topologie en wanneer deze logisch wordt ingedeeld kan aggregatie optimaal worden toegepast.

Eén toepassing waar LISP het BGP protocol wel zou kunnen vervangen is multihoming. Op het moment is BGP nog de favoriet voor het realiseren van multihoming, maar LISP zou daar verandering in kunnen brengen. Wanneer uitgaand verkeer aankomt bij een LISP-router wordt voordat het verkeer in de richting van de eindbestemming wordt verstuurd eerst een koppeling opgezocht in de database. Bij de gevonden EID-to-RLOC koppeling kunnen meerdere RLOC adressen aangegeven zijn die voorzien zijn van priority en weight paramaters. Hiermee is load balancing en redundantie in te regelen met LISP. Om multihoming met LISP te realiseren is geen zware apparatuur nodig of speciale AS nummers zoals bij BGP. De enige vereisten zijn twee IP-adressen en apparatuur dat LISP ondersteund. Tegenwoordig is LISP ondersteund door de laagste routermodellen van Cisco waardoor het een goedkoop alternatief is.

7.2 MPLS

In de jaren tachtig werd de verwerking van internetverkeer geregeld door routeringsoftware in tegenstelling tot de manier waarop men dat tegenwoordig vooral in de hardware doet. Daar werd geconstateerd dat het doorsturen van het explosief groeiende verkeer op basis van L3-informatie steeds meer impact had op de prestaties van het apparatuur. Een oplossing was noodzakelijk en werd gevonden in label switching. Een techniek waarbij verkeer afkomstig van verschillende protocollen kan worden doorgestuurd op basis van een label in plaats van de L3-informatie. Deze label switching techniek was aantrekkelijk, omdat het geïmplementeerd kon worden in de hardware wat voor betere prestaties zorgde. Na een korte dip laaide de interesse in label switching in de jaren negentig weer op. In 1997 werd de Multi-Protocol Label Switching (MPLS) werkgroep opgericht door de Internet Engineering Task Force (IETF).

IP-routing gebeurt op basis van L3-informatie. Bij elke router die op het pad ligt wordt er opnieuw beoordeeld waar het pakket naar toe moet worden gestuurd. MPLS doet dit eenmalig. Wanneer verkeer aankomt bij een MPLS router wordt het verkeer beoordeeld en wordt er een label geplaatst. Het routeren van het verkeer gebeurt voor de rest op basis van dat label door switches. Omdat MPLS maar eenmalig gebruikt maakt van L3-informatie en voor de rest het verkeer afhandelt met switches wordt MPLS als techniek geplaatst tussen laag twee en drie van het OSI-model. MPLS is zelf geen protocol, omdat het gebruik maakt van informatie en mechanismen uit andere protocollen voor het opstellen van paden (Label Switched Path) waarover het labelverkeer later verstuurd wordt. MPLS wordt om die reden gezien als een architectuur (Brocade, 2014).



Hoewel label switching vroeger aantrekkelijk was voor de betere prestaties dat het opleverde ten opzichte van routering is dat niet langer het geval. De snelheid waarmee MPLS verkeer verwerkt ten opzichte van apparatuur dat op het moment beschikbaar is, is de snelheidswinst niet langer significant. Tenzij de versturing van verkeer over een totaal pad wordt bekeken kan MPLS als sneller worden gezien.

Toch is MPLS wel een techniek dat aantrekkelijk is voor grote ondernemingen zoals ISP's en Enterprises. MPLS brengt grote flexibiliteit met zich met door het ondersteunen van zeer veel protocollen en heeft ondersteuning voor quality of service (QoS) en VPN's door slim gebruik te maken van de labels.

Toepassing

MPLS is ontwikkeld als een techniek om verkeer sneller bij een bestemming te krijgen, maar is de laatste jaren ingehaald door nieuwe technologie. Toch blijft MPLS door slim gebruikt van labels een interessante techniek met veel toepassingen.

- **Quality of Service.** Doordat er labels worden toegekend aan verkeer is het mogelijk om op verschillende manieren QoS toe te passen op het verkeer dat zich in het MPLS netwerk bevindt.
    - Er kan prioriteit worden toegekend aan verschillende soorten labels om bijvoorbeeld Voice over IP (VoIP) verkeer voorrang te verlenen.
    - Er kan soortgelijk verkeer over een specifieke lijn worden gestuurd om de lijn optimaal te gebruiken.
    - Er kunnen specifieke labels omgeleid worden via andere routes als de hoofdroute vertraging oplevert. Ook kan er verkeer tijdelijk worden vastgehouden om bepaald belangrijk verkeer voorrang te verlenen.
- **Flexibiliteit.** MPLS is een multi-protocol techniek wat betekent dat het ondersteuning biedt voor meerdere protocollen. Het is om die reden voor bijvoorbeeld ISP's aantrekkelijk om MPLS te

gebruiken. Zo kan de ene omgeving connectie zoeken via het IP-protocol, terwijl de ander via ATM verbinding zoekt.
- **Beveiliging.** MPLS biedt ondersteuning voor Virtual Private Networks (VPN), Virtual Private LAN Services (VPLS) en Virtual Leased Lines (Vll) op basis van de labels.

Benodigdheden
Voor het installeren van MPLS in een netwerk zijn drie componenten nodig:

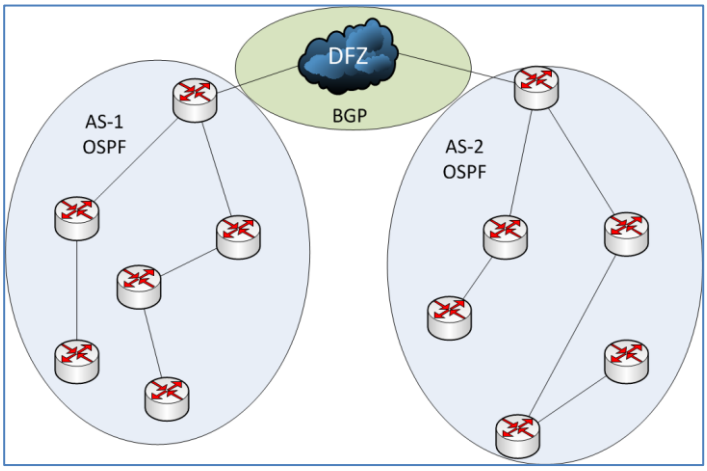
- **Label Edge Router**. De router die initieel het verkeer ontvangt en deze voorziet van een label. Ook bepaald deze router het pad dat gevolgd gaat worden.
- **Label Switching Router**. De router die switching van verkeer regelt binnen het MPLS netwerk.
- **Egress Router**. De router die aan het eind van het pad het verkeer ontdoet van een label en vervolgens verkeer doorstuurt naar zijn eindbestemming.

Vergelijking met LISP
LISP en MPLS zijn beide met verschillende doeleinden bedacht dan waarvoor ze op het moment worden toegepast. Waar LISP ontstaan is voor het terugdringen van de routes in het DFZ wordt het ook gebruikt voor onder andere multihoming en waar MPLS is ontwikkeld voor het snel doorsturen van verkeer wordt het gebruikt als QoS en beveiliging. Hoewel de hoofddoeleinden van MPLS en LISP nog wel gelden zijn beide technieken uitgegroeid tot architecturen en daarin bevindt zich ook de overlap. MPLS en LISP gebruiken beide informatie van andere protocollen voor het uitvoeren van werkzaamheden en het zijn beide technieken die geen vaste plek hebben binnen het OSI-model.

Dit betekent niet dat LISP ooit MPLS zal vervangen. Hoewel er overlap zit in de kern van de architecturen is overlap in toepassingen niet volledig. LISP kan met zijn priority en weight wel enige vorm van QoS toepassen, maar lang niet zo uitgebreid als MPLS dat kan. Daarbij ondersteund MPLS ook veel meer protocollen dan LISP. Het punt waar LISP de functionaliteit van MPLS wel zou kunnen vervangen is in beveiliging. Het is mogelijk om met LISP instance ID’s toe te voegen aan verkeer die op het internet fungeren als een tag voor een VPN. Hiermee kunnen VPN’s die op basis van MPLS/BGP werken worden vervangen. De instance ID’s in LISP kunnen aan de EID in de header worden toegevoegd en via de ITR’s worden encapsulated en later door ETR’s decapsulated. Daar is verder geen extra apparatuur voor nodig in tegenstelling tot de MPLS/BGP VPN waar je verplicht bent MPLS en BGP apparatuur aan te schaffen met alle problemen die daarbij komen, zoals het verkrijgen van proivder independent addressen.

7.3 OSPF

Open Shortest Path First (OSPF) is een routeringsprotocol dat dynamisch veranderingen in de topologie ontdekt en die informatie gebruikt om verkeer door te sturen op basis van het bestemmingsadres. OSPF is één van de meeste gebruikte routeringsprotocollen binnen AS'en en is vooral in gebruik door Enterprises.



OSPF is een link state protocol. Dat houdt in dat elke router dat mee doet aan het OSPF netwerk zijn eigen database beheert van de gehele topologie. Deze link-state databases zijn identiek voor elke router. Wanneer er een verandering in de topologie wordt gedetecteerd wordt dat aan de hand van een link-state advertisement (LSA) bekend gemaakt aan alle direct verbonden routers (neighbours) die de informatie verwerken in hun database. Na deze update sturen ook deze routers weer een LSA naar hun buren en op die manier is uiteindelijk iedereen op de hoogte van een verandering. Aan de hand van de informatie in de link-state databases wordt door iedere router een boomstructuur gegenereerd met zichzelf als de basis. Aan de hand van die structuur is elke bestemming te bereiken door middel van het kortste pad. OSPF gebruikt voor het berekenen van het kortste pas het Dijkstra algoritme.

Vergelijking met LISP
OSPF is een routingprotocol dat erg in trek is binnen AS'en, maar meer dan dat is OSPF niet. In tegenstelling tot protocollen als BGP en MPLS zijn er naast de primaire doeleinden nog interessante toepassingen voor het protocol, maar dat is hier niet het geval. LISP zal de werking van OSPF nooit vervangen, omdat LISP geen routingprotocol is. LISP is afhankelijk van protocollen als OSPF voor het versturen van verkeer.

7.4 IS-IS

Intermediate System to Intermediate System (IS-IS) is een de facto standaard routeringsprotocol voor grote ISP's en de grote concurrent van OSPF. Net als OSPF is IS-IS een link state protocol waarbij routers op basis van routeringsinformatie een database bijhouden van de topologie en het Dijkstra algoritme gebruiken voor het berekenen van het kortste pad. Het verschil met OSPF is dat OSPF actief is op laag drie en initieel alleen ondersteuning gaf aan IPv4 terwijl IS-IS actief is op laag twee en geen onderscheid maakt over het protocol waarmee gewerkt wordt.

IS-IS verdeelt een netwerk in twee lagen en kan net als OSPF een groot netwerk opdelen in meerdere gebieden (area's). Wanneer routering plaatsvindt binnen één area valt dat onder laag één en wanneer er verkeer naar een ander gebied verstuurd moet worden valt dat onder laag twee. Om dit te realiseren houden laag 1 routers informatie bij over hun eigen gebied terwijl laag twee routers informatie bijhouden over alle eindbestemmingen. Verkeer dat tussen twee of meer gebieden moet verplaatsen zal altijd via een laag één naar laag twee en terug naar laag één getransporteerd worden om een eindbestemming te bereiken.

Vergelijking met LISP
Er zijn geen toepassingen gevonden waar LISP en IS-IS overlap hebben. Naast het feit dat LISP geen routingprotocol is, maakt IS-IS ook geen gebruikt van IP-informatie om te routeren wat een combinatie met LISP of een vervangen door LISP onmogelijk maakt.

8. LISP TECHNIEKEN

In dit hoofdstuk zullen de vier hoofdtechnieken worden omschreven waar LISP voor toegepast kan worden naast het fungeren als een optie voor het terugdringen van de routetabellen in het DFZ. De technieken die aan bod zullen komen zijn multihoming, IPv4-IPv6 transitie en VM/IP mobility. De technieken zullen worden vergeleken met hedendaagse standaarden op basis van topologie- en apparatuurvereisten en voor- en nadelen van de standaarden. Tevens zal worden besproken welke problemen ontstaan en worden weggenomen wanneer LISP als vervanging wordt ingericht.

8.1 MULTIHOMING

Multihoming is een techniek waarbij één netwerklocatie is verbonden met meerdere externe locaties. Er zijn vier vormen waarin multihoming voorkomt:

- Eén link met meerdere IP-adressen actief
- Meerdere ethernet interfaces met ieder interface een eigen IP-adres
- Meerdere links met één IP-adres (blok)
- Meerdere links met iedere link een eigen IP-adres (blok)

De meest voorkomende optie is nummer drie waarbij één adresblok door middel van BGP over meerdere links wordt gedistribueerd. Wanneer de ene link niet langer beschikbaar is, is hetzelfde IP-blok nog steeds bereikbaar over de andere link. Een andere techniek die vaak voorkomt is optie twee waarbij meerdere interfaces worden geconfigureerd worden met een eigen IP-adres. Door middel van een NAT-constructie kan er verkeer door de ene interface worden gestuurd, wanneer de andere niet langer bereikbaar is.

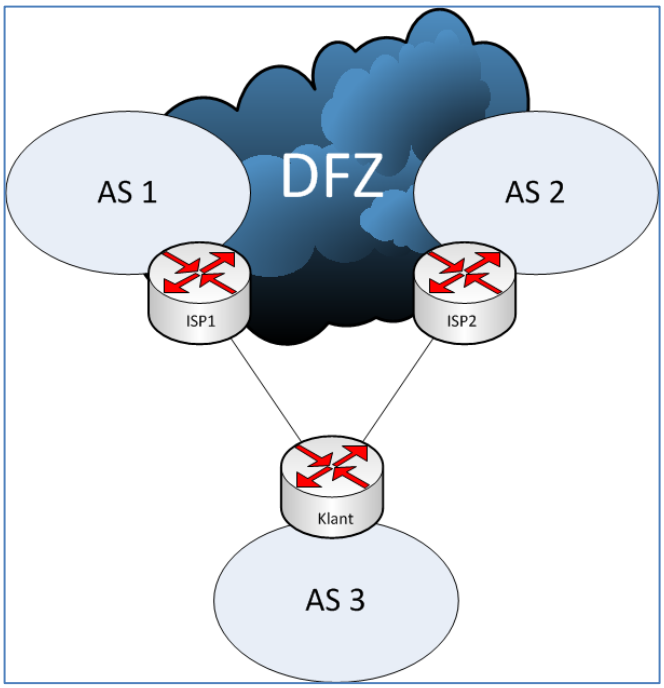
8.1.1 BGP MULTIHOMING

In het vorige hoofdstuk is multihoming op basis van BGP al kort besproken. Dit is een veel voorkomende techniek voor grote ondernemingen die niet afhankelijk willen zijn van één internetverbinding. Deze vorm van multihoming komt in verschillende gradaties voor. Het IP-adres blok dat gebruikt wordt voor het verbinden kan afkomstig zijn van één ISP, maar ook van twee ISP's wanneer een onderneming ook de ISP redundant wil uitvoeren. De tweede optie waarbij gebruik wordt gemaakt van twee ISP's wordt in dit hoofdstuk behandeld, omdat dit de meest voorkomende variant van BGP multihoming is voor klanten van Qi ict.

Om multihoming met BGP en twee ISP's te realiseren zijn er drie componenten nodig:

- **AS nummer.** Om deel te mogen nemen aan het DFZ en daarin een IP-adresblok te distribueren dient de omgeving in bezit te zijn van een AS nummer. Deze kan aangevraagd worden bij instanties die verantwoordelijk zijn voor de uitgifte hiervan zoals het IANA tegen een kleine vergoeding.
- **Provider Independent Address Space.** Het IP-blok dat door middel van BGP wordt gedistribueerd over de twee verbindingen dient onafhankelijk te zijn van een ISP. Normaliter zou dit aangevraagd moeten worden bij het Réseaux IP Européens (RIPE), de Europese afvaardiging van het IANA, maar dit is niet langer mogelijk. RIPE geeft op de website aan dat het niet langer PI adressen kan uitgeven, omdat de adressen allemaal uitgegeven zijn. Het is wachten op IPv6 tot deze adressen weer uitgegeven kunnen worden.
- **BGP router(s).** Aan de grens van het netwerk dienen BGP routers aanwezig te zijn die de connectie met het DFZ realiseren. Het aantal routes loopt inmiddels in de honderdduizenden, waardoor apparatuur met BGP ondersteuning over veel rekenkracht moet beschikken.

Voor de partijen die wel beschikken over de drie componenten is het mogelijk om BGP multihoming op te zetten. In de onderstaande afbeelding is de topologie zichtbaar die daarvoor nodig is.



Figuur 8.1 – BGP Multihoming topologie

De configuratie van BGP multihoming is niet eenvoudig en zeer belangrijk. Door middel van BGP wordt het klantnetwerk deel van het internet, wat betekend dat er geen fouten aanwezig mogen zijn in de configuratie. Misconfiguraties die wel voorkomen kunnen er voor zorgen dat verkeer in de verkeerde richting wordt gestuurd, doordat een ander netwerk wordt overlapt.

De configuratie van BGP multihoming komt neer op het aangeven welke netwerken aanwezig zijn in het klant AS, het installeren van filters om te zorgen dat het klantnetwerk niet als doorgeefluik wordt gezien op het internet, aangeven wie de 'buren' van het netwerk zijn en het opstellen statische routes in de richting van de twee ISP's.

Voordelen:

- **Provider Independent.** Hoewel het op het moment niet mogelijk is om aan PI-adressen te komen is het voor de partijen die wel over deze adressen beschikken een groot voordeel. Met een onafhankelijk adres blok maakt het niet uit met welke ISP's de partij verbindt. Je hebt altijd dezelfde adressen, waardoor migratie geen probleem is. Het brengt grote flexibiliteit met zich mee.
- **Load Balancing.** BGP heeft een groot aantal eigenschappen die meewegen bij het kiezen van de juiste route. Door deze eigenschappen te manipuleren is het mogelijk om inkomend verkeer te verdelen over beide lijnen. Uitgaand verkeer kan door middel van een policy over beide lijnen worden verdeeld.
- **Hoge Beschikbaarheid.** Wanneer één van de ISP's offline gaat is het mogelijk om via de ander door de werken zonder onderbreking. Een groot deel van de bestaande sessies blijven actief mits de omschakeling snel genoeg verloopt.

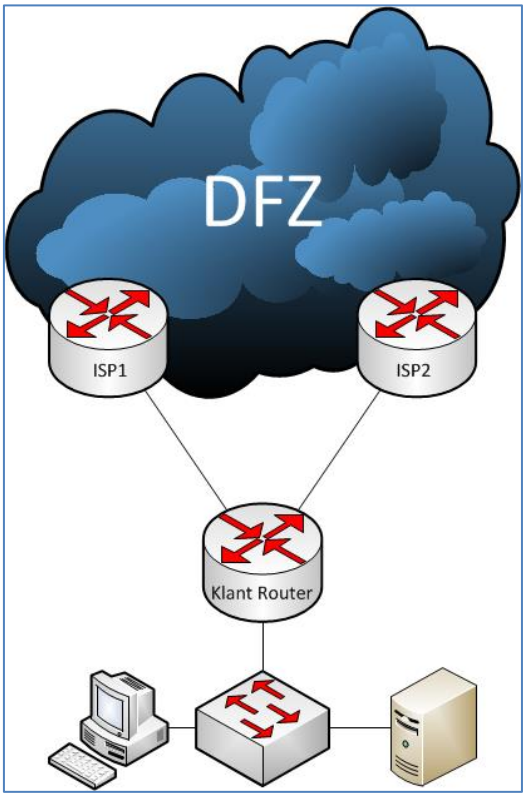
Nadelen:

- **Grote investering.** Afgezien van het feit dat het hebben van twee ISP lijnen al duur kan zijn is het aanschaffen van routers die BGP ondersteunen een grote investering. Instapmodellen van routers die BGP ondersteunen bevinden zich in de tienduizenden euro's reeks.
- **Moeilijk aanschafproces.** Het is op het moment onmogelijk om aan IPv4 PI-adressen te komen, omdat deze niet meer beschikbaar zijn, maar in de tijd dat er nog wel adressen waren was het ook moeilijk. Bij het aanvragen van een blok adressen worden er 256 IP-adressen toegewezen. Deze worden niet zomaar vrijgegeven. Er moet in een plan bewezen kunnen worden dat een groot deel van die adressen ook daadwerkelijk gebruikt worden.
- **BGP is een langzaam protocol.** Wanneer je kiest voor BGP in plaats van NAT, omdat je geen sessies wilt verliezen kan dat nog steeds voorkomen, omdat BGP een langzaam protocol is. Voordat elke router op de hoogte is van een wijzigingen kan een sessie al verlopen zijn.
- **Slecht voor de globale routeringstabellen.** Multihoming zorgt voor extra routes in een de ruim overgelopen routetabel van het DFZ.

8.1.2 NAT MULTIHOMING

Een tweede mogelijkheid om een multihomed omgeving te creëren is met NAT. Sinds het niet meer mogelijk is om PI-adressen te verkrijgen en het feit dat dit een goedkopere oplossingen is maakt het een goed alternatief voor kleinere ondernemingen.

Multihoming met NAT is een eenvoudige techniek en er is niets meer nodig dan twee IP-adressen en een router. De adressen kunnen van één of meerdere ISP's afkomstig zijn. Wanneer de lijn van ISP-A faalt, is het mogelijk om met een NAT-constructie het verkeer over de andere lijn te sturen. Hiervoor is geen AS-nummer of speciale reeks nodig, waardoor het een stuk toegankelijker wordt. Op de firewalls van Check Point die op het moment veelvuldig aanwezig zijn bij klanten van Qi ict werkt de NAT constructie als volgt. Allereerst wordt er in de regelgeving een dynamisch object aangemaakt dat over meerdere IP-adressen kan beschikken. Wanneer de lijn van ISP-1 actief is wordt door een script gezorgd dat het dynamisch object wordt verschuilt achter het IP-adres dat afkomstig is van ISP-1. Wanneer ISP-1 faalt detecteert een script connectieverlies en wordt het dynamisch object verscholen achter het IP-adres van ISP-2. Hierbij gaan wel alle sessies verloren, omdat je te maken hebt met twee verschillende IP-adressen.



Figuur 8.2 – NAT multihoming

Cisco werkt anders dan Check Point. Bij Cisco zijn er te allen tijde twee NAT-regels actief en twee statische routes naar de twee default gateways van de ISP's. De ene route heeft een hogere metric dan de ander en wordt gezien als de primaire verbinding. De verbindingen worden constant gepolled op beschikbaarheid. Wanneer connectieverlies wordt gedetecteerd wordt de statische route die niet langer bereikbaar is verwijderd, waardoor de ander actief wordt. Ook hier is de verbinding niet statefull, omdat het om twee aparte verbindingen gaat.

Voordelen:

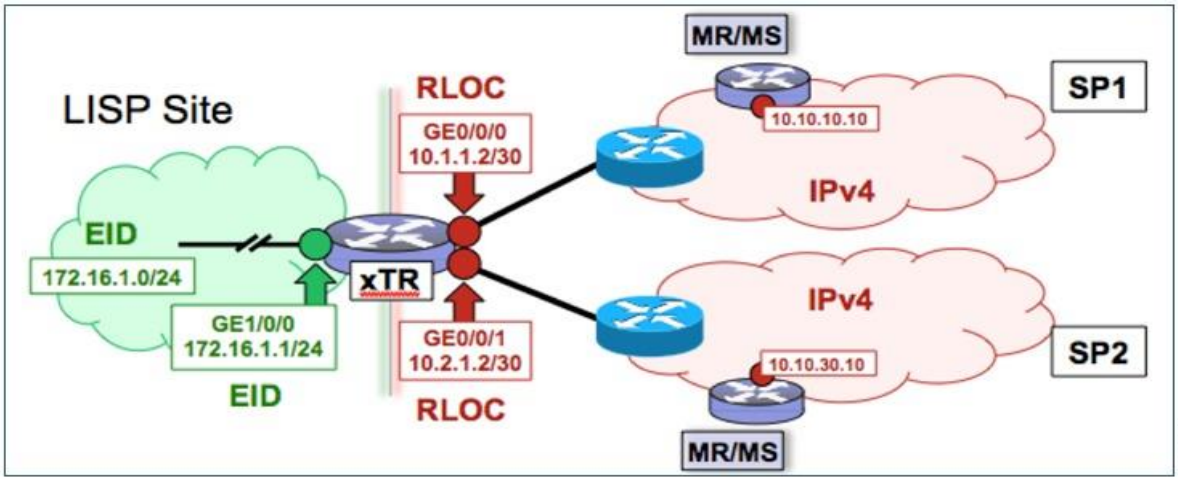
- **Toegankelijk.** Multihoming opbouwen door middel van NAT is een stuk toegankelijker voor kleine partijen, omdat je niet meer nodig hebt dan twee lijnen van ISP's en een router.
- **Goed voor de globale routeringstabellen.** Multihoming met NAT brengt geen extra routes mee voor de tabellen in het DFZ.

Nadelen:

- **Sessieverlies.** Alle sessies die op het moment actief zijn zullen verloren gaan, omdat je in feite niet multihomed bent, maar twee keer singlehomed. Je hebt twee IP-adressen, waardoor sessies niet blijven bestaan zoals bij BGP multihoming.
- **NAT Tabellen.** NAT maakt gebruik van tabellen om de translaties van alle sessies bij te houden. Uit ervaring bij Qi ict is gebleken dat het voorkomt dat deze tabellen hun limiet overschrijden.

8.1.3 LISP MULTIHOMING

Het LISP protocol is ontwikkeld om als oplossing te fungeren voor het terugdringen van overgelopen routetabellen in het DFZ. Een groot deel van de onnodige routes die aanwezig zijn in de routetabel van het DFZ zijn afkomstig van multihomed locaties. Om deze routes te kunnen verwijderen en daarbij niet afhankelijk te zijn van NAT als multihoming optie is het mogelijk om multihoming te implementeren met behulp van LISP.



Figuur 8.3 – LISP Multihoming Bron: (Cisco Systems, 2014)

Er zijn verschillende vormen van multihoming met LISP mogelijk. De bovenstaande afbeelding geeft een omgeving met één router en een redundant uitgevoerde mapping-system weer. Andere mogelijkheden zijn redundante uitgevoerde xTR's met één of meer mapping-systems. De topologie maakt voor de werking van LISP multihoming niet uit. De enige vereiste is dat er twee of meer lijnen aanwezig zijn.

Bij het opzetten van de ETR wordt de volgende configuratie opgegeven:

- database-mapping 172.16.1.0/24 10.1.1.2 priority 1 weight 50
- database-mapping 172.16.1.0/24 10.2.1.2 priority 1 weight 50

Deze database-mappings worden door de ETR geregistreerd bij de MS en worden opgenomen in het DDT-netwerk. Wanneer een eindsysteem een verzoek doet om verkeer te sturen naar een eindsysteem in het LISP EID netwerk (172.16.1.0/24) gaat het normale proces van start zoals dat in hoofdstuk zes is uitgelegd. Het enige verschil is dat bij het ontvangen van een EID-to-RLOC koppeling er nu twee RLOC's worden geretourneerd. Aan de hand van de priority en weight parameters kan de ontvanger bepalen over welke lijn verkeer ontvangen moet worden en in welke mate. Er zijn geen ingewikkelde metrics nodig. Door middel van deze oplossing kan multihoming met de voordelen van BGP worden gerealiseerd op basis van twee normale ISP lijnen zonder BGP of NAT.

Voordelen:

- **Toegankelijk.** Net als bij NAT is multihoming met LISP zeer toegankelijk voor alle partijen. Er is geen zware apparatuur nodig om LISP te draaien en er komen geen ingewikkelde zaken als PI-adressen en AS nummers aan te pas.
- **Load balancing.** Door middel van de weight parameters is verkeer gemakkelijk te verdelen. Er hoeven geen metrics te worden gemanipuleerd zoals bij BGP.
- **Hoge beschikbaarheid.** Het uitvallen van een router of ISP zal het proces niet verstoren. Als de ene RLOC niet langer bereikbaar is zal het verkeer via de andere RLOC doorstromen, omdat het eindsysteem waar het verkeer heen moet (EID) hetzelfde blijft.

Nadelen:

- **Adoptie van LISP.** Wanneer er gekozen wordt om multihoming door LISP te implementeren is het nodig om LISP in zijn geheel te adopteren. Dit hoeft niet perse een nadeel te zijn, maar er dient wel rekening mee gehouden te worden dat multihoming met LISP net als het originele protocol nog experimenteel is. Het gevolg van een experimenteel protocol is dat de documentatie het alleen nog maar heeft over voordelen. Tijdens het bouwen van het lab zullen wellicht wel nadelen naar voren komen.

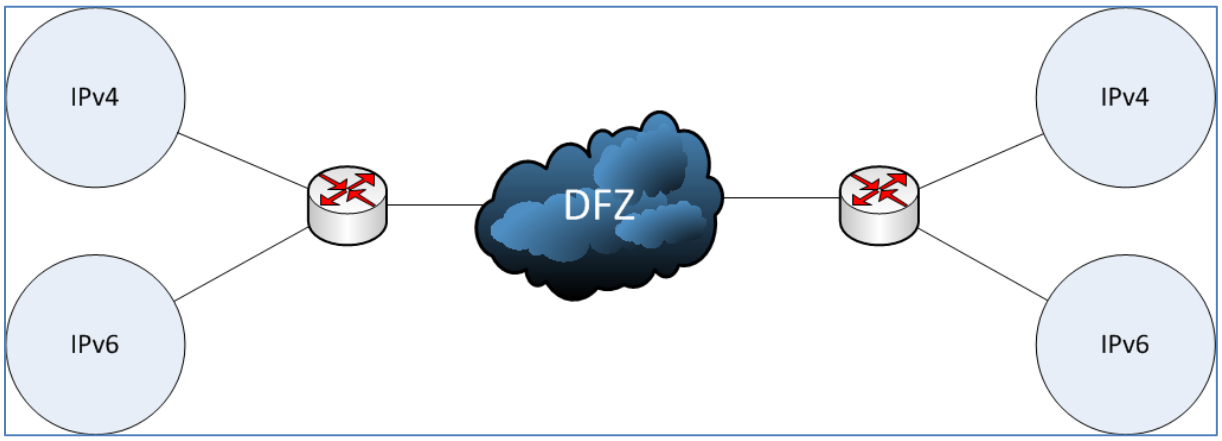
8.2 IPv4-IPv6 Transitie

Het IPv4-adres is een 32-bits veld dat ongeveer 4,3 miljard unieke adressen toestaat. In de begintijd van het internet werd verwacht dat die 4,3 miljard adressen nooit allemaal uitgegeven zouden worden. Door de explosieve groei van het internet is de grens zeer snel bereikt. Om aan de groei van het internet te kunnen voldoen is een nieuwe protocol ontwikkeld; IPv6. IPv6 beschikt over 128-bits adressen waarmee in theorie elke zandkorrel op aarde een eigen IP-adres zou kunnen krijgen.

Om IPv6 te kunnen implementeren in het huidige internetmodel zal elk apparaat dat verbonden is over de mogelijkheid moeten beschikken om met IPv6 te werken. Hier zijn fabrikanten al enige tijd mee bezig en inmiddels beschikken de nieuwere apparaten over die functionaliteit. De volgende stap is het omzetten van alle netwerken van IPv4 naar IPv6. Het wordt niet mogelijk geacht om het internet compleet offline te halen, omdat er teveel processen afhankelijk zijn van het internet. Om die reden wordt er gekozen voor een gefaseerde aanpak. Het probleem dat hierbij komt kijken is dat er ook een transitietechniek nodig is, omdat IPv4 en IPv6 niet samen kunnen werken. In dit hoofdstuk zullen een aantal bestaande technieken worden toegelicht en vergeleken met LISP.

8.2.1 Dualstack

Dualstack als transitietechniek houdt in dat zowel een IPv4 als IPv6 infrastructuur wordt uitgerold in een netwerkomgeving en daarin volledig onafhankelijk van elkaar werken. Dualstack is de meest gewenste oplossing op het moment, omdat je na het implementeren in tegenstelling tot oplossingen zoals tunneling niet te maken krijgt met problemen zoals MTU bij encapsulation.



Figuur 8.4 – Dualstack topologie

Voordelen:

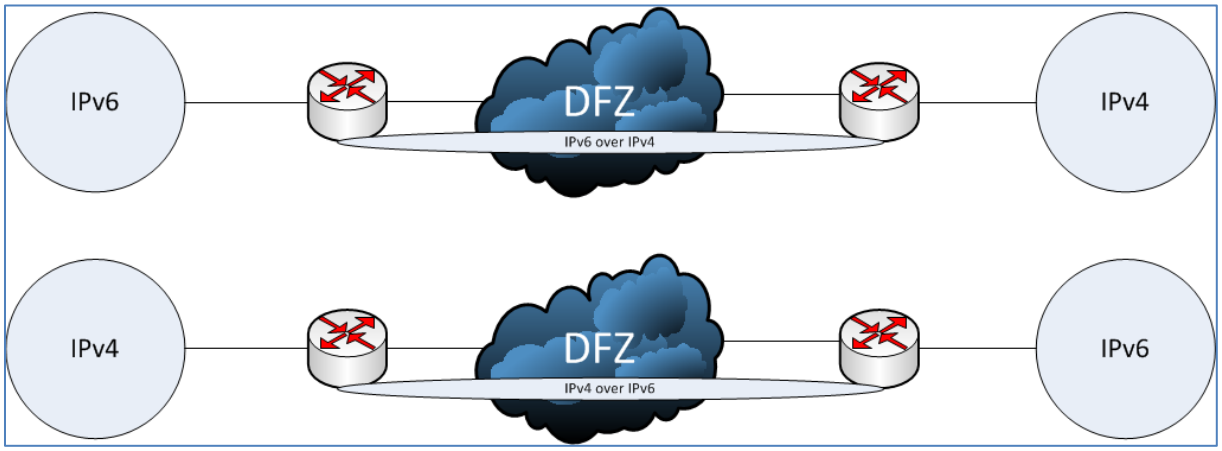
- **Twee netwerken**. IPv4 en IPv6 draaien onafhankelijk van elkaar en verkeer wordt via een gekozen netwerk verstuurd op basis van het source- en destinationadres. Dit concept kan net zo lang worden gebruikt tot dat IPv6 volledig over is.
- **Geen encapsulation**. In tegenstelling tot technieken als tunneling is er geen encapsulation nodig. Hierdoor hoeft er geen extra data te worden toegevoegd aan de IP-pakketten, waardoor problemen met MTU niet voorkomen.
- **Geen nieuwe beveiliging**. Omdat IPv4 en IPv6 volledig onafhankelijk naast elkaar draaien kunnen beveiligingsmechanismen die standaard bestaan worden toegepast, zonder dat er rekening gehouden hoeft te worden met het andere protocol. Er hoeven geen extra beveiligingsprotocollen te worden geschreven om verkeer te beschermen.

Nadelen:

- **Mogelijk hoge kosten**. Dualstack werkt alleen als al het apparatuur in het netwerk over zowel IPv4 als IPv6 beschikt. Oudere apparatuur dat alleen over IPv4 beschikt zal vernieuwd moeten worden wat mogelijk tot hoge kosten leidt.
- **Mogelijk extra beveiligingsproblemen**. Er dient na de implementatie rekening gehouden te worden met aanvallen van zowel IPv4 als IPv6. Dit kan leiden tot extra problemen.
- **Meer management**. Er moet in een dualstack omgeving voor IPv4 en IPv6 management worden gezorgd. Dat houdt in dat monitoring plaatsvindt op beide infrastructuren, wat op zijn beurt leidt tot extra apparatuur en uitgaven.

8.2.2 TUNNELING

Netwerkomgevingen die niet in aanmerking komen voor een dualstack oplossing kunnen ook kiezen voor tunneling. Voor tunneling zijn verschillende technieken bekend, waarvan de meest bekende Teredo is, omdat die standaard is geïmplementeerd op alle Windows machines sinds Windows XP. Het werkprincipe van tunneling is het inpakken van IPv4 verkeer in IPv6 pakketten en andersom, om zo een netwerk te overbruggen die het initiële IP-versie niet ondersteund. Dit gebeurt door twee routers die zich op de grens van een netwerk bevinden. In een voorbeeld waarbij de DFZ IPv4 hanteert en een intern netwerk IPv6, bevindt zich IPv6 verkeer dat ingepakt is in een IPv4 pakket tussen de grensrouters. Eenmaal aangekomen bij de router wordt de IPv4 informatie verwijderd en wordt het originele verkeer doorgestuurd naar het eindsysteem.



Figuur 8.5 – Tunneling topologie

Voordelen:

- **Geen wijzigingen aan het netwerk.** Het maakt bij tunneling niet uit of het netwerk van de klant op basis van IPv4 of IPv6 werkt. Er zijn geen wijzigingen nodig. Voordat verkeer de tunnel op gaat zullen pakketten ingepakt worden waar nodig.
- **Weinig tot geen configuratie.** Over het algemeen worden tunnels opgezet en geconfigureerd door ISP's, waardoor er weinig tot geen configuratie nodig is.

Nadelen:

- **Dualstack hosts**. Hoewel de tunnel beide vormen van IP-verkeer zonder problemen zal verplaatsen zal een eindsysteem uiteindelijk wel dualstack moeten zijn als het verkeer van beide protocollen wilt ontvangen.
- **Beveiliging**. Omdat verkeer wordt ingepakt in een ander protocol kan het zich (onbewust) vermommen voor inspectie door firewalls. Bijvoorbeeld schadelijk IPv6 verkeer dat zich verschuilt in een IPv4 pakket dat getunneled wordt.
- **MTU problemen**. Het toevoegen van informatie zorgt ervoor dat de maximale MTU van een router overschreden wordt waardoor fragmentatie optreedt. Als ICMP "Packet Too Big Message" berichten worden geblokkeerd kan het zijn dat verkeer niet aankomt.

8.2.3 TRANSLATIE

De laatste optie die op het moment gebruikt wordt is translatie. Hierbij wordt bepaalde informatie uit het IPv4 verkeer herschreven naar waarden die wel in het IPv6 netwerk kunnen fungeren en andersom. Het herschrijven van informatie kan op drie lagen.

- **Netwerklaag**. Door het herschrijven van de IP-header informatie, zoals NAT dat bijvoorbeeld ook doet. De source- en destinationadres van het IPv4 pakket dienen gewijzigd te worden naar waarden die routeerbaar zijn in het IPv6-netwerk.
- **Transportlaag**. Alleen in native IPv6 netwerken. Verkeer dat naar een IPv6 bestemming gestuurd moet worden gaat via het normale circuit, terwijl IPv4 verkeer via een relay wordt verstuurd. De relay breekt de originele sessie af en bouwt een nieuwe sessie op met het IPv4 netwerk.
- **Applicatielaag**. Door gebruik te maken van een dual-stack webcache kunnen bepaalde applicaties, zoals SMTP, DNS en SIP gebruik maken van zowel IPv4 als IPv6.

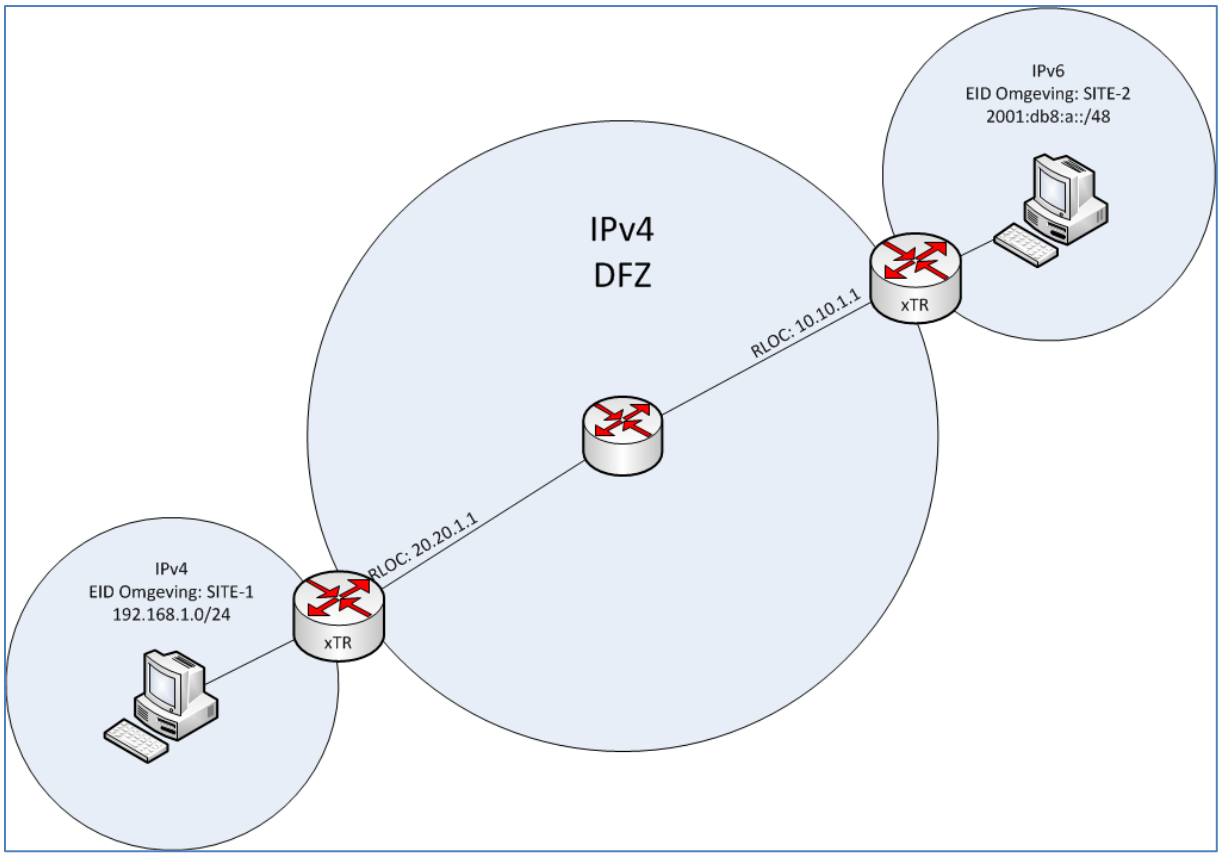
Transleren van informatie om connectie te verzorgen tussen IPv4 en IPv6 is altijd al gezien als een tijdelijke oplossing zoals NAT origineel ook is bedacht als tijdelijke oplossing tegen het snel uitgeven van IP-adressen. Omdat translatie meer problemen met zich meebrengt dan oplost is de techniek (RFC4966) tegenwoordig deprecated en wordt om die reden niet langer meegenomen in de vergelijking.

8.2.4 LISP

LISP is een architectuur dat werkt op basis van twee adressen. De EID en RLOC. Het is mogelijk om binnen de architectuur van LISP deze EID en RLOC adressen te zien als IPv4 en IPv6. Het is slechts een kwestie van encapsulation dat bepaald welke type de adressen aannemen. Zo is het mogelijk volledig IPv4 of IPv6 te zijn, of de EID IPv4 en de RLOC IPv6 en andersom. Doordat er vrijheid is in het bepalen welke vorm de adressen aannemen is het mogelijk LISP te gebruiken voor de transitie van en naar IPv6. Een goed voorbeeld waar dit is gebeurt is bij Facebook. Hier is in vier uur tijd met een toevoeging van één router het netwerk beschikbaar gemaakt voor IPv6 voordat de omgeving volledig dualstack ging.

Omdat LISP werkt met encapsulation wordt het vaak gezien als een tunnelprotocol. Dit is niet helemaal terecht. Waar een tunnelprotocol afhankelijk is van een volledig geconfigureerde tunnel om een andere type netwerk te overbruggen is LISP slechts afhankelijk van een EID-to-RLOC koppeling die aangeeft wat voor adres er toegevoegd dient te worden bij het encapsulationproces.

In de onderstaande afbeelding zijn twee EID omgevingen aangegeven. Eén daarvan is IPv4 en de ander IPv6. Wanneer SITE-1 verkeer zou willen sturen naar SITE-2 zou de mapping-database aangeven dat bij EID: 2001:db8:a::/48 de RLOC 10.10.1.1 gekoppeld zit. In de LISP header dat in hoofdstuk zes beschreven is, zou in de RLOC source- en destination gebruik gemaakt worden van de IPv4 adressen, terwijl de EID source- en destination gevuld worden met een IPv4 source en IPv6 destination. Dit proces kan andersom ook werken met een IPv6 DFZ en een IPv4 bestemming. Dat maakt voor encapsulation niet uit.



Figuur 8.6 – Voorbeeld topologie IPv6 transitie

Voordelen:

- **Weinig tot geen kosten**. Als de bestaande routers over LISP technologie beschikken kan IPv6 transitie kosteloos ingeregeld worden. Er hoeven ook geen wijzigingen doorgevoerd te worden in het bestaande (IPv4) netwerk.
- **Korte installatietijden**. De configuratie van LISP is vrij gemakkelijk. Zelfs wanneer rekening gehouden moet worden met verbinding tussen wel- en niet-LISP omgevingen. Dit zorgt voor korte installatietijden, zoals de vier uur die nodig was om Facebook in zijn geheel IPv6 ready te maken.
- **Goede overgangstechniek.** Het is ook mogelijk om het interne netwerk volledig om te zetten naar IPv6 als voorbereiding op de toekomst en door middel van LISP connectie behouden met IPv4 netwerken. Op die manier is LISP een goede kandidaat voor overgang.

Nadelen:

- **Adoptie van LISP.** Wanneer er gekozen wordt om IPv6 transitie door LISP te implementeren is het nodig om LISP in zijn geheel te adopteren. Dit hoeft niet perse een nadeel te zijn, maar er dient wel rekening mee gehouden te worden dat LISP experimenteel is. Het gevolg van een experimenteel protocol is dat de documentatie het alleen nog maar heeft over voordelen. Tijdens het bouwen van het lab zullen wellicht wel nadelen naar voren komen.
- **MTU Problemen**. LISP blijft een encapsulation techniek, waarbij extra informatie wordt toegevoegd aan de header. Hierdoor krijg je altijd te maken met MTU problemen. Hier zijn wel oplossingen voor bekend.

8.3 VM/IP MOBILITY

Tegenwoordig wordt steeds meer gebruik gemaakt van virtuele omgevingen. Werkplekken en programma's verplaatsen naar servers in de cloud en werken is per definitie mobiel geworden. Dit wordt nog verder versterkt doordat tegenwoordig bijna iedereen beschikt over en laptop, mobiel of tablet die overal wordt gebruikt. Om te zorgen dat verkeer dat bestemd is voor een mobiel object toch bij de juiste bestemming aankomt is IP mobilty nodig. IP mobilty zorgt ervoor dat sessies behouden blijven terwijl een apparaat van locatie wijzigt. LISP kan door middel van het dynamisch wijzigen van de EID-to-RLOC koppelingen zorgen voor IP-mobility. Op het moment is deze techniek alleen nog voor virtuele machines beschikbaar onder de naam VM mobility. Wel zijn er ontwikkelingen in gang om deze techniek beschikbaar te maken voor mobiele telefoon, maar deze techniek vereist een snellere omschakeling, omdat mobiele telefoons vaker veranderen dan bijvoorbeeld virtuele machines. In dit hoofdstuk zullen bestaande technieken worden vergeleken met LISP VM Mobilty.

8.3.1 ROUTE HEALTH INJECTION (RHI)

Route Health Injection (RHI) is een simpele techniek dat zorgt dat verkeer aankomt bij een eindsysteem die constant verplaatst. Om RHI te implementeren in een netwerk zijn routers nodig die RHI ondersteunen. Het is om die reden ook een techniek die gebruikt wordt binnen een intranet en niet op het internet zelf. RHI wordt gezien als een simpele techniek, omdat het niet meer doet dan het injecteren van nieuwe routes in een routingprotocol wanneer een eindsysteem van locatie veranderd. Voordat zo'n nieuwe route kan worden geïnjecteerd wordt door middel van probing gecontroleerd of het eindsysteem te bereiken is. Wanneer dit het geval is wordt een route geïnjecteerd die andere systemen kunnen gebruiken voor het bereiken van de bestemming.

Voordelen:

- **Simpel**. Het enige voordeel van RHI is de simpliciteit. Wanneer een eindsysteem verplaatst wordt er een route naar de nieuwe bestemming geïnjecteerd.

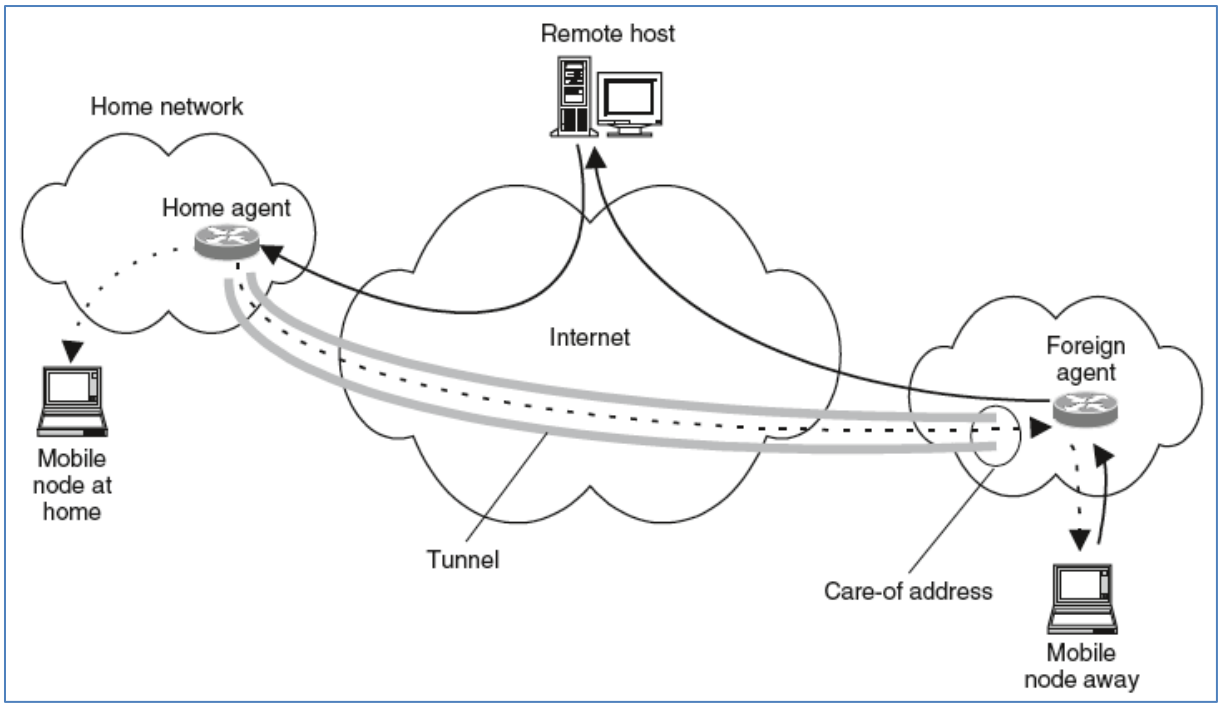
Nadelen:

- **Vervuiling**. Doordat er constant nieuwe routes worden geïnjecteerd wordt de routetabel snel vervuild met routes die niet langer geldig zijn.

8.3.2 MOBILE IPV4/IPV6

Mobile IPv4 en IPv6 zijn een stuk geavanceerder dan RHI. Om te garanderen dat een mobiel eindsysteem geen sessieverlies leidt worden twee adressen toegekend aan een eindsysteem. Het eerste adres, de home-adres, wordt permanent toegekend aan een eindsysteem en wordt gebruikt wanneer een eindsysteem in zijn thuisomgeving bevindt. Het tweede adres, care-of-address, wordt toegekend aan het eindsysteem wanneer het zich in een ander netwerk bevindt. Binnen deze thuis- en buitennetwerken zijn twee agents gestationeerd. In het thuisnetwerk is een home-agent actief die informatie opslaat over de permanente adressen en locaties van die permanente eindsystemen. In de buitennetwerken zijn foreign-agents actief die informatie opslaan over bezoekers van het netwerk en delen care-of-adressen uit aan de bezoekers.

Wanneer een mobiel eindsysteem van locatie veranderd zoekt het eindsysteem de agents van het netwerk op en maakt op die manier bekend wat zijn locatie is. Wanneer er verkeer gestuurd wordt naar het mobiele eindsysteem wordt dat richting de home-agent van het eindsysteem gestuurd. Als het eindsysteem bekend heeft gemaakt dat hij in zijn thuisnetwerk aanwezig is zal het verkeer worden ontvangen via het traditionele circuit. Als dat niet het geval is en het eindsysteem in een ander netwerk bevindt zal de home-agent als een soort proxy dienen en het verkeer doorsturen naar het care-of-adres door met encapsualtion het verkeer te voorzien van een nieuw IP-header.



Figuur 8.7 – Mobile IPv4 werking – Bron: (TechTarget, 2009)

Mobile IPv6 gaat een stap verder en maakt niet langer gebruik van een home-agent, maar zorgt ervoor dat verkeer direct wordt verstuurd naar een care-of-adress. Dit wordt gerealiseerd door een care-of-adress te binden aan het eindsysteem. Op deze manier kan er een direct pad worden opgezet tussen het systeem dat verkeer wil sturen aan de ontvanger, zonder dat verkeer omgeleid moet worden door de home-agent.

Voordelen:

- **Geen sessieverlies**. Zowel mobile IPv4 als IPv6 zorgen voor een constante verbinding die kan verplaatsen, zonder dat er sessieverlies optreedt.

Nadelen:

- **Eén type ondersteuning**. Als er gebruik gemaakt wil gaan worden van mobile IPv4 of IPv6 moet het gehele pad wel over dezelfde type beschikken. Bijvoorbeeld voor IPv6 moeten de eindsystemen beide IPv6 ondersteuning hebben, moet het gevolgde pad IPv6 zijn en de agents moeten IPv6 ondersteunen.
- **Omleiding**. In dit geval alleen voor mobile IPv4. Verkeer moet altijd worden omgeleid via de home-agent wat kan resulteren in het feit dat niet altijd het kortste pad wordt gekozen.
- **Route injection**. Als een home-agent verkeer moet sturen naar een foreign-netwerk dat niet direct verbonden is, moet er een route worden geïnjecteerd in het bestaande routingprotocol. Dit zorgt voor vervuiling van routetabellen. Dit is ook één van de redenen waarom LISP is bedacht.

8.3.3 DNS Based Redirection

Voor servers die verplaatsen is het mogelijk om door middel van DNS voor connectie te zorgen. Wanneer een server verplaatst naar een nieuw netwerk wordt het DNS-record vernieuwd en voorzien van het nieuwe IP-adres die toegewezen is op de nieuwe locatie. Het dynamisch wijzigen van DNS-records wordt aangeboden door partijen als DynDNS. DynDNS is een veel gebruikte techniek bij klanten van Qi ict, omdat veel klanten te maken hebben met een dynamisch IP-adres. Omdat de hostname in de record hetzelfde blijft terwijl het IP-adres veranderd is connectie altijd mogelijk.

Voordelen:

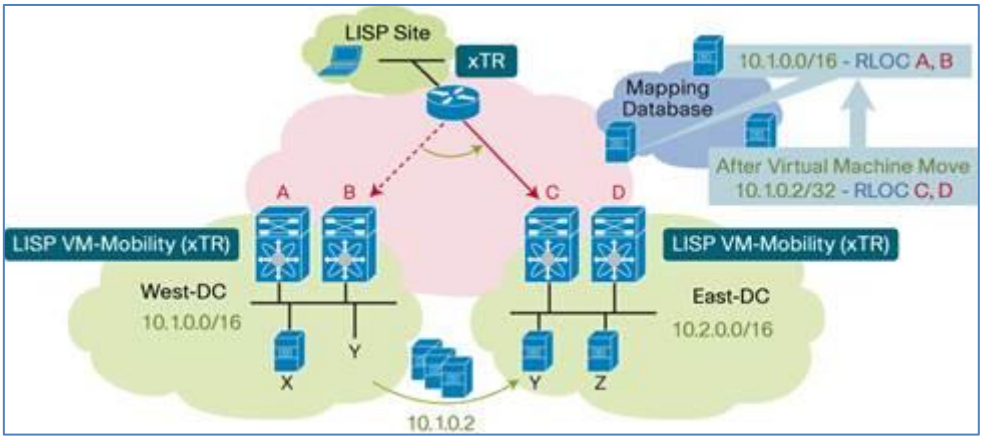
- **Goedkoop**. Services als DynDNS zijn vaak gratis tot een bepaald aantal eindsystemen. Voor partijen die alleen te maken hebben met inkomend verkeer op de servers is het een goedkope oplossing.
- **Simpel**. Er is niet meer nodig dan een update-client op de servers die het nieuwe IP-adress bekend maken aan de beheerder van de DNS-records. De rest wordt automatisch geregeld. Tevens maakt het niet uit of het om IPv4 of IPv6 gaat.

Nadelen:

- **Alleen inkomend verkeer.** Gebruik maken van DNS heeft alleen zin op inkomend verkeer, omdat de hostname niet veranderd.
- **Sessieverlies.** Als het IP-adres van de server wijzigt gaat de sessie verloren, omdat er een nieuwe sessie opgezet dient te worden met het nieuwe IP-adres

8.3.4 LISP VM/IP MOBILITY

VM/IP Mobility van LISP bouwt zich voort op de koppeling tussen EID en RLOC. De EID van een eindsysteem blijft hetzelfde terwijl de RLOC verandert wanneer de EID zich verplaatst. Deze IP mobility techniek richt zich vooral op virtuele machines die actief zijn in datacenters, maar er wordt op het moment ook gewerkt aan mobility technieken voor mobile telefoons. In dit hoofdstuk blijft de focus op VM mobility.



Figuur 8.8 – LISP VM/IP Mobility – Bron: (Cisco Systems, 2011)

De werking van de techniek is vergelijkbaar met het proces dat normaal door LISP gevolgd wordt. De ETR registreert de EID's van zijn lokale netwerk die deze waarden doorgeeft aan de MS en het DDT-netwerk die daarachter zit. Verbinden met een eindsysteem is zoals altijd op basis van een opgezochte koppeling uit de DDT-database. In het bovenstaande mobility voorbeeld is het enige verschil dat de ETR op de hoogte moet zijn dat er een nieuw eindsysteem in zijn lokale netwerk verplaatst is.

Bij het verplaatsen van een eindsysteem kunnen er twee situaties voorkomen. Het eindsysteem komt uit een netwerk met hetzelfde subnet (LISP_EXTENDED_SUBNET), of het komt uit een netwerk met een ander subnet (LISP_ACROSS_SUBNET). Als het eerste het geval is, zal er een laag twee techniek zoals overlay transport virtualization (OTV) actief moeten zijn tussen de vestigingen.

Wanneer er een verplaatsing gaat plaatsvinden zijn er drie stappen die uitgevoerd moeten worden:

- Detecteren dat een eindsysteem is verplaatst
- Registreren van het nieuwe eindsysteem in de mapping-system
- Het LISP netwerk op de hoogte brengen van de wijzigingen

Hieronder zullen voor zowel verschillende subnets als dezelfde subnets het stappenplan worden uitgewerkt hoe verbinding weer tot stand komt.

LISP – Twee verschillende subnetten

1. De eerste stap in het proces is configuratie. Op beide vestigingen dient één of meer interfaces geconfigureerd te worden met het "lisp mobility roamer" commando. Daarnaast wordt een mac-adres aangegeven waarvan gebruikt kan worden om te communiceren met de lokale gateway, ondanks dat het IP-adres niet in het subnet voorkomt.
2. De tweede stap is het verplaatsen van het eindsysteem zelf. Dit kan het verplaatsen van een VM zijn in een datacenter naar een andere verdieping, een andere vestiging of zelfs een ander land.
3. Stap drie is het detecteren van de verplaatsing. Wanneer bevestigd is dat de interface waarop het nieuwe eindsysteem is aangesloten ook daadwerkelijk een mobility poort is wordt er een route opgenomen in de routingtabel van de xTR. Deze route wijst altijd naar het /32 subnet van de verplaatste EID.
4. Stap vier is optioneel. Hierin worden redundante LISP routers die in de omgeving aanwezig zijn, zoals met multihoming, op de hoogte gebracht van de verplaatsing door middel van map-notify berichten.
5. Stap vijf is het registreren van de nieuwe EID bij de MS door middel van een map-register bericht.
6. Dit wordt verwerkt door de MS en het DDT netwerk dat erachter zit.
7. Stap zeven is het inlichten van de xTR's die voorheen verantwoordelijk waren voor de EID dat er een verplaatsing heeft plaatsgevonden door middel van map-notify berichten.
8. De xTR's gebruiken deze informatie om map-caches aan te passen en sturen deze informatie door aan eventuele redundante routers in de omgeving, zodat zij hetzelfde kunnen doen.

ITR's kunnen gebruik maken van deze nieuwe informatie om verkeer te sturen naar de nieuwe locatie van de host, terwijl dezelfde eindbestemming (EID) gebruikt wordt. Hiervoor dient wel opnieuw het EID-to-RLOC opzoekproces afgewerkt te worden, om een nieuwe koppeling te ontvangen. Wanneer verkeer aankomt bij de nieuwe ETR kan op basis van MAC-adres en proxy-ARP verkeer worden doorgestuurd naar de EID, ondanks dat zijn IP-adres uit een ander subnet afkomstig is. De tijd die verloren gaat tussen het verplaatsen van het eindsysteem en het opnieuw verkeer te kunnen sturen is ongeveer anderhalf keer de round trip tijd van een verbinding.

LISP – Twee dezelfde subnetten

Wanneer twee dezelfde subnetten actief zijn in twee verschillende locaties is er een laag twee techniek nodig zoals OTV om de synchronisatie tussen netwerken te regelen. Verder is het proces voor een groot deel hetzelfde als de voorgaande optie.

1. Stap één is het configureren van de lisp mobility roamer interface.
2. Stap twee is het verplaatsen van het eindsysteem
3. Stap drie is het detecteren van de verplaatsing. Het verschil met de vorige optie is dat in de routetabel van de originele xTR een null0 route wordt aangemaakt naar het IP-adres dat verdwenen is en in het nieuwe netwerk de xTR een /32 route aanmaakt naar dat IP.
4. Stap vier is het registreren van de nieuwe locatie bij het mapping-system

Na het volbrengen van deze vier stappen is de mapping-data weer in orde en kan na een nieuwe map-request weer verkeer verzonden worden naar de nieuwe locatie van het eindsysteem.

Voordelen:

- **Snelle omzetting**. De omzetting van RLOC kan zeer snel worden volbracht. Ongeveer anderhalf tot twee keer de round trip tijd van een verbinding.
- **IP-based oplossing**. De oplossing is gebaseerd op laag drie IP-verkeer (EID & RLOC) waardoor het onafhankelijk is van de manier waarop het getransporteerd wordt.
- **Globaal beschikbaar**. De techniek kan over de hele wereld worden toegepast zonder problemen. Het is zelfs mogelijk om geologische data op te nemen in de mapping-system, om nog beter te bepalen waar het verkeer heen moet op aarde.

Nadelen:

- **Firewall**. Bij een omgeving met twee dezelfde subnetten kan verkeer via OTV op laag twee worden doorgestuurd naar de andere vestiging. Wanneer het later op laag drie wordt opgepakt kan het worden tegen gehouden door de firewall, omdat het verkeer initieel niet op de andere vestiging is binnen gekomen.
- **Adoptie van LISP.** Wanneer er gekozen wordt om VM Mobility met LISP te implementeren is het nodig om LISP in zijn geheel te adopteren. Dit hoeft niet perse een nadeel te zijn, maar er dient wel rekening mee gehouden te worden dat LISP experimenteel is. Het gevolg van een experimenteel protocol is dat de documentatie het alleen nog maar heeft over voordelen. Tijdens het bouwen van het lab zullen wellicht wel nadelen naar voren komen.

9. VOORLOPIG CONCLUSIE

Op basis van de informatie uit dit document is het mogelijk om een voorlopige conclusie te maken over LISP. De conclusie zal later worden bijgesteld aan de hand van het adviesrapport dat geschreven wordt na het bouwen en testen van verschillende LISP-opstellingen.

Wat is het LISP protocol en welke problemen lost het op?
LISP is in verschillende documenten op websites aangegeven als de vervanger van BGP en is om die reden vaak verward als een routeringsprotocol. Dit is niet het geval. LISP is een architectuur die als verrijking kan dienen voor het huidige internetmodel. LISP zorgt voor een scheiding tussen de identiteit (EID) en locatie (RLOC) van een eindsysteem. Door deze twee elementen te scheiden en de koppeling tussen identiteit en locatie op te slaan in een database kan het aantal routes in de BGP-routers van het internet worden verlaagd. Dit met de reden dat aggregatie optimaal toegepast kan worden op RLOC's die topologie afhankelijk zijn en extra routes voor eindsystemen die verplaatsen niet langer geïnjecteerd hoeven worden, omdat EID adressen topologie onafhankelijk zijn.

Naast het verlagen van het aantal routes kan LISP ook gebruikt worden voor situaties waarbij multihoming, IPv6 transitie, IP mobility en netwerk virtualisatie gewenst zijn op een kosteneffectieve wijze met weinig configuratie.

Hoe werkt LISP en wat is nodig om het te kunnen implementeren in een netwerk?
Bij het routeren van verkeer is het nog steeds nodig om via protocollen als OSPF en BGP het verkeer van A naar B te krijgen. LISP brengt hier verandering in door de informatie te verbeteren door middel van een database. Voordat het verkeer verstuurt wordt zorgen LISP routers voor informatie over de locatie van het eindsysteem. Vervolgens encapsulate de LISP-router het verkeer met gegevens uit de database. Eenmaal aangekomen bij de LISP-router die zich voor de eindbestemming bevindt wordt de encapsulation data verwijderd en wordt het verkeer doorgestuurd.

Om LISP te kunnen gebruiken is niet meer nodig dan een netwerkcomponent met LISP functionaliteit. Dit kunnen Cisco routers zijn of één van de Opensource projecten.

Wat is het verschil met bestaande routingprotocollen en bestaande overlay- en tunneling methoden?
In dit document is alleen ruimte gemaakt voor vergelijkingen met de protocollen BGP, MPLS, OSPF en IS-IS. Er zijn geen overlay- en tunnelprotocollen vergeleken, omdat deze initieel buiten de projectgrenzen vielen. Deze zouden alleen worden vergeleken als er tijd over was in het onderzoek, wat hier niet het geval is. Voor de protocollen die wel vergeleken zijn was er veel verschil te zien. Er zijn weinig zaken waarin overlap te vinden is. Dit komt doordat LISP zich in een unieke positie bevindt tussen routering en tunneling. LISP zorgt voor routeringsinformatie en encapsulation, maar meer dan dat ook niet. Het kan daardoor gebruikt worden voor zaken als multihoming, maar blijft afhankelijk van onderliggende protocollen.

Op welke manier vervangt LISP andere protocollen/mechanismen in bestaande technieken?
Er zijn drie technieken onderzocht:

- **Multihoming**. LISP kan in een multihomed opstelling BGP en NAT vervangen door in de database twee RLOC addressen op te nemen en daarover het verkeer te verdelen.
- **IP Mobility**. Bij mobiliteit van IP-adressen kan LISP protocollen als DNS, IPv4 en IPv6 mobile en Route Health Injection. Het gaat dan wel om specifieke gevallen zoals VM mobility. Voor zaken als mobiele telefoons zijn er nog ontwikkelingen in gang.
- **IPv6 transitie**. LISP kan voor een goedkope IPv6 transitie oplossing zorgen door zijn encapsulation dat tunneling, translatie en dualstack kan vervangen.

Wat zijn de voor- en nadelen van LISP?
LISP heeft een groot aantal voordelen die het met zich meebrengt. Het grootste voordeel is het zorgen dat het aantal routes in het DFZ drastisch verlaagd kunnen worden, wat voor snellere schakelingen over het internet zorgt. Door de scheiding tussen identiteit en locatie zorgt LISP voor schaalbaarheid en flexibiliteit op een zeer goedkope wijze, omdat de goedkoopste routers het protocol ondersteunen. Het grootste nadeel blijft de experimentele aard van het protocol. Er zijn nog bijzonder veel onduidelijkheden over het protocol en hoe het functioneert in een live omgeving. Om die reden kan er nog niet teveel over worden gezegd en zullen de resultaten uit het volgende rapport afgewacht moeten worden.

Voor welke omgevingen is LISP een geschikt protocol?
Hierover kan weinig uitspraak worden gedaan. LISP biedt een aantal technieken aan die geschikt zijn voor allerlei omgevingen, maar de testresultaten uit het volgende deel van het onderzoek zullen bepalen of de technieken ook geschikt zijn.

10. LITERATUURLIJST

APNIC. (2014, 12 26). *bgp.potaroo.net*. Opgehaald van BGP Analysis Reports: http://bgp.potaroo.net/index-bgp.html

Barry M, V. G. (2012, 10 15). *Brief history of the internet*. Opgehaald van www.internetsociety.org: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

Brocade. (2014, 12 23). *MPLS*. Opgehaald van www.brocade.com: http://www.brocade.com/solutions-technology/technology/ethernet-technology/mpls.page

Cisco Systems. (2011, 01 01). *Locator/ID Separation Protocol (LISP) Virtual Machine Mobility Solution White Paper*. Opgehaald van www.cisco.com: http://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/white_paper_c11-693627.pdf

Cisco Systems. (2013, 10 12). *LISP - Delegated Database Tree (LISP-DDT)*. Opgehaald van lisp.cisco.com: http://lisp.cisco.com/docs/LISP-DDT-details-v12.pdf

Cisco Systems. (2014, 12 29). *Configuring LISP (Locator ID Separation Protocol)*. Opgehaald van www.cisco.com: http://www.cisco.com/c/dam/en/us/td/i/300001-400000/300001-310000/300001-301000/300192.tif/_jcr_content/renditions/300192.jpg

Cisco Systems. (2014, 04 24). *LISP Feature Support by Operating System.* Opgeroepen op 12 04, 2014, van lisp.cisco.com: http://lisp.cisco.com/lisp_hwsw.html#HW

D. Farinacci, C. S. (2013, 01 01). *The Locator/ID Separation Protocol (LISP) (RFC6830)*. Opgehaald van tools.ietf.org: https://tools.ietf.org/html/rfc6830#section-1

D. Lewis, D. M. (2013, 01 01). *Interworking between Locator/ID Separation Protocol (LISP) and NON-LISP sites (RFC6832).* Opgeroepen op 12 04, 2014, van tools.ietf.org: https://tools.ietf.org/html/rfc6832

D. Meyer, L. Z. (2007, September 01). *Report from the IAB Workshop on Routing and Addressing (RFC4984).* Opgeroepen op 12 03, 2014, van www.tools.ietf.org: https://tools.ietf.org/html/rfc4984

D. Saucez, I. L. (2014, 07 04). *LISP Threats Analysis.* Opgeroepen op 12 04, 2014, van tools.ietf.org: https://tools.ietf.org/html/draft-ietf-lisp-threats-10#section-2.1.4

E. Lear, C. S. (2013, 01 01). *A Not-so-novel Endpoint ID (EID) to Routing Locator (RLOC) Database (RFC6837).* Opgeroepen op 12 10, 2014, van tools.ietf.org: https://tools.ietf.org/html/rfc6837

F. Maino, V. E. (2014, 10 16). *LISP-Security (LISP-SEC).* Opgeroepen op 12 04, 2014, van tools.ietf.org: https://tools.ietf.org/html/draft-ietf-lisp-sec-07

Groningen, R. (2012, 10 30). *Systematisch literatuur zoeken*. Opgeroepen op 11 26, 2014, van www.rug.nl: http://www.rug.nl/education/other-study-opportunities/hcv/schriftelijke-vaardigheden/voor-studenten/bronnen-literatuur/systematisch-literatuur-zoeken

Halabi, B. (1997). *The definitive resources for interworking design alternatives and solutions.* Indianapolis, USA: Cisco Systems.

Heimlich, S. (2014, 12 05). LISP+ALT (E-mail). Delft, Zuid-Holland, Nederland.

Hill, C. (2011, 09 13). *LISP - A Next Generation Routing Architecture*. Opgehaald van www.netcraftsmen.com: http://www.netcraftsmen.com/wp-content/uploads/2014/12/20110913_cmug_LISP_Use_Cases.pdf

Moreno, V. (2014, 01 01). *LISP - A Next Generation Networking Architecture (2014 Melbourne) - 90 Mins.* Opgeroepen op 12 04, 2014, van www.ciscolive.com: https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=77826&backBtn=true

S. Brim, N. C. (2008, 10 11). *LISP-CONS: A Content distribution Overlay Network Service for LISP.* Opgeroepen op 12 11, 2014, van tools.ietf.org: https://tools.ietf.org/html/draft-meyer-lisp-cons-04

Slot Webcommerce BV. (2014, 01 01). *Nederlandse Encyclopedie*. Opgehaald van www.enclyclo.nl: http://www.encyclo.nl/begrip/identiteit

TechTarget. (2009, 10 01). *Mobile IP Networks: An overview.* Opgehaald van techtarget.com: http://cdn.ttgtmedia.com/digitalguide/images/Misc/mobile-ip-ch10-1.gif

V. Fuller, D. F. (2013, 01 01). *Locator/ID Separation Protocol Alternative Logical Topology (LISP+ALT) (RFC6836).* Opgeroepen op 12 10, 2014, van tools.ietf.org: https://tools.ietf.org/html/rfc6836

V. ONTWERPRAPPORT

INHOUDSOPGAVE

1. INLEIDING

In het onderzoeksrapport zijn de verschillende vormen waarin LISP voorkomt door middel van theorie toegelicht. Hierin bevonden zich een aantal onzekerheden en uitzonderingen. Er is om die reden behoefte aan praktijktesten om te bepalen hoe LISP reageert in bepaalde situaties. In dit rapport worden drie opstellingen toegelicht die in een periode van twee weken worden gebouwd en getoetst. Aan de hand van de resultaten die hieruit voortkomen kan in een advies rapport worden bepaald in hoeverre LISP geschikt is voor Qi ict en haar klanten.

Het document bestaat uit informatie over drie opstelling. Een demonstratie van het bèta-netwerk, een standalone omgevingen waar LISP technieken worden getoetst en een klantnetwerk dat LISP adopteert.

2. TOELICHTING ONTWERPEN

Het doel is om voor *23 maart 2015 een onderzoek te hebben uitgevoerd dat Qi ict inzicht geeft in het gebruik en de implementatie van het LISP protocol in het bestaande internet model. Het onderzoek dient een rapport en een testopstelling op te leveren die als basis gaat fungeren voor het beter adviseren van klanten die geïnteresseerd zijn in deze techniek.*

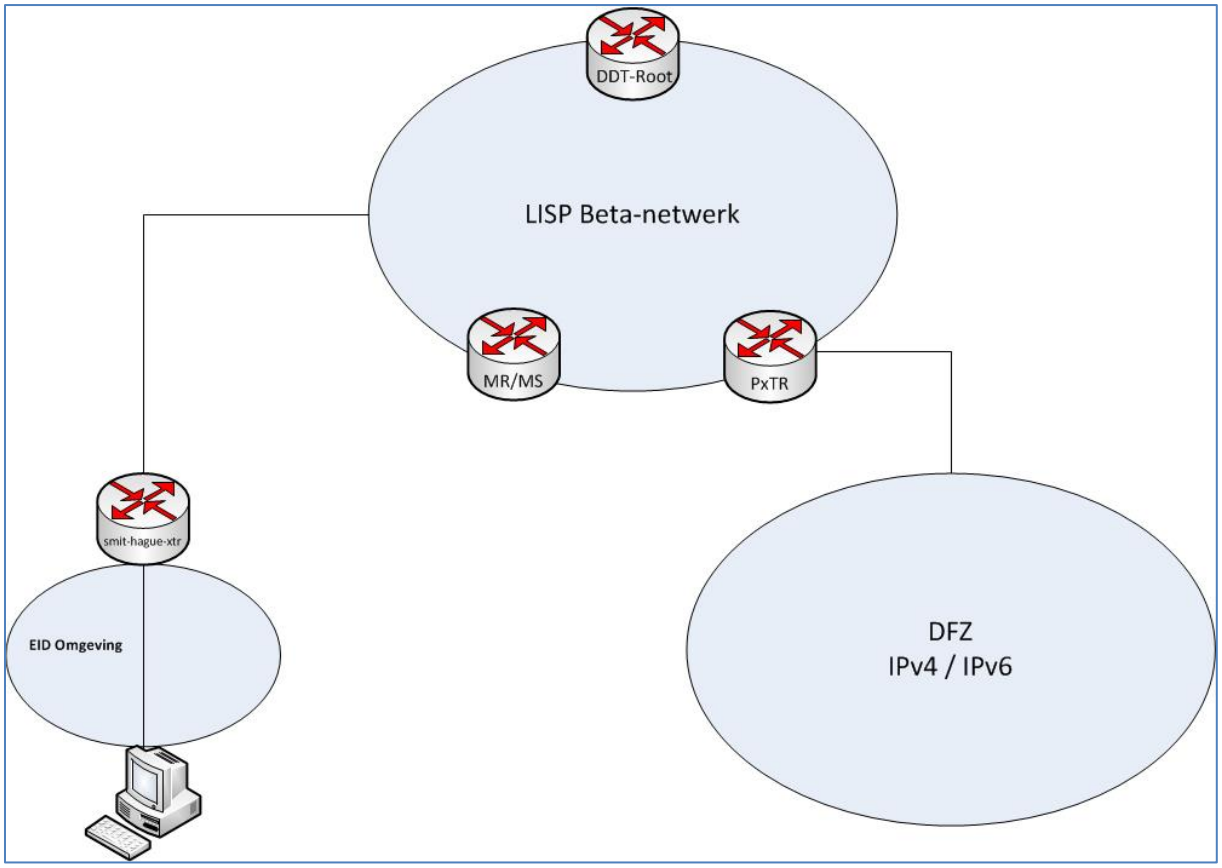
De bovenstaande tekst beschrijft het doel van het onderzoek zoals deze in het plan van aanpak reeds is beschreven. Een deel van dit doel is gerealiseerd door het schrijven van een onderzoeksrapport waarin de werking van LISP is toegelicht. Hierin is duidelijk geworden dat LISP een architectuur is dat gebruikt kan worden voor he terugdringen van routers in het DFZ, maar daarnaast ook verschillende protocollen kan vervangen in specifieke situaties. Het feit dat LISP het aantal routes in het DFZ kan terugdringen is belangrijk, maar zal pas in relevant zijn wanneer LISP op een globaal niveau word geïmplementeerd. Het blijft speculatie of dat ooit zal gebeuren. De verschillende toepassingen waarvoor LISP gebruikt kan worden, multihoming, IPv6 transitie en VM/IP Mobilty, kunnen daarentegen wel verder worden getoetst. Daar is dit ontwerprapport voor bedoeld. In dit rapport zullen drie opstellingen worden uitwerkt die na het bouwen in de volgende fasen worden getest.

Let wel, de ontwerpen die hierin worden beschreven worden ontwikkeld om Qi ict een beter beeld te geven van het LISP protocol en waar het protocol staat in het huidige internetmodel. Hierin staat de werking en implementatie van LISP centraal. Hiervoor zullen ook testplannen worden geschreven. Onderzoek in hoeverre LISP beter is dan alternatieve technieken blijft een bijzaak. Vergelijkingen zullen dan ook alleen maar voorkomen als daar tijd en middelen voor zijn.

3. OPSTELLING BÈTA-NETWERK

De eerste opstelling die gebouwd wordt is bedoeld om LISP te demonstreren door middel van het bèta-netwerk dat op het moment actief is. Het doel is om aan te geven in hoeverre de adoptie van LISP gevolgen heeft op de bereikbaarheid van het bestaande netwerk.

3.1 TOPOLOGIE



Figuur 3.1 – Topologie o.b.v. LISP beta-netwerk

De bovenstaande afbeelding geeft de topologie van het netwerk weer. De Windows 7 machine (Host A) en de LISP router die het interne netwerk verbindt (smit-hague-xtr) met het LISP bèta-netwerk dienen zelf te worden geconfigureerd. De gegevens die hiervoor nodig zijn worden door de LISP afdeling van Cisco verstuurd na een aanvraag via de website. De resterende componenten, het bèta-netwerk en het DFZ, bestaan al in het huidige internetmodel.

De LISP-router, smit-hague-xtr, wordt aan de buitenkant voorzien van een publiek IPv4-adres, ook wel het RLOC-adres genoemd. Aan de binnenkant wordt zowel een IPv4 als IPv6 subnet geconfigureerd dat zal fungeren als de EID omgeving. Host A zal voorzien worden van een IPv4- en IPv6-adres om dualstack te kunnen verbinden met het internet.

De DDT-root en MR/MS die zich in het béta-netwerk bevinden worden gebruikt voor het opsporen van bestaande LISP-omgevingen die bereikt kunnen worden. De PxTR wordt gebruikt voor het verbinden met omgevingen die geen LISP ondersteunen in het DFZ.

3.2 BENODIGDHEDEN

Voor deze opstelling zijn de volgende onderdelen nodig:

- Publiek IP-adres
- Component met LISP functionaliteit
- (Windows 7) eindsysteem

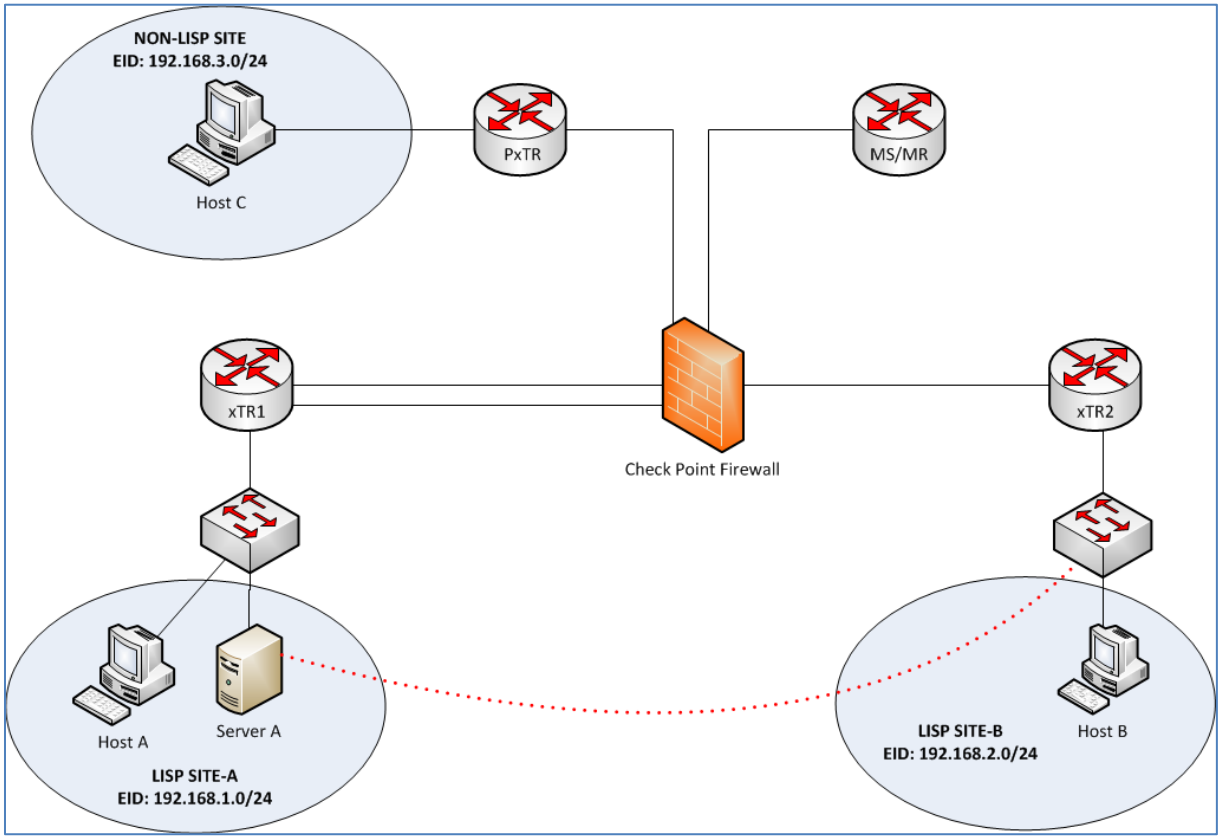
3.3 TESTPLAN

LISP bèta-netwerk	
Doel	Demonstratie van het bèta-netwerk. Bepalen in hoeverre de bereikbaarheid van het interne netwerk is na het adopteren van LISP
Toelichting	Als een onderneming gebruik zou willen maken van de functionaliteiten van LISP is gebruik maken van een LISP-ISP veruit de meest eenvoudige optie. Door middel van deze opstelling kan bepaald worden hoeveel configuratie nodig is voor het gebruik maken van LISP en welke voor- en nadelen er bij komen kijken.
Testomgeving	De topologie van de testomgeving is te vinden op pagina twee van het ontwerprapport. De opstelling omvat een zelf geconfigureerde xTR dat in verbinding staat met het LISP bèta-netwerk.
Benodigdheden	- Publiek IP-adres - Component met LISP functionaliteit - Eindsysteem
Testen	**Vanuit de EID-omgeving:** - Ping non-LISP IPv4-omgeving. - Ping LISP IPv4-omgeving. - Ping non-LISP IPv6-omgeving. - Ping LISP IPv6-omgeving. **Vanaf een machine in het DFZ:** - Ping machine in EID-omgeving over IPv4. - Ping machine in EID-omgeving over IPv6. **Op de machine in de LISP omgeving:** - Doe een IPv6 ready test: www.test-ipv6.com

4. STANDALONE OPSTELLING

De tweede opstelling is een op zichzelf staande LISP omgeving zonder een koppeling met het bèta-netwerk. In deze opstelling kunnen de verschillende LISP technieken worden getoetst, zoals multihoming, IPv6 transitie en VM/IP Mobility.

4.1 TOPOLOGIE



Figuur 4.1 – Standalone topologie

De bovenstaande topologie geeft de tweede opstelling weer. De opstelling bestaat uit drie privé-netwerken, waarvan twee LISP ondersteunen en de derde niet. De twee LISP omgevingen bevinden zich achter een xTR en de niet-LISP omgeving achter een PxTR. Tevens is er nog een mapping-system aanwezig in het netwerk dat bestaat uit een MS en MR. Doordat het netwerk over alle mogelijke LISP-componenten beschikt, plus een niet-LISP omgeving is het mogelijk om alle technieken en scenario's te testen die op het moment ook voor kunnen komen in het huidige internet model. Alle netwerkcomponenten worden aan elkaar gekoppeld via een Check Point firewall om het DFZ van het internet te simuleren. Verder kan de Check Point firewall ook gebruikt worden om te inventariseren hoeveel impact een firewall op LISP kan hebben. De keuze voor Check Point als firewall komt voort uit het feit dat Qi ict op het moment een grote partner is van Check Point en ontzettend vaak deze firewalls wegzet bij klanten.

Deze opstelling wordt gebruikt voor het testen van de algemene werking van LISP en daarbij vooral de focus op de technieken VM/IP mobility, IPv6 transitie en multihoming. Multihoming wordt getoetst door xTR1 die een dubbele lijn heeft naar de firewall. Vm mobility wordt getoetst door server A te verplaatsen van LISP-SITE-A naar LISP-SITE-B. IPv6 transitie kan op verschillende wijzen worden getoetst, maar zal wellicht vervallen, omdat opstelling één al genoeg informatie levert over de bereikbaarheid van IPv4- en IPv6 adressen via LISP.

4.2 BENODIGDHEDEN

Voor deze opstelling zijn de volgende onderdelen nodig:

- Drie (Windows 7) machines
- Vier componenten met LISP functionaliteit. In dit geval wordt de mapping-system en PxTR virtueel aangemaakt op een Cisco CSR1000x en zijn de xTR's Cisco 2900 series.
- Check Point firewall als router en voorzien van Gaia R77.20. Het OS dat op het moment het meest in gebruik is bij klanten van Qi ict.
- Twee switches

4.3 TESTPLAN

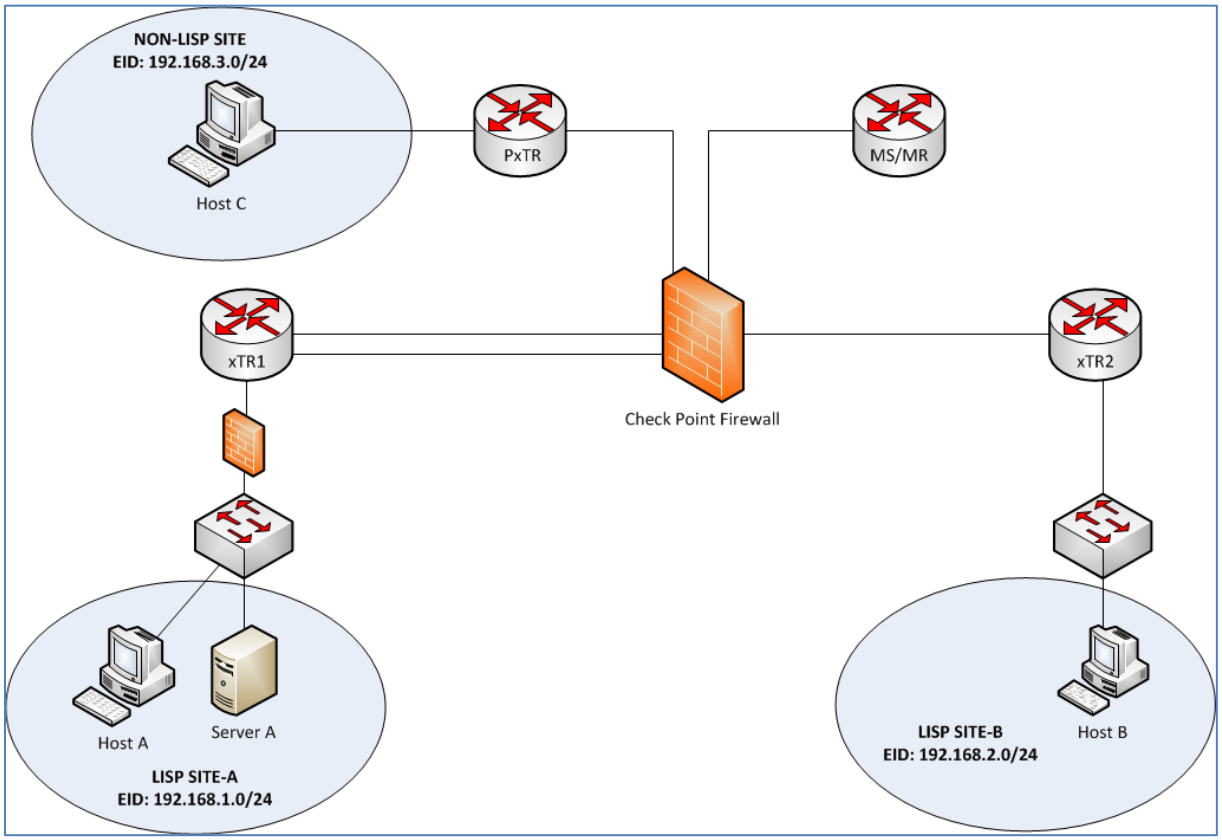
Standalone Netwerk	
Doel	Demonstratie van LISP functionaliteiten.
Toelichting	De drie hoofdfunctionaliteiten die LISP heeft naast het terugdringen van onnodige routers in het DFZ zijn multihoming, IPv6 transitie en VM mobility. Deze technieken zijn ook te demonstreren met het bèta-netwerk, maar het is dan moeilijker om data te verzamelen in onderdelen die zelf niet beheert worden. Door middel van een standalone netwerk kan op elk punt door middel van programma's als Wireshark data worden verzameld over de werking.
Benodigdheden	- Drie eindsystemen - Vier componenten met LISP functionaliteit - Twee switches - Check Point firewall
Testomgeving	De topologie van de testomgeving is te vinden op pagina vier van het ontwerprapport. De opstelling omvat een volledige geconfigureerd LISP omgeving waarin alle mogelijk LISP componenten aan bod komen (xTR, PxTR, MS, MR).
Testen	**Multihoming (IPv4/IPv6)** - Verstuur een ping naar de overzijde met afzenderadres link één. - Verstuur een ping naar de overzijde met afzenderadres link twee. - Ontvang een ping van de overzijde over link één. - Ontvang een ping van de overzijde over link twee. - Ping overzijde constant en verwijder de actieve verbinding. Meet de tijd van connectieherstel, als deze aanwezig is. - Start een ftp-sessie van het ene eindsysteem naar de ander en verwijder actieve verbinding. Meet de tijd van herstel, als deze aanwezig is. **VM/IP Mobility (IPv4/IPv6)** - Verplaats het ene eindsysteem naar het netwerk aan de overzijde. Meet hoe lang het duurt voordat de mapping-server op de hoogte is van de verandering. - Hetzelfde als bovenstaand, maar ook met een ping lopend om connectieherstel te meten. - Ping het verplaatste systeem vanaf een eindsysteem uit beide LISP omgevingen en de niet-LISP omgeving. - Start een FTP sessie voor het verplaatsen en controleer of de sessie wordt voortgezet na het verplaatsen. Meet de hersteltijd. **IPv6 Transitie** - De bovenstaande testen van multihoming en VM/IP mobility uitvoeren met het "internet" als volledig IPv4 en IPv6 om de overbrugging van een ander netwerk te testen. Dit is echter minder belangrijk, omdat het in de vorige

opstelling vrij veel aan bod komt.

5. KLANTNETWERK OPSTELLING

Hoewel opstelling twee ontzettend veel inzicht kan geven in de werking van LISP en de verschillende toegepaste technieken is dit niet een reëel beeld voor Qi ict. In opstelling twee verbinden de eindsystemen via een switch direct aan de “last-hop” router van het netwerk. Dit komt bij klanten van Qi ict zelden voor. Normaliter staat er voor de last-hop-router nog een firewall die het verkeer van het privénetwerk NAT achter zijn publieke IP-adres. In deze opstelling wordt die techniek ook toegepast. Op die manier kan bepaald worden hoeveel van de functionaliteit van opstelling twee nog overblijft na het plaatsen van een firewall die NAT uitvoert.

5.1 TOPOLOGIE



Figuur 5.1 – Topologie opstelling drie

De bovenstaande topologie geeft opstelling drie weer. Deze topologie verschilt qua opzet niet van die van opstelling twee op de firewall na die geplaatst is voor xTR1. Deze firewall zal verkeer van zijn interne netwerk door midden van NAT verschuilen achter zijn publieke IP-adres. De LISP-router, xTR1, zal op basis van de publieke IP-adres die hij krijg van de firewall zijn technieken moeten uitvoeren.

De focus ligt in deze opstelling vooral op VM/IP mobility. Van multihoming en IPv6 transitie wordt verwacht dat zich geen problemen voordoen, omdat het voor deze twee technieken niet uit maakt of zij direcht van een machine een IP-adres ontvangen of via NAT. Voor VM/IP mobility maakt het waarschijnlijk wel uit. Er wordt verwacht dat de machines achter de firewall door NAT niet gedetecteerd worden bij het verplaatsen.

5.2 BENODIGHEDEN

- Drie (Windows 7) machines
- Vier componenten met LISP functionaliteit
- Twee Check Point firewalls
- Twee switches

5.3 TESTPLAN

Klantnetwerk	
Doel	Demonstratie van LISP functionaliteiten in een standaard QI ict klantnetwerk
Toelichting	Hoewel de technieken in opstelling twee gedemonstreerd zijn, ging het hier wel om een ideale opstelling. Deze opstelling komt normaliter niet voor bij klanten van Qi ict. Het toevoegen van een firewall die eindsystemen verschuilt achter zijn publieke IP-adres is voor Qi ict wel een relevante omgeving.
Benodigdheden	- Drie eindsystemen - Vier componenten met LISP functionaliteit - Twee switches - Twee Check Point firewalls
Testomgeving	De topologie van de testomgeving is te vinden op pagina zes van het ontwerprapport. De opstelling omvat een volledige geconfigureerd LISP omgeving waarin alle mogelijk LISP componenten aan bod komen (xTR, PxTR, MS, MR), met daarbij ook een Check Point firewall die verkeer voorziet van NAT en inspectie.
Testen	**Multihoming (IPv4/IPv6)** - Verstuur een ping naar de overzijde met afzenderadres link één. - Verstuur een ping naar de overzijde met afzenderadres link twee. - Ontvang een ping van de overzijde over link één. - Ontvang een ping van de overzijde over link twee. - Ping overzijde constant en verwijder de actieve verbinding. Meet de tijd van connectieherstel, als deze aanwezig is. - Start een ftp-sessie van het ene eindsysteem naar de ander en verwijder actieve verbinding. Meet de tijd van herstel, als deze aanwezig is. **VM/IP Mobility (IPv4/IPv6)** - Verplaats het ene eindsysteem naar het netwerk aan de overzijde. Meet hoe lang het duurt voordat de mapping-server op de hoogte is van de verandering. - Hetzelfde als bovenstaand, maar ook met een ping lopend om connectieherstel te meten. - Ping het verplaatste systeem vanaf een eindsysteem uit beide LISP omgevingen en de niet-LISP omgeving. - Start een FTP sessie voor het verplaatsen en controleer of de sessie wordt voortgezet na het verplaatsen. Meet de hersteltijd. **IPv6 Transitie** - De bovenstaande testen van multihoming en VM/IP mobility uitvoeren met het “internet” als volledig IPv4 en IPv6 om de overbrugging van een ander netwerk te testen. Dit is echter minder belangrijk, omdat het in de vorige opstelling vrij veel aan bod komt.

VI. ADVIESRAPPORT + TESTRESULTATEN

SAMENVATTING

Het Locator/ID Separation Protocol (LISP) is een protocol met veel potentie. Het hoofddoel om het aantal routes in de routers van het DFZ terug te dringen wordt versterkt met technieken als multihoming, IPv6 transitie, VM/IP mobility en network virtualization. In een drietal opstellingen is de werking van LISP geanalyseerd met de focus op de eerste drie technieken. Uit de resultaten is gebleken dat, wanneer er aan de voorwaarden wordt voldaan, het mogelijk is om een veelzijdige LISP omgeving te bouwen. Deze omgeving is multihomed, bereikbaar over IPv4 en IPv6 en heeft ook de mogelijkheid om eindsystemen tussen netwerken te verplaatsen. Tevens is dat allemaal realiseerbaar met ongeveer twintig regels configuratie. Daarbij komt ook nog het punt dat doordat LISP een encapsulation techniek is die het originele IP-pakket in takt laat, het mogelijk is om internetlijnen te laten falen, zonder dat een sessie verloren gaat. De eindpunten merken niet dat een andere verbinding is gekozen om het eindpunt te bereiken, omdat de het IP-adres in de header slechts veranderd tijdens het toepassen van encapsulation.

Het is echter niet alleen maar rooskleurig. Er zijn een aantal vereisten en uitzonderingen die bij de adoptie van LISP komen kijken die het een stuk minder aantrekkelijk maken. Het grootste probleem is het feit dat de EID-prefix die gebruikt wordt door het interne netwerk globaal uniek moet zijn. Tenzij een onderneming al in een vroeg stadium een PI-reeks heeft bemachtigd is de enige optie het kopen van PA-adressen bij een LIR. Dit zal ook steeds duurder en moeilijker worden aangezien de laatste /8 is aangebroken. Daarnaast komen er nog enkele problemen kijken zoals het conflict tussen inspectie en encapsulation en het feit dat er geen officiële ondersteuning is voor het protocol.

Deze problemen hoeven niet het einde van LISP te betekenen. LISP is een protocol in ontwikkeling, wat betekent dat het nog niet perfect hoeft te zijn. Het protocol groeit elke week weer verder. Dat wordt bevestigd door het aantal LISP omgevingen dat inmiddels de honderd duizend is gepasseerd en het aantal LISP implementatie mogelijkheden dat steeds toeneemt.

Voor de adoptie van LISP is gekeken naar twee partijen; Enterprises en ISP's. Voor beide partijen is duidelijk geworden dat de kosten die komen kijken bij de adoptie van LISP afhankelijk zijn van vier factoren.

- Keuze van adoptietechniek
- Opensource software versus betaalde licenties
- Grootte van de onderneming
- In welke mate apparatuur kan worden hergebruikt

Veel meer kan er helaas niet over worden gezegd, omdat het sterk afhankelijk is van de onderneming en haar middelen in welke mate LISP kan worden geadopteerd.

Ondanks de potentie van LISP is het advies op het moment om LISP nog niet te adopteren. Althans niet in een productieomgeving. Ook al lijken technieken als multihoming zeer aantrekkelijk blijft het feit bestaan dat volledige adoptie van LISP nodig is. Er moet ten slotte een xTR worden geplaatst en verbonden worden met een mapping-system. Daar is op het moment nog te weinig draagvlak en ondersteuning voor wat de adoptie risicovol maakt. Het protocol is wel sterk in ontwikkeling, waardoor dit advies snel kan veranderen. Het advies is om nog even geduld te hebben en/of LISP te testen in een niet-productie omgeving.

VERKLARENDE WOORDENLIJST

Woord	Betekenis
Decapsulation	Data dat tijdens het encapsulationproces is bijgevoegd verwijderen.
DFZ	Default Free Zone. Vrij vertaald de “Kern” van het internet waar alle autonomous systems met elkaar verbinden.
EID	Endpoint ID. Een 32- of 128 bits IP-adres van een eindsysteem dat gebruikt wordt voor de afzender- of bestemmingsadres in de LISP-header.
EID-Prefix	Een blok EID’s dat door een autoreiteit wordt uitgegeven. Deze blok van EID’s wordt aan een RLOC gekoppeld in het mapping-system database.
Encapsulation	Het “inpakken” van verkeer en tijdens het proces het pakket voorzien van nieuwe data, zoals het bijvoegen van een LISP header.
ETR	Egress tunnel router. Een router die op de grens tussen EID en RLOC omgevingen werkt en zorgt dat encapsulated verkeer van de ITR wordt decapsulated en doorgestuurd naar de gezochte EID.
ISP	Internet Service Provider. Een partij die connectie met het internet levert aan derde partijen.
ITR	Ingress tunnel router. Een router die op de grens tussen EID en RLOC omgevingen werkt en zorgt voor de encapsulation van LISP-verkeer.
Mapping System	Overkoepelende term voor de map-server, map-resolver en de mapping-system-database.
Mapping-system database	Omschrijf een database techniek die gebruikt wordt voor het opzoeken van de koppeling tussen EID en RLOC.
MR	Map-resolver. Component dat map-request berichten ontvangt van een ITR en deze verwerkt door bijvoorbeeld door te sturen naar een DDT-Root of Map-server
MS	Map-server. Component waar een ETR zijn registraties doet. Hier worden de koppelingen tussen EID en RLOC opgeslagen
PITR	Proxy ITR. Zorgt voor een koppeling tussen wel- en niet LISP omgevingen door bekende LISP routes te distribueren in het traditionele internetmodel via BGP.
PETR	Proxy ETR. Een ETR dat verkeer kan decapsulaten dat niet voor een LISP omgevingen bestemt is. Dit kan nodig zijn bij het overbruggen van een netwerk met een ander type IP protocol.
RLOC	Routing locator. Een IPv4 of IPv6 adres van een xTR aan de zijde dat in verbinding staat met het DFZ. Tevens het resultaat van zoekopdracht in de database.
(P)xTR	Router dat de functionaliteit kan hebben van een ITR, ETR, PITR of PETR

INHOUDSOPGAVE

1. INLEIDING

Het internetmodel dat op het moment wordt gebruikt is in het verleden ontwikkeld op het concept dat een uniek IP-adres bepaald wie jij bent en waar je bent als eindsysteem. Dit concept heeft over de jaren voor de nodige problemen gezorgd in de routetabellen van de default free zone (DFZ), omdat een conflict tussen locatie en identiteit het aggregeren van routes tegenwerkt. In 2006 is op een conferentie dit probleem nog eens aangehaald en is er werk van gemaakt om een oplossing voor het probleem te vinden. Het Locator/ID Separation Protocol (LISP) is daar het product van. Door middel van LISP is het mogelijk om in een database een koppeling op te slaan tussen twee adressen, waarbij het ene adres de locatie aangeeft van het eindsysteem en het andere adres de identiteit bepaald.

De werking van dit protocol en de plaatsing in het internetmodel ten opzichte van andere protocollen is reeds beschreven in het onderzoeksrapport. Op basis van die informatie zijn drie opstellingen gebouwd en getoetst. De resultaten van die testen worden in dit rapport toegelicht. Allereerst worden de verschillende netwerkcomponenten en hun configuratie geanalyseerd. Dit gebeurt in het volgende hoofdstuk ook voor de technieken multihoming, IPv6 transitie en VM/IP mobility met daarop volgend een toelichting van een aantal technieken die wel bestaan maar niet getoetst zijn. In hoofdstuk vijf wordt de adoptie van LISP besproken voor de internet service providers (ISP's) en Enterprises. Hierin komen de voor- en nadelen en kosten aan bod. In hoofdstuk zes wordt de toekomst van LISP besproken. Als laatste wordt er een algemene conclusie over LISP gegeven met daarop volgend het advies voor klantensituaties.

2. ANALYSE NETWERKCOMPONENTEN

Tijdens het bouwen van de drie opstellingen uit het ontwerprapport zijn alle mogelijke componenten gebruikt die in een netwerk dat LISP gebruikt kunnen voorkomen. In dit hoofdstuk zal een korte analyse plaatsvinden over de moeilijkheidsgraad van het opzetten van de verschillende componenten en de hard- en software dat er voor nodig is.

2.1 CONFIGURATIE

Allereerst zal er per netwerkcomponent een toelichting gegeven worden op de configuratie die nodig is voor het opzetten. In de paragraaf 2.2 komt de hard- en software aan bod.

2.1.1 ITR

De ingress tunnel router (ITR) is verantwoordelijk voor initiëren van het zoekproces dat nodig is om een RLOC-adres op te sporen en het toepassen van encapsulation waar nodig. De configuratie van een ITR is eenvoudig en bestaat uit slechts drie regels.

```
!
   ipv4 itr
   ipv4 itr map-resolver 12.12.12.2
   ipv4 use-petr 14.14.14.2
!
```

De eerste regel activeert de ITR functionaliteit op een router. De tweede regel geeft de map-resolver (MR) aan waar de verzoeken om een EID-to-RLOC-koppeling naartoe gestuurd worden. De laatste regel is optioneel en geeft aan welke proxy egress tunnel router (PETR) gebruikt mag worden wanneer verkeer gestuurd wordt naar een omgeving dat geen LISP ondersteund.

Zoals te zien is in de configuratie hierboven gaat het in dit geval om netwerken die voorzien zijn van IPv4. Als het interne netwerk over IPv6 zou beschikken zijn de commando's hetzelfde, op het begin na dat logischerwijs ipv6 zou zijn in plaats van ipv4.

2.1.2 ETR

De egress tunnel router (ETR) is verantwoordelijk voor het registeren van de EID-omgeving achter zijn RLOC-adres bij een map-server (MS) en het toepassen van decapsulation wanneer het verkeer ontvangt van een ITR.

De eerste stap is het aangeven van een locator-set. Hierin wordt aangegeven welke RLOC-adres in een later stadium gekoppeld moet worden aan de EID-omgeving in het netwerk van ETR. Hierin wordt tevens aangegeven wat de 'priority' en 'weight' van een lijn zijn. Hiermee kan verdeling van verkeer over lijnen worden gerealiseerd wanneer meerdere RLOC-adressen worden aangegeven.

```
!
router lisp
   locator-set SITE-B
   13.13.13.2 priority 1 weight 100
!
```

De tweede stap is het aangegeven van het subnet dat achter de eerdere opgegeven locator-set bevindt. Deze informatie wordt later doorgespeeld aan een MS die hier een koppeling voor aanmaakt.

```
!
 eid-table default instance-id 0
      database-mapping 192.168.1.0/24 locator-set SITE-A
!
```

De laatste stap is het aangeven van de MS en gedeelde sleutel die gebruikt wordt om de database te beschermen tegen ongeautoriseerde registreerberichten. Tevens moet de ETR functionaliteit worden geactiveerd met het laatste commando.

```
!
   ipv4 etr map-server 12.12.12.2 key SITEAKEY
   ipv4 etr
!
```

2.1.3 MAPPING-SYSTEM (MR/MS)

De verantwoordelijkheid van het mapping-system is om verzoeken die afkomstig zijn van een ITR te wijzen in de richting van de juiste ETR. Dit kan op twee manieren worden gerealiseerd. In opstelling één (zie bijlage hoofdstuk één) wordt gebruik gemaakt van een publiek mapping-system dat op basis van het DDT-netwerk de zoekopdrachten verwerkt. In de standalone omgeving van opstelling twee en drie (bijlage hoofdstuk twee en drie) worden de MR en MS functionaliteiten op één component geregeld en is het DDT-netwerk niet nodig.

MR

De configuratie van een MR is slechts één regel, omdat de functionaliteit in opstelling twee en drie zich op één component bevindt met de MS. Wanneer dit niet het geval zou zijn, zou een extra regel configuratie opgenomen moeten worden een DDT-ROOT aan te geven waar de verzoeken naar doorgestuurd worden.

```
!
router lisp
   ipv4 map-resolver
!
```

MS

Voor de MS dient soortgelijke informatie opgegeven te worden als de ETR. Per bekende LISP omgeving dient een gedeelde sleutel opgegeven te worden en een EID-prefix die daarbij hoort. Dit alles om te garanderen dat derde partijen niet zomaar informatie in de database kunnen injecteren. Ook hier is het laatste commando nodig om de functionaliteit van de MS te activeren. De configuratie laat ook zien dat een RLOC-adres opgeven niet nodig is. Dit gebeurt op een ETR die zichzelf registreert bij een MS. Hierdoor blijft het netwerk dynamisch.

```
!
router lisp
 site SITE-A
  authentication-key SITEAKEY
  eid-prefix 192.168.1.0/24
  exit
 !
 site SITE-B
  authentication-key SITEBKEY
  eid-prefix 192.168.2.0/24
  exit
 !
 ipv4 map-server
 exit
!
```

2.1.4 PxTR

De proxy tunnel router (PxTR) in opstelling twee en drie is verantwoordelijk voor de koppeling tussen eindsystemen die in niet- en wel-LISP omgevingen bevinden. De enige verantwoordelijkheid van een PETR is het verwijderen van de encapsulation, voordat verkeer het traditionele internet opgaat. Daar is slecht één regel code voor nodig, namelijk het activeren van PETR functionaliteit.

```
!
   ipv4 proxy-etr
!
```

De PITR heeft meer verantwoordelijkheid. De PITR moet bekende LISP EID-prefixes distribueren naar routeringstabellen van routers op het traditionele internet. In het bèta-netwerk gebeurt dit door middel van BGP, maar dat is in de standalone omgeving die hier gebouwd is niet nodig.

```
!
router lisp
   ipv4 proxy-itr 14.14.14.2
   map-cache 192.168.1.0/24 map-request
   map-cache 192.168.2.0/24 map-request
   ipv4 itr map-resolver 12.12.12.2
 exit
!
```

Allereerst wordt de PITR functionaliteit geactiveerd. Vervolgens wordt aangegeven welke EID-prefixes statisch in de cache opgenomen moeten worden. Normaliter zouden deze statische gegevens wordt gedistribueerd via BGP. Tevens wordt een map-resolver opgenomen, zodat wanneer een niet-LISP eindsysteem verkeer verstuurt naar de PITR er toch een zoekopdracht uitgevoerd kan worden om het LISP-eindsysteem te bereiken.

2.2 HARD- EN SOFTWARE

In het onderzoeksrapport is een overzicht gegeven van de hard- en software dat LISP ondersteund. In dit geval ligt de focus op Cisco en niet op de opensource variant.. Voor de basisfunctionaliteit van LISP kan je voor de software terecht bij alle besturingssystemen van Cisco mits de juiste licenties aanwezig zijn. Voor een volledig overzicht van de nodige licenties wordt verwezen naar lisp.cisco.com (Cisco Systems, LISP Hardware and Software Support, 2014).

Over de hardware kan weinig worden gezegd. LISP wordt ondersteund door ontzettend veel series van Cisco routers. Ook op de goedkopere modellen zoals de 1800 series die slechts over een halve gigabyte aan RAM-geheugen beschikken. Als er gekeken wordt naar de invloed van LISP op de hardware die gebruikt is in de drie opstelling van dit lab is er niets te zien. De CPU-load van de hardware komt niet hoger dan 1% en ook het geheugengebruik is miniem. Dit is wel een vertekend beeld aangezien er slechts drie netwerken zijn met ieder één eindsysteem die verkeer versturen.

Een ander punt, wat later in het verslag aan bod komt, is de druk op het netwerk die ontstaat door de periodieke berichten die gestuurd moeten worden zoals het registeren en bevestigen van EID-prefixes. In een gesprek met Cisco is hierover duidelijk geworden dat de impact van deze berichten miniem is. De berichten zijn efficiënt geprogrammeerd om meerdere handelingen tegelijk uit te voeren. Hierdoor blijft de impact beperkt.

3. ANALYSE LISP TECHNIEKEN

In dit hoofdstuk worden de getoetste technieken multihoming, IPv6 transitie en VM/IP mobility toegelicht. Dit omvat een toelichting van de configuratie om de werking te verduidelijken en een analyse van de manier waarop de technieken zich hebben geuit ten op zichtte van de theorie.

3.1 MULTIHOMING

Bij de configuratie van een ETR is uitgelegd dat een locator-set aangegeven moet worden waarin de RLOC-adressen van de ETR aanwezig zijn. Op basis van deze configuratie wordt multihoming geïmplementeerd. Op xTR1 van opstelling twee en drie is multihoming toegepast met de volgende configuratie.

```
!
router lisp
 locator-set SITE-A
  10.10.10.2 priority 1 weight 100
  11.11.11.2 priority 1 weight 0
  exit
 !
```

De twee RLOC-adressen 10.10.10.2 en 11.11.11.2 worden opgenomen in de locator-set SITE-A en kunnen voorzien worden van 'priority' en 'weight' om het verkeer te verdelen. Meer configuratie dan dit is niet nodig. Wanneer een ITR een EID-to-RLOC koppeling opvraagt en het bericht bij de verantwoordelijke ETR aankomt zal deze zelf aangeven op welke manier het verkeer ontvangen moet worden. Deze informatie wordt met de map-reply teruggestuurd naar de ITR.

Om de multihomed verbinding te testen is er een constante ping en ftp-sessie opgezet tussen twee eindsystemen, waarbij het ene eindsysteem zich achter een multihomed verbinding bevindt. Tevens zijn er traceroutes uitgevoerd waarbij beide lijnen eenmaal als primaire lijn geconfigureerd waren om de bereikbaarheid van de lijnen te testen. Voor de topologie die hiervoor gebruikt is wordt verwezen naar hoofdstuk 2.1 en 3.1 van de bijlagen van dit document. In de onderstaande afbeelding (3.1) is te zien wat de output is van het commando "lig 192.168.1.2". Hiermee kan handmatig een map-request procedure worden gestart om een eindsysteem op te zoeken. Hieruit wordt duidelijk dat het netwerk 192.168.1.0/24 zich inderdaad achter twee lijnen bevindt.

```
pxtr#lig 192.168.1.2
Mapping information for EID 192.168.1.2 from 11.11.11.2 with RTT 4 msecs
192.168.1.0/24, uptime: 01:11:34, expires: 23:59:59, via map-reply, complete
  Locator     Uptime    State      Pri/Wgt
  10.10.10.2  01:11:34  up           1/50
  11.11.11.2  01:11:34  up           1/50
```

Figuur 3.1 – Multihoming informatie

Uit de resultaten van hoofdstuk 2.3 en 3.3 van de bijlage is duidelijk geworden dat met de eenvoudige configuratie die eerder aangegeven is, het interne netwerk via beide lijnen bereikbaar is. De extra firewall in opstelling drie heeft hier geen invloed op. Dit was ook de verwachte uitkomst van de test, aangezien bij verkeer dat een xTR passeert op weg naar het interne netwerk de encapsulation wordt verwijderd. Het is dan alleen nog maar standaard IP-verkeer.

Het meten van hersteltijden is onder twee situaties gemeten. De ene keer met RLOC-probing aan en de andere keer uit. RLOC-probing is een techniek op een ITR om voorafgaand aan het sturen van verkeer de RLOC-adressen die aanwezig zijn in de map-cache te controleren met een zogeheten 'probe'.

In de meetresultaten van bijlage hoofdstuk 2.3 en 3.3 is de te zien dat de hersteltijden van de verbinding gemiddeld vier seconden zijn. De vier seconden die nodig zijn om te herstellen omvat het detecteren van een gebroken lijn, het uitvoeren van een map-register-cyclus en het updaten van de routeringstabel/map-cache. Vooral de ftp-sessie is goed hersteld, want de downloadsessie die aan de gang was werd niet afgebroken en opnieuw gestart, maar simpelweg hervat zo gauw de nieuwe mapping-informatie aanwezig was. Dit is de danken aan het feit dat het IP-verkeer eigenlijk hetzelfde blijft. Alleen de header met het RLOC-adres dat wordt bijgevoegd veranderd en daar merkt het eindsysteem niets van.

Hoe hoog de hersteltijd normaliter zou moeten zijn is niet bekend. Dit komt waarschijnlijk doordat het afhankelijk is van de prestaties van het gebruikte apparatuur en de afstand tussen locaties.

Bevindingen:
Tijdens het testen zijn er een tweetal bevindingen gedaan die niet verwacht waren of tijdens het literatuuronderzoek naar voren zijn gekomen.

- Wanneer de actieve link is verwijderd en de verbinding is herstelt wordt de verandering bijna direct opgenomen in het mapping-system door een map-register bericht van de verantwoordelijke xTR. Wanneer de link wordt teruggeplaatst wordt dit niet direct opgemerkt. De terugplaatsing wordt pas weer in de nieuwe ronde opgenomen in de database wanneer de zestig seconden timer van de mapping-system is verlopen. Dit zou in theorie kunnen betekenen dat wanneer de ene lijn faalt en terugkomt en toevallig de tweede lijn ook faalt je maximaal zestig seconden zonder verbinding zit, ondanks dat je een live verbinding hebt.
- RLOC-probing is een techniek dat een verzender xTR gebruikt om externe xTR's die zich in zijn map-cache bevinden preventief te controleren op beschikbaarheid, voordat verkeer wordt verstuurd. Normaliter zou dit het proces van een kapotte verbinding detecteren sneller moeten herstellen, maar omdat het zonder RLOC-probing al bijzonder snel gebeurt is dat hier niet het geval. Dat is hier wellicht te verklaren met het feit dat het om een klein netwerk gaat. Updaten van het mapping-system gebeurt hier al binnen een seconde. Dat zou onder de omstandigheden van het DFZ wel eens langer kunnen duren, waardoor RLOC-probing wel sneller is.

De focus van de testen met betrekking tot multihoming lagen op de beschikbaarheid en connectieherstel, omdat klantnetwerken meestal gebruik maken van een "high avaliability" modus. Dat wil zeggen dat de tweede lijn pas actief wordt wanneer de eerste lijn faalt. Multihoming met LISP laat ook verdeling en prioriteit van lijnen toe. Deze techniek is zelf niet getoetst, maar een bachelor thesis uit 2013 van de universiteit van Darmstadt omschrijft het gedrag van deze techniek wel (Herrmann, 2013). In deze thesis wordt bewezen dat de verdeling van verkeer op basis van LISP multihoming nagenoeg het optimum van bijvoorbeeld 50/50 bereikt wanneer dit is geconfigureerd. Na een serie testen is gebleken dat een maximale afwijking van 5% voorkomt op de percentage verdeling die ingesteld is.

3.2 IPv6 TRANSITIE

IPv6 transitie is een onderwerp dat met de opkomst van IPv6 steeds belangrijker wordt. Het DFZ is op het moment nog grotendeels IPv4, maar er komt in de toekomst een moment waarbij dit volledig IPv6 wordt. Hierop moeten bedrijven zich gaan voorbereiden, omdat hun interne IPv4-netwerk straks niet meer kan communiceren met het DFZ. De oplossing hiervoor is een transitietechniek. Hiermee kan gewerkt worden met het bestaande IPv4 en het toekomstige IPv6 DFZ.

IPv6 transitie is niet zozeer een techniek in LISP waar je bewust voor kiest, zoals multihoming. Het is meer een proces dat LISP altijd uitvoert en je kan het als voordeel gebruiken. LISP maakt gebruikt van encapsulation. Wanneer IP-verkeer een LISP-router (ITR) passeert wordt er een header toegevoegd met het RLOC-adres van de eindbestemming. Dit RLOC-adres kan zowel IPv4 als IPv6 zijn. Er wordt slechts een andere header toegevoegd bij het encapsulation proces. Omdat het een proces is dat altijd wordt uitgevoerd is er eigenlijk ook geen specifieke configuratie voor. Wat wel kan worden toegelicht is het volgende:

```
!
      ipv4 itr
      ipv4 etr
      ipv4 itr map-resolver 195.50.116.18
      ipv4 etr map-server 195.50.116.18 key smit-hague-xtr
      ipv4 use-petr 217.8.98.33 priority 1 weight 100

      ipv6 itr
      ipv6 etr
      ipv6 itr map-resolver 195.50.116.18
      ipv6 etr map-server 195.50.116.18 key smit-hague-xtr
      ipv6 use-petr 217.8.98.33 priority 1 weight 100
!
```

Bij het configureren van LISP op een router kan gekozen worden voor IPv4 en IPv6 commando's. Deze hebben betrekking op het interne netwerk achter de xTR. In opstelling één waarbij een dualstack omgeving is gebruikt worden zoals hierboven aangegeven beide commando's gebruikt. De IP-adressen die in de commando's hierboven worden gebruikt kunnen voor zowel de IPv4- als IPv6-commando's worden voorzien van IPv4- en IPv6 adressen. Het maakt voor LISP niet uit. Op basis van de IP-adres type die aangegeven is, zal de xTR de juiste encapsulation toepassen. Om te bewijzen dat het inderdaad zo werkt is de opstelling gebouwd die in paragraaf 1.1 van de bijlage aanwezig is. Hier is te zien dat een internet (lab-)netwerk van Qi ict is verbonden met een LISP-ISP. In dit geval het bèta-netwerk van LISP.

Om de bereikbaarheid van een netwerk te testen na het adopteren van LISP zijn verschillende ping-testen uitgevoerd van en naar IPv4- en IPv6-locaties. Tevens is er ook een IPv6-ready test uitgevoerd.

De resultaten (bijlage 1.3) bewijzen dat na de adoptie van LISP de bereikbaarheid van een netwerk niet afneemt. Alle combinaties van IPv4 en IPv6 naar zowel wel- als niet-LISP omgevingen zijn bereikbaar via het bèta-netwerk van LISP. Tevens is de hoogste score behaald op een IPv6-ready test, wat betekent dat door middel van LISP en een aantal commando's een netwerk volledige klaargemaakt kan worden voor de toekomstige omschakeling naar IPv6. Er is slechts één xTR nodig. Dezelfde techniek is ooit door Facebook gebruikt om binnen vier uur tijd het volledige netwerk IPv6-ready te maken voordat zij volledige dualstack gingen.

Bevindingen:

- Initieel waren de bovenstaande resultaten zo overtuigend dat de bereikbaarheid van het internet niet geschaad werd na de adoptie van LISP. Om die reden werd er gekozen om de IPv6 transitie testen in opstelling twee en drie niet uit te voeren. Omdat er aan het eind van de testfase wat tijd over was is er toch een test gedaan waarbij een intern IPv4 netwerk een IPv6 netwerk moest overbruggen. Hoewel de LISP-processen van de control plane goed gingen werd het verkeer waarop LISP-encapsulation is toegepast, data plane, geblokkeerd door een Check Point firewall die als centraal routeringspunt fungeerd. Dit kwam door een zogeheten 'zero checksum' in de header. Dit probleem heeft verder niet specifiek met LISP te maken. Alle tunnelprotocollen plaatsen een zero checksum in een header tijdens het encapsulationproces. Volgens RFC6936 (G. Fairhurst, 2013) is dit toegestaan en had dit niet geblokkeerd mogen worden. Dit gedrag is gemeld aan Check Point.
- Door het toevoegen van encapsulation worden een aantal bytes toegevoegd aan het verkeer dat afkomstig is van een LISP router. Er werd verwacht dat dit enige problemen zou opleveren met betrekking tot MTU. Tijdens het testen is er geen enkel spoor opgetreden van MTU problemen. Na wat onderzoek is hiervoor een goede reden gevonden. De extra bytes die door encapsulation worden toegevoegd zijn alleen maar aanwezig binnen het LISP-netwerk. Zo gauw het netwerk wordt verlaten wordt de encapsulation verwijderd. Alle routers met LISP functionaliteit hebben standaard path-mtu-discovery aan staan, waardoor MTU problemen niet voorkomen. Tenzij partijen handmatig deze functionaliteit uitzetten.

3.3 VM/IP MOBILITY

VM/IP Mobility is een techniek die de ware kracht van LISP laat zien. Hiermee kan bewezen worden dat identiteit en locatie van een eindsysteem wel degelijk gescheiden kunnen worden. Het idee achter deze techniek is dat een eindsysteem vanuit het ene EID-omgeving verplaatst kan worden naar een andere EID-omgeving met een andere prefix. Het IP-adres van het eindsysteem wordt niet aangepast en toch blijft connectie met het internet mogelijk.

De manier om VM/IP mobility te implementeren berust op configuratie van twee omgevingen. Het is niet zo dat een willekeurig eindsysteem verplaatst kan worden en gelijk opgepakt wordt. De twee omgevingen waarin de verplaatsing plaatsvindt moeten wel over de mogelijk verplaatsing op de hoogte zijn. Dat wordt op de volgende wijze gedaan:

SITE-A

```
!
interface GigabitEthernet0/1
 mac-address 0000.0d0e.010c
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 lisp mobility MOBILE-SITE
!
!
 eid-table default instance-id 0
 dynamic-eid MOBILE-SITE
 database-mapping 192.168.1.0/24 locator-set SITE-A
!
```

SITE-B

```
!
interface GigabitEthernet0/1
 mac-address 0000.0d0e.010c
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
 lisp mobility MOBILE-SITE
!
!
 eid-table default instance-id 0
 database-mapping 192.168.2.0/24 locator-set SITE-B
 dynamic-eid MOBILE-SITE
 database-mapping 192.168.1.0/24 locator-set SITE-B
 map-server 12.12.12.2 key SITEAKEY
!
```

In de bovenstaande configuratie is het de bedoeling om de EID-omgeving die zich achter SITE-A bevindt (192.168.1.0/24) mobiel te maken en in staat te laten zijn om verplaatst te worden naar SITE-B en automatisch opgepakt te worden. Zoals eerder vermeld moeten beide sites wel verwachten dat er een verplaatsing voor kan komen. Dit wordt gedaan door één interface beschikbaar te maken voor mobiliteit. Dit gebeurt met het 'lisp mobility' commando. Tevens moet worden aangegeven dat de omgeving 192.168.1.0/24 een 'dynamic-eid' is, dat zowel achter SITE-A als SITE-B mag werken. De laatste eis is dat het MAC-adres van beide mobility-interfaces voor beide sites hetzelfde is. Dit is nodig om connectie te behouden voor een verplaatste eindsysteem in een ander subnet.

In de tweede opstelling is VM mobility getest waarbij de xTR de first-hop router van het interne netwerk is. Er werd via ftp een download gestart van de ftp-server 192.168.1.3 naar het eindsysteem 192.168.3.2. Terwijl de download actief was werd de ftp-server verplaatst van 192.168.1.0/24 naar 192.168.2.0/24. Binnen zes á zeven seconden werd de download hervat. Dit is mogelijk doordat er een specifieke /32 route wordt opgenomen in het mapping-sysem voor het verplaatste eindsysteem (zie figuur 3.2). Verder wordt er ook door de xTR die voor de verplaatsing verantwoordelijk was voor de ftp-server een speciaal bericht gestuurd naar naar xTR's die aanwezig zijn in zijn map-cache om iedereen op de hoogte te stellen van de verplaatsing.

```
mapping-system#show lisp site
LISP Site Registration Information
* = Some locators are down or unreachable

Site Name      Last      Up   Who Last          Inst     EID Prefix
               Register       Registered        ID
SITE-A         00:00:45  yes  11.11.11.2                 192.168.1.0/24
               00:00:27  yes  11.11.11.2                 192.168.1.3/32
SITE-B         00:00:38  yes  13.13.13.2                 192.168.2.0/24
mapping-system#show lisp site
LISP Site Registration Information
* = Some locators are down or unreachable

Site Name      Last      Up   Who Last          Inst     EID Prefix
               Register       Registered        ID
SITE-A         00:00:01  yes  11.11.11.2                 192.168.1.0/24
               00:00:00  yes  13.13.13.2                 192.168.1.3/32
SITE-B         00:00:53  yes  13.13.13.2                 192.168.2.0/24
```

Figuur 3.2 – Map-Server informatie

Uit de resultaten van de tweede opstelling is ook gebleken dat de connectiviteit van het verplaatste eindsysteem ook niet minder is geworden. Het is voor het eindsysteem nog steeds mogelijk om alle sites te bereiken. Dit is mogelijk doordat de interface die geconfigureerd is als mobility poort door middel van arp-spoofing kan antwoorden op de arp-berichten van het verplaatste systeem. Op deze manier denkt het verplaatste eindsysteem dat het nog steeds tegen zijn originele default gateway praat.

De resultaten van de derde opstelling zijn minder positief. Het is niet mogelijk gebleken om LISP mobility werkend te krijgen wanneer de xTR niet de first-hop router van het netwerk is. Dit was een verwachte uitkomst, aangezien de voorwaarde dat beide first-hop routers hetzelfde MAC-adres en mobility geconfigureerd moeten hebben niet aan voldaan wordt. Daarbij komt ook nog het feit kijken dat de verplaatste eindsystemen die achter NAT bevinden niet langer over een IP-adres beschikken dat bekend is in het mapping-system.

Dit betekent dat voor de partijen die VM/IP mobility willen implementeren er een keuze gemaakt moet worden. Implementatie is mogelijk, maar dan wordt eventuele inspectie van verkeer en NAT wel moeilijk. Een alternatief zou zijn om gebruikt te maken van een firewall als xTR die LISP-aware is, zoals een Cisco ASR1K ZBF of het gebruik maken van een techniek als Multihop ESM. Met deze techniek wordt door een extra LISP-router in te zetten het mogelijk gemaakt om een xTR als first-hop te hebben, vervolgens tijdelijk de encapsulation te verwijderen om te kunnen inspecteren, en daarna opnieuw encapsulation toe te passen om het door te sturen. Hier hanger echter ook een aantal eisen aan, zoals het hebben van twee omgevingen met dezelfde subnets en het gebruik van OTV.

Bevindingen:

- Hoewel de ftp-sessie wordt hersteld betekent dat niet dat in alle anders gevallen ook sessies worden hervat in plaats van afgebroken. Het hangt af van de timers die een programma heeft ingesteld die bepalen wanneer een sessie wordt afgebroken of niet.

3.4 ALGEMENE BEVINDINGEN

In de vorige paragrafen zijn al een aantal bevindingen benoemd waar tegenaan gelopen is tijdens het toetsen van de verschillende technieken. De nadruk lag hier op bevindingen die specifiek waren voor een bepaalde techniek. Hieronder worden nog een aantal bevindingen benoemd die algemeen zijn voor LISP.

Globale adressen
De adressen die gebruikt zijn in de verschillende labopstellingen zijn privé adressen volgens RFC1918. Het gebruik van deze adressen heeft wat misleidend gewerkt met betrekking tot de resultaten over bereikbaarheid. Volgens de resultaten is het mogelijk om alle netwerken te bereiken zonder het gebruik van NAT, of door het privé-netwerk met NAT te transleren in een voor LISP bekend netwerk. Deze resultaten kloppen voor verbindingen binnen het LISP bèta-netwerk, omdat tussen twee LISP routers de encapsulation zorgt voor een soortgelijk effect als NAT. De adressen die door encapsulation worden toegevoegd zijn globaal routeerbaar en worden gebruikt voor het overbruggen van het DFZ. Wanneer het eindstation wordt bereikt wordt de encapsulation verwijderd en blijft het standaard IP-pakket over, waarmee communicatie binnen het interne netwerk wordt volbracht. Bij verbindingen tussen non-LISP en LISP gaat dit anders. Verkeer tussen deze partijen wordt door middel van een PxTR volbracht en encapsulation is alleen aanwezig tussen de xTR en PxTR. Wanneer de PxTR is gepasseerd wordt de encapsulation verwijderd en blijft het standaard IP-pakket over. De adressen die in dit pakket overblijven moeten wel globaal routeerbaar zijn als het DFZ overbrugt moet worden. Dat is niet het geval in de labopstellingen die gebouwd zijn. Daar wordt gebruikt gemaakt van RFC1918 adressen die in het DFZ normaliter tegengehouden worden. De enige reden dat het hier heeft gewerkt is omdat er geen “DFZ” aanwezig is om het verkeer te stoppen. Hiermee moet rekening gehouden worden tijdens het bouwen van een opstelling. Het interne netwerk moet standaard voorzien zijn van globaal routeerbare EID-adressen, of het interne netwerk moet net als in opstelling drie worden ge-NAT naar een EID-space dat globaal routeerbaar is. Dit gedrag is bevestigd in RFC6830 met de definitie van een EID (D. Farinacci, 2013).

De adressen die hiervoor gebruikt kunnen worden mogen zowel provider aggregatable (PA) of provider independent (PI) adressen zijn. De enige vereiste is dat de adressen globaal uniek zijn en dat is voor beide het geval. Een belangrijk punt over PI-adressen is dat deze niet langer worden uitgegeven door de RIPE. De adressen zijn allemaal uitgedeeld. Als je als onderneming niet over deze adressen beschikt zijn PA-adressen kopen van een LIR de enige mogelijkheid om LISP te implementeren. De nadelen van PA-adressen in tegenstelling tot PI-adressen zijn dat bij het wijzigen van ISP deze adressen niet meegenomen mogen worden en dat bij uitval van de ISP deze ook niet meer te bereiken zijn.

Firewall inspectie
Qi ict is een bedrijf dat voor een groot deel bekend staat om haar beveiligingsoplossingen. Het is daarom ook een logisch gegeven dat als LISP ooit geïmplementeerd wordt bij een klant er gegarandeerd ook firewall inspectie aan bod komt. Het probleem met LISP is dat zo gauw het encapsulationproces is uitgevoerd de firewall alleen nog maar UDP verkeer voorbij ziet komen. Inspectie is daarom niet meer mogelijk. Om toch inspectie voor elkaar te krijgen is het mogelijk om een firewall voor de xTR te plaatsen die het verkeer inspecteert voordat encapsulation wordt uitgevoerd, maar hier kleven nadelen aan, zoals het niet langer gebruik kunnen maken van VM/IP Mobility. Voor IPv6 transitie en multihoming heeft het verder geen invloed. Daar is inspectie mogelijk.

Map-register load
Voor het bijhouden van het mapping-system wordt elke zestig seconden een map-register bericht verzonden van een ETR naar de MS. De opstellingen die gebouwd zijn tijdens dit onderzoek bevatten slechts twee EID-omgevingen die gemeld worden aan het MS, waardoor het niet veel invloed heeft op het netwerk. Stel dat LISP op een groter platform wordt geïmplementeerd, zoals bij een ISP of Enterprise, kan dat betekenen dat er constante druk op het netwerk komt door het constant sturen van register-berichten. Elke ETR heeft wel zijn

eigen timer, waardoor het niet zo is dat elke zestig seconden een piek aan verkeer wordt verstuurd, maar het is wel degelijk iets waar rekening mee gehouden moet worden.

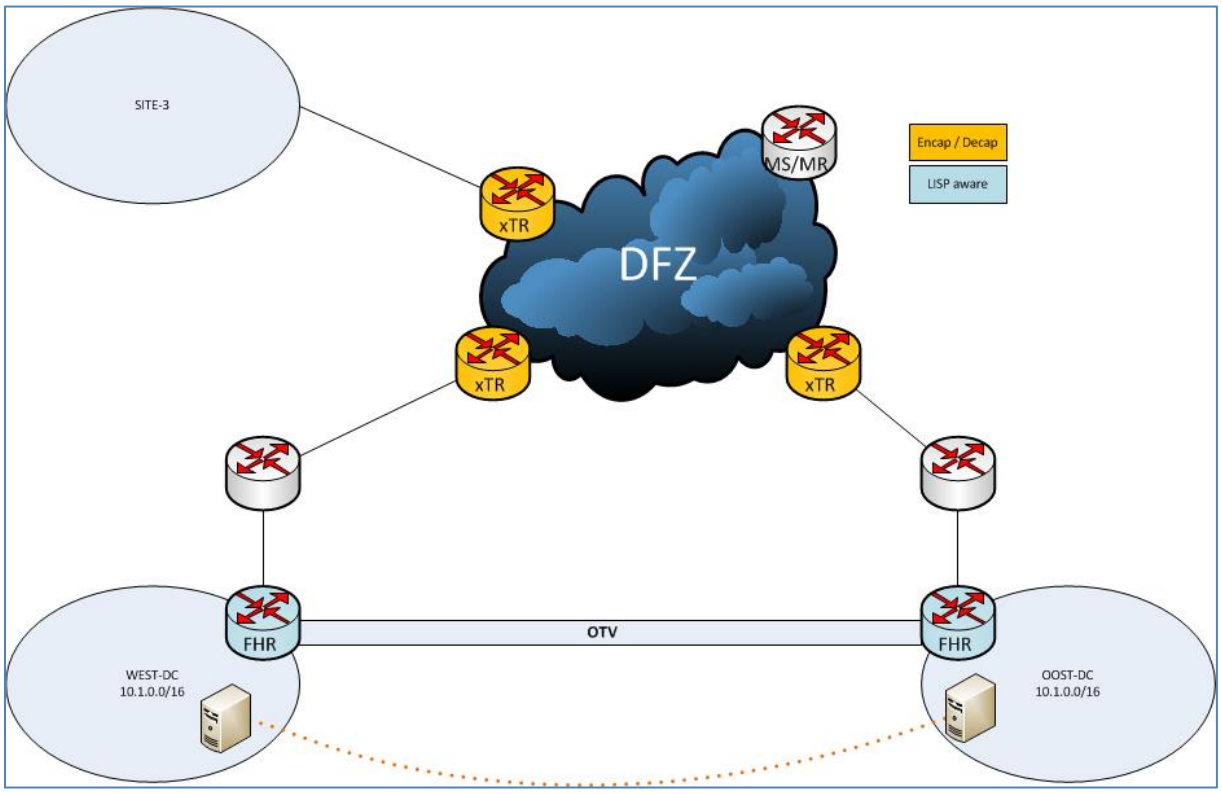
Naar aanleiding van dit vraagstuk is er informatie opgevraagd over de invloed van LISP-berichten op de prestaties van een netwerkcomponent. De engineers van Cisco geven aan dat dit niet noemenswaardig is. Map-register berichten zijn efficiënt geprogrammeerd om meerdere registraties tegelijk uit te voeren. Zelf als dit niet het geval was en elk bericht maar één registratie voltooide, zou dat voor honderd netwerken om honderd pakketten per zestig seconden gaan. De kleinste routers van Cisco die LISP ondersteunen, de ISRG1 800-series, kunnen al tussen de tien- en honderdduizend pakketten per seconden verwerken. Dit is ruim voldoende.

4. OVERIGE TECHNIEKEN

Tijdens het bouwen van de opstellingen hebben zich een aantal bevindingen voorgedaan die opgelost kunnen worden door nieuwe technieken die tijdens het literatuuronderzoek niet naar voren zijn gekomen. Een groot deel van deze technieken is nog in ontwikkeling en er is om die reden weinig informatie over te vinden. Toch zullen de verschillende technieken hieronder kort worden toegelicht.

4.1 MULTIHOP ESM

Uit de resultaten van opstelling drie is gebleken dat VM/IP mobility niet langer bruikbaar is wanneer er voor de xTR een firewall wordt geplaatst die inspectie doet. Dat VM/IP mobility niet werkt is niet te danken aan het feit dat er inspectie plaatsvindt, maar simpelweg omdat de xTR de verplaatsingen niet langer kan detecteren, omdat het niet de first-hop-router is. Door middel van een techniek genaamd “multihop” is het mogelijk om VM/IP mobility toch te realiseren in een omgeving waar netwerkcomponent wordt toegevoegd om bijvoorbeeld inspectie uit te voeren.



Figuur 4.1 – Multihop ESM – Bron: (Cisco Systems, LISP ESM Multihop Mobility, 2013)

De bovenstaande afbeelding geeft de topologie weer van een netwerk, waarbij een extra netwerkcomponent is toegevoegd voor de xTR. Dit kan ook een firewall zijn die inspectie doet. De techniek baseert zich op het gebruik van twee componenten die LISP ondersteunen en daartussen een component of netwerk dat gebruikt wordt voor andere toepassingen. Het proces is eenvoudig. De first-hop-router detecteert de verplaatsing van een eindsysteem, geeft dat door aan de xTR aan de grens van het netwerk en voor de rest werkt de techniek zoals het normaal ook doet. Er wordt een specifieke /32 route opgenomen in de mapping-database om verkeer te routeren in de goede richting en door middel van solicit-map-berichten worden alle partijen op de hoogte gebracht van de verplaatsing.

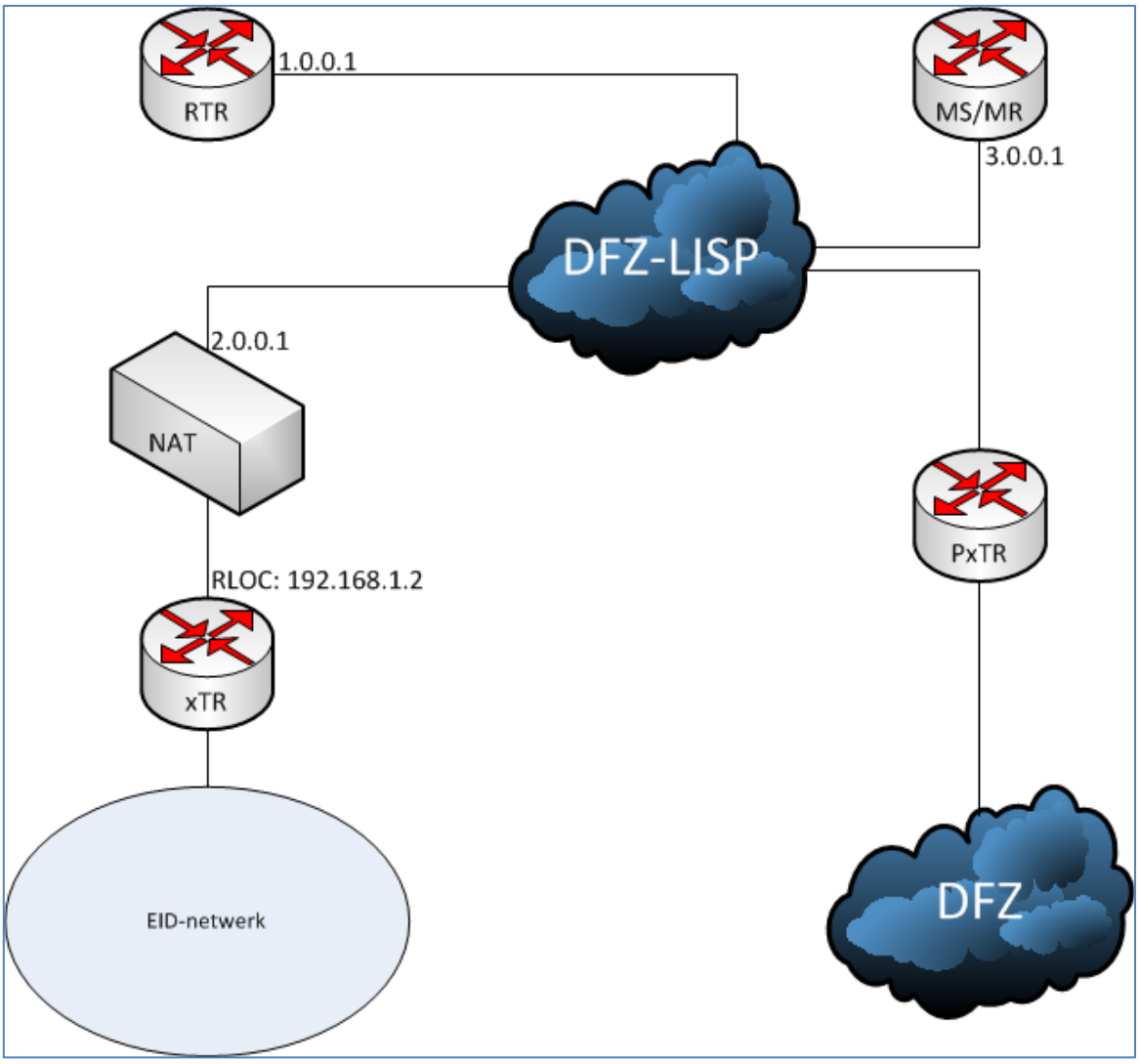
Er zitten wel een paar restricties aan het gebruik van deze techniek:

- Multihop ESM wordt alleen ondersteund in mobility-netwerken waarbij extended-subnet-mode actief is. Dat houdt in dat beide vestigingen over deze EID-prefix beschikken en daartussen OTV aanwezig is. OTV is een techniek om laag twee verkeer over laag drie te verplaatsen. Hierdoor heb je eigenlijk één groot netwerk dat zich op meerdere locaties bevindt.
- Het gebruikt van het OTV First Hop Redundancy Protocol is verplicht als twee first-hop-routers worden gebruikt om de verplaatsingen te detecteren.
- De techniek kan niet gebruikt worden in combinatie met NAT.

De techniek kan helaas niet worden getest, omdat er geen middelen zijn om een netwerk op basis van OTV te bouwen.

4.2 NAT Traversal

Als er een situatie voorkomt waarbij de xTR van een netwerk zich niet aan de grens van een netwerk bevindt, maar achter een apparaat dat NAT uitvoert, kan dat betekenen dat een xTR niet langer bereikbaar is over het internet. Er is tenslotte een goede kans dat de RLOC van de xTR een privé IP-adres is dat niet over het internet opgevraagd kan worden. Om toch een connectie te kunnen opstellen met de RLOC van de xTR achter NAT is er een techniek genaamd NAT traversal ontwikkeld.



Figuur 4.2 – Voorbeeld NAT Traversal

Om NAT traversal werkend te krijgen zijn ten opzichte van het standaard LISP-model drie extra componenten nodig. Eén component is de Re-encapsulating Tunnel Router (RTR) en de andere twee componenten zijn twee LISP-berichten, de info-request en info-reply, die nodig zijn voor het registreren.

Bij het opzetten van de xTR zal deze zich proberen te registeren bij een MS. Hiervoor wordt een info-request uitgezonden. Dit bericht met afzenderadres 192.168.1.2 wordt door het NAT-apparaat herschreven met afzender 2.0.0.1 en doorgestuurd naar de MS. De MS ontvangt het bericht en reageert met een info-reply. Dit bericht wordt teruggestuurd naar het NAT-apparaat met IP-adres 2.0.0.1 en wordt daarnaast ook voorzien van een lijst met mogelijke RTR IP-adressen. De xTR ontvangt dit bericht, bepaald aan de hand van de lokale en globale RLOC in het bericht dat het zich achter NAT bevindt en kiest om die reden een RTR uit de lijst de meegezonden is.

De xTR probeert zich opnieuw te registeren bij een MS, maar doet het nu op een andere wijze. Er wordt een map-register bericht verstuurd naar zijn gekozen RTR. De RTR slaat de koppeling tussen lokale en globale RLOC op, met daarbij de poorten die door het NAT-apparaat zijn gekozen voor de vertaling van adressen. Vervolgens wordt het map-register bericht doorgestuurd naar de MS die de EID-prefix van de omgeving registreert met daarbij het IP-adres van de RTR als RLOC. De MS verstuurd na de registratie een map-notify naar de RTR die vervolgens doorgestuurd wordt naar de ETR om de registratieprocedure te voltooien. Op deze manier is door middel van de RTR een soort “gat” in het NAT-apparaat gemaakt, waarmee de ETR beschikbaar wordt voor het publiek.

Gebruik van deze techniek is op het moment nog niet overal mogelijk. Het is vooralsnog alleen implementeerbaar in bepaalde testversies van IOS, IOS-XE en LISPMob. De informatie die de techniek beschrijft is op het moment ook nog een working-draft (Systems & D. Farinacci, 2014) van de IETF en nog geen officiële RFC.

4.3 Network Virtualization

Nog een techniek waarvoor LISP gebruikt kan worden is “network virtualization”. Deze techniek valt officieel buiten de grenzen van het onderzoek, maar zal kort worden toegelicht.

Bedrijven die meerdere vestigingen willen koppelen kiezen vaak voor een virtueel netwerk, omdat een volledige fysieke koppeling erg kostbaar is. Om een virtueel netwerk op te zetten wordt gebruik gemaakt van virtual routing and fowarding (VRF). Door middel van VRF kan een logische scheiding tussen verschillende netwerken worden opgezet, die anders last zouden hebben van overlappende IP-adressen en dergelijke. Op basis van de VRF technologie kan ook quality of service (Qos), beveiliging, management en routing wordt toegepast.

VRF wordt op het moment vaak gecombineerd met 802.1q VLAN-tags om virtuele netwerken op te zetten, maar dat kan vervangen worden met LISP. Door gebruik te maken van LISP instance ID’s en deze te koppelen aan een VRF kan een EID en/of RLOC worden gevirtualiseerd. Deze techniek kan gebruikt worden om VPN verbindingen op te zetten tussen meerdere LISP locaties.

5. PARTIJEN

Op basis van informatie uit het onderzoeksrapport, gesprekken met vakgenoten en de resultaten van de testen die uitgevoerd zijn op de demo-opstellingen worden in dit hoofdstuk besproken of LISP adoptie aantrekkelijk is voor ISP en Enterprises. Hierbij wordt gekeken naar de manieren van adoptie, de voor- en nadelen en een mogelijke schatting van de kosten die komen kijken bij de adoptie.

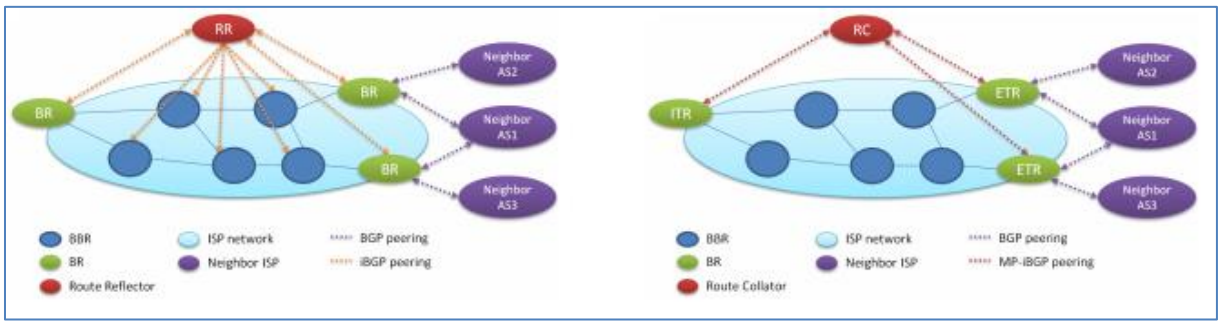
5.1 INTERNET SERVER PROVIDER

Voor een internet service provider (ISP) is het adopteren van LISP aantrekkelijk om twee redenen. De eerste reden is het verkleinen van de routeringstabellen in het DFZ en de tweede reden is het eenvoudiger leveren van technieken als multihoming. Het adopteren van LISP met deze twee redenen in gedachte wordt hieronder toegelicht.

5.1.1 ADOPTIE

De ingrijpbaarheid van LISP adoptie voor een ISP hangt af van de mate waarin het wordt geadopteerd in het netwerk. Er zijn namelijk verschillende vormen van adoptie. De drie mogelijke adoptietechnieken voor een ISP worden hieronder beschreven.

1. **Optie één, minimaal ingrijpend.** De eerste vorm is het minst ingrijpend. De ISP kan er voor kiezen om het interne netwerk van de onderneming niet te wijzigen en puur te fungeren als backbone van het internet dat routering verzorgt. De xTR's van de ondernemingen verzorgen de EID-to-RLOC opzoekopdrachten en andere instanties verzorgen de mapping-systems en proxy-services, waardoor de ISP alleen maar hoeft te zorgen voor routering van verkeer. Het is wellicht niet de meest sociale manier van ondernemen om anderen het werk te laten doen, maar wel aantrekkelijk voor ISP's die niet over de middelen beschikken om LISP volledig te adopteren.
2. **Optie twee, gemiddeld ingrijpend.** De tweede vorm van adoptie vereist ook geen ingrijpende wijzigingen. Slechts een aantal componenten moeten worden toegevoegd. Om niet afhankelijk te zijn van een publiek mapping-system en proxy-service kan een ISP er voor kiezen om mee te doen aan de globale adoptie van LISP door een eigen service op te zetten. Hierdoor voorziet de ISP ondernemingen niet langer alleen van routering, maar kan de ISP ook actief meewerken aan de connectiviteit. De ISP kan hierin ook een stap verder gaan door EID-prefixes, oftewel PA-adressen, te gaan uitdelen aan onderneming en deze via haar eigen proxy-service bekend te maken op het internet.
3. **Optie drie, zeer ingrijpend.** De laatste vorm van adoptie is zeer ingrijpend en vereist wat veranderingen aan het interne netwerk. Dit is tevens een speculatieve adoptie, omdat er alleen theoretische voorbeelden van zijn. In de whitepaper "Implementing a BGP-free ISP Core with LISP" (Florin Coras, 2012) wordt een manier omschreven om de kern van een ISP-netwerk niet langer van (i)BGP te voorzien, door de routers aan de grens van het ISP netwerk te vervangen met xTR's.



Figuur 5.1 – BGP-Free Core

Het idee is dat wanneer verkeer aankomt bij een ITR van een ISP, het verkeer van encapsulation wordt voorzien en doorgestuurd naar de ETR die in de mapping-system is gekoppeld aan het netwerk dat gezocht wordt.

Hierdoor hoeft er maar eenmalig bepaald te worden waar een pakket heen moet, in tegenstelling tot de hedendaagse techniek waarbij elke router opnieuw moet bepalen waar het verkeer naar toe moet. De hedendaagse techniek is omslachtig en overbodig, doordat elke router moet kunnen bepalen waar een pakket heen moet. Voor deze techniek bevat de router immens grootte routeringstabellen. Hierbij komt ook nog eens kijken dat een router vaak twee tabellen bevat. Eén voor intern en één voor extern verkeer.

5.1.2 VOOR- EN NADELEN

De adoptietechnieken uit de vorige paragraaf hebben ieder zijn eigen voor- en nadelen. Deze worden op de volgende bladzijde opgesomd in een tabel. Voorafgaand worden er nog een aantal algemene voor- en nadelen opgesomd die LISP heeft voor een ISP ongeacht de manier van adoptie.

Algemene voordelen:

- **Verkleining globale routeringtabellen.** Het zal nog even duren voordat dit voordeel zichtbaar wordt, maar LISP zorgt voor een verkleining van de routeringstabellen in het DFZ. Een kleinere tabel heeft als voordeel dat routers niet langer constant voorzien moeten worden van nieuwe hardware om het rap groeiende aantal routes te kunnen bijbenen en kunnen de routers minder hard gaan werken, waardoor de levens duur van apparatuur toeneemt.
- **Minder BGP kennis.** Het internetmodel wordt minder afhankelijk van BGP, doordat veel gebruikte services zoals multihoming nu zonder BGP kunnen worden aangeboden. Daarbij komt ook een kostenverlaging kijken, omdat dure BGP-apparatuur en personeel die verstand van BGP heeft niet meer veelvuldig nodig is.
- **IPv4/IPv6 ondersteuning.** LISP ondersteund standaard zowel IPv4 als IPv6. Dit kan als ISP gebruikt worden als voordeel in tijdens de transitieperiode naar IPv6 die op het moment bezig is.
- **Open source.** LISP wordt ontwikkeld als open standaard met implementaties van verschillende partijen en geschreven in verschillende programmeertalen. Hierdoor is het mogelijk om goedkoop gebruikt te maken van de techniek. Hierbij komt ook het feit dat het mogelijk is om ouder apparatuur te voorzien van LISP code, om zo ouder apparatuur nieuw leven in te blazen en kosten te besparen.

Algemene nadelen:

- **Protocol in ontwikkeling.** Ondanks dat er wereldwijd ruim 100.000 omgevingen zijn die LISP hebben geadopteerd blijft het een experimenteel protocol. Engineers die werken aan LISP noemen het protocol “productie kwaliteit”, maar het feit dat er nog technieken zich in de ontwikkelfase bevinden blijft bestaan. Tevens wordt het protocol gedragen door vrijwilligers, waardoor hulp niet gegarandeerd is, tenzij dat wordt afgesloten met een bepaalde partij.
- **Globale adoptie.** LISP is net als IPv6 een protocol dat globaal geadopteerd moet worden om volledig tot zijn recht te komen en daar is op het moment is er nog weinig draagvlak voor. Bijvoorbeeld in Nederland is er slechts één ISP bekend die LISP services levert.

Tabel 5.1 – Voor- en nadelen van adoptietechnieken ISP

Optie één	Optie twee	Optie drie
Voordelen: - Goedkope oplossing. Laat andere partijen het werk doen en profiteer van de voordelen. Wanneer een onderneming een xTR aanschaft kan bijvoorbeeld goedkoop multihoming worden gerealiseerd zonder BGP. Hier hoeft de ISP verder niets voor te doen. Slechts het leveren van één of meer internetlijnen.	**Voordelen:** - Tevens een goedkope oplossing. Een eigen mapping-system en proxy server kan opensource worden geregeld. Logischerwijs wordt het leveren van zo'n service duurder wanneer meer partijen er gebruik van gaan maken, maar het verdient zich later ook terug in de verkleining van routetabellen en minder BGP gebruik. - Niet langer afhankelijk van publieke servers. Het is nu mogelijk om eigen beheer uit te voeren.	**Voordelen:** - BGP is niet langer verplichte kost binnen een autonomous system. Dit scheelt kosten in de vorm van BGP apparatuur en personeel dat kennis moet hebben van BGP. - Niet alleen globale, maar ook interne routeringstabellen nemen af in grootte. - De encapsulation aan de ISP kant laat ook instance ID's toe die gebruikt kunnen worden voor bijvoorbeeld VPN's of QoS. Hierdoor kan MPLS wellicht vervangen worden. Dit scheelt ook weer in de kosten aangezien MPLS een ingewikkeld protocol is dat veel geld kost in de vorm van trainingen en MPLS-beschikbaar apparatuur. - Als er xTR's worden gebruikt aan de grenzen van een AS betekent dat ook dat multihoming gebruikt kan worden. Hiermee is loadbalancing en prioriteit eenvoudig toe te kennen aan verkeer. Daarnaast zijn er ook snelle fail-overs mogelijk zoals de resultaten hebben laten zien in het testplan.
Nadelen: - De voordelen van LISP worden groter naar mate meer partijen deelnemen. Als iedereen deze instelling heeft komt er nooit verandering.	**Nadelen:** - Uiteindelijk verruil je kennis van BGP voor kennis van LISP. Daarnaast komen er kosten kijken bij de management van LISP services.	**Nadelen:** - Het blijft een (risicovolle) investering die uiteindelijk voor niets kan zijn als LISP niet wordt overgenomen op globaal niveau.

5.1.3 KOSTEN VOOR DE ISP

De adoptie van een nieuwe techniek brengt veranderingen aan een (netwerk)omgeving en over het algemeen vereisen veranderingen een investering voordat het zich gaat terugverdienen. Dat geldt ook voor LISP. In deze paragraaf zal geprobeerd worden een grove schatting te geven van de investering die nodig is om LISP te adopteren in het netwerk van een ISP.

Wanneer een ISP de keuze maakt om alleen de voordelen van LISP te omarmen, maar verder niet te implementeren zoals in adoptietechniek één kost dit in theorie niets. Er worden geen wijzigingen gemaakt aan het netwerk en het enige voordeel dat behaald wordt is het dalen van routeringstabelgrootte dat in theorie gebruik van goedkoper apparatuur toelaat in de toekomst. De keerzijde is wel dat als teveel partijen deze instelling hebben er geen verandering plaatsvindt in het DFZ, waardoor het aantal routes blijft groeien en de kosten van apparatuur voor de ISP blijft stijgen.

Wanneer een ISP mee gaat werken aan de globale adoptie van LISP door een eigen mapping-system en proxy-service op te zetten is er direct een investering nodig. Er zijn minimaal twee systemen nodig. Eén PxTR en één gecombineerde MR/MS. Deze systemen kunnen geïmplementeerd worden op gratis Linux systemen met bijvoorbeeld de LISPMob implementatie, maar er kan ook gekozen worden voor een Cisco implementatie waar betaalde licenties voor nodig zijn. Daarbij komt ook nog eens de grootte van de ISP kijken, omdat een grotere ISP met meer locaties logischerwijs over betere componenten moet beschikken om meer (LISP-)verkeer te kunnen verwerken.

De laatste adoptietechniek brengt de meeste verandering met zich mee, maar hoeft niet perse een grote investering te zijn. In de whitepaper waarin deze techniek wordt toegelicht wordt ook toegelicht dat een groot deel van het apparatuur kan worden hergebruikt in het nieuwe netwerk. Code voor LISP komt ten slotte in veel verschillende vormen voor, dus er is een goede kans dat apparatuur een nieuw leven ingeblazen kan worden.

Zoals hierboven te lezen is komt de investering neer op de volgende punten:

- Keuze van adoptietechniek
- Opensource software versus betaalde licenties
- Grootte van de onderneming
- In welke mate apparatuur kan worden hergebruikt

Een schatting maken van de kosten die komen kijken bij de adoptie van LISP door een ISP is niet mogelijk. Er zijn teveel factoren die meespelen waarover geen informatie bekend is, dus elke ISP zal voor zichzelf een schatting moeten maken op basis van de bovenstaande factoren.

5.2 ENTERPRISES

De adoptie van LISP voor een Enterprises komt net als bij een ISP ook op verschillende manieren voor. Afhankelijk van de beschikbare middelen kan een Enterprise kiezen voor adoptie via een LISP-ISP of in zijn geheel een eigen LISP omgeving op zetten. In dit hoofdstuk worden de verschillende manieren van adoptie, de voor- en nadelen en een grove schatting van de kosten toegelicht.

5.2.1 ADOPTIE

De drie manieren van adoptie voor Enterprises worden hieronder opgesomd:

1. **Optie één, minimaal ingrijpend.** De eerste adoptietechniek die besproken wordt is een techniek waarbij de xTR aan de kant van een ISP wordt geplaatst en onder het beheer van de ISP valt. Deze adoptietechniek wordt door de IETF aangedragen als optie voor ondernemingen die geen wijzigingen willen doorvoeren aan hun eigen netwerk en om die reden alle verantwoordelijkheid bij de ISP leggen. De interne omgeving van een onderneming staat in direct contact met een xTR bij een LISP-ISP die op al het verkeer encapsulation zal toepassen.
2. **Optie twee, minimaal/gemiddeld ingrijpend.** De tweede adoptietechniek haalt de verantwoordelijkheid van beheer naar de Enterprise zelf door een xTR te plaatsen aan de grens van het netwerk, maar wel de mapping-system en proxy-services te gebruiken van de LISP-ISP. Dit is de meest gebruikelijke manier van LISP adoptie. Het plaatsen van een xTR aan de grens van het netwerk brengt in principe geen verandering aan het netwerk. Het enige waar rekening mee gehouden moet worden is dat de EID-prefix die gebruikt wordt voor het interne netwerk globaal routeerbaar moet zijn. Dit wordt door bepaalde LISP-ISP's geregeld door zelf EID-prefixes uit te delen in de vorm van PA-adressen, maar als een Enterprise zelf over een blok PI-adressen beschikt kunnen die ook gebruikt worden. Let wel, het interne netwerk hoeft niet perse omgenummerd te worden. Er kan ook gebruik worden gemaakt van NAT om het bestaande interne netwerk te transleren naar een IP-adres uit de gegeven EID-prefix. Dit is idee is ook geïntroduceerd bij thuisgebruikers van LISP. Door een /32 adres toe te kennen aan de xTR en een RFC1918 privé reeks te natten achter dat adres kan LISP functionaliteit gerealiseerd worden in een privé-netwerk zonder dat daar een volledig publieke reeks aan toegekend hoeft te worden.
3. **Optie drie, gemiddeld ingrijpend.** De laatste adoptietechniek is voor Enterprises die over de middelen beschikken om een geheel eigen LISP omgeving op te zetten. Dit betekent dat naast het gebruikt van xTR's als grensrouter bij alle vestigingen ook de mapping-system en proxy-router onder de verantwoordelijkheid van de Enterprise vallen. Dit is vergelijkbaar met ondernemingen die tussen alle vestigingen hun eigen private (internet)lijnen hebben.

3.1.1 VOOR- EN NADELEN

Net als bij de voor- en nadelen van ISP worden hieronder eerst de algemene voor- en nadelen van LISP adoptie door Enterprises opgesomd met daarop volgend een overzicht van specifieke voor- en nadelen per techniek.

Voordelen:

- **Geen BGP bij multihoming.** Uit een gesprek met de oprichter van de enige LISP-ISP in Nederland is duidelijke geworden dat de grootste motivatie voor onderneming om voor LISP te kiezen het gebrek aan BGP is bij multihoming. Het gebruik van BGP is duur in apparatuur en onderhoud en daar zit niemand op te wachten. Door LISP te gebruiken kunnen die prijzen sterk worden teruggedrongen.
- **IPv4/IPv6 support.** LISP ondersteund standaard zowel IPv4 als IPv6. Hierdoor is het een interessante techniek voor Enterprises om de transitie naar IPv6 voor te bereiden met een redelijk kleine impact op de bestaande omgeving.

- **VPN op basis van instance ID's.** De instance ID's die standaard door LISP worden ondersteund kunnen worden gekoppeld aan VRF's. Deze koppeling kan gebruikt worden om eenvoudig VPN's op te zetten tussen vestigingen.
- **Host mobility.** Zolang aan de voorwaarden van VM/IP mobility wordt voldaan kan het een zeer krachtige techniek zijn voor ondernemingen die eindsystemen willen verplaatsen. Denk hierbij ook aan uitwijksituaties. Sessies blijven bestaan ondanks de (geografische) verplaatsing van een systeem.

Nadelen:

- **Weinig ondersteuning.** Officieel is er geen ondersteuning voor LISP. Alles gebeurt nog op vrijwillige basis. Dit kan voor partijen als Qi ict goed zijn aangezien zij extra onderhoudspraktijken kunnen verkopen, maar als Qi ict zelf niet het probleem kan oplossen is er geen directe partij waar hulp aan gevraagd kan worden.
- **Globale EID-prefix.** De prefix die gebruikt wordt moet globaal routeerbaar zijn over het internet. Voorheen konden PI-adressen worden opgevraagd worden door LIR te worden bij de RIPE, maar dit is niet langer mogelijk. De enige optie is om PA-adressen op te vragen bij een LIR, maar daarvoor zal betaald moeten worden. Daarbij komt ook dat de voorraad PA-adressen snel slinkt.
- **IPv6.** Het omslagpunt naar IPv6 komt steeds dichterbij. Wanneer dat moment komt blijft het hoofddoel van LISP wel relevant, maar zaken als IPv6 transitie en IP mobility worden minder interessant, omdat elke systeem dan een uniek IPv6-adres heeft. Het is de vraag of LISP dan nog wel interessant is om over te nemen.

Figuur 5.2 - Voor- en nadelen van adoptietechnieken Enterprises

Optie één	Optie twee	Optie drie
Voordelen: - Geen beheerverantwoordelijkheden. Die neemt de ISP voor zijn rekening. In theorie veranderd er niets aan de manier waarop de onderneming nu een internetverbinding ontvangt. Er wordt slechts een internetverbinding afgenomen. - Geen wijzigingen aan het netwerk in zowel hardware als software.	**Voordelen:** - Doordat de xTR nu aan de eigen omgeving is gekoppeld kan eenvoudig multihoming worden ingeregeld. Daarbij komen ook de voordelen van load balancing en prioriteit toekenning. - Hoeft officieel geen verandering aan het netwerk te betekenen. De xTR kan aan de grens van het netwerk worden geplaatst. - Intern geen kennis meer nodig van BGP, of apparatuur dat BGP ondersteund.	**Voordelen:** - Volledig netwerk in eigen hand. Een voorbeeld van de voordeel hiervan zijn uitwijksituaties. Door één regel te veranderen in de proxy-router en mapping-system kan je verbindingen van buitenaf naar een totaal andere locatie laten gaan.
Nadelen: - De xTR verzorgt load balancing en prioriteit toekenning aan verkeer dat binnenkomt met een multihomed verbinding. Door de xTR bij de provider te plaatsen verlies je deze mogelijkheid. Hierdoor gaat één van de grootste voordelen van LISP verloren. - Kosten zijn waarschijnlijk hoger dan een regulier consumentenlijn, omdat er een extra service geleverd moet worden in de vorm van een mapping-system en proxy-service.	**Nadelen:** - Geen specifieke nadelen voor deze adoptietechniek.	**Nadelen:** - Het opzetten van een eigen mapping-system en proxy-service vereist extra apparatuur. Daarnaast vereist het opzetten van een proxy-service ook BGP om routes te distribueren in het DFZ zolang LISP niet op globaal niveau totaal is overgenomen.

3.1.2 KOSTEN VOOR DE ENTERPRISE

De kosten voor een Enterprise die LISP wil adopteren zijn over het algemeen wat inzichtelijker dan bij een ISP, omdat deze voorbeelden ook daadwerkelijk gebouwd zijn in het testlab, plus het feit dat er een partij is in Nederland die LISP services levert.

Voor adoptietechniek één is dat niet het geval. Het scenario waarbij je net als nu een internetlijn uit de muur krijgt en daarmee verbindt met een ISP die werkt op basis van LISP is onwaarschijnlijk. Je verliest daarmee het grootste voordeel van LISP voor ondernemingen; goedkope multihoming. Mocht dit toch worden toegepast kan er op gerekend worden dat de kosten in het begin van globale LISP adoptie wat hoger zullen uitvallen dan een internetlijn tegenwoordig kost, omdat er een mapping- en proxy-service opgezet moet worden dat meer geld kost dan een normale ISP. Naar mate het gebruik van LISP toeneemt en de tabellen in het DFZ afnemen, waardoor ISP's minder goede apparatuur nodig hebben zullen de prijzen afnemen.

De tweede optie is wel inzichtelijk, omdat er in Nederland één partij bekend is die LISP-services levert. Wanneer een onderneming zijn bestaande netwerk voorziet van een xTR kan er voor 65 euro per maand gebruikt worden gemaakt van de services van Steffann ISP. Deze ISP levert een aantal IPv4- en IPv6-adressen die gebruikt kunnen worden als EID-prefix om het interne netwerk te verbinden met het internet via zijn mapping-system en proxy. Let wel dat er evengoed één of meer internetlijnen afgesloten dienen te worden bij andere ISP's om gebruik te maken van het internet op basis van LISP. Steffann ISP levert dus de EID-prefix, niet de RLOC's. Daarbij komt ook de kosten van de xTR die aan de grens van het netwerk geplaatst dient te worden. Deze kan net als bij de ISP's op basis van gratis opensource software worden gebouwd, of door middel van betaalde licenties. Tegen een vergoeding levert Steffann ISP ook service op de xTR's.

Voor de derde optie kan voor een deel worden overgenomen wat bij de bovenstaande optie is vermeld. Elke vestiging kan een eigen xTR plaatsen op basis van opensource of betaalde licenties en sluit internetlijnen af bij verschillende ISP's. Echter om een verbinding te maken met het internet zal er een koppeling gemaakt moeten worden met de mapping-system en proxy-service van de hoofdvestiging. Hier zullen de meeste kosten bij komen kijken. Afhankelijk van het aantal vestigingen nemen de vereiste prestaties van het apparatuur toe en ook hierin kan weer onderscheidt gemaakt tussen opensource en betaalde licenties.

Ook voor Enterprises blijkt het lastig om te bepalen hoeveel de adoptie van LISP zou kunnen kosten. Het hangt hier ook af van dezelfde factoren als bij adoptie door een ISP:

- Keuze van adoptietechniek
- Opensource software versus betaalde licenties
- Grootte van de onderneming
- In welke mate apparatuur kan worden hergebruikt

Om een klein beetje van de sluier te kunnen doen oplichten is contact gezocht met enige bekende LISP partij in Nederland, Steffann ISP. Over de kwestie van adoptie had hij het volgende te zeggen:

"Het voordeel van LISP is dat multihoming (en de bijbehorende redundantie en capaciteits-bundeling) mogelijk is zonder dat de gebruiker PI adressen hoeft aan te vragen, zonder dat de gebruiker BGP moet snappen en zonder dat de bijbehorende dure verbindingen nodig zijn. Met LISP kun je dat alles op basis van simpele consumenten-verbindingen doen. Het nadeel is wel dat er meerdere providers nodig zijn. Één of meerdere providers die de fysieke verbinding leveren plus de LISP provider. Daardoor zijn de kosten wat hoger dan bij een normale small-business verbinding, maar lager dan bij een volledige BGP verbinding. LISP is daardoor het interessantste voor middelgrote bedrijven."

Deze opmerking heeft betrekking op adoptie van LISP door middel van optie twee, waarbij Steffann ISP de mapping-service en proxy-routers regelt.

4. TOEKOMST VAN LISP

LISP is in 2006 bedacht als oplossing voor een probleem die de toekomst van het internet in gevaar brengt. Een voorbeeld om te bevestigen dat het probleem inderdaad aanwezig is, is het onlangs voorgekomen 512K-Day. Op twaalf augustus 2014 bereikte het aantal routes in de tabellen van het DFZ een aantal van 512.000. Een aantal dat veel (oudere) routers niet aan kon. Hierdoor gingen de routers oude routes verwijderen om ruimte te maken voor de nieuwe. Dit resulteerde in grote problemen bij ISP's als Comcast, AT&T en Verizon. De partijen die verantwoordelijk waren voor de routers hebben het probleem snel weten te verhelpen door ouder apparatuur te vervangen met nieuwe, maar een oplossing als deze is natuurlijk niet permanent. Het is nu slechts een kwestie van tijd voordat het volgende limiet bereikt wordt.

Als we gaan kijken naar wat LISP over de afgelopen negen jaar heeft bereikt lijkt het de goede weg op te gaan. Inmiddels draait er al een aantal jaar een stabiel bèta-netwerk dat de voordelen van LISP demonstreert. Daarnaast wordt de interesse in het protocol op evenementen als CiscoLive steeds groter. Tevens zijn er op het moment zeer veel verschillende implementaties van LISP actief, waardoor er voor iedere partij wat is. Een kleine opsomming van LISP implementaties is als volgt:

- Cisco IOS, IOS-XE, NX-OS, IOS-XR en Cat 6K
- LISPMob
- OpenLISP
- LISPLab
- Steffann LISP (Python implementatie)

Hoewel de draagvlak voor LISP in Nederland nog niet erg uitgebreid is met slechts één bekende partij die LISP-services levert, neemt het wereldwijd wel toe. Voorbeeld van publieke mapping-systems en proxy-services zijn NJEdge, Intouch en VxNET en natuurlijk het publieke bèta-netwerk. Aan deze publieke systemen hangen inmiddels ruim honderd duizend LISP omgevingen.

In een gesprek met CIsco technical marketing engineer Gregg Schudel is duidelijk geworden dat LISP op het moment zeer veel aandacht krijgt binnen Cisco na jarenlange ontwikkeling. Daarnaast is onlangs bekend gemaakt dat de non-profit organisatie lispers.net samen met de partijen Arista, HP, Aruba en A10 een open netwerk voor LISP wil creëren. Dit is zeer goed nieuws, omdat de afgelopen jaren Cisco de enige netwerkfabrikant was die zich bezighield met LISP.

De bovenstaande berichten lijken een positieve toekomst voor LISP aan te geven. Het zal nog wel even gaan duren voordat de echte voordelen van LISP in het DFZ zichtbaar worden, maar acties zoals de 512K-Day helpen wel bij de bewustwording om het traject te versnellen.

Persoonlijk zit ik wel met twijfels over de toekomst van LISP. LISP is een protocol en architectuur die het internet nodig heeft om te blijven werken. Als LISP, of iets soort gelijks, niet wordt ingevoerd neemt het aantal routes alleen maar toe en dat zal met IPv6 niet minder worden. IPv6 heeft namelijk nog steeds het conflict dat locatie en identiteit samen worden genomen in één IP-adres waardoor aggregatie lastig is. Mensen zijn zich niet goed bewust van dit probleem. Dat blijkt wel uit het gegeven dat partijen zijn gewaarschuwd voor 512K-Day maar er niets aan veranderen.

Als je dan ook bedenkt dat geprobeerd word om LISP aan de man te brengen door ondernemingen in te palmen met mooie beloftes over goedkope multihoming en IPv6 transitie wordt het doel van LISP niet goed vertaald aan het publiek. Daarnaast zullen veel bedrijven waarschijnlijk ook denken dat ze LISP niet nodig hebben, omdat hun bestaande netwerk werkt zoals het nu staat. Ze vergeten echter dat het DFZ noodzakelijk is.

5. CONCLUSIE

Uit het onderzoeksrapport en de resultaten van de testplannen is gebleken dat LISP een indrukwekkend protocol en architectuur is met veel mogelijkheden. Afgezien van het feit dat er wel een aantal uitzonderingen en vereisten zijn om de volledige potentie te benutten blijft het een protocol met een bijzonder eenvoudige configuratie dat voor diverse zaken kan worden toegepast.

Op het moment wordt LISP vooral aan de man gebracht door de voordelen die het biedt in multihoming, IPv6 transitie, VM/IP mobility en network virtualization. De eerste drie technieken zijn onderzocht en leveren inderdaad veel voordelen op voor een onderneming, mits wordt voldaan aan een aantal eisen, waarbij de belangrijkste is dat de EID-prefix van de onderneming een globale routerbare reeks moet zijn. Dit kan een probleem gaan opleveren voor veel partijen aangezien PI-adressen niet langer leverbaar zijn en PA-adressen ook schaarser worden.

Als het gegeven dat één of meer globaal routeerbare IP-adressen nodig zijn even wordt vergeten houdt je een configuratie over van ongeveer twintig regels. Hierme kun je een multihomed omgeving creëren dat bereikbaar is over zowel IPv4 als IPv6 terwijl eindsystemen ook nog eens van vestiging kunnen wisselen. Daarbij komt ook dat het allemaal gebeurt zonder dat een sessie wordt afgebroken en hersteltijden van maximaal 7 seconden bij het falen van een verbinding.

Specifiek gekeken naar de geschiktheid van het protocol voor Enterprises en ISP's is duidelijk geworden dat kosten die komen kijken bij de adoptie van LISP afhankelijk zijn van vier factoren:

- Keuze van adoptietechniek
- Opensource software versus betaalde licenties
- Grootte van de onderneming
- In welke mate apparatuur kan worden hergebruikt

Vooral in de categorie "keuze van adoptietechniek" lopen de kosten hevig uiteen, omdat er mogelijkheden zijn om niets te doen en te profiteren, of om het netwerk volledig om te klussen.

Wat betreft de toekomst van LISP kan alleen maar worden gezegd dat op het moment er steeds meer aandacht aan wordt besteed. Het is niet langer een protocol dat alleen maar door Cisco wordt voortgeduwd. Steeds meer partijen tonen interesse. Dat zie je ook terug in de verschillende soorten implementaties van LISP die worden ontwikkeld. Toch is de toekomst van LISP net als alle andere protocollen die worden ontwikkeld onzeker. Het overnemen van LISP op globaal niveau is vergelijkbaar met IPv6. Het protocol lost een probleem op die al jaren bekend is, maar de implementatie wordt net zo lang uitgesmeerd tot dat we echt niet meer zonder kunnen en dat is zonde.

6. ADVIES

LISP is een indrukkend protocol. De configuratie is eenvoudig, de mogelijkheden breed en de resultaten goed. Normaliter zou een bevestiging als deze voldoende zijn om een partij te adviseren het protocol te adopteren, maar dat ligt bij LISP een stuk ingewikkelder.

Technieken als multihoming en IPv6 transitie hebben tijdens het toetsen goede resultaten opgeleverd. Het advies om deze technieken te gebruiken zou dan ook positief zijn. Helaas is het gebruiken van alleen de techniek niet mogelijk. Als één onderdeel van LISP gebruikt gaat worden en een xTR wordt geplaatst in een netwerk, komt daar de algehele adoptie van LISP bij kijken. Wanneer een xTR wordt geplaatst betekent dat namelijk automatisch ook dat het gebruik van een mapping-system en proxy-service nodig is. Het draagvlak van deze twee onderdelen is op het moment nog summier. Dat geldt vooral voor Nederland waar slechts één partij deze service aanbiedt. Daarbij komt ook dat voor het protocol geen officiële ondersteuning aanwezig is, omdat het beheer op het moment gebeurt door vrijwilligers van onder ander LISPMob en Cisco.

Om dit draagvlak te vergroten op de wereld zijn op het moment een aantal initiatieven in gang gezet. Onder andere het open control netwerk (OCN) van lispers.net in samenwerking met verschillende netwerkfabrikanten zal het draagvlak gaan vergroten. Het is echter nog te vroeg om te zeggen of dit netwerk ook een succes wordt. Daarbij komt ook dat de verschillende implementaties van LISP die zorgen voor beter hergebruik van apparatuur ook toenemen.

Een ander belangrijk punt is het feit dat LISP pas echt zin heeft voor het DFZ als het merendeel van de wereld ervan gebruik maakt. Tot die tijd is LISP niets meer dan extra routes die in de tabellen van het DFZ worden gedistribueerd met BGP. Als hierbij het feit wordt betrokken dat publieke IP-adressen nodig zijn voor het gebruik van LISP en deze zo goed als op zijn, is het de vraag of volledige adoptie van LISP überhaupt mogelijk is. Daarbij is nog niet eens gesproken over het feit dat alleen PA-adressen beschikbaar zijn, wat betekent dat bij het wijzigen van ISP de adressen niet meegenomen kunnen worden en dat werkt het concept van LISP tegen. Dit zou betekenen dat gewacht moet worden op IPv6, omdat iedereen dan publieke adressen krijgt, maar hoe lang IPv6 nog op zich laat wachten weet niemand.

Met de bovenstaande punten in gedachte kan een tweedeling advies worden gegeven. Het eerste advies is voor netwerken die op voorhand over alle nodige middelen beschikken en green kritische apparatuur bevatten. Netwerken als deze zijn prefect voor het proberen van LISP en zullen bijdragen aan de evolutie van het protocol wat logischerwijs leidt tot een breder draagvlak. Het tweede advies is voor alle andere netwerken waar wel kritische apparatuur draait. Als dit het geval is wordt geadviseerd om LISP niet te implementeren. Althans niet zo lang er geen officiële ondersteuning bestaat. Mocht LISP toch geprobeerd willen worden wordt geadviseerd om een netwerk te gebruiken die schaduw draait. Hierdoor is het altijd mogelijk om terug te vallen op een andere netwerk als het protocol niet geschikt blijkt.

Ondanks dat het advies op het moment vooral nijgt naar het niet adopteren van LISP is het duidelijk dat LISP of een soortgelijke oplossing nodig is. Problemen zoals het 512K-Day bevestigen dat. Toch is LISP op het moment niet de antwoord op het probleem. LISP lijkt op het moment op een driedelig stappenplan waarvan stap twee ontbreekt. LISP heeft te tijd nodig om verder te evolueren en de komende jaren zullen daar een breekpunt voor zijn.

7. BIBLIOGRAFIE

Cisco Systems. (2013, 03 19). *LISP ESM Multihop Mobility*. Opgeroepen op 02 02, 2015, van www.cisco.com: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/15-mt/irl-15-mt-book/irl-lisp-esm-multihop-mobility.html

Cisco Systems. (2014, 04 04). *LISP Hardware and Software Support*. Opgeroepen op 11 17, 2014, van lisp.cisco.com: http://lisp.cisco.com/lisp_hwsw.html#HW

D. Farinacci, C. S. (2013, 01 01). *The Locator/ID Separation Protocol (LISP) (RFC6830)*. Opgehaald van tools.ietf.org: https://tools.ietf.org/html/rfc6830#section-1

Florin Coras, D. S.-A.-P. (2012). Implementing a BGP-Free ISP Core with LISP. *Global Communications Conference (GLOBECOM), 2012 IEEE* (pp. 2772-2778). Anaheim, CA: IEEE.

G. Fairhurst, U. o. (2013). *Applicability Statement for the Use of IPv6 UDP Datagrams with Zero Checksums.* Schotland: IETF.

Herrmann, D. (2013). *Incoming Interdomain Traffic Engineering with LISP.* Duitsland: Universiteit van Darmstadt.

Systems, C., & D. Farinacci, V. E. (2014, 09 12). *NAT traversal for LISP.* Opgeroepen op 02 08, 2015, van tools.ietf.org: https://tools.ietf.org/html/draft-ermagan-lisp-nat-traversal-06

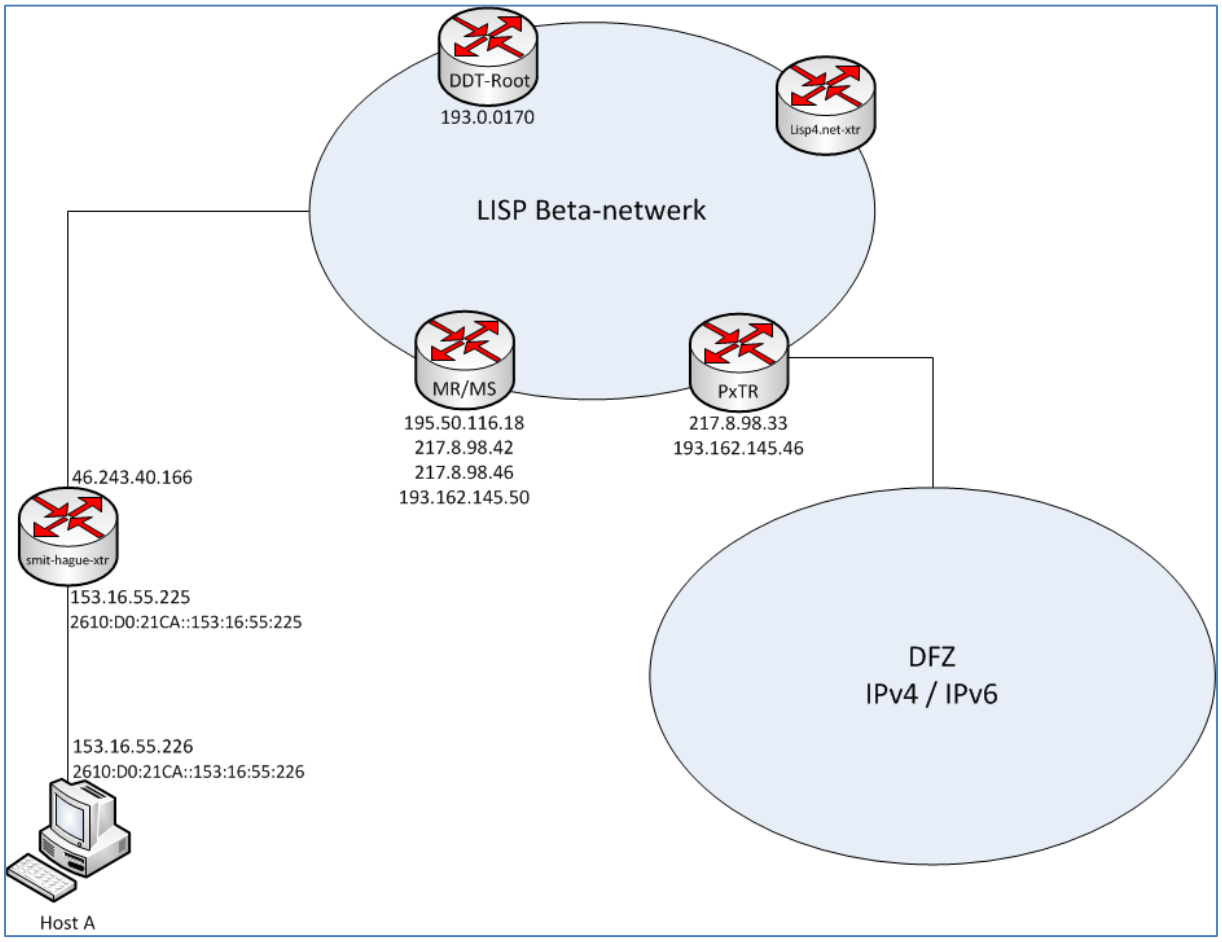
8. BIJLAGE - TESTRESULTATEN

INHOUDSOPGAVE

1. OPSTELLING ÉÉN

In de eerste opstelling wordt de bereikbaarheid van een netwerk na de adoptie van LISP gedemonstreerd. Om als klant over LISP functionaliteit te beschikken in een netwerk is de makkelijkste optie het verbinden met een LISP-ISP. Normaliter staat daar een vergoeding tegenover, maar er zijn ook mogelijkheden om het gratis te testen. Eén van die mogelijkheden is het LISP bèta-netwerk. Hieronder staat de definitieve topologie van de opstelling, de configuratie en de resultaten van het testen.

1.1 TOPOLOGIE



Figuur 2.1 Topologie opstelling één

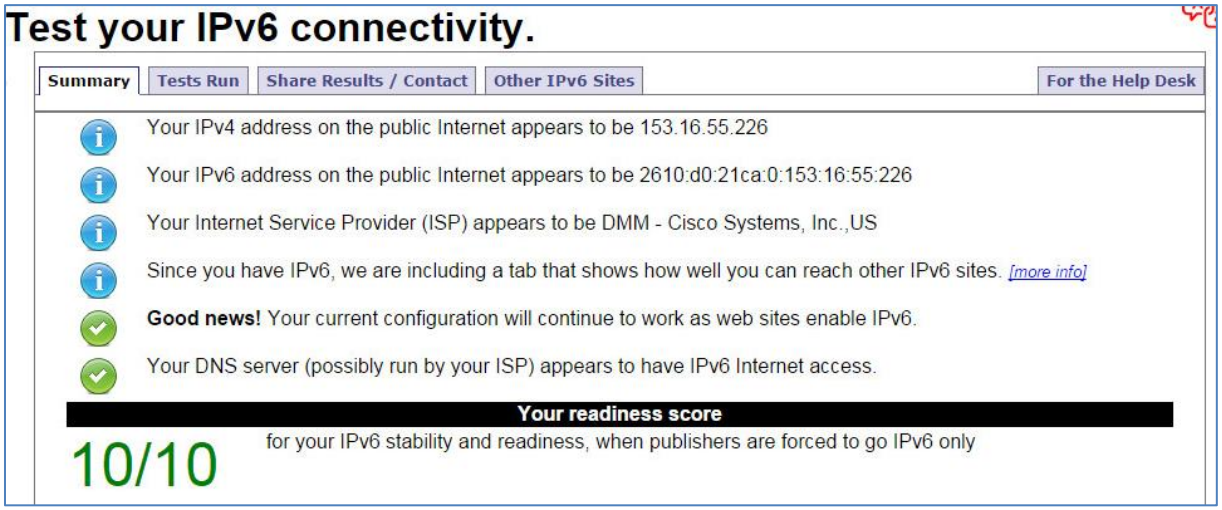
1.2 CONFIGURATIE

De configuratie van de opstelling bevindt zich in hoofdstuk vier. Zoals vermeld in het ontwerprapport dient voor deze opstelling alleen de smit-hague-xtr en host A geconfigureerd te worden. De configuratie van de host is niets meer dan een IPv4- en IPv6 adres. De configuratie van smit-hague-xtr omvat het plaatsen van IP-adressen op de interfaces, het aangeven van de RLOC en zijn lokale EID-omgeving en het aangeven van de MR, MS en PxTR waarmee externe locaties opgezocht en bereikt kunnen worden.

1.3 RESULTATEN

Te testen maatwerk		Opstelling één			
Project		Location/ID Separation Protocol			
Test ontworpen door		Shaun Smit			
Datum		05-01-2015			
Globale beschrijving		Voor deze opstelling wordt een zelf geconfigureerde xTR gebruikt om een intern (lab-)netwerk van Qi ict te verbinden met een LISP-ISP, het bèta-netwerk, om de bereikbaarheid van een netwerk te testen na de adoptie van LISP			
Test datum		12-01-2015			
Door		Shaun Smit			
Nr.	**Omschrijving**	**Verwacht Resultaat**	**Resultaat**	**Ok/Fout**	**Opmerking**
1.	IPv4 LISP naar IPv4 LISP: Ping van 153.16.55.226 naar 153.16.5.30	Volledige connectiviteit	**Eerste poging:** Packets (Sent/Recieved/Lost): 4/2/2 Round trip times (Min/Max/Avg ms): 156/156/156 **Tweede poging:** Packets (Sent/Recieved/Lost): 4/4/0 Round trip times (Min/Max/Avg ms): 155/155/155	OK	N.v.t
2.	IPv6 LISP naar IPv6 LISP: Ping van 2610:D0:21CA::153:16:55:225 naar 2610:D0:110C:1::3	Volledige connectiviteit	**Eerste poging:** Packets (Sent/Recieved/Lost): 4/2/2 Round trip times (Min/Max/Avg ms): 151/152/151 **Tweede poging:** Packets (Sent/Recieved/Lost): 4/4/0 Round trip times (Min/Max/Avg ms): 151/155/152	OK	N.v.t

3.	IPv4 LISP naar standaard IPv4: Ping van 153.16.55.226 naar 8.8.8.8	Volledige connectiviteit	**Eerste poging:** Packets (Sent/Recieved/Lost): 4/4/0 Round trip times (Min/Max/Avg ms): 4/7/4 **Tweede poging:** Packets (Sent/Recieved/Lost): 4/4/0 Round trip times (Min/Max/Avg ms): 4/4/4	OK	N.v.t
4.	IPv6 LISP naar standaard IPv6: Ping van 153.16.55.226 naar 2001:4860:4860::8888	Volledige connectiviteit	**Eerste poging:** Packets (Sent/Recieved/Lost): 4/4/0 Round trip times (Min/Max/Avg ms): 24/29/25 **Tweede poging:** Packets (Sent/Recieved/Lost): 4/4/0 Round trip times (Min/Max/Avg ms): 24/25/24	OK	N.v.t
5.	Standaard IPv4 naar IPv4 LISP Ping van 172.20.12.64 naar 153.16.55.226	Volledige connectiviteit	**Eerste poging:** Packets (Sent/Recieved/Lost): 4/3/1 Round trip times (Min/Max/Avg ms): 16/19/18 **Tweede poging:** Packets (Sent/Recieved/Lost): 4/4/0 Round trip times (Min/Max/Avg ms): 17/21/19	OK	N.v.t
6.	Standaard IPv6 naar IPv6 LISP	Volledige connectiviteit	Geen gegevens van de ping. Echter wel bevestiging gehad van lisp.cisco.com dat de site over IPv6 te bereiken is.	OK	N.v.t
7.	IPv6 ready test	Volledige connectiviteit	**Score 10/10**	OK	N.v.t



1.4 Conclusie

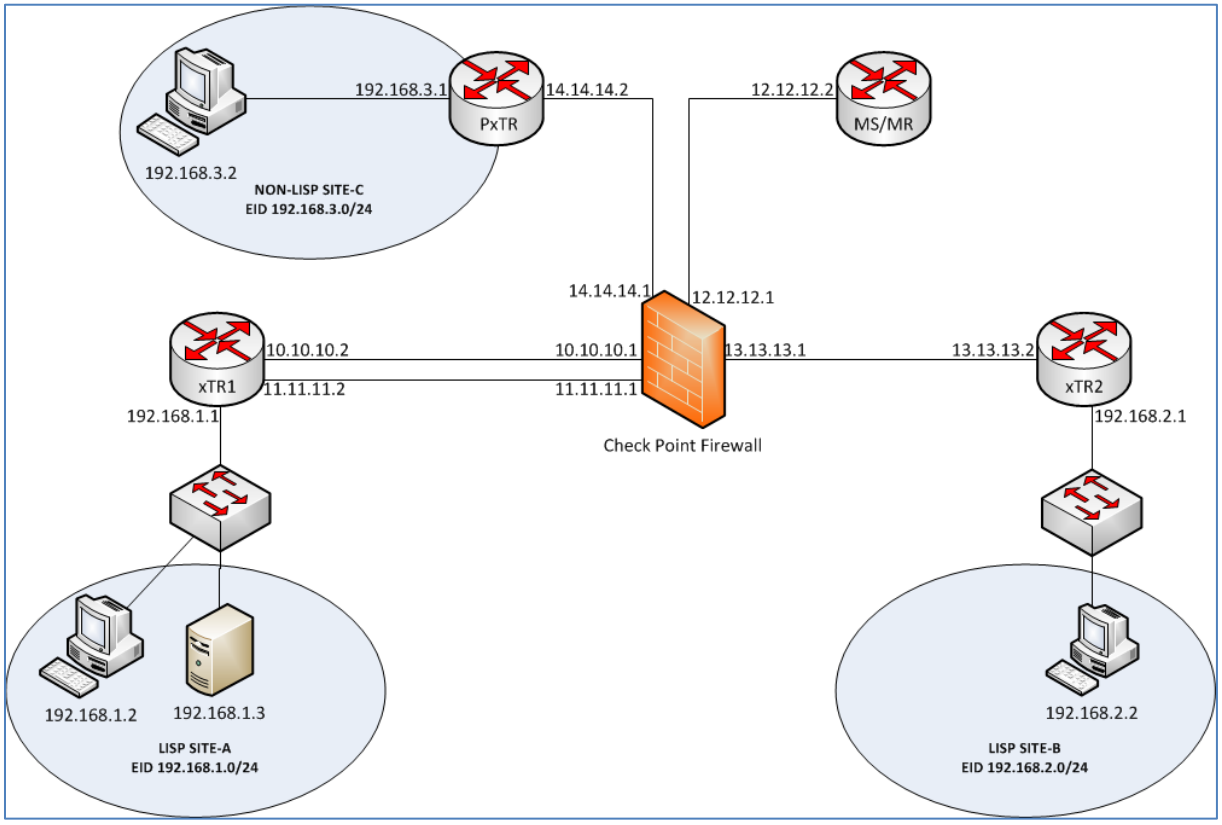
Het is duidelijk dat het verbinden met het internet door middel van LISP weinig impact heeft op de bereikbaarheid van een netwerk. In alle pogingen is het te zien dat er twee pings verloren gaan aan de tijd dat nodig is om de eerste keer een EID-to-RLOC koppeling op te zoeken, maar daarna het verbinden goed gaat. Dit geldt voor zowel IPv4 als IPv6 en zowel LISP als non-LISP. De round-trip-times zijn wel wat aan de hoge kant, maar dit is verklaarbaar met het feit dat het bèta-netwerk uit ouder gedoneerd apparatuur bestaat. Een echte LISP-ISP zal hier minder last van hebben.

Verder is het ook belangrijk om te melden dat de IPv6-test een maximale score heeft behaald. Dat betekent dat het interne netwerk volledige klaar is voor de overgang naar IPv6 en dat met slecht een aantal regels code.

2. OPSTELLING TWEE

In de tweede opstelling worden de technieken multihoming, VM/IP mobility en IPv6-transite getest binnen een op zichzelf staande opstelling met LISP functionaliteiten. In dit hoofdstuk wordt de topologie, configuratie van componenten, resultaten van het testplan, speciale bevindingen en de conclusie omschreven.

2.1 TOPOLOGIE



Figuur 3.1 – Topologie opstelling twee

2.2 CONFIGURATIE

In hoofdstuk vijf bevindt zich de configuratie van de verschillende netwerkcomponenten die nodig zijn voor deze opstelling. Naast de normale configuratie waarbij lokale EID-netwerken worden geconfigureerd achter een RLOC, worden bij xTR1 twee RLOC-adressen aangegeven en wordt aan de binnenkant van beide xTR's aangegeven dat het netwerk 192.168.1.0/24 mobiel is.

2.3 RESULTATEN

Resultaten					
Te testen maatwerk	Opstelling twee				
Project	Location/ID Separation Protocol				
Test ontworpen door	Shaun Smit				
Datum	06-01-2015				
Globale beschrijving	Voor deze opstelling wordt een standalone omgeving voorzien van alle mogelijk LISP netwerkcomponenten. Door middel van dit lab kan de werking van LISP worden gedemonstreerd met daarbij ook de technieken multihoming, IPv6 transitie en VM/IP Mobility.				
Test datum	13-01-2015 – 16-01-2015				
Door	Shaun Smit				
Nr.	**Omschrijving**	**Verwacht Resultaat**	**Resultaat**	**Ok/Fout**	**Opmerking**
		Multihoming			
1.	Bereikbaarheid Link 1 Traceroute van 192.168.1.2 naar 192.168.2.2 en andersom met 10.10.10.2 als primaire link.	Een connectie met de overzijde via lijn 10.10.10.2	1. 192.168.1.1 2. 10.10.10.1 3. 13.13.13.2 4. 192.168.2.2 1. 192.168.2.1 2. 13.13.13.1 3. 10.10.10.2 4. 192.168.1.2	OK	N.v.t
2.	Bereikbaarheid Link 2 Traceroute van 192.168.1.2 naar 192.168.2.2 en andersom met 11.11.11.2 als primaire link	Een connectie met de overzijde via lijn 11.11.11.2	1. 192.168.1.1 2. 11.11.11.1 3. 13.13.13.2 4. 192.168.2.2 1. 192.168.2.1 2. 13.13.13.1 3. 11.11.11.2 4. 192.168.1.2	OK	N.v.t

3.	Connectieherstel Ping tegelijk: - 192.168.3.2 naar 192.168.1.2 - 192.168.2.2 naar 192.168.1.2 Verwijder de actieve link en tel het aantal verloren pings en meet de hersteltijd van de verbinding. Doet dit met rloc-probing uit	Updaten van de database gebeurt elke 60 seconden. Afhankelijk van het moment waarop de verbinding verbroken wordt duurt het maximaal zestig seconden.	1 ping “request timed out”. Gemiddeld 4 seconden om te herstellen.	OK	De xTR houdt zijn interfaces zelf ook in de gaten, waardoor een update eerder wordt doorgevoerd
4.	Connectieherstel Ping tegelijk: - 192.168.3.2 naar 192.168.1.2 - 192.168.2.2 naar 192.168.1.2 Verwijder de actieve link en tel het aantal verloren pings en meet de hersteltijd van de verbinding. Doet dit met rloc-probing aan	Als de xTR zijn verbindingen uit de map-cache in de gaten houdt met probing wordt verwacht dat het binnen 5 seconden de verbinding wordt herstelt.	1 ping “request timed out”. Gemiddeld 4 seconden om te herstellen.	OK	Aangezien de vorige test ook al 4 seconden was kan het zijn dat rloc-probing in zo’n kleine omgeving geen efffect heeft, maar op het DFZ wel.
5.	Connectieherstel FTP-sessie - 192.168.3.2 naar 192.168.1.3 Verwijder de actieve link en meet de tijd die nodig is om de sessie te laten vervolgen, als dat gebeurt. Doet dit met rloc-probing uit	Updaten van de database gebeurt elke 60 seconden. Afhankelijk van het moment waarop de verbinding verbroken wordt duurt het maximaal zestig seconden.	Gemiddeld 4 seconden nodig om de verbinding te herstellen en door te gaan met versturen.	OK	Zie test drie
6.	Connectieherstel FTP-sessie - 192.168.3.2 naar 192.168.1.3 Verwijder de actieve link en meet de tijd die nodig is om de sessie te laten vervolgen, als dat gebeurt. Doet dit met rloc-probing aan	Als de xTR zijn verbindingen uit de map-cache in de gaten houdt met probing wordt verwacht dat het binnen 5 seconden de verbinding wordt herstelt.	Gemiddeld 4 seconden nodig om de verbinding te herstellen en door te gaan met versturen.	OK	Zie test vier

VM/IP Mobility					
7.	Mapping-system Verplaats server A (192.168.1.3) van netwerk 192.168.1.0/24 naar 192.168.2.0/24 en meet hoe lang het duurt voordat de mapping-system op de hoogte is van de wijziging.	Updaten zou maximaal 1,5 keer de round trip time van een verbinding mogen zijn. Voor het updaten van de mapping-system wordt een seconden of minder verwacht.	Gecontroleerd met het commando “show lisp site”. Op 00:00:41 werd de server verplaatst. 00:00:42 – 11.11.11.2 00:00:43 – 13.13.13.2 Binnen een seconde was de mapping-server op de hoogte van de verandering. Dit geldt tevens voor de PxTR die door middel van een sollicit-map-request op de hoogte is gesteld.	OK	De verbinding werd op 00:00:42 losgekoppeld. Op 00:00:43 was de server op de hoogte van de wijziging.
8.	Bereikbaarheid Ping voor de verplaatsing: - 192.168.3.2 naar 192.168.1.3 - 192.168.1.2 naar 192.168.1.3 - 192.168.2.2 naar 192.168.1.3 Ping na de verplaatsing: - 192.168.3.2 naar 192.168.1.3 - 192.168.1.2 naar 192.168.1.3 - 192.168.2.2 naar 192.168.1.3	Ondanks het feit dat het verplaatste eindsysteem een IP-adres heeft dat niet onder het subnet valt wordt verwacht dat connectie met alle systemen mogelijk is.	Alle connecties zijn voor en na de verplaatsing actief. Het verplaatsen heeft geen invloed op de bereikbaarheid van de server.	OK	Doordat het MAC-adres van de first-hop router altijd hetzelfde is bij mobility is connectie mogelijk
9.	Connectieherstel Start een ftp-download van 192.168.3.2 (host C) naar 192.168.1.3 (server A) terwijl server A zich in SITE-A bevindt. Verplaatst server A naar SITE-B en meet de tijd die nodig is om met de download door te gaan.	Als de mapping-system binnen een seconden op de hoogte is van de wijzigingen moet binnen 10 seconden het totale netwerk op de hoogte moeten zijn om te verbinding te herstellen.	1. 7 seconden 2. 6 seconden (terugplaatsing) 3. 6 seconden 4. 6 seconden (terugplaatsing) 5. 6 seconden 6. 6 seconden (terugplaatsing)	OK	
Ipv6 Transitie					
De testen om IPv6 transitie te toetsen zijn vervallen. De resultaten van de eerste opstelling zijn overtuigend genoeg om te bewijzen dat LISP door middel van encapsulation zowel een IPv4- als IPv6-netwerk kan overbruggen.					

2.4 BEVINDINGEN

Connectieherstel multihoming:

- Wanneer de actieve link is verwijderd en de verbinding is herstelt wordt de verandering bijna direct opgenomen in het mapping-system door een map-register bericht van de verantwoordelijk xTR. Wanneer de link wordt teruggeplaatst wordt dit niet direct opgemerkt. De terugplaatsing wordt pas weer in de nieuwe ronde opgenomen in de database wanneer de zestig seconden timer van de mapping-system is verlopen.
- RLOC-probing is een techniek dat een verzender xTR gebruikt om externe xTR's die zich in zijn map-cache bevinden preventief te controleren op beschikbaarheid, voordat verkeer wordt verstuurd. Normaliter zou dit het proces van een kapotte verbinding detecteren sneller moeten herstellen, maar omdat het zonder RLOC-probing al bijzonder snel gebeurt is dat hier niet het geval. Dat is hier wellicht te verwijten aan het feit dat het om een klein netwerk gaat. Updaten van het mapping-system gebeurt hier al binnen een seconde. Dat zou onder de omstandigheden van het DFZ wel eens langer kunnen duren, waardoor RLOC-probing wel sneller is.

Connectieherstel mobility:

- Hoewel de hersteltijden van mobility zeer goed zijn kan een (ftp-)sessie nog steeds falen tijdens het verplaatsen van een machine. Dit gedrag is ook gezien bij de ftp-sessie die hier is getoetst. Dit gedrag is te wijten aan de connectiontimers van de ftp-client. Deze timers kunnen standaard op lage waarden staan, zoals 3 seconden bij filezilla, waardoor connectieherstel niet plaatsvindt. De ftp-client breekt de verbinding dan vroegtijdig af. Dit kan verholpen worden door de timers te verhogen.

Algemene bevinding:

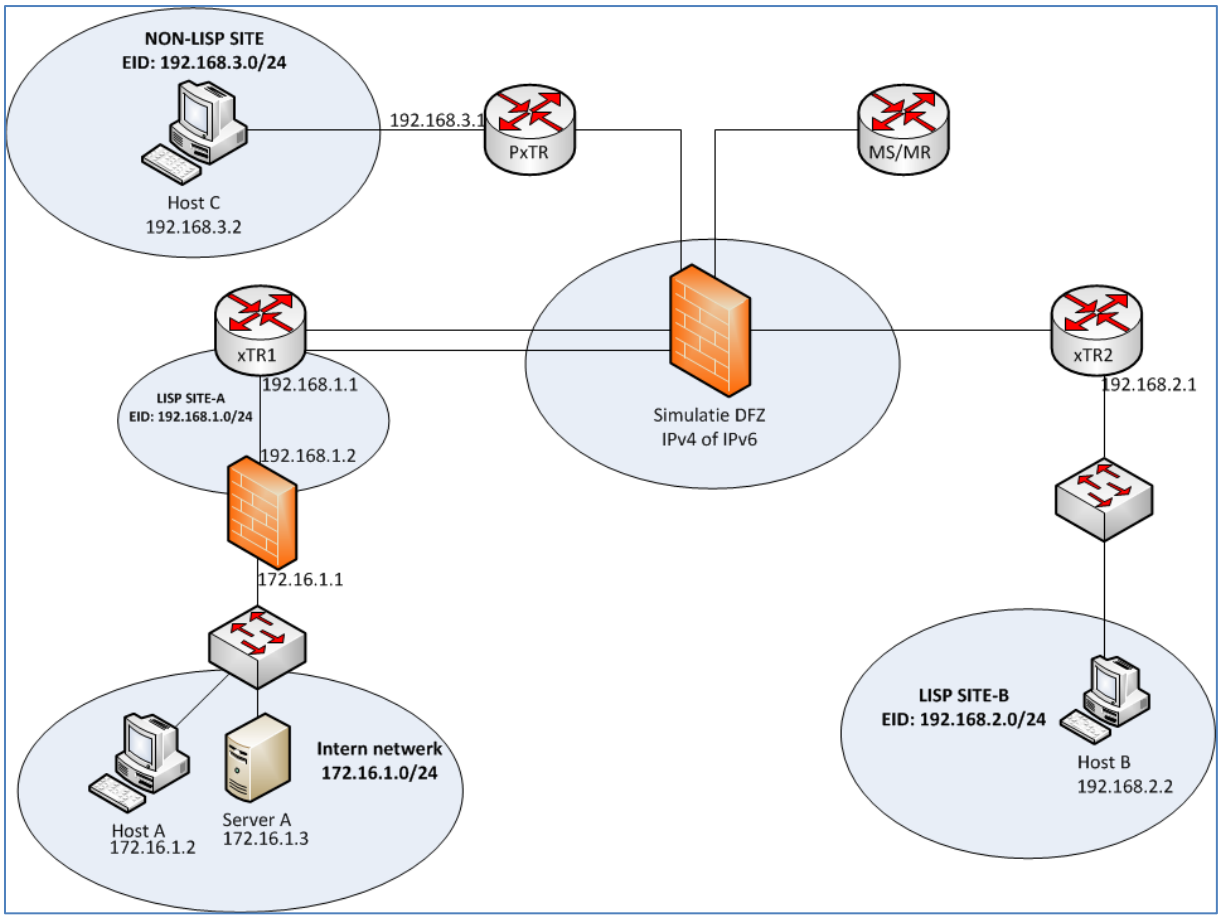
- Hoewel de processen en hersteltijden bijna altijd constant verlopen bij het verwijderen van een link of het verplaatsen van een eindsysteem komen er ook situaties voor waarbij het langer duurt. Het is niet gelukt om de omstandigheden te reproduceren, maar van de tientallen testen zijn er een paar geweest waarbij de hersteltijden ineens sterk toenamen. De tijden bleven wel onder de dertig seconden, wat nog steeds een goede tijd is, maar een verklaring is er niet. Het kan zijn dat het map-register bericht dat verstuurt moest worden verloren is gegaan, doordat het UDP verkeer is, of het kan zijn dat de ESX-server waarop de database zich bevindt het zwaar heeft met de vele machines die erop draaien.

2.5 CONCLUSIE

De drie hoofdtechnieken werken in deze labopstelling zeer goed. Een opstelling als deze zou voor bijvoorbeeld datacenters een mooie oplossing zijn. Zo kan een partij met meerdere vestigingen machines verplaatsen, met een zeer korte onderbreking. Tevens kan er met één regel configuratie een extra koppeling worden toegevoegd om verkeer over te verdelen. Er is echter wel een probleem en dat is security. Zo gauw het verkeer van encapsulation is voorzien, valt er niets aan te inspecteren.

3. OPSTELLING DRIE

3.1 TOPOLOGIE



Figuur 3.1 – Topologie opstelling drie

3.2 CONFIGURATIE

De configuratie van de netwerkcomponenten is hetzelfde al bij de vorige opstelling. Het enige verschil is dat op xTR1 nu niet het volledige subnet als mobiel wordt aangegeven, maar een meer specifieke prefix.

In de nieuwe firewall worden een aantal NAT-regels opgenomen. De eerste NAT-regel verschuilt het interne netwerk 172.16.1.0/24 achter het bekende LISP-IP-adres 192.168.1.2. Hierdoor weet de xTR dat LISP encapsulation toegepast dient te worden. De andere NAT-regels zijn statisch geconfigureerd om bijvoorbeeld het bekende LISP-adres 192.168.1.3 om te zetten tot 172.16.1.3. Hierdoor blijven de hosts van buiten ook beschikbaar.

3.3 RESULTATEN

Resultaten					
Te testen maatwerk		Opstelling drie			
Project		Location/ID Separation Protocol			
Test ontworpen door		Shaun Smit			
Datum		06-01-2015			
Globale beschrijving		Voor deze opstelling wordt een standalone omgeving voorzien van alle mogelijk LISP netwerkcomponenten. Door middel van dit lab kan de werking van LISP worden gedemonstreerd met daarbij ook de technieken multihoming, IPv6 transitie en VM/IP Mobility.			
Test datum		17-01-2015 – 21-01-2015			
Door		Shaun Smit			
Nr.	**Omschrijving**	**Verwacht Resultaat**	**Resultaat**	**Ok/Fout**	**Opmerking**
Multihoming					
1.	Bereikbaarheid Link 1 Traceroute van 192.168.1.3 (172.16.1.3) naar 192.168.2.2 en andersom met 10.10.10.2 als primaire link.	Een connectie met de overzijde via lijn 10.10.10.2	1. 192.168.1.3 2. 192.168.1.1 3. 10.10.10.1 4. 13.13.13.2 5. 192.168.2.2 1. 192.168.2.1 2. 13.13.13.1 3. 10.10.10.2 4. 192.168.1.3	OK	N.v.t
2.	Bereikbaarheid Link 2 Traceroute van 192.168.1.3 (172.16.1.3) naar 192.168.2.2 en andersom met 11.11.11.2 als primaire link	Een connectie met de overzijde via lijn 11.11.11.2	1. 192.168.1.3 2. 192.168.1.1 3. 11.11.11.1 4. 13.13.13.2 5. 192.168.2.2 1. 192.168.2.1 2. 13.13.13.1 3. 11.11.11.2	OK	N.v.t

			4. 192.168.1.3		
3.	Connectieherstel Ping tegelijk: - 192.168.3.2 naar 192.168.1.3 - 192.168.2.2 naar 192.168.1.3 Verwijder de actieve link en tel het aantal verloren pings en meet de hersteltijd van de verbinding. Doet dit met rloc-probing uit	Updaten van de database gebeurt elke 60 seconden. Afhankelijk van het moment waarop de verbinding verbroken wordt duurt het maximaal zestig seconden.	1 ping “request timed out”. Gemiddeld 4 seconden om te herstellen.	OK	De xTR houdt zijn interfaces zelf ook in de gaten, waardoor een update eerder wordt doorgevoerd
4.	Connectieherstel Ping tegelijk: - 192.168.3.2 naar 192.168.1.3 - 192.168.2.2 naar 192.168.1.3 Verwijder de actieve link en tel het aantal verloren pings en meet de hersteltijd van de verbinding. Doet dit met rloc-probing aan	Als de xTR zijn verbindingen uit de map-cache in de gaten houdt met probing wordt verwacht dat het binnen 5 seconden de verbinding wordt herstelt.	1 ping “request timed out”. Gemiddeld 4 seconden om te herstellen.	OK	Aangezien de vorige test ook al 4 seconden was kan het zijn dat rloc-probing in zo’n kleine omgeving geen efffect heeft, maar op het DFZ wel.
5.	Connectieherstel FTP-sessie - 192.168.3.2 naar 192.168.1.3 Verwijder de actieve link en meet de tijd die nodig is om de sessie te laten vervolgen, als dat gebeurt. Doet dit met rloc-probing uit	Updaten van de database gebeurt elke 60 seconden. Afhankelijk van het moment waarop de verbinding verbroken wordt duurt het maximaal zestig seconden.	Gemiddeld 4 seconden nodig om de verbinding te herstellen en door te gaan met versturen.	OK	Zie test drie
6.	Connectieherstel FTP-sessie - 192.168.3.2 naar 192.168.1.3 Verwijder de actieve link en meet de tijd die nodig is om de sessie te laten vervolgen, als dat gebeurt.	Als de xTR zijn verbindingen uit de map-cache in de gaten houdt met probing wordt verwacht dat het binnen 5 seconden de verbinding wordt herstelt.	Gemiddeld 4 seconden nodig om de verbinding te herstellen en door te gaan met versturen.	OK	Zie test vier

	Doet dit met rloc-probing aan				
VM Mobility					
7.	Mapping-system Verplaats server A (192.168.1.3) van netwerk 192.168.1.0/24 naar 192.168.2.0/24 en meet hoe lang het duurt voordat de mapping-system op de hoogte is van de wijziging.	Volgens de documentatie van Cisco dient een LISP router first-hop te zijn voor het realiseren van VM/IP mobility. Dat is hier niet het geval, waardoor het niet zal werken.	Geen resultaten. Niet werkend te krijgen	OK	Naast het niet hebben van een first-hop LISP router is het interne netwerk dat achter NAT zit niet langer bekend bij LISP.
8.	Bereikbaarheid Ping voor de verplaatsing: - 192.168.3.2 naar 192.168.1.3 - 192.168.1.2 naar 192.168.1.3 - 192.168.2.2 naar 192.168.1.3 Ping na de verplaatsing: - 192.168.3.2 naar 192.168.1.3 - 192.168.1.2 naar 192.168.1.3 - 192.168.2.2 naar 192.168.1.3	Volgens de documentatie van Cisco dient een LISP router first-hop te zijn voor het realiseren van VM/IP mobility. Dat is hier niet het geval, waardoor het niet zal werken.	Geen resultaten. Niet werkend te krijgen	OK	Zie test 3
9.	Connectieherstel Start een ftp-download van 192.168.3.2 (host C) naar 192.168.1.3 (server A) terwijl server A zich in SITE-A bevindt. Verplaatst server A naar SITE-B en meet de tijd die nodig is om met de download door te gaan.	Volgens de documentatie van Cisco dient een LISP router first-hop te zijn voor het realiseren van VM/IP mobility. Dat is hier niet het geval, waardoor het niet zal werken.	Geen resultaten. Niet werkend te krijgen	OK	Zie test 3
IPv6 Transitie					
Hoewel er tijdens de vorige opstelling is besloten dat de resultaten van opstelling één overtuigend genoeg waren om de connectiviteit van LISP te garanderen is er toch besloten om nog een korte test uit te voeren, omdat deze opstelling representatief is voor Qi ict klantnetwerken. De koppelingen met centrale firewall zijn omgezet tot IPv6 adressen. Deze omzetting had voor het uitwisselen van informatie via de controle plane geen invloed. Alle LISP-omgevingen waren op de hoogte van elkaar. Wat wel bleek is dat verkeer van de data plane wel werd tegengehouden door de firewall. Wanneer intern IPv4 verkeer wordt voorzien van een IPv6 header door LISP wordt er een UDP checksum van 0 geplaatst. Dit wordt niet geaccepteerd door een Check Point firewall. Dit betekent dat omgevingen waarbij er nog een Check Point firewall voor de xTR wordt geplaatst geen IPv6 netwerk kunnen overbruggen.					

Dit hoort echter niet. Volgens RFC6935 zou een UDP checksum van nul geaccepteerd moeten worden wanneer het om een tunnelprotocol gaat.

Dit is wel een vrij specifieke situatie. Het zal ook niet vaak voorkomen, omdat het grootste gedeelte van het internet nog over IPv4 beschikt, maar het is wel een zeer belangrijk punt voor Qi ict, omdat er ontzettend veel wordt gewerkt met Check Point hardware.

3.4 CONCLUSIE

Het blijkt dat het toevoegen van een firewall wel degelijk invloed heeft op de opstelling. Hoewel multihoming en IPv6 transition werken, op het probleem met de UDP checksum na, werkt multihoming niet. Dit is geen definitieve conclusie want er zijn wel mogelijkheden om dit aan de praat te krijgen met technieken als multihop, maar er zijn geen middelen om dat te testen.

4. CONFIGURATIE OPSTELLING ÉÉN

```
hostname smit-hague-xtr

interface GigabitEthernet 1
    ip address 46.243.40.166 255.255.255.192
    no shutdown

interface GigabitEthernet 2
ip address 153.16.55.225 255.255.255.255
    ipv6 address 2610:D0:21CA::153:16:55:225/128
    no shutdown

ipv6 unicast

router lisp
locator-set BETA
46.243.40.166 priority 1 weight 1

eid-table default instance-id 0
    database-mapping 153.16.55.224/28 locator-set BETA
    database-mapping 2610:D0:21CA::/48 locator-set BETA

ipv4 itr
ipv4 etr
ipv4 itr map-resolver 195.50.116.18
ipv4 itr map-resolver 217.8.98.42
ipv4 itr map-resolver 217.8.98.46
ipv4 itr map-resolver 193.162.145.50
ipv4 etr map-server 195.50.116.18 key smit-hague-xtr
ipv4 etr map-server 217.8.98.42 key smit-hague-xtr
ipv4 etr map-server 217.8.98.46 key smit-hague-xtr
ipv4 etr map-server 193.162.145.50 key smit-hague-xtr
ipv4 use-petr 217.8.98.33 priority 1 weight 100
ipv4 use-petr 193.162.145.46 priority 1 weight 100

ipv6 itr
ipv6 etr
ipv6 itr map-resolver 195.50.116.18
ipv6 itr map-resolver 217.8.98.42
ipv6 itr map-resolver 217.8.98.46
ipv6 itr map-resolver 193.162.145.50
ipv6 etr map-server 195.50.116.18 key smit-hague-xtr
ipv6 etr map-server 217.8.98.42 key smit-hague-xtr
ipv6 etr map-server 217.8.98.46 key smit-hague-xtr
ipv6 etr map-server 193.162.145.50 key smit-hague-xtr
ipv6 use-petr 217.8.98.33 priority 1 weight 100
ipv6 use-petr 193.162.145.46 priority 1 weight 100

ip route 0.0.0.0 0.0.0.0 46.243.40.129
```

5. CONFIGURATIE OPSTELLING TWEE

xTR1

```
hostname xtr1

interface LISP0
!
interface GigabitEthernet0/0
 ip address 11.11.11.2 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 mac-address 0000.0d0e.010c
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 lisp mobility MOBILE-SITE
!
interface GigabitEthernet0/2
 ip address 10.10.10.2 255.255.255.0
 duplex auto
 speed auto
!
!
router lisp
 locator-set SITE-A
  10.10.10.2 priority 1 weight 50
  11.11.11.2 priority 1 weight 50
  exit
 !
 eid-table default instance-id 0
  dynamic-eid MOBILE-SITE
   database-mapping 192.168.1.0/24 locator-set SITE-A
   exit
  !
  exit
 !
 loc-reach-algorithm rloc-probing
 ipv4 use-petr 14.14.14.2
 ipv4 itr map-resolver 12.12.12.2
 ipv4 itr
 ipv4 etr map-server 12.12.12.2 key SITEAKEY
 ipv4 etr
 exit

ip route 0.0.0.0 0.0.0.0 10.10.10.1
ip route 0.0.0.0 0.0.0.0 11.11.11.1
```

xTR2

```
hostname xtr2
!
interface LISP0
!
interface GigabitEthernet0/0
 ip address 13.13.13.2 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 mac-address 0000.0d0e.010c
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
 lisp mobility MOBILE-SITE
!
!
router lisp
 locator-set SITE-B
  13.13.13.2 priority 1 weight 100
  exit
 !
 eid-table default instance-id 0
  database-mapping 192.168.2.0/24 locator-set SITE-B
  dynamic-eid MOBILE-SITE
   database-mapping 192.168.1.0/24 locator-set SITE-B
   map-server 12.12.12.2 key SITEAKEY
   exit
  !
  exit
 !
 loc-reach-algorithm rloc-probing
 ipv4 use-petr 14.14.14.2
 ipv4 itr map-resolver 12.12.12.2
 ipv4 itr
 ipv4 etr map-server 12.12.12.2 key SITEBKEY
 ipv4 etr
 exit
!
ip route 0.0.0.0 0.0.0.0 13.13.13.1
!
```

PxTR

```
!
hostname pxtr
!
!
interface LISP0
!
interface GigabitEthernet1
 ip address 14.14.14.2 255.255.255.0
 negotiation auto
!
interface GigabitEthernet2
 no ip address
```

```
 shutdown
 negotiation auto
!
interface GigabitEthernet3
 ip address 192.168.3.1 255.255.255.0
 negotiation auto
!
router lisp
 map-cache 192.168.1.0/24 map-request
 map-cache 192.168.2.0/24 map-request
 ipv4 proxy-etr
 ipv4 proxy-itr 14.14.14.2
 ipv4 itr map-resolver 12.12.12.2
 exit
!
```

Mapping-system

```
!
hostname mapping-system
!
interface GigabitEthernet1
 ip address 12.12.12.2 255.255.255.0
 negotiation auto
!
interface GigabitEthernet2
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet3
 no ip address
 shutdown
 negotiation auto
!
router lisp
 site SITE-A
  authentication-key SITEAKEY
  eid-prefix 192.168.1.0/24 accept-more-specifics
  exit
 !
 site SITE-B
  authentication-key SITEBKEY
  eid-prefix 192.168.2.0/24 accept-more-specifics
  exit
 !
 ipv4 map-server
 ipv4 map-resolver
 exit
!
ip route 0.0.0.0 0.0.0.0 12.12.12.1
!
```

VII. AANTONEN COMPETENTIES

A1- Analyseren van probleemdomein

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

Voorafgaand aan het onderzoek was er weinig kennis over het onderzoeksonderwerp aanwezig binnen Qi ict. Dit was gelijk ook de probleemstelling van het onderzoek. Om klanten te kunnen adviseren over de laatste ontwikkelingen moet er kennis in huis zijn en die was er op dat moment niet. Het doel van het onderzoek was dan ook om rapporten en demo-opstellingen op te leveren waarmee de kennis kan worden vergroot. Dit was echter niet zo specifiek. Om er ook een TI-probleem bij de betrekken is voorafgaand aan het onderzoek een korte literatuurstudie gedaan om de kernpunten van het onderwerp op papier te zetten. Aan de hand van deze kernpunten heb ik samen met de opdrachtgever wat specifieker kunnen uitwerken wat voor informatie er gezocht wordt. Deze informatie is ook gedocumenteerd in het afstudeerplan en het plan van aanpak.

A3 – Achterhalen van behoeften van belanghebbenden

Activiteiten	Het vaststellen van de behoeften en verwachtingen die de verschillende belanghebbenden hebben van een systeem en het opstellen van een beschrijving van wat een systeem moet doen.
Product	Document met opsomming van behoeften.
Toelichting	Het vergaren van de behoeften van belanghebbenden kan met verschillende middelen gebeuren zoals: - interviews - enquêtes - bestuderen van documentatie - prototype/demo voor afstemmen eisen. - opstellen van een business case
Toetscriteria	1. De belanghebbenden zijn in kaart gebracht. 2. De keuze voor het inzetten van een middel om de benodigde informatie te verkrijgen is beargumenteerd. 3. Het middel is correct toegepast. 4. Er is overeenstemming bereikt met de belanghebbenden over hun behoeften. 5. De behoeften zijn volledig in kaart gebracht.

Bij het schrijven van het plan van aanpak is een stakeholdersanalyse uitgevoerd. Daaruit kwam logischerwijs dat Qi ict en haar klanten belanghebbenden zijn. Beide partijen hebben ten slotte baat bij een goed onderzoek naar een nieuwe techniek. Qi ict beschermt de belangen van de klanten en weet wat zij willen. Bijvoorbeeld het inregelen van multihoming is iets wat op het moment veel voorkomt. Dat is ook een deel van reden geweest om dit onderzoek te starten. Als uitvoerder van het onderzoek was het mijn taak om de behoeften van Qi ict te achterhalen en daarmee indirect die van de klant.

Om dit te doen zijn aan het begin van het onderzoek wekelijkse gesprekken ingepland met het doel om te praten over de voortgang van het onderzoek. Hierbij zijn ook zaken als eisen en wensen geïnventariseerd die later zijn omgezet tot een programma van eisen. Doordat het onderzoek uiteindelijk heeft voldaan aan de eisen heb ik ook voldaan aan de behoeften van de belanghebbenden.

C9 – Ontwerpen van een infrastructuur

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

In het onderzoeksrapport zijn diverse technieken onderzocht waarvoor LISP gebruikt kan worden. De opdrachtgever heeft aangegeven geïnteresseerd te zijn in de werking van deze technieken in de praktijk, omdat de theorie wel eens wat aan de verbeelding overlaat.

Voor het ontwerpen van de opstellingen is geen specifieke ontwerpmethode gekozen. Er is gekeken naar de beschikbare middelen en bepaald wat voor opstellingen daarmee gebouwd kunnen worden die overeenkomen met de eisen en wensen van de opdrachtgever. Hieruit kwamen drie opstellingen tevoorschijn waarmee alle technieken en werkingen van LISP gedemonstreerd kunnen worden. Deze opstellingen zijn in het ontwerprapport toegelicht. Er is een globale topologie toegelicht met daarbij het doel van de opstelling, de benodigdheden en de manier waarop de opstelling getoetst zal worden. In een later stadium, de implementatiefase, is een adviesrapport geschreven waarin de definitieve topologie van de opstellingen is vermeld en de configuraties van de apparatuur.

D18 – Testen van een infrastructuur

Activiteiten	- Het opstellen van een testplan - Het verwerven en opbouwen van de testopstelling - Het uitvoeren van de geplande metingen - Het opstellen van een testrapport
Product	- Testplan - Testopstelling met documentatie - 'how to' testopstelling die de opstelling reproduceerbaar maakt - Testrapport met resultaten
Toelichting	Met het testen wordt aangetoond dat het ontwerp voldoet aan vooraf gestelde eisen (zie A5). Van testen die niet succesvol zijn, dient de oorzaak te worden onderzocht zoals beschreven in taak E23.
Toetscriteria	Het testplan bevat minimaal: - Voorafgestelde eisen die getest moeten worden (bijv. performance, failover) - Vragen die beantwoord moeten worden door de test - De wijze van meten - Metingen die de gestelde eisen moeten aantonen - Verwachte uitkomsten die de gestelde eisen bevestigen of verwerpen Het testrapport bevat minimaal: - Antwoord op de vragen van het testplan - Documentatie die de testopstelling reproduceerbaar maakt - Verslag van het meetproces - Resultaten van de metingen - Conclusies

De drie opstellingen die in het ontwerprapport zijn beschreven hebben ieder een eigen testplan. De format hiervan is geïnspireerd door voorbeelden van ASL-BISL. Voor elke opstelling is in een testplan aangegeven wat het doel is van de opstelling, een toelichting van de testen, de testomgeving, benodigdheden en welke specifieke testen worden uitgevoerd. Daarnaast is bij het uitvoeren van de testen ook het voorbeeld van ASL-BISL gevolgd door alle resultaten overzichtelijk in een tabel op te nemen met de volgende punten:

- Projectinformatie
- Testnummer
- Omschrijving van test
- Verwacht resultaat
- Gemeten resultaat
- GO/NO-GO
- Opmerkingen (Bevindingen die niet onder de gemeten testresultaten vielen, maar wel interessant bleken)

Tevens is bij elke opstelling de definitieve topologie en configuratie genoemd, waardoor de testen reproduceerbaar zijn.

Door middel van het volgen van ASL-BISL voorbeelden is een duidelijk en overzichtelijk beeld gemaakt van de uitgevoerde testen en resultaten. De opdrachtgever was ook erg onder de indruk van de goede documentatie.

H5 – Zelfstandig werken

Activiteiten	Voorbeelden: initiatief vertonen, weinig sturing nodig hebben, niet snel in paniek raken, zelf taken signaleren, een eigen inbreng leveren, je eigen werk overzien als deel van een groter geheel, hoofd- en bijzaken scheiden, anticiperen op ontwikkelingen, dingen zien in hun context, e.d.
Product	Het product van zelfstandig werken is een vorm van gedrag van de student, dat kan worden toegepast op allerlei verschillende ICT-producten.
Toelichting	Professioneel werken houdt in, dat je opdrachtsituaties goed kunt beoordelen en dat je zelfstandig binnen de gestelde tijd en tegen beperkte kosten een prestatie met een hoge kwaliteit kunt leveren, die getuigt van creativiteit.
Toetscriteria	1. Er is gewerkt zonder dat derden vooraf de werkzaamheden gepland hebben (muv. de einddatum) 2. Er is gewerkt zonder dat projectmatige en inhoudelijke methoden en technieken de totstandkoming van het product op detailniveau zijn vastgelegd (vrijheid van handelen) 3. De student heeft zijn taak breder opgevat dan de letterlijke opdracht die hij heeft meegekregen (hij is in staat mee te denken met de opdrachtgever). Dit kan de student illustreren bijvoorbeeld dmv. adviezen die hij gegeven heeft om zaken anders aan te pakken of adviezen over vervolgstappen die genomen kunnen worden. 4. In de planning van het op te leveren product is aantoonbaar rekening gehouden met de hoofd- en bijzaken die betrekking hebben op de totstandkoming van het product.

Van school uit ben ik gewend dat tijdens projecten het einddoel vaak wel zichtbaar is en dat je daarmee vrij gemakkelijk kan inschatten of je op schema loopt of niet. Dat is bij het afstuderen wel even andere koek gebleken. Vooral omdat de opdrachtgever verder ook niet zoveel over het onderwerp af wist. Bij de aanvang van het project waren er drie dingen duidelijk, de begindatum, de einddatum en het feit dat er een onderzoek plaats moest vinden. Het was aan mij de taak om dit zelf te gaan indelen. Ik heb mezelf de eerste twee weken bezig gehouden met gesprekken met de opdrachtgever en het schrijven van een plan van aanpak. Ik heb hier serieus nagedacht over de risico's van een onderzoek naar een experimenteel onderwerp en heb mijn planning daarop aangepast. Zo heb ik mijzelf genoeg speling gegeven voor verschillende fasen van het onderzoek en heb ik wekelijkse gesprekken ingepland met de opdrachtgever.

Om het onderzoek uit te voeren heb ik zelfstandig een keuze gemaakt voor een aanpakmethode. De keuze heb ik in het afstudeerverslag uitgebreid toegelicht. Een belangrijk punt voor mezelf was het zoeken van een goede manier van literatuuronderzoek, omdat er weinig informatie bekend is over het onderwerp. Ik wilde zeker weten dat ik geen informatie mistte en dat is gelukt aan de hand van systematisch literatuur zoeken.

VIII. EMAILCONTACT

EMAIL 1: GREGG SCHUDEL

Dear lisp-engineers,

I've been working with LISP for the last couple of weeks and it works great, but my network is only small and I was wondering how it works on a higher level.

Hi Shaun

Thanks for putting such detailed efforts into your LISP investigations.

The ETR's are sending map-register messages every 60 seconds to a map-server which causes a constant load on the network. In my lab this is not a problem, because I only have a few EID-prefixes that have to be registered, but I was wondering how this behavior affects the lisp beta-network

When a few hundred EID-prefixes are registered every 60 seconds. Does that nog effect the network a lot and put a lot of strain on the mapping-server?

i think you'll find part of your answer in RFC 6830 Map-Register section:
https://tools.ietf.org/html/rfc6830#section-6.1.6

and note in the Map-Register message format that a "single" map-regiater message is quite
capable of registering multiple EID prefixes belonging to this site - up to the "record count" value.

> Record Count: This is the number of records in this Map-Register message. A record is comprised of that portion of the packet labeled 'Record' above and occurs the number of times equal to Record Count.

For the Cisco implementation, we pack all EIDs that share a common map-register header up to a number of mapping records depending on the MTU or max record count (255), whichever comes first.

In your LISP Beta registration you only have two EIDs (v4 and v6), and so it may not be clear.

So from an "ETR perspective", he is very efficient we think on sending Map-Registers.

From a Map-Server perspective, he is likelyk receiving 'numerous' map-register messages from all of his correspondant ETRs, and also sending Map-Notify messages in reply. But still, this "control plan burden" is still quite small typically. Say a router can handle 1000 packets per second — i.e. registrations per second - in the control plane — this would be a very small router - say Cisco 800 even - means you could handle 60,000 ETRs registering.

If one considered using a "server" as an MSMR (and not a router) - and applied more CPU power (say maybe even a cisco CSR1KV virtual router), then they map-registration challenges will seem trival.

Don’t forget that MS/MR also hanlde Map-Requests, and in certain cases, Map-Replies as well. In addition, in the mobilty use-cases, the Map-Server is also sending Map-Notifies for moved-hosts, and handling additional Map-Requests caused by SMRs.

keep us posted on your progress!

Thanks!
Best regards,
Gregg

EMAIL 2: GREGG SCHUDEL

Hi Gregg,

I seem to have found the problem. I had a mobile site defined behind xTR2, but I also have to define the same site als mobile behind xTR1, so that moves can be detected and solicit-map-request can be sent.

:)
gotta like when people solve their own problems :) yes - the dynamic-eid config needs to be on both sides (the “theoretical home site” plus the site it can “move to”) for exactly the reason you describe. when a host moves away, the new site registers the /32, the MS notifies the “old site” — who now knows teh host is “away” — and then when the old site receives packets destined to the “moved /32” — it sends an SMR to the sender of the data - which causes the sender to do Map-Req/Map-Rep updates to map-cache - now having the current location. It’s a few control plane messages but it happens pretty quickly!
(and as you noted, this updates the PITR - so it’s great even for Internet cases where the PITR is the gateway :)

good news!! thank you for the update Shaun!

> As a test I set up a FTP on server A and migrated it while Host C was downloading.
> After a short delay the download continued.
>
> Very awesome!

if you continue posting to LISP Group on linkedin (or your favorite sites) we’d appreciate it!!

LISP is gaining (huge) traction in cisco (finally) - and mobility is one of the key reasons.

keep us posted

Best regards,
Gregg

EMAIL 3: STEFANN ISP

Hi,

Ik heb toch nog een vraag voor u, als u daar tijd voor heeft. Voor mijn onderzoek ben ik ook aan het kijken in hoeverre LISP aantrekkelijk is voor Enterprises en ISP's.
Aangezien uw eigen ISP op basis van LISP is gebouwd heeft u daar vast een idee over.

Uit mijn eigen onderzoek heb ik de conclusie getrokken dat een ISP op basis van LISP een stuk goedkoper is dan de standaard ISP-core dat werkt op basis van BGP/MPLS. Ook is het een stuk eenvoudiger om zaken als multihoming in te regelen. Tevens is er natuurlijk nog de hoofdzaak van LISP om de BGP-tabel-grootte terug te dringen.

Heeft u nog enige toevoegingen op deze conclusie? Nog speciale redenen waarom u voor een ISP op basis van LISP bent gegaan?

Het voordeel van LISP is dat multihoming (en de bijbehorende redundantie en capaciteits-bundeling) mogelijk is zonder dat de gebruiker PI adressen hoeft aan te vragen, zonder dat de gebruiker BGP moet snappen en zonder dat de bijbehorende dure verbindingen nodig zijn. Met LISP kun je dat alles op basis van simpele consumenten-verbindingen doen. Het nadeel is wel dat er meerdere providers nodig zijn. Één of meerdere providers die de fysieke verbinding leveren plus de LISP provider. Daardoor zijn de kosten wat hoger dan bij een normale small-business verbinding, maar lager dan bij een volledige BGP verbinding. LISP is daardoor het interessantste voor middelgrote bedrijven.

Cheers,
Sander