Marika Santa

Verkon migraatio IPv6-verkoksi

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Tieto- ja viestintätekniikan tutkinto-ohjelma
Insinöörityö
14.5.2017

Metropolia

Tekijä Otsikko Sivumäärä Aika	Marika Santa Verkon migraatio IPv6-verkoksi 24 sivua 14.5.2017
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Tieto- ja viestintätekniikka
Pääaine	Communication Networks and Applications
Ohjaaja	Yliopettaja Matti Puska

Insinöörityön tarkoituksena oli kuvitteellisen keskikokoisen suomalaisen liikunta-aiheisia verkkopalveluja tarjoavan yrityksen verkon migraatio IPv6-verkoksi. Lisäksi työssä perehdyttiin IPv6-migraation tietoturvaan.

Insinöörityön tavoitteena oli löytää juuri tälle esimerkkiyritykselle sopivat IPv6-migraatiotekniikat ja toteuttaa ne soveltuvilta osin migraatiotekniikoiden teorioita tukemaan. Tavoitteena oli tuottaa käytännön osaamista oikeiden IPv6-migraatiotekniikoiden ja osoitteiden valinnassa sekä osoittaa käytännössä, kuinka yritys voi päivittää verkkonsa katkottomasti IPv6-yhteensopivaksi.

Työssä käytettiin kahta IPv6-migraatiotekniikkaa: kaksoispinotekniikkaa sisäverkon migraatioon ja IPv4-upotettua IPv6-osoitetekniikkaa yrityksen ulkoverkon migraatioon.

Kaksoispinotekniikkaan sisäverkon osalta päädyttiin lähinnä tekniikan pitkäikäisyyden vuoksi: IPv4-protokollaa tullaan käyttämään vielä pitkään ja kaksoispinototeutuksella ei tarvitse verkkoylläpidossa huolehtia mahdollisista siirtymistä jompaan kumpaan protokollaan, kun konfiguraatio kumpaakin protokollaa varten on kerran toteutettu.

IPv4-upotetun IPv6-osoitetekniikan merkittävimpänä etuna on helppous: yritys voi tavallaan muuntaa tällä tekniikalla olemassa olevat julkiset IPv4-osoitteensa IPv6-osoitteiksi.

Työ koostui kokonaisverkkotopologian suunnittelusta, määrittelystä ja toteutusvaiheesta, johon sisältyi paljon verkkolaitteiden konfiguraatioiden toteutusta kahdella eri protokollalla ja lisäksi näiden konfiguraatioiden testaamista.

Insinöörityön tuloksena syntyi teoriatutkimuksen ja suunnittelun lisäksi käytännön toteutustyö, jossa suunniteltiin IPv4-verkko keskikokoisen yrityksen tarpeisiin ja määriteltiin tämä verkko toimimaan myös IPv6-verkkona ja IPv6-osoitteilla.

Avainsanat	IPv6, migraatio, kaksoispinotekniikka, Dual-Stack

Author Title Number of Pages Date	Marika Santa Migration of the IPv6 network 24 pages 14th May 2017
Degree	Bachelor of Engineering
Degree Programme	Information and Communication Technology
Specialisation option	Communication Networks and Applications
Instructor	Matti Puska, Principal Lecturer

The topic of this thesis is migration of the IPv6 network for an imaginary middle size Finnish company. In addition, this thesis deals with IPv6 migration data security.

The objectives of the study were to find the most suitable IPv6 migration techniques for the company and to implement real migration in a laboratory environment to support the theories presented in this thesis. One of the most important objectives was to increase understanding of real IPv6 migration techniques and selection of suitable IPv6 addresses and to demonstrate how this type of a company can upgrade its network device configurations seamlessly to make them IPv6 compatible.

In this study two migration techniques were used: the dual stack technique for private network migration and the IPv4 embedded IPv6 address technique with the well-known prefix for the public addresses and external network migration. The dual stack technique was chosen mostly because of its long lifecycle. The IPv4 protocol will still be used for long a time and with the dual stack technique the company does not need to worry about whether its network is capable of communicating with other networks no matter what protocols they use.

This study included theoretical studies and practical laboratory work. Network design was put into reality by implementing the configurations for laboratory network devices according to the topology.

The migration study could be further developed by researching IPv6 migration techniques in more detail and testing, comparing and rating them. Also further and more deep research regarding the security of the migration techniques would be useful if this study was to be continued.

Keywords	IPv6, migration, Dual-Stack

Sisällys

Lyhenteet

Dual-Stack IPv6 migraatiomenetelmä, kaksoispinotekniikka. Kaikille verkon laitteille määritellään sekä IPv4- että IPv6-osoite ja konfiguraatiot.

HSRP Hot Standby Router Protocol. Menetelmä, jolla voi parantaa verkon saatavuutta (uptime). HSRP:n avulla verkossa on ikään kuin varajärjestelmä, jonka avulla verkko toipuu nopeasti ja katkottomasti esimerkiksi ensimmäisen hypyn (first hop) epäonnistumisesta. HSRP tekniikan avulla Ciscon reitittimet voivat jakaa MAC ja IP-osoitteensa ja toimia näin yhtenä virtuaalireitittimenä ja tarjota verkolle vakautta, mikäli jokin topologian reitittimistä olisi syystä tai toisesta poissa käytöstä.

IANA Internet Assigned Numbers Authority. Kansainvälinen organisaatio ja viranomainen, joka hallinnoi maailmanlaajuisesti IP-osoitteiden jakelua ja allokointia paikallisille internetosoitteiden jakeluorganisaatioille (RIR).

IEEE 802.1Q Protokolla, jonka avulla Ethernet-verkossa siirretään VLAN-tietoliikennettä.

IETF Internet Engineering Task Force. Kansainvälinen voittoa tavoittelematon organisaatio, jonka päätehtävä on kehittää internetin toimintaa. Se on avoin kaikille toimintaan mukaan haluaville asiantuntijoille. IETF:n työn näkyvimmät tulokset ovat RFC:t eli viralliset dokumentit, joissa tiettyä internetin teknistä toiminnallisuutta kuvataan.

IGP Interior Gateway Protocol. Protokolla, jonka avulla esimerkiksi reitittimet vaihtavat reititystietoja keskenään. Esimerkki IGP:stä on OSPF-tekniikka.

IKE Internet Key Exchange Protocol. IKE on tietoliikenneyhteyksiin liittyvien tietoturva-avainten hallintaprotokolla ja standardi, jota käytetään IPsec-määrittelyjen yhteydessä.

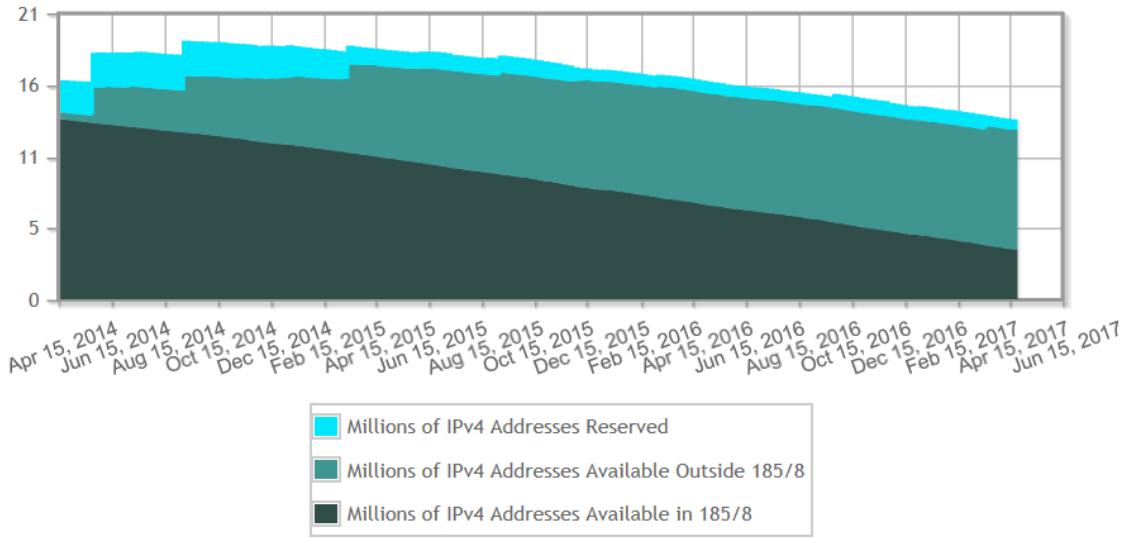
IKE on hybridiprotokolla, joka toteuttaa Oakleyn ja Skemen avaintenvaihtotekniikkaa ISAKMP-viitekehyksessä (framework).

Inter-VLAN	Inter-VLAN:n avulla eri VLAN:t pystyvät siirtämään tietoa keskenään.
IPsec	IP Security. IETF:n kehittämä avoimiin standardeihin perustuva viitekehys (framework), jonka tarkoituksena on suojata sensitiivisen tiedon siirtämistä suojaamattomissa verkoissa, kuten Internetissä. IPsec toimii OSI-mallin verkkokerroksella suojaamassa ja todentamassa IP-paketteja, jotka liikkuvat verkon laitteiden, kuten reitittimien, välillä.
IPv4	Internetprotokollan versio 4. Teknologia, jonka avulla julkisessa tai yksityisessä verkossa olevat laitteet voivat kommunikoida keskenään. Jokaisella verkon laitteella on internetissä toimimiseksi oma, uniikki IP-osoite. IPv4-osoite on 32-bittinen.
IPv6	Internetprotokollan versio 6. IPv4:n tavoin myös teknologia, jonka avulla IPv6-verkon laitteet pystyvät kommunikoimaan keskenään. Myös IPv6:ssa laitteilla on uniikki, numeerinen IPv6-osoite. IPv6-osoite on 128-bittinen.
ISAKMP	Internet Security Association Key Management Protocol. Internetverkon protokolla, joka määrittelee verkkolaitteella toisten verkkolaitteiden tunnistamisen (authentication) käytännöt (procedures) ja luo ja ylläpitää SA:ita (security associations). ISAKMP huolehtii avainten generoinnista ja hallinnoi tietoturvauhkia, kuten palvelunestohyökkäyksiä (denial of service).
ISP	Internet Service Provider. Internetpalveluja tarjoava kaupallinen yritys, esimerkiksi Telia tai Elisa Suomessa.
RFC	Request For Comments. IETF-organisaation kansainvälisen asiantuntijayhteisön tuottama tekninen dokumentti jostakin Internetin toiminnallisuuden osa-alueesta, esimerkiksi IPv6-migraatiosta.
RIR	Regional Internet Registry. Viisi IANA-organisaation valtuuttamaa tahoa IP-osoitteiden alueelliseen hallinnointiin ja jakamiseen. Alueet jakautuvat Eurooppaan (RIPE NCC), Etelä-Amerikkaan ja Karibiaan (LATNIC), Pohjois-Amerikkaan (ARIN), Aasiaan ja Tyynenmeren alueeseen (APNIC) sekä Afrikkaan (AFRINIC).

OSPF	Open Shortest Path First. Link-state IGP-reititysprotokolla. OSPF huomaa muutokset verkkotopologiassa ja osaa vaihtaa nopeasti reititystä laskien uuden, toimivan reitin Dijkstran algoritmilla.
SA	Security Association. Kahden tai useamman kohteen välinen suhde (relationship), joka määrittää miten nämä kohteet hyödyntävät tietoturvapalveluja turvalliseen tiedonsiirtoon. Tällaisia tietoturvapalveluja ovat esimerkiksi 3DES-salaus ja MD5 tai SHA eheyden (”Integrity”) säilyttämiseksi.
TRUNK	Runko, runkoyhteys kytkimien välillä. Trunk-yhteyttä tarvitaan, jotta useiden eri VLAN:ien tietoliikenne reitittyy kytkimien ja reitittimien välillä.
VLAN	Virtual Local Area Network, virtuaalilähiverkko. Tällä tekniikalla voidaan hyödyntää yksi fyysinen verkkolaiteportti, tyypillisimmin reitittimen portti, jakamalla se konfiguraation avulla useammaksi loogiseksi liitännäksi (interface).
VPN	Virtual Private Network. Yksityinen ja suojattu verkko, joka käyttää julkista verkkoa, tyypillisimmin Internetiä, yhdistääkseen useita erillisiä verkkoja toisiinsa. Esimerkkinä yrityksen sisäinen verkko, jota työntekijät käyttävät suojatusti VPN:n avulla Internetin kautta.

1 Johdanto

IPv4-verkon migraatio IPv6-verkkoon on edelleen vuonna 2017 varsin ajankohtainen aihe, sillä viimeiset IPv4-osoitteet ovat jaossa esimerkiksi Euroopassa IP-osoitteita hallinnoivalla organisaatiolla Ripe NCC:llä [51].



Kuva 1. RIPE NCC jaossa olevien viimeisten IPv4-osoitteiden tilanne [51].

Kuvassa 1 näkyy viimeisten jaossa olevien IPv4-osoitteiden tilanne alkuvuodesta 2017. Kuvassa tummimmalla vihreällä osoitetaan osoiteavaruuden 185.0.0.0/8 jäljellä olevien osoitteiden lukumäärää miljoonina. Vaaleampi vihreä kuvaa muiden vapaana olevien osoitteiden lukumäärää. Sininen alue kuvaa varattujen osoitteiden lukumäärää [51]. Suomessa vietettiin kesäkuussa vuonna 2015 kansallista IPv6-käyttöönottopäivää Viestintäviraston johdolla [52].

Tässä insinöörityössä käytetään lähtökohtana kuvitteellista pienehköä suomalaista hyvinvointipalveluille suunnattua verkkopalvelualustaa tarjoavaa yritystä. Työssä perehdytään yrityksen verkkotopologiaan ja IPv6-migraatioon tarvittaviin tekniikoihin ja käytännön tehtäviin. Työn tärkeimpänä tavoitteena on hankkia teoriatietoa ja käytännön kokemusta työelämää varten IPv6-verkkoihin siirtymisestä pohtien lyhyesti myös IPv6-tietoturvanäkökulmia vuonna 2017. Tavoitteena on myös selvittää ne keskeiset tehtävät, jotka täytyy suorittaa, jotta esimerkkiyrityksessä voidaan IPv4-verkon lisäksi käyt-

tää myös IPv6-verkkojen palveluja. Verkkotopologiana käytetään kuvitteellista, mutta täysin toteuttamiskelpoista pienehkön suomalaisen yritysverkon mallia.

Migraatiossa tarvittavat tehtävät selvitetään teoriatiedon hankkimisen lisäksi myöhemmin tässä insinöörityössä kuvattavien tekniikoiden avulla käytännön työnä. Toimivan virtuaalilaitteistoympäristön ja -verkon valmistuttua tavoitteena on tuottaa käytännön esimerkkitoteutus oikeilla verkkolaitteilla ja dokumentoida tehdystä työstä keskeiset ja IPv6-migraation kannalta oleellisimmat havainnot.

2 Esimerkkiyritys

Esimerkkiyritys on kuvitteellinen noin kymmenen työntekijän kasvava digitaalisia hyvinvointipalveluja internetissä tarjoava yritys. Yrityksen toimialaksi valittiin verkossa toimivat liikuntapalvelut, koska toimiala luo puitteet varsin mielenkiintoisen verkkotopologian rakentamiselle ja koska verkkoratkaisussa täytyy miettiä suurien reaaliaikaisten ja tallennettujen multimediadatamäärien siirtoa User Datagram Protocol -protokollan (UDP) avulla. Lisäksi kuvitteellisen yrityksen toimiala ja siihen kehiteltävä verkkoratkaisu voisi tarvittaessa olla toteutettavissa todelliselle tämän toimialan yritykselle.

Esimerkkiyrityksellä on omaa henkilöstöä myynti- ja markkinointitehtävissä, järjestelmäkehitystehtävissä sekä tietoliikenne- ja verkkopalvelujen hallinnoinnissa. Yritys omistaa verkkolaitteet, palvelimet ja työasemat, ja ne sijaitsevat yrityksen omissa tiloissa. Yrityksellä on toimitiloissaan käytössään 100 Mbit/s -internetyhteys yhden palveluntarjoajan kautta.

Yrityksen oma henkilöstö suunnittelee, asentaa, konfiguroi ja ylläpitää etäyhteydellä verkkolaiteympäristöä, joka sijaitsee yrityksen omassa laitehuoneessa. Muutokset verkkolaitteiden konfiguraatioihin tekee ainoastaan yrityksen oma henkilöstö. Yrityksen palvelujen lähdekoodi, versiohallinta ja kehitys- ja testiympäristö sijaitsevat myös yrityksen omissa tiloissa. Ohjelmakoodin tuotantoon siirrot tehdään yrityksen tuotantotestiympäristöstä varsinaiseen tuotantoympäristöön. Yrityksen asiantuntijat työskentelevät sekä yrityksen tiloissa että yrityksen toimitilojen ulkopuolelta Virtual Private Network -yhteyksiä hyödyntäen.

Yrityksen palvelumallin vuoksi nopea ja häiriötön internetyhteys on ensiarvoisen tärkeä samoin kuin tietoturvallinen verkkotopologia, sillä yritys ylläpitää henkilötietolain piiriin kuuluvaa asiakasrekisteriä ja lähettää asiakkaiden maksutapahtumia pankkeihin ja maksujen välittäjäyrityksille.

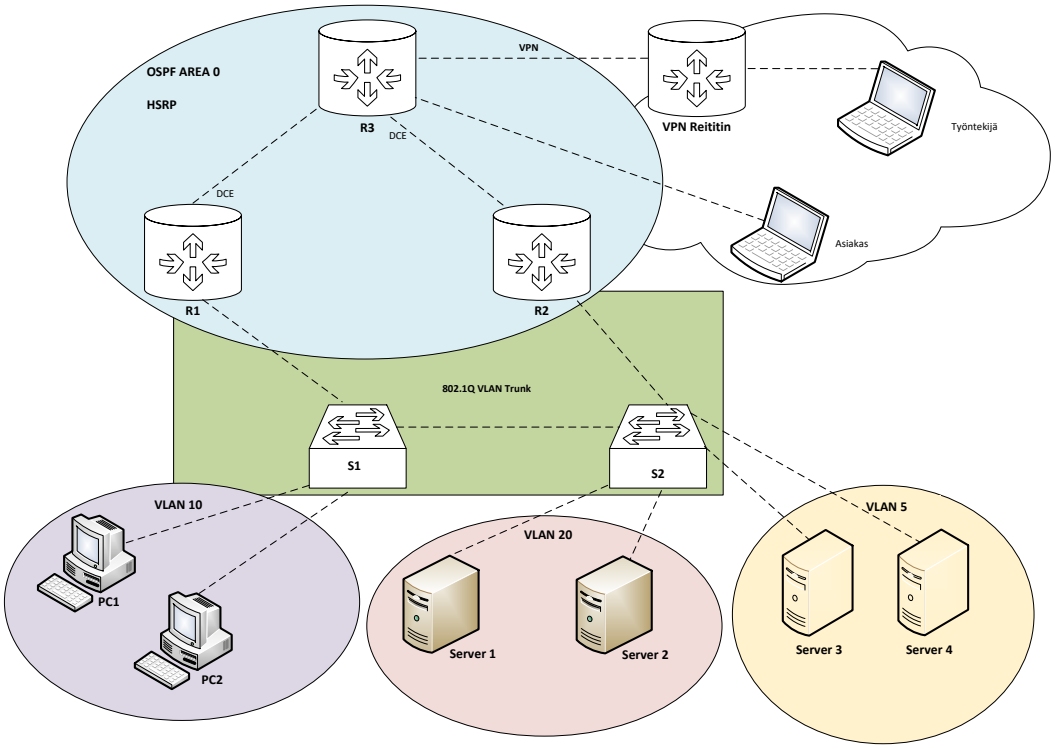
Yrityksen palvelualustalla asiakkaat voivat tarjota erilaisia hyvinvointipalveluja, kuten jooga- ja liikuntatunteja joko suoratoistona tai videotallenteina. Asiakkaiden kannalta on ensiarvoisen tärkeää, että palvelua kyetään tarjoamaan keskeytyksettä mihin kellonaikaan tahansa ja ettei kookkaiden videotallenteiden tarvitsema levytila lopu kesken. Yrityksen palvelut ovat avoimessa internetissä saatavilla, ja loppukäyttäjähallinta hoidetaan IP-protokollan sovelluskerroksessa.

Yrityksen syy migroida IPv6-verkko on liiketoiminnan jatkuvuuden varmistaminen riittävän ajoissa ennen IPv4-palvelujen häviämistä. Yritys haluaa välttää riskit palvelutarjonnan katkoksiin käytettävän verkkotekniikan osalta.

3 Esimerkkiyrityksen verkkotopologia

Esimerkkiyrityksen verkkotopologiaan (kuva 2) valittiin kolme erillistä virtuaalilähiverkkoa, jotta tietoliikenne saadaan eriytettyä asiakkaiden ja yrityksen työntekijöiden kesken. Verkossa on PC-laitteita, palvelimia, tulostimia, kytkimiä ja reitittimiä.

Asiakkailla on pääsy 80- ja 443 Hypertext Transfer Protocol- ja Hypertext Transfer Protocol Secure -tietoliikenteen porteista asiakkaille tarkoitettuun virtuaalilähiverkkoon. Yrityksen työntekijät pääsevät kaikkiin virtuaalilähiverkkoihin sekä yrityksen lähiverkkoon kytkeytyneenä että VPN:n kautta.



Kuva 2. Esimerkkiyrityksen verkkotopologia.

Yrityksen sisäverkossa on käytetty inter-VLAN-reititystä, jossa on 802.1Q-runkoyhteyskonfiguraatio. Käytännössä tämä tarkoittaa sitä, että reitittimen yksi fyysinen portti on jaettu useampaan loogiseen porttiin (subinterface). Tämän metodin avulla on mahdollista kytkeä yhteen ja mahdollistaa tietoliikenne useammasta virtuaalilähiverkosta yhden tai useamman kytkinlaitteen kautta käyttäen vain yhtä fyysistä kytkinporttia. Tämä tekniikka valittiin, jotta topologiassa ei tarvittaisi niin montaa fyysistä laitetta ja liitäntää. Tämä on pienelle yritykselle myös kustannustehokkaampaa laiteinvestoinnin ja ylläpitokustannusten näkökulmasta.

Verkkotopologiassa on käytetty myös yhden alueen OSPF-reititysprotokollaa. Versio 2 on konfiguroitu IPv4-verkkoa varten ja versio 3 IPv6-verkkokonfiguraatiota varten. Reitittimissä käytetään HSRP-tekniikkaa IPv4-verkon osalta. HSRP-tekniikkaa haluttiin käyttää verkon vakauden ja käytettävyyden parantamiseksi. Ciscon mukaan [37] HSRP-tekniikan avulla voidaan saavuttaa lähes 100 prosentin saatavuus reitittimien osalta.

4 IPv6-migraatiotekniikkoja

4.1 Yleistä

Erilaisia IPv6-migraatiomenetelmiä tarvitaan, sillä internetin verkkolaitteet siirtyvät IPv6-osoitteisiin hyvin pitkällä aikavälillä ja siirtymäkauden aikana eri verkkolaitteiden tulee tukea molempia protokollia. Hyvin toteutettu IPv6-migraatio on loppukäyttäjille näkymätön [9]. IPv6-migraatiotekniikat voidaan jakaa kolmeen kategoriaan: kaksoispinotekniikkaan (Dual-Stack), tunnelointiin ja tulkkaukseen (Translation).

4.2 Kaksoispinotekniikka

IPv6-siirtymistekniikoista kaksoispinotekniikka (Dual-Stack) on menetelmä, jossa jokaisella verkon laitteella on sekä IPv4- että IPv6-osoite ja osoitteet toimivat toisistaan riippumattomasti, rinnakkain, kahta TCP/IP-protokollaa käyttäen. Verkon laitteet käyttävät IPv4-osoitetta verkkoyhteyden muodostamiseksi IPv4-verkkolaitteisiin ja IPv6-osoitetta kommunikoidakseen IPv6-solmuihin. Rinnakkaisuus on mahdollista yhdessä ja samassa verkossa, koska kummallakin protokollalla on oma erityinen Layer 2 Ethernet -tyyppinsä.

Kaikki yleisimmät käyttöjärjestelmät käyttävät ensisijaisesti IPv6-osoitetta ja -yhteyttä, mikäli sellainen on saatavilla [13].

Kaksoispinotekniikan hyviä puolia on sen pitkäikäisyys ratkaisuna, IPv4-verkkoja ja verkkolaitteita sekä -palveluja saattaa olla internetissä hyvinkin pitkään, ja niiden toimivuudesta ei tarvitse tällä tekniikalla huolehtia.

Dual-Stack-tekniikan huonoja puolia ovat muun muassa reitittimillä kasvava muistinkulutus, koska reitittimen tulee ylläpitää kahta reititystaulua yhden sijaan. Tämän migraatiotekniikan huonoja puolia ovat myös kalliit ylläpitokulut sekä mahdollisten laiteinvestointien muodossa, koska verkon laitteiden tulee tukea molempia protokollia, muuten tämä migraatiotekniikka ei ole mahdollinen [2, s. 417−419].

Yrityksen verkkotopologiaan voidaan myös joutua tekemään uudelleensuunnittelua ja -toteutusta, mikäli uusia verkkolaitteita joudutaan hankkimaan puuttuvan IPv6-tuen vuoksi tätä migraatiotekniikkaa käytettäessä [30].

4.3 Tunnelointi

Tunnelointitekniikassa IPv6-paketteja siirretään IPv4-verkossa. Tunnelointitekniikat jaetaan kahteen pääkategoriaan: Site-to-Site -tyyppinen tunnelointi ja Remote access -tunnelointi. Site-to-Site -tunnelointitekniikassa tunnelointi yhdistää useita IPv6-verkkoja toisiinsa. Remote access -tunnelointitekniikassa tunnelointi yhdistää yksittäisen IPv6-isäntäkoneen (host) IPv6-verkkoihin [2, s. 419].

IPv6-tunnelointi mahdollistaa IPv6-verkkolaitteiden tiedonsiirron IPv4-verkossa. IPv6-tunneloinnin merkittävin hyöty tulee mahdollisuudesta ottaa verkossa käyttöön IPv6, samalla kun IPv4-verkon yhteensopivuus säilyy verkkolaitteiden kanssa [54].

4.4 Protokollan ja osoitteiden muunnos

Verkko-osoitteen ja -protokollan tulkkaustekniikassa (Network Address Translation-Protocol Translation, NAT-PT) natiivit IPv6-isäntäkoneet, eli koneet, jotka tukevat ainoastaan IPv4-protokollaa, kommunikoivat natiivien IPv4-laitteiden kanssa. Verkkotopologiassa käytetään IPv4- ja IPv6-verkkojen rajalla erityistä NAT-PT-reititintä, johon on konfiguroitu globaalisti reitittyvät IPv4-osoitteet, jotka on dynaamisesti määritelty IPv6-solmuihin.

NAT-PT on IETF:n RFC4966:n mukaan vanhentunutta tekniikkaa, jota ei enää suositella käytettäväksi sen teknisten ja toiminnallisten vaikeuksien ja rajoitteiden vuoksi [2, s. 437−439].

5 IPv6-osoitteet

IPv6-osoite on 128 bittiä pitkä. Sen yleisin esitysmuoto on heksadesimaalimuotoisena lukuna. IPv6-osoite koostuu kahdeksasta hekstetistä eli kahdeksasta 16 bitin kokoisesta heksadesimaaliluvusta, jotka on erotettu toisistaan kaksoispisteellä. Useampi peräkkäinen, pelkkiä nollia sisältävä hekstetti voidaan myös esittää osoitteessa lyhennettynä kahdella peräkkäisellä kaksoispisteellä. IPv6-osoitteen etunollat yksittäisessä hekstetissä ovat vapaaehtoisia [3;26].

IPv6-osoitteen ensimmäiset 64 bittiä ovat yleensä osoitteen verkko-osa ja toiset 64 bittiä liitännän osoiteosa.

Ensimmäinen 16 bitin lohko kertoo IPv6-osoitteesta sen tyypin, kuten onko kyseessä Unique Local-, Multicast-, Link Local-, Global Unicast- vai Loopback-osoite. Näitä erilaisia IPv6-osoitetyyppejä esitellään taulukossa 1.

Taulukko 1. IPv6-osoitetyyppejä [3].

IPv6 osoitteen tyyppi	**Osoitteen ensimmäiset 16 bittiä**
Link Local	FE80−FEBF
Loopback	0000−00FF
Global Unicast	2000−3FFF
Multicast	FF00−FFFF
Unique Local	FC00−FCFF

Vertailun vuoksi: IPv4-osoitteet taas ovat 32 bittiä pitkiä ja ne on totuttu esittämään desimaalilukuina. IPv4-osoite koostuu neljästä oktetista eli neljästä kahdeksan bitin kokoisesta desimaaliluvusta, jotka on erotettu toisistaan pisteellä. 192.168.1.1 ja 10.10.1.2 ovat esimerkkejä IPv4-osoitteista [3].

5.1 Global Unicast -osoitteet

IPv6 Global Unicast -osoitteet vastaavat IPv4-julkisia osoitteita.

2001:0DB8:0001:ACAD:0000:0000:0000:0001/64 on esimerkki internetissä reitittyvästä Global Unicast IPv6 -osoitteesta [3], ja sen rakenne esitellään tarkemmin taulukossa 2.

Toisena esimerkkinä tässä insinöörityössä käytetty 64:FF9B:1::172.2.2.3-osoite on esitelty taulukossa 5.

Taulukko 2. Esimerkki IPv6-osoitteen rakenteesta [3].

IPv6 osoitteen osa	Osoitteen bitit	Selitys
200	1−12	IANA-organisaation globaali reititysnumero
1:0D	12−23	RIR eli Regional Internet Registry -bitit
B8:	23−32	ISP eli Internet Service Provider prefix -bitit
:0001:	32−48	Site Prefix, ISP asettaa
:ACAD:	48−64	Aliverkon prefix, verkon hallinnoija voi asettaa
0000:0000:0000:0001	64−128	Verkon hallinnoija määrittelee loput 64 bittiä

5.2 Link Local -osoitteet

Link Local -osoite on IPv6-unicast -osoite. Kaikilla IPv6-verkon laitteilla on Link Local -osoite. Link Local -osoite voidaan määritellä verkon laitteille manuaalisesti tai se voidaan määrittää automaattisesti. Link Local -osoitteita voi käyttää ainoastaan suoraan toisiinsa kytkettyjen verkkolaitteiden välillä [31].

5.3 Unique Local -osoitteet

Unique Local -osoitteet (ULA) on tarkoitettu ainoastaan sisäisen verkon osoitteiksi, ja ne eivät reitity julkisessa verkossa, mutta ne reitittyvät useammassa sisäisessä verkossa. Tässä insinöörityössä on käytetty ULA-osoitetta sisäverkon osoitteina, ja niiden generoimiseksi hyödynnettiin verkkopalvelua http://unique-local-ipv6.com/ [21].

5.4 Ryhmälähetysosoitteet

IPv6-protokollassa ei ole enää IPv4:stä tuttua Broadcast-osoitetta lainkaan. IPv6:ssa on ryhmälähetysosoitteet (multicast address). RFC 4291 määrittelee IPv6-

ryhmälähetysosoitteen näin: ”Multicast-osoite on tunniste, johon kuuluu useita portteja (interfaces), jotka tyypillisesti kuuluvat eri solmuihin (nodes). TCP/IP-paketti, joka on lähetetty multicast-osoitteeseen, toimitetaan kaikkiin portteihin (interfaces), joilla on kyseisen multicast-osoitteen tunniste.” [42].

Kaikkien IPv6-julkisen verkon solmujen täytyy tukea multicast-osoitteita [41].

6 Migraatioympäristön IP-osoitesuunnitelmat

6.1 Migraation IPv4-osoitteet

Esimerkkiyrityksen IPv4-osoitteiksi valittiin sisäiseen verkkoon yksityisiä IP-osoitteita, jotka eivät reitity internetverkossa, siitäkin huolimatta, että julkisia, ISP:ltä saatavia julkisessa verkossakin reitittyviä osoitteita voisi myös IPv6-sisäverkoissa melko huoletta käyttää niiden runsaan lukumäärän vuoksi. Syy tähän osoitetyyppivalintaan oli lähinnä koulutuksellinen: insinöörityön laatija halusi opetella ja tutustua monentyyppisiin IPv6-osoitteisiin tämän työn myötä.

/24-verkkoja haluttiin käyttää lähinnä niiden yksinkertaisuuden vuoksi. Tämä työ ei kuitenkaan keskity IPv4-osoitteiden optimaaliseen käyttöön ja osoitteiden säästämiseen ja aliverkkojen laskentaan, vaan IPv6-verkon migraatioon, ja siten ei ole perusteltua käyttää ylläpidon kannalta monimutkaisempia vaihtuvamittaisia osoitteita juuri tämän työn fokuksessa. Olen myös omalla työurallani huomannut, etteivät kokeneimmatkaan verkkojen ylläpitäjät juurikaan käytä vaihtuvamittaisia osoitteita sisäverkoissa, vaan /24-verkkojen käyttö on hyvin yleistä ja tavallista.

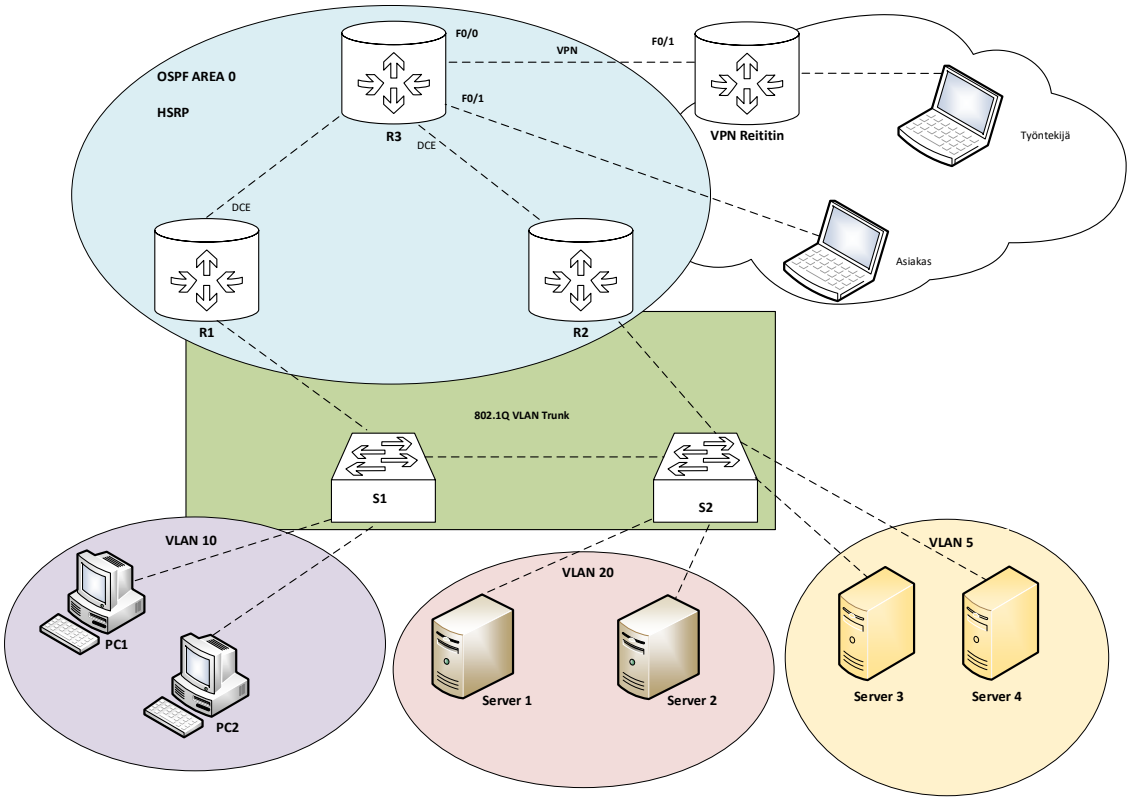
Työssä käytetyt IPv4-osoitesarjat on esitelty taulukossa 3.

Taulukko 3. Esimerkkiyrityksen migraation IPv4-osoitesarjat sisäverkossa.

Käyttötarkoitus	**Isäntänimi**	**Liitäntä**	**Osoitesarja**	**VLAN**
Työntekijöiden työasemat, enintään 100 kpl	PC1−PC100		192.168.10.0/24	VLAN10
Palvelimet yrityk-	Server1−Server10		192.168.20.0/24	VLAN20

sen käyttöön, enintään 20 kpl				
Asiakasverkko, palvelimet, enintään 5 kpl	Server11−Server15		192.168.5.0/24	VLAN5
Rajareititin, internetistä sisään tulevat VPN-yhteydet sisäverkkoon	R3	f0/0	172.2.2.3/24	Ei tarpeellinen
Rajareititin, sisään tulevat internetyhteydet asiakasverkkoon	R3	f0/1	172.3.3.1/24	Ei tarpeellinen
VPN reititin, yrityksen henkilöstön VPN-yhteydet koko yrityksen verkkoon	VPN-reititin	f0/1	172.1.1.2/24	Ei tarpeellinen

Kuvassa 3 näkyvät migraation laitteiden isäntänimet ja oleellisimmat liitännät taulukon 3 laitteille, kuten esimerkiksi rajareititin tunnisteella R1 ja liitännät f0/0 ja f0/1.



Kuva 3. Esimerkkiyrityksen migraation laitteiden isäntänimet ja liitännät verkkotopologiassa.

6.2 Migraation IPv6-osoitteet

6.2.1 Sisäverkko

Koska IPv6-osoiteavaruus on niin valtava, 340 sekstiljoonaa (340 x 10^{36}) käytettävissä olevaa osoitetta, vuonna 2017 ollaan sitä mieltä, että ei ole tarvetta enää säästää IPv6-osoitteita vaan myös yrityksen sisäverkkoon voidaan huoletta valita ISP:ltä saatavat julkiset osoitteet [7].

Esimerkkiyrityksen verkon sisäisiksi IPv6-osoitteiksi valittiin osoiteavaruuden laajuudesta huolimatta Unique Local -osoitteet (ULA), jotta tässä työssä tulisi tekijälle enemmän osaamista erilaisista IPv6-osoitteista. ULA-osoitteet ovat hyvin samankaltaisia

kuin IPv4-verkkojen yksityiset osoitteet. Jokaisella koneella on oma uniikki osoitteensa. ULA-osoitteita on mahdollista reitittää useamman sisäverkon läpi. Ne eivät reitity internetverkossa. ULA-osoitteiden käyttö on järkevää esimerkiksi tilanteessa, jossa verkkopalvelujen tarjoajaa eli ISP:tä vaihdetaan ja verkon julkinen IP-osoitenumerointi muuttuu. Yrityksen sisäisiä IPv6-ULA-osoitteita ei tällaisessa tilanteessa tarvitsisi vaihtaa ja ylläpitotyötä olisi huomattavasti vähemmän verrattuna julkisten osoitteiden hallitsemiseen vaihtotilanteessa [12;19].

Sisäverkon ULA-osoitesarja luotiin sivuston http://simpledns.com/private-ipv6.aspx ULA-osoitegenerointipalvelun avulla, ja ne on esitelty taulukossa 4. Lisäksi sisäverkon IPv6-osoitteissa käytettiin IPv4-verkoista tuttua virtuaalilähiverkon (”VLAN”) numerointia osoitteiden neljännessä hekstetissä selkeyden ja migraation yhdenmukaisuuden vuoksi. Vastaavat VLAN-numeroinnit löytyvät tämän migraatiotyön IPv4-osoitteista.

/64-verkon valinnassa pohdittiin lähinnä IPv6-osoitteiden runsasta lukumäärää ja riittävyyttä, ja siten laajempikin verkko oli mahdollinen. Lisäksi insinöörityön fokus on pyritty koko ajan pitämään migraatioon mahdollistamiseen liittyvissä seikoissa eikä niinkään aliverkon laskentaan liittyvissä asioissa [19].

Taulukko 4. Esimerkkiyrityksen migraatiossa käytetyt IPv6-osoitesarjat sisäverkossa.

Käyttötarkoitus	**Osoitesarja**	**VLAN**
Työntekijöiden työasemat, enintään 100 kpl	FD01:F58C:2A17:**10**::1-64/64	VLAN10
Palvelimet yrityksen käyttöön	FD01:F58C:2A17:**20**::1-A/64	VLAN20
Asiakasverkko, palvelimet	FD01:F58C:2A17:**5**::1-5/64	VLAN5

6.2.2 Ulkoverkko

Ulkoverkon osoitteiksi valittiin internetissä reitittyvät IPv4-upotetut IPv6-osoitteet (IPv4 embedded IPv6 addresses). Tämäntyyppisiä IPv6-osoitteita tuskin pääsisi todellisessa IPv6-migraatiossa valitsemaan, koska osoiteavaruudet jaetaan paikallisten palveluntarjoajien osoiteavaruudesta.

IPv4-upotetut IPv6-osoitteet tulivat käytännön konfiguraatiotyössä hieman yllätyksellisesti mukaan toiseksi migraatiomenetelmäksi, kun työssä joutui konkreettisesti pohtimaan sopivia osoitevalintoja julkisessa verkossa reitittyviksi osoitteiksi. Puoltavia seikkoja tämäntyyppisille julkisille osoitteille on esimerkiksi niiden käyttökelpoisuus verkkolaitteissa, jotka tukevat edelleen ainoastaan IPv4-protokollaa, ja helppous, koska yritys voi muuntaa olemassa olevat julkiset IPv4-osoitteensa IPv6-osoitteiksi, toki sillä edellytyksellä, että käytettävä osoiteavaruus on varattavissa paikalliselta IPv6-osoitteiden myöntäjältä [10]. Tämän insinöörityön migraation oleellisimmat julkisen verkon osoitteet on esitelty taulukossa 5.

Taulukko 5. Esimerkkiyrityksen migraation IPv6-osoitteet julkiseen verkkoon.

Käyttötarkoitus	**Laitteen tunniste kuvassa 3**	**Liitäntä**	**Osoite**
Rajareititin, sisään tulevat VPN-yhteydet sisäverkkoon	R3	f0/0	64:ff9b::172.2.2.3/96
Rajareititin, sisään tulevat internetyhteydet asiakasverkkoon	R3	f0/1	64:ff9b:2::172.3.3.1/96
VPN-reititin, yrityksen henkilöstön sisään tulevat yhteydet koko sisäverkkoon	VPN-reititin	f0/1	64:ff9b:4::172.1.1.2/96

IPv4-upotetussa IPv6-osoitteessa Well-Known Prefix -osuus koostuu heksadesimaaleista 64:ff9b::/96, seuraava osa koostuu IPv4-osoitteesta positioissa 96−127 ja koko osoite näiden yhdistelmästä. Esimerkkinä on osoite 64:ff9b::172.2.2.3 kuvassa 4.

```
+------------------+--------------+---------------------------+
| Well-Known Prefix | IPv4 address | IPv4-Embedded IPv6 address |
+------------------+--------------+---------------------------+
| 64:ff9b::/96      |  172.2.2.3   | 64:ff9b::172.2.2.3         |
+------------------+--------------+---------------------------+
```

Kuva 4. Well-Known Prefix ja IPv4-upotettu IPv6-osoite [23].

7 IPv6-migraation tietoturvanäkökulmia

Siinä missä IPv6-osoitteiden lukumäärä verrattuna IPv4-osoitteiden määrään saattaa tuntua potentiaaliselta mahdollisuudelta laajentaa internetin käyttöä esimerkiksi esineiden internetiksi (internet of things, IoT), se tuo mukanaan myös uudenlaisia haasteita. Verkkorikollisilla on entistä paremmat mahdollisuudet suojautua viranomaisten seurannalta (tracking) vaihtamalla entistä laajemmasta osoiteavaruudesta uusia osoitteita verkkojälkien peittämiseksi. Myös monet verkkojen tietoturvakontrollit käyttävät hyödykseen IP-osoitteiden niin sanottuja mustia listoja (blacklist). Tällaiset listat muuttuvat melko hyödyttömiksi, tai ainakin ne tuovat mukanaan melkoisen suorituskykyhaasteen listojen läpikäymiseksi, kun pelkästään yhden pienen yrityksen verkon käyttöön voi olla allokoituna miljoonia IPv6-osoitteita [59;61].

Merkittävä IPv6-verkon haavoittuvuus tulee verkkojen ylläpitäjien IPv6-tietoturvaan liittyvän tiedon puuttumisesta. Yritysten tulisi nyt ja ainakin ennen IPv6-verkon migraatiota hankkia verkkoasiantuntijoilleen riittävä koulutus ja osaaminen IPv6-tietoturvasta. Verkon tietoturvan näkökulmasta on vaarallista tuudittautua olettamukseen, että IPv6 on vain kopio tai samankaltainen, mutta uudistettu versio IPv4:stä [58].

Toinen potentiaalinen merkittävä haavoittuvuus IPv6-migraatioissa liittyy siihen, että useimmissa käyttöjärjestelmissä IPv6 on käytössä oletuksena ja IPv6-tietoliikenne saattaa olla toiminnassa jopa ilman verkon ylläpitäjän tai loppukäyttäjän toimenpiteitä. IPv4-verkko ilman IPv6-migraatiota voi siis sellaisenaan olla jo altis IPv6-tietoturvahyökkäyksille, jos joissain verkon laitteissa on oletuksena IPv6 käytössä. Laitteet voivat esimerkiksi lähettää verkkoon IPv6-paketteja ja laitteen liitännät (socket) voivat olla auki. Useimmiten IPv6 on järjestelmissä ensisijainen protokolla, jota käytetään, jos se vain on saatavilla. Linux, BSD, Mac OS X, Microsoft Windows, iOS ja Android kaikki tukevat jo IPv6:ta [2, s. 440−441, s. 463;59].

Vaikka yrityksen verkko olisikin edelleen periaatteessa pelkkä IPv4-verkko, on syytä ottaa käyttöön IPv6-palomuurisäännöt ja IPv6-monitorointi, jotta verkossa mahdollisesti, ja lähes varmasti, tapahtuvaa IPv6-tietoliikennettä voidaan seurata, kontrolloida ja analysoida [59].

Natiivi IPv6-yhteys internetpalveluntarjoajalta on aina parempi ratkaisu kuin IPv6-tietoliikenteen tunnelointi IPv4-verkossa. Tunnelointi lisää monimutkaisuutta tietoturvatarpeisiin ja siten todennäköisyyttä esimerkiksi palvelunestohyökkäyksille ja man-in-the-middle -tyyppisille verkkohyökkäyksille [58].

Kun IPv6-migraatioita tehdään, IPv6-tietoturvakonfiguraatiot saattavat jäädä tekemättä tai huomiotta, samalla kun yritysverkon IPv4-tietoturvakonfiguraatiot ovat moitteettomassa kunnossa. Kaikissa markkinoilla olevissa tietoturvaohjelmistoissa ei välttämättä ole IPv6-tukea lainkaan tai se on puutteellinen verrattuna vastaavaan IPv4-tukeen [2, s. 440−441].

IPv4-protokolla on ollut käytössä hyvin pitkään, ja sitä tukemaan ohjelmoidut käyttöjärjestelmät, palomuuriohjelmistot ja tietoturvaohjelmistot on saatu vuosikymmenien aikana toimimaan melko virheettömästi ja stabiilisti. Kun näitä järjestelmiä ja ohjelmistoja nyt uudistetaan IPv6:ta varten, uusien virheiden ja haavoittuvuuksien mahdollisuus lisääntyy. On myös mahdollista, ettei edes kaikkia IPv6-haavoittuvuuksia ole osattu vielä ennakoida ja ottaa huomioon [58].

On IPv6-tietoturvassa joitain etujakin, esimerkiksi IPsec (”Internet Protocol Security”), joka on alun perin kehitetty juuri IPv6:ta varten ja sen jälkeen sovellettu (back-engineered) IPv4:lle. Toisin kuin IPv4:ssa, IPsec on pakollinen IPv6:ssa [61].

8 Migraation toteutus käytännössä

8.1 Yleistä

Insinöörityön empiirinen tutkimus osoittaa, ettei alkuperäistä IPv4-verkolle suunniteltua laitekantaa ja verkkotopologiaa tarvinnut päivittää tai vaihtaa migraation vuoksi. Kaikille tarvittaville laitteille oli mahdollista määritellä kahden protokollan osoitteet ja toiminnallisuudet.

Hieman yllätyksellisesti käytännön konfigurointityön myötä kävi ilmi, että migraatiossa käytetäänkin kahta migraatiotekniikkaa alkuperäisen suunnitelman eli yhden migraa-

tiotekniikan sijaan. Ulkoverkkoon valittu IPv4-upotettu IPv6-osoitetekniikka helpottaa yrityksen verkon ylläpitäjiä IPv6-siirtymävaiheessa, lähinnä koska siinä on tuttuja osia IPv4-osoitteesta. IPv6-osoitteet ovat hyvin erilaisia verrattuna IPv4-osoitteisiin, ja on inhimillistä, että verkon ylläpitäminen on työläämpää juuri osoitteiden erilaisuuden vuoksi. Tässä työssä pyrittiin helpottamaan siirtymävaiheen hallintatyötä osoite- ja migraatiovalinnalla.

Ilahduttava huomio IPv6-tietoturvan kannalta oikeilla verkkolaitteilla oli, että oletusarvoisesti loogiset IPv6-verkkoliitännät olivat passiivisia ja poissa käytöstä.

8.2 Suunnittelu

Käytännön laitelaboratoriotyön toteutuksen suunnittelun pohjana käytettiin jo tehtyä suunnittelua simulointiohjelman toteutusta varten ja siihen liittynyttä valmista konfigurointiointoteutusta. Simulointiohjelmasta oli mahdollista tallentaa valmiit laitekonfiguraatiot. Niitä hiukan muokkaamalla, kuten liityntöjen (interface) kirjoitusasua muuttamalla, konfiguraatiot oli kuitenkin mahdollista siirtää lähes sellaisinaan oikeille verkon laitteille.

Vaikka valmiiden konfiguraatioiden siirto ehkä kuulostaa helpolta ja nopeasti toteutettavalta työvaiheelta, se ei sitä käytännössä ollut. Yllättävän paljon oli edessä vielä iterointia ja konfiguraatioiden viimeistelyä ja etenkin testausta ja ongelmanselvitystä.

8.3 Simulointi

Kaikki Cisco-konfiguraatiokomennot, IOS-versiot ja IPv6-osoitetyypit eivät toimineet Packet Tracer -simulointiohjelmassa, ja jonkin verran täytyi tehdä iterointia, jotta oikeat konfiguraatiot löytyivät. Esimerkiksi konfigurointityön alussa oli tarkoitus käyttää IPv4-mapped-osoitteita, joita ei pystynyt PT-ohjelmassa käyttämään. Julkisten IPv6-osoitteiden empiirinen osuus jäi työn laitelaboratoriovaiheeseen kokonaisuudessaan.

PT-simulointiohjelman käyttö helpotti ehdottomasti työn ohessa tehdyn insinöörityön empiiristä osuutta erilaisten konfiguraatioiden mieleen palauttamisessa ja testaamises-

sa, joskin ajallisesti siitä ei ollut hyötyä. Enemmän aikaa meni Cisco-laitelaboratorion konfiguraatioiden toimintakuntoon saattamisessa.

8.4 Toteutus

8.4.1 Virtuaaliset lähiverkot

Verkkoympäristö jaettiin kolmeen virtuaaliseen lähiverkkoon (VLAN). Yksi oli tarkoitettu esimerkkiyrityksen työntekijöille, ja siihen suunniteltiin enintään sadan verkkolaitteen määrä. Toinen VLAN oli tarkoitettu esimerkkiyrityksen palvelimille, ja siihen suunniteltiin enintään kymmenen verkkolaitetta. Kolmas VLAN oli suunniteltu enintään viidelle verkkolaitteelle, ja se oli asiakasverkko, jossa yrityksen internet-palvelut tarjottiin. Käytännön toteutuksessa käytettiin kahta kytkintä ja niihin yhdistettyjä kahta reititintä. Reitittimien liitännöille määritettiin 802.1Q-runkoverkkopohjainen Inter-VLAN-reititys (802.1Q trunk-based inter-VLAN routing). Kytkimien välissä oli runkoverkkopohjainen määrittely (trunk).

Inter-VLAN -määrittely mahdollistaa yhden fyysisen liitännän jakamisen useiksi loogiseksi liitännäksi. Lisäksi se mahdollistaa usean VLAN:n reitittämisen verkkotopologiassa, jossa on yksi tai useampi kytkin mutta yksi reititinliityntä [4, Lab 5.1.3.7].

Kytkimien välille määritelty runkoyhteys (trunk) mahdollisti niin ikään useamman VLAN:n reitittämisen yhden linjan kautta. Verkkolaitelaboratoriossa eri VLAN:hin liittyviä verkkolaitteita, kuten palvelimia ja työasemia, määriteltiin minimimäärä testejä varten eli vain yksi isäntäkone yhtä VLAN:ia kohden. VLAN:ien toimivuutta testattiin VLAN-konfiguraatiot listaavilla Cisco IOS -komennoilla sekä TCP/IP-protokollan *ping*-komennolla, jolla voi kokeilla halutun verkkolaitteen saavutettavuutta [55].

8.4.2 HSRP

Oikeat verkkolaitteet eivät tukeneet kaikkia topologiaan suunniteltuja toiminnallisuuksia IPv6-osoitteilla. Esimerkiksi HSRP-protokollaa ei pystynyt konfiguroimaan IPv6:lle lainkaan. Sen edellytyksenä on HSRP-versio 2, jota laboratorion reitittimiltä ei löytynyt.

Näin ollen HSRP konfiguraatio toteutettiin ja testattiin vain IPv4-protokollalla. Tällä puutteella ei kuitenkaan ollut migraation kannalta oleellista merkitystä.

Verkkotopologiassa VLAN 10:n laitteilla on oletusyhdyskäytävälaitteena reititin R1 ja VLAN 20:n ja VLAN 5:n laitteilla reititin R3, joka on havainnollistettu kuvassa 3.

HSRP valittiin, jotta verkon työasemilla ja palvelimilla olisi todennäköisemmin oletusyhdyskäytäväreititin saatavilla myös tilanteessa, jossa esimerkiksi verkon jompikumpi kytkin vikaantuisi [5, Lab 2.4.3.4].

Show standby brief -komentojen avulla todennettiin reitittimillä R1 ja R2, että tallennetut konfiguraatiot olivat oikein. Reititin R1 oli määritelty prioriteetiltaan korkeammaksi HSRP:ssä, ja komento osoitti R1-reitittimen olevan tämän reititysprotokollan aktiivinen reititin, kuten pitikin.

HSRP-toteutusta testattiin myös tutkimalla ensin VLAN 10:n työaseman käyttämää reittiä R3-rajareitittimen internet-yhteyden liitännälle f0/0. Tämä tehtiin Cisco IOS -komennolla *tracert*. Tämän testin avulla nähtiin, että kyseinen työasema käyttää reittiinsä oletusyhdyskäytävää eli reititintä R1. Tämän jälkeen fyysinen kaapelointi poistettiin reitittimen R1 ja kytkimen S1 väliltä, mikä aiheutti tietoliikenneyhteyden katkeamisen laitteiden väliltä. Kun *tracert*-komento uusittiin, nähtiin, että sama työasema sai yhteyden käyttäen reittiä verkon toisen oletusyhdyskäytävän, eli reitin R2:n kautta.

8. 4.3 OSPF

OSPF2- ja OSPF3-konfigurointityö sujui ilman mainittavia ongelmia. Joitakin kirjoitusvirheitä tuli kummankin protokollan osoitteiden kanssa OSPF-määrittelyjen yhteydessä, ja niiden selvittäminen oli yllättävän työlästä.

OSPF3-konfigurointityö on hieman nopeampaa verrattuna OSPF2:een, koska verkon (network) määrityskomennot ovat jääneet kokonaan pois ja OSPF3-reititystä varten määritellään vain reitittimien liitännät.

OSPF-ratkaisuksi valittiin yhden alueen OSPF, molempia protokollia varten. Usean alueen OSPF:lle ei ollut tarvetta, koska insinöörityön aiheena oli kuitenkin IPv6-migraatio ja tärkein osuus myös OSPF:ssä oli osoittaa IPv6-verkon migraatiotyöt siihen liittyen, ei niinkään OSPF-ratkaisun monimutkaisuus.

Molempien protokollien OSPF-määrittelyjä testattiin *ping*-komennon avulla. Tällä varmistettiin, että eri VLAN:ien työasemien ja palvelimien välinen tietoliikenne toimi ja laitteet olivat saatavilla toisilleen.

OSPF3-määrittelyjen oikeellisuutta tarkasteltiin *show ip/ipv6 ospf neighbor* -komennon avulla. Kukin OSPF2- ja OSPF3-määritelty reititin listasi oikein reititysprotokollan kaksi muuta reititintä naapurikseen tällä komennolla.

OSPF2-komennolla laitteen naapuritunnisteena (neighbor id) listautui laitteen OSPF2-liitännän IP-osoite. OSPF3-komennolla naapuritunnisteeksi listautui reitittimen ospf-tunniste (router-id), joka oli aiemmin jokaiselle ospf-reitittimelle erikseen määritelty.

8.4.4 IPv6 VPN-tunnelointi

Mielenkiintoisin osuus käytännön toteutuksesta oli IPv6-tekniikalla toteutettu Ipsec Site-to-Site VPN VTI -tunnelointi.

IPsec on toiminnallisuuksiltaan samanlainen IPv4:ssa ja IPv6:ssa, mutta Site-to-Site -tunnelointimoodi on mahdollista vain IPv6:ssa. Tämä oli myös syy, miksi juuri tämä IPv6-VPN -menetelmä valittiin tähän insinöörityöhön: tämän VPN-ratkaisun avulla oli mahdollista oppia uutta [44].

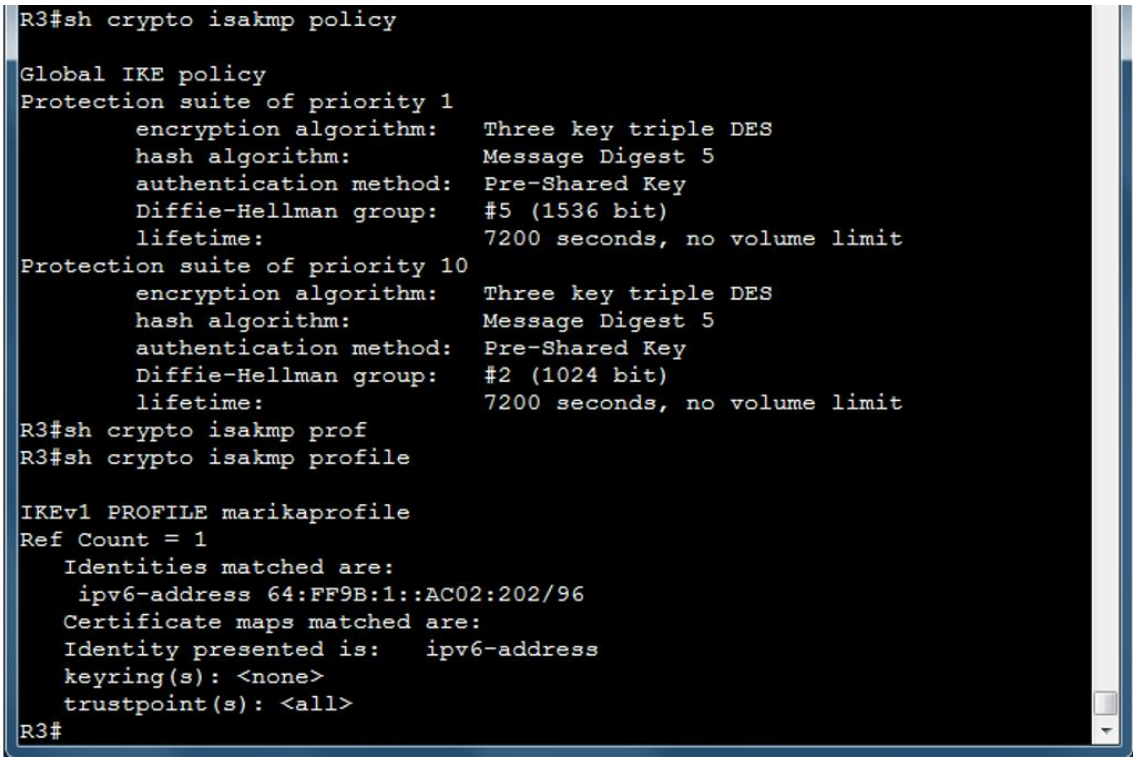
VPN:n toteutus alkoi IKE-menettelytavan (internet key exchange policy) ja Pre-Shared-avaimien määrittelyllä Ciscon sivuilta löytyneen mainion konfigurointiesimerkin avulla. IKE-menettelytapa määriteltiin samanlaiseksi molemmille VPN-tunnelin reitittimille. Menettelytavan määrittelyssä reitittimille kerrotaan esimerkiksi, millaista salaustapaa käytetään. IKE:n määrittelyssä oli migraatiossa syytä olla tarkkana, koska samoilla parametreilla oli samoille reitittimille määritelty myös IPv4 VPN.

Yhteyden aloittava reititin lähettää vastaanottavalle reitittimelle kaikki IKE-määrittelyt (policy) jotka sillä on, ja vastaanottava reititin koettaa löytää vastinparin. Vastaanottava reititin (remote Peer) aloittaa yhteyden muodostamisvaiheessa (IKE negotiation) korkeimman prioriteetin IKE-määrittelystään ja koettaa löytää sille vastinparin vastaanottamistaan tiedoista jatkaen prioriteettilistaa laskevassa järjestyksessä. Numero 1 on korkein prioriteetti. Tässä insinöörityössä IPv4-IKE:ssä oli prioriteetti numero 1 ja IPv6-IKE:ssä prioriteetti numero 10. Eri IP-protokollan määrittelyissä on syytä huomioida, että niillä ei ole päällekkäiset IKE-prioriteettinumerot [44, s.193].

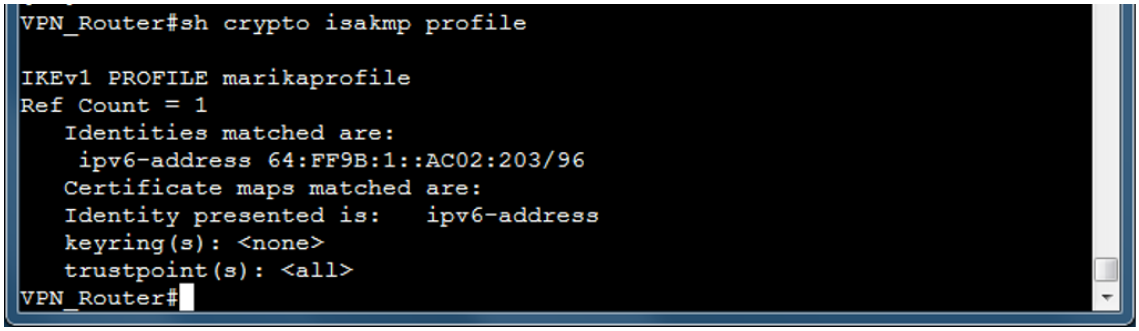
Seuraavaksi määriteltiin IPv4:n kaltaiset IPsec Transform Set- ja IPsec ISAKMP -profiili (IP security internet security association key management protocol profile). Nämä nimettiin erinimisiksi kuin IPv4-määrittelyissä selkeyden vuoksi.

ISAKMP-profiilin identiteetin (identity) arvoksi liitetty IPv6-osoite on Cisco-reitittimillä oletuksena vastapuolen tunnelin osoite. Se voi olla myös isäntänimi, mutta identiteetin arvojen tulee olla yhteneväiset molemmilla reitittimillä. Toisella reitittimellä ei voi olla määritettynä isäntänimeä ja toisella IPv6-osoitetta.

Kuvissa 5 ja 6 on esimerkkejä IKE- ja ISAKMP-määrittelyistä tässä insinöörityössä.

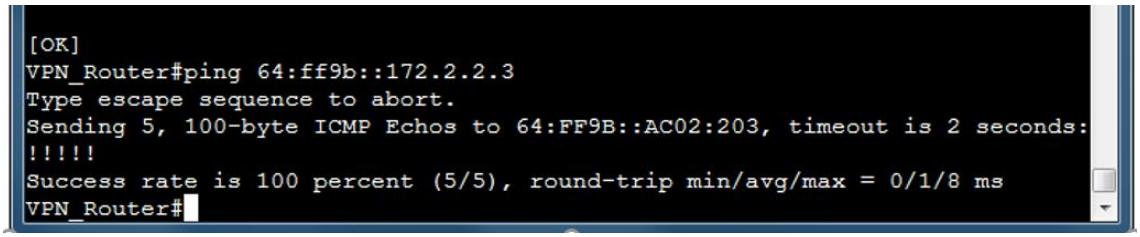


Kuva 5. R3-rajareitittimen IPv6-VPN -konfiguraatioita.



Kuva 6. VPN-reitittimen IPv6-VPN -profiilin konfiguraatio.

Lopuksi määriteltiin tunnelin osoitteet molemmille reitittimille. Kuvassa 7 näkyy onnistunut yhteys VPN-reitittimeltä R3-rajareitittimelle.



Kuva 7. Onnistunut IPv6-VPN -yhteys VPN-reitittimeltä R3-rajareitittimelle.

9 Johtopäätökset

Insinöörityö kartoitti yhden mahdollisen tavan, kahdella eri migraatiotekniikalla, tehdä keskikokoisessa internetpalveluja tarjoavassa yrityksessä siirtyminen IPv6-osoitteiden ja verkon käyttöön.

Tärkein tavoite tälle työlle oli hankkia mahdollisimman paljon teoriatietoa ja käytännön kokemusta IPv6-osoitteista ja IPv6-verkkomigraatiosta. Lisäksi tutkimuksen kohteena oli migraation toteuttaminen ilman tietoliikennekatkosta esimerkkiyrityksessä. Tämä tavoite toteutui hyvin. Molempien IP-protokollien mukainen verkkoympäristö oli mahdollista toteuttaa laitteille ilman, että laitteita esimerkiksi olisi tarvinnut uudelleen käynnistää.

Työn toteuttajan lähtötilanne ja osaaminen aiheesta oli aika lailla olematon. Työn myötä tuli melko kattavasti tutustuttua erilaisiin IPv6-osoitteisiin, niiden rakenteeseen ja käyttötarkoituksiin. Lisäksi työn käytännön toteutus tuotti arvokasta osaamista ja ymmärrystä verkon IPv6-migraation vaiheista ja haasteistakin. Insinöörityö toi ehdottomasti hyötyjä työn toteuttajan päivittäiseen työhön tietoliikennetekniikan IPv6-osa-alueen tuntemuksen myötä. Toimiminen tietoliikenneaiheisissa projekteissa projektijohtajan roolissa verkkoasiantuntijoiden kanssa helpottui, esimerkiksi VPN-yhteyksien ongelmanselvityksessä pystyy nyt hyödyntämään omaakin osaamistaan ja ohjaamaan asiantuntijoiden työtä oikeaan suuntaan.

Myös IPv6-migraatioprojektien johtamistyöhön tuli tämän insinöörityön myötä osaamista ja projektien onnistumisen todennäköisyyttä, jollaista ilman tämän työn tekemistä ei olisi olemassa.

IPv6-migraatiosta ei ole vielä vuonna 2017 kovin paljoa olemassa kirjallisuutta, jota voisi suoraan hyödyntää yrityksissä IPv6-käyttöönotossa. Tällä insinöörityöllä pyrittiin mahdollisimman selkeästi kuvaamaan sitä käytännön työtä, joka yrityksen tulee tehdä siirtyessään IPv6-protokollan käyttöön. Ilman tätä insinöörityötä ei olisi käyttökelpoista ja käytännönläheistä tutkimustyötä ja käytännön toteutusta verkon migraatiosta IPv6-verkoksi. Ei olisi myöskään suomenkielistä dokumenttia, kuinka tällaisen migraation voi toteuttaa. Aiheesta ei vielä ole kovin paljoa käytännönläheistä dokumentaatiota, varsinkaan suomen kielellä.

Tätä insinöörityötä voisi jatkaa ja edelleen kehittää tutkimalla useampia mahdollisia migraatiotekniikoita, niiden hyviä ja huonoja puolia, sekä testaamalla niitä käytännössä. Ne olisi hyvä toteuttaa oikeassa yrityksessä ja verkkoympäristössä. Olisi hyödyllistä tehdä oikea migraatio ISP:ltä saaduilla, oikeasti internetissä reitittyvillä osoitteilla. Lisäksi työtä voisi jatkaa pohtimalla ja selvittämällä käytännössä lisää IPv6-haavoittuvuuksia ja käytännön tietoturvatoimenpiteitä.

Lähteet

1 Davies, Joseph. 2012. Understanding IPv6. California. O´Reilly Media Inc.

2 Hogg, Scott ja Vyncke, Eric. 2011. IPv6 Security. Indianapolis. Cisco Press.

3 Cisco CCNA1 kurssi- ja laboratoriotehtävämateriaali, Lab PDF dokumentit numerot 0.0.0.1 – 11.4.2.8.

4 Cisco CCNA2 kurssi- ja laboratoriotehtävämateriaali, Lab PDF dokumentit numerot 0.0.0.1 – 11.3.1.5.

5 Cisco CCNA3 kurssi- ja laboratoriotehtävämateriaali Lab PDF dokumentit numerot 2.4.3.4 – 6.2.3.8.

6 Kansallinen IPv6:n käyttöönottopäivä 9.6.2015-seminaari. 2015. Verkkodokumentti. Viestintävirasto. <https://www.viestintavirasto.fi/ipv6seminaari2015/index.html>. Luettu 7.9.2016.

7 IPv6. Verkkodokumentti. Wikimedia Foundation. <https://fi.wikipedia.org/wiki/IPv6>. Luettu 7.9.2016.

8 Packet Tracer Lab 6 – Remote Access VPN. 2015. Verkkodokumentti. RemoteTrainingSolutions. <https://www.youtube.com/watch?v=lkUq6Pl6his>. 4.5.2015. Luettu 7.9.2016.

9 Understanding Dual Stacking of IPv4 and IPv6 Unicast Addresses. 2015. Verkkodokumentti. Juniper Networks. <http://www.juniper.net/documentation/en_US/junos15.1/topics/concept/ipv6-dual-stack-understanding.html>. 17.4.2015. Luettu 1.1.2017.

10 Kozierok, Charles M. 2005. IPv6/IPv4 Address Embedding. Verkkodokumentti. <http://www.tcpipguide.com/free/t_IPv6IPv4AddressEmbedding-2.htm>. 20.9.2005. Luettu 12.9.2016.

11 Hogg, Scott. 2007. Dual stack where you can; tunnel where you must. Verkkodokumentti. <http://www.networkworld.com/article/2285078/tech-primers/ipv6--dual-stack-where-you-can--tunnel-where-you-must.html>. 5.9.2007. Luettu 1.1.2017.

12 Johnson, Alastair. 2011. IPv6 Transition Technologies. Verkkodokumentti. <http://www.menog.org/presentations/menog-10/Alastair%20Johnson%20-%20IPv6%20Transition%20Technologies.pdf>. Huhtikuu 2011. Luettu 1.1.2017.

13 Dual Stack Network. 2017. Verkkodokumentti. Techopedia Inc. <https://www.techopedia.com/definition/19025/dual-stack-network>. Luettu 1.1.2017.

14 Chapter: Configuring VPNs Using an IPSec Tunnel and Generic Routing Encapsulation. Verkkodokumentti. Cisco. <http://www.cisco.com/c/en/us/td/docs/routers/access/1800/1801/software/configuration/guide/scg/vpngre.html#48743>. Luettu 3.9.2016.

15 Chapter: Site-to-Site and Extranet VPN Business Scenarios. Verkkodokumentti. Cisco. <http://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342site3.html>. Luettu 3.9.2016.

16 Steps to configure an IPSEC site to site VPN on a Cisco IOS device (GNS3 Lab). 2011. Verkkodokumentti. <https://www.m00nie.com/2011/03/steps-to-configure-an-ipsec-site-to-site-vpn-on-a-cisco-ios-device-gns3-lab/>. 1.3.2011. Luettu 3.9.2016.

17 IPSEC VPN tunneling in Cisco Packet Tracer. 2015. Verkkodokumentti. Cisco Systems. <http://www.packettracernetwork.com/tutorials/ipsec-vpn.html>. 6.2.2015. Luettu 3.9.2016.

18 Packet Tracer – Configuring VPNs. 2013. Verkkodokumentti. Cisco. <https://static-course-assets.s3.amazonaws.com/CN503/en/course/files/7.1.2.4%20Packet%20Tracer%20-%20Configuring%20VPNs%20%28Optional%29%20Instructions.pdf>. Luettu 3.9.2016.

19 Morimoto, Rand. 2011. IPv6 Addressing, Subnets, Private Addresses. Verkkodokumentti. <http://www.networkworld.com/article/2228449/microsoft-subnet/ipv6-addressing--subnets--private-addresses.html>. 6.2.2011. Luettu 12.9.2016.

20 Private IPV6 address range. Verkkodokumentti. JH Software. <http://www.simpledns.com/private-ipv6.aspx>. Luettu 7.9.2016.

21 IPv6 link-local vs unique local. 2014. Verkkodokumentti. Stack Exchange Inc. <http://networkengineering.stackexchange.com/questions/6505/ipv6-link-local-vs-unique-local>. Luettu 7.9.2016.

22 IPv6 Address Types. Verkkodokumentti. RIPE Network Coordination Centre. <https://www.ripe.net/participate/member-support/new-lir/ipv6_reference_card.pdf>. Luettu 1.1.2017.

23 Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., Li, X. 2010. IETF RFC IPv6 Addressing of IPv4/IPv6 Translators. Verkkodokumentti. <https://tools.ietf.org/html/rfc6052>. Lokakuu 2010. Luettu 25.11.2016.

24 NAT64. Verkkodokumentti. Wikimedia Foundation, Inc. <https://en.wikipedia.org/wiki/NAT64>. Luettu 12.9.2016.

25 Chown, T. 2006. Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks. Verkkodokumentti. <https://www.ietf.org/rfc/rfc4554.txt>. Kesäkuu 2006. Luettu 7.9.2016.

26 Configuring IPv6 host. 2016. Verkkodokumentti. Cisco. <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swipv6.html>. 17.10.2016. Luettu 25.11.2016.

27 Interior gateway protocol. 2017. Verkkodokumentti. Wikimedia Foundation, Inc. <https://en.wikipedia.org/wiki/Interior_gateway_protocol>. Luettu 1.1.2017.

28 NAT64 Technology: Connecting IPv6 and IPv4 Networks. 2012. Verkkodokumentti. Cisco. <http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html>. 27.4.2012. Luettu 16.9.2016.

29 IPv4-mapped IPv6 addresses. 2014. Verkkodokumentti. IBM Knowledge Center. <http://www.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.hale001/ipv6d0031001726.htm>. Luettu 18.9.2016.

30 Wilkins, Sean. 2013. IPv6 Translation and Tunneling Technologies. Verkkodokumentti. <www.ciscopress.com/articles/article.asp?p=2104947>. 26.6.2013. Luettu 12.9.2016.

31 Understanding IPv6 Link Local Address. Verkkodokumentti. Cisco. <http://www.cisco.com/c/en/us/support/docs/ip/ip-version-6-ipv6/113328-ipv6-lla.html>. Luettu 21.9.2016.

32 Chapter: IPv6 Routing: OSPFv3. 2017. Verkkodokumentti. Cisco. <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-15-sy-book/ip6-route-ospfv3.html>. 18.1.2017. Luettu 12.10.2016.

33 Sample Configuration for OSPFv3. 2010. Verkkodokumentti. Cisco. <http://www.cisco.com/c/en/us/support/docs/ip/ip-version-6-ipv6/112100-ospfv3-config-guide.html>. 11.8.2010. Luettu 12.10.2016.

34 Chapter: IPv6 Addressing and Basic Connectivity. Verkkodokumentti. Cisco. <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-3s/ip6b-xe-3s-book/ip6-add-basic-conn-xe.html>. Luettu 16.12.2016.

35 The global coordination of the DNS Root, IP addressing, and other Internet protocol resources performed as the Assigned Numbers Authority (IANA) functions. Verkkodokumentti. Iana. <http://www.iana.org>. Luettu 1.1.2017.

36 The Internet Registry System. 2016. Verkkodokumentti. RIPE Network Coordination Centre. <https://www.ripe.net/participate/internet-governance/internet-technical-community/the-rir-system>. 30.9.2016. Luettu 1.1.2017.

37 Hot Standby Router Protocol Features and Functionality. Verkkodokumentti. 2006. Cisco. <http://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html>. 25.5.2006. Luettu 1.1.2017.

38 Aoun, C., Davies, E. 2007. Reasons to Move the Network Address Translator – Protocol Translator (NAT-PT) to Historic Status. Verkkodokumentti. <https://www.ietf.org/rfc/rfc4966.txt>. Heinäkuu 2007. Luettu 1.1.2017.

39 Private IPv6 address range. Verkkodokumentti. JH Software. <http://simpledns.com/private-ipv6.aspx>. Luettu 7.9.2016.

40 Jajish, Thomas. 2017. Unique Local IPv6 Addresses. Verkkodokumentti. <http://www.omnisecu.com/tcpip/ipv6/unique-local-ipv6-addresses.php>. Luettu 1.1.2017.

41 IPv6: Goodbye to broadcast, say hello to Multicast.. 2011. Verkkodokumentti. <http://ipv6friday.org/blog/2011/12/ipv6-multicast/>. Luettu 1.1.2017.

42 Hinden, R., Deering, S. 2006. IP Version 6 Addressing Architecture. Verkkodokumentti. <https://tools.ietf.org/html/rfc4291>. Helmikuu 2006. Luettu 3.2.2017.

43 Shirkar, Ashish. 2014. Configuration Example : Site-to-Site VPN for IPv6 IPsec. Verkkodokumentti. <https://supportforums.cisco.com/document/112896/configuration-example-site-site-vpn-ipv6-ipsec>. 5.4.2014. Luettu 5.3.2017.

44 IPv6 Configuration Guide, Cisco IOS XE Release 3S. 2012. Verkkodokumentti. Cisco Systems Inc. <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/xe-3s/ipv6-xe-36s-book.pdf>. Luettu 25.3.2017.

45 Getting Started in the IETF. Verkkodokumentti. The Internet Society. <https://www.ietf.org/newcomers.html>. Luettu 26.3.2017.

46 How Virtual Private Networks Work. Verkkodokumentti. Cisco Support Community. <http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html>. Luettu 26.3.2017.

47 Hucaby, David, McQuerry, Stephen. 2002. VLANs and Trunking. Verkkodokumentti. <http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=3>. 25.10.2002. Luettu 26.3.2017.

48 Maughan, D., Schneider, M., Turner, J. 1998. RFC: Internet Security Association and Key Management Protocol (ISAKMP). Verkkodokumentti. <https://tools.ietf.org/html/rfc2408>. Marraskuu 1998. Luettu 26.3.2017.

49 Mason, Andrew. 2002. VPNs and VPN Technologies. Verkkodokumentti. <http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=7>. 4.1.2002. Luettu 26.3.2017.

50 Shaw, Graham. 2016. IEEE 802.1Q VLAN Tutorial. Verkkodokumentti. <http://www.microhowto.info/tutorials/802.1q.html>. Luettu 26.3.2017.

51 RIPE NCC IPv4 Available Pool – Graph. 2017. Verkkodokumentti. RIPE Network Coordination Centre. <https://www.ripe.net/publications/ipv6-info-centre/about-ipv6/ipv4-exhaustion/ipv4-available-pool-graph>. Luettu 26.3.2017.

52 Kansallinen IPv6:n käyttöönottopäivä 9.6.2015 -seminaari. 2015. Verkkodokumentti. Viestintävirasto. <https://www.viestintavirasto.fi/ipv6seminaari2015/>. Luettu 26.3.2017.

53 Inter-VLAN Routing. Verkkodokumentti. CCNA Blog. <http://www.ccnablog.com/inter-vlan-routing/>. Luettu 26.3.2017.

54 Kaushik, Das. 2008. IPv6 Transition Technologies. Verkkodokumentti. <http://ipv6.com/articles/gateways/IPv6-Tunnelling.htm>. Luettu 26.3.2017.

55 Ping. 2016. Verkkodokumentti. Wikimedia Foundation. <https://fi.wikipedia.org/wiki/Ping>. Luettu 2.4.2017.

56 Comparing OSPFv3 & OSPFv2 Routing Protocol. 2017. Verkkodokumentti. Cisco Support Community. <https://supportforums.cisco.com/document/97766/comparing-ospfv3-ospfv2-routing-protocol>. Luettu 2.4.2017.

57 Parr, Ben. 2011. IPv4 & IPv6: A Short Guide. Verkkodokumentti. <http://mashable.com/2011/02/03/ipv4-ipv6-guide/#3QveKSj2mOq3>. Verkkodokumentti. Luettu 2.4.2017.

58 Sinclair, Bruce. 2013. Biggest risks in IPv6 security today. Verkkodokumentti. <http://www.networkworld.com/article/2171504/tech-primers/biggest-risks-in-ipv6-security-today.html>. Luettu 2.4.2017.

59 IPv6 Security. Verkkodokumentti. IPv6 Now Pty Ltd. <http://www.ipv6now.com.au/primers/IPv6SecurityIssues.php>. Luettu 2.4.2017.

60 TCP/IP Overview and History. 2005. Verkkodokumentti. <http://www.tcpipguide.com/free/t_TCPIPOverviewandHistory.htm>. Luettu 2.4.2017.

61 Ashford, Warwick. 2011. IPv6: The security risks to business. Verkkodokumentti. <http://www.computerweekly.com/feature/IPv6-The-security-risks-to-business>. Luettu 2.4.2017.