

Mikko Pasanen

IPv6 kuluttaja-arkkitehtuurin suunnittelu ja testaus

Opinnäytetyö
Tietotekniikan koulutusohjelma

2018



**Kaakkois-Suomen
ammattikorkeakoulu**

Tekijä/Tekijät	Tutkinto	Aika
Mikko Pasanen	Insinööri (AMK)	Toukokuu 2018
Opinnäytetyön nimi		33 sivua
IPv6 kuluttaja-arkkitehtuurin suunnittelu ja testaus		
Toimeksiantaja		
LPOnet Oy		
Ohjaaja		
Vesa Kankare		
Tiivistelmä		
<p>Opinnäytetyö selvittää internetpalveluntarjoajan IPv6-siirtymää verkon asiakasosuuden osalta. Tavoitteena oli löytää hyviä toimintatapoja ja malleja dual stack -verkossa toimivalle IPv6-toteutukselle sekä luoda näistä dokumentti työn toimeksiantajalle.</p> <p>Työ tehtiin Kaakkois-Suomen ammattikorkeakoululla ja toteutuksen apuna käytettiin Xamkin virtuaalilaboratorioympäristöä, jossa suunnitelman mukaisen verkon toimintaa voitiin testata. Työ alkoi toteutustapojen tutkimisella ja suunnittelulla. Suunnitelman mukainen malli toteutettiin virtuaalisesti, jonka jälkeen toimintaa testattiin.</p> <p>Suunnitelma perustui DHCPv6:n prefix-delegaatio-malliseen toteutukseen ja asiakkaan verkon osalta automaattiseen konfiguraatioon. Prefix-delegaation hyötyinä on kuluttajan kannalta suuri määrä osoitteita ja operaattorin kannalta yksinkertaisuus DHCP-palvelimen jakaessa vain yhden prefiksin.</p> <p>Työstä saatiin aikaiseksi toimeksiantajalle dokumentti, joka voi toimia askelmerkkeinä heidän toteutukselleen. Työ sisälsi paljon uutta asiaa ja olisi hyötynyt paremmasta rajauksesta ja keskittymisestä tiettyyn osa-alueeseen. Tästä syystä etenkin toteutuksen testaus jäi vajavaiseksi.</p>		
Asiasanat		
IPv6, DHCPv6, palveluntarjoaja, laboratorio		

Author (authors)	Degree	Time
Mikko Pasanen	Bachelor of Engineering	May 2018
Thesis title		
IPv6 consumer access design and testing		33 pages
Commissioned by		
LPOnet Oy		
Supervisor		
Vesa Kankare		
Abstract		
<p>The goal of this thesis work was to research the use of IPv6 in customer segment of a service provider network. The aim was to find current best practices and methods used in such dual-stack networks and create a document for the client LPOnet Oy.</p>		
<p>The thesis work was carried out in South-Eastern Finland University of Applied Sciences. The implementation phase and the testing of operation was done in Xamk virtual laboratory environment. The work began with research and design of implementation strategies.</p>		
<p>The design was based on DHCPv6 prefix delegation architecture and autoconfiguration in the customer side of network. Prefix delegation allows for simple allocation of a large amount of addresses for customer as only a single address prefix is needed to be delegated to the customer from service provider DHCP server.</p>		
<p>The finished work was a document for the commissioner which would work as a guide for their own implementation. This thesis work included a lot of new content in many areas and would have benefited from better defining on what to include into the thesis and what to focus on. Especially the testing phase suffered because of this.</p>		
Keywords		
IPv6, DHCPv6, service provider, laboratory		

SISÄLLYS

AVAINSANAT JA SELITYKSET	6
1 JOHDANTO	7
2 TEORIA.....	7
2.1 IPv6-osoite	8
2.2 Osoitetyypit	9
2.2.1 Unicast	9
2.2.2 Link-local unicast.....	9
2.2.3 Unique local unicast	10
2.2.4 Global unicast.....	10
2.2.5 Multicast	10
2.2.6 Anycast.....	10
2.3 Neighbor discovery protocol.....	11
2.3.1 Router solicitation.....	11
2.3.2 Router advertisement	12
2.4 Osoitteiden dynaaminen konfigurointi	13
2.4.1 Tilallinen konfigurointi.....	13
2.4.2 Tilaton konfigurointi	14
2.4.3 EUI-64	14
2.5 DHCPv6	14
3 SUUNNITTELU	15
3.1 Arkkitehtuuri	15
3.2 Topologia	17
3.3 Asiakkaan tunnistus	17
3.4 Prefix-delegaatio	17
3.4.1 Prefix-delegaation kulku	18
3.4.2 Asiakkaan prefiksi	19
3.5 DHCPv6-palvelin.....	19

3.6	DHCPv6-relay agent	20
3.7	DHCPv6-asiakas	20
4	TOTEUTUS JA TESTAUS	20
4.1	Asiakastoteutus	22
4.1.1	Päätelaitteet	22
4.1.2	Asiakasreititin	23
4.2	Operaattoritoteutus.....	25
4.2.1	Asiakaskeskitin.....	26
4.2.2	Reunareititin	27
4.2.3	DHCPv6-palvelin	28
4.3	Delegoitu prefiksi.....	28
5	JATKOKEHITYS	29
6	POHDINTA.....	30
	LÄHTEET	31
	KUVALUETTELO	

AVAINSANAT JA SELITYKSET

CIDR	Classless Inter-Domain Routing on IPv4-osoitteiden luokallisen järjestelmän korvannut menetelmä, jossa IPv4-osoitteet jaetaan verkkoihin verkkomaskilla.
CPE	Customer Premises Equipment kuvaa yleensä asiakkaan verkossa olevaa verkkolaitetta, jolla asiakas on yhteydessä palveluntarjoajaan.
DHCP	Dynamic Host Configuration Protocol jakaa IP-osoitteita ja mahdollisesti muita konfiguraatietietoja verkon laitteille.
DHCPv6	Dynamic Host Configuration Protocol version 6 on uudempi versio DHCP:stä, joka jakaa konfiguraatietietoja verkon IPv6-laitteille.
DUAL STACK	Dual stack- eli kaksoispinokonfiguraatio, jossa verkon laitteella on sekä IPv4- että IPv6-ominaisuudet käytössä.
INTERFACE	Verkkorajapinta on rajapinta, jonka avulla verkkolaite on yhteydessä muihin laitteisiin verkon yli.
IoT	Internet of Things eli asioiden internet on kehityssuunta, jossa yhä useampi laite on yhteydessä muihin laitteisiin tietoverkon ylitse.
IPv4	Internet Protocol version 4 on nykyisin käytetyin versio internet-protokollasta.
IPv6	Internet Protocol version 6 on IPv4:n korvaajaksi kehitetty versio internet-protokollasta.
MAC	Media Access Control on yleensä kiinteä laitevalmistajan lisäämä tunniste verkkolaitteen ethernet-verkkorajapinnalle.
PE	Provider Edge kuvaa palveluntarjoajan verkon reunalaitetta, joka on yhteydessä asiakkaisiin.
SCOPE	IPv6-osoitteilla oleva käyttöalue, jolla osoite on relevantti.

1 JOHDANTO

Tämän opinnäytetyön on tarkoituksena selvittää internet-palveluntarjoajan mahdollisuuksia siirtymässä IPv4-protokollasta uudempaan, nykyaikaisille verkoille sopivampaan IPv6-protokollaan. Työn tavoitteena on luoda tiivistetty dokumentti avustamaan toimeksiantajaa omassa IPv6-toteutuksessaan. Työn tutkimusote on kvalitatiivinen ja osittain toiminnallinen. Aineiston on haussa on suosittu suurelta osin verkkolähteitä.

Opinnäytetyöaihe on saatu loviisalaiselta palveluntarjoajalta LPOnetiltä. Opinnäytetyö keskittyy operaattorin ja kuluttajan välisen osuuden IPv6-toteutuksessa käytettäviin teknologioihin ja protokolleihin. Suunnitelmaan valitut ratkaisut pyrkivät noudattamaan tämänhetkisiä hyväksi todettuja toimintatapoja. Vaatimuksena oli IPv6-protokollan toiminta IPv4-toteutuksen rinnalla, eli niin sanottuna kaksoispinona (dual stack). Näin molemmat teknologiat ovat tuettuina ja siirtymä uudempaan protokollaan on kuluttajalle sulava, eikä siitä aiheudu verkon käytölle ongelmia.

Työ selittää aluksi IPv6-protokollan tuomia uudistuksia ja muita ominaisuuksia, jotka ovat toteutuksen kannalta oleellisia. Suunnitelman testausta varten luodaan XAMK:n virtuaalilaboratio-ympäristöön yksinkertaistettu toteutus sisältäen työlle keskeiset laitteet ja palvelut. Virtuaalilaboratoriototeutuksen ei ole tarkoitus olla suoraan LPOnetin verkkoa vastaava toteutus, vaan sen tarkoitus on testata suunnitelmaan valittuja ratkaisuja. Esimerkiksi virtuaalisessa toteutuksessa käytetyt ohjelmistot todennäköisesti eroavat palveluntarjoajalla käytössä olevista.

2 TEORIA

Vielä nykyisin yleisimmin käytössä oleva versio IP-protokollasta on versio 4, eli lyhyemmin IPv4. Se kehitettiin jo 70-luvulla Yhdysvaltojen sisäisiin tarpeisiin ja on näin suhteellisen iäkäs teknologia tietotekniikan nopeasti kehittyvässä ympäristössä. IPv4:n alkuaajoista tietoverkot ovat kasvaneet ja kehittyneet valtavasti. Tämän johdosta myös IPv4:lle asetetut vaatimukset ovat jäämässä riittämättömiksi.

IPv4:n jatkajaksi kehitetty IPv6-protokolla pyrkii vastaamaan nykyaikaisten verkkojen tarpeisiin tuomalla uusia ominaisuuksia ja korjaamalla havaittuja IPv4-protokollan ongelmakohtia. Selkein IPv6-protokollan tuoma muutos on osoitteen pituuden kasvatus 32 bitistä 128 bittiin. Tämä korjaa jo pitkään IPv4-verkkoja vaivanneen osoitteiden säännöstelyn tarpeen. Isomman osoitemäärän myötä myös osoitteiden jakoa on pyritty helpottamaan lisäämällä IPv6-laitteille mahdollisuus konfiguroida itsensä suoraan reitittimeltä saatavilla tiedoilla. Muita muutoksia on tehty muun muassa liikenteen autentikointiin, yksityisyyteen ja sujuvuuteen. (Deering & Hinden 2017, 3.)

2.1 IPv6-osoite

IPv6-osoitteet esitetään heksadesimaalissa, jolloin jokainen merkki vastaa neljää bittiä. Lisäksi osoite jaotellaan neljän heksadesimaalin välein kaksoispisteellä. IPv6-osoitteessa perättäisistä nolista koostuvat osuudet voidaan lyhentää merkitsemällä vain viimeisin nolla. Mahdollista on myös jättää kokonaan merkitsemättä yhdestä tai useammasta vain nolliä sisältävästä 4 heksadesimaalin osuudesta muodostuva kokonaisuus. Prefiksillä tarkoitetaan osoitteen alussa olevaa verkko-osaa. Prefiksiin kuuluvien bittien määrä merkitään osoitteen perään kauttaviivalla ja bittien lukumäärällä. (Hinden 2006, 5.)

Kuvassa 1 on esitettyinä kolme erilaista hyväksyttyä tapaa esittää sama 60-bit-tinen IPv6-prefiksi. Huomionarvoista on nollien erilaiset merkkaustavat.

```
2001:0DB8:0000:CD30:0000:0000:0000:0000/60
2001:0DB8::CD30:0:0:0:0/60
2001:0DB8:0:CD30::/60
```

Kuva 1. Esimerkki 60-bittisen prefiksin esitystavoista (Hinden. 2006, 5)

Julkisen eli global unicast IPv6-osoitteen voidaan katsoa koostuvan kolmesta osasta. Globaalista reititysprefiksistä, aliverkon tunnisteesta ja rajapinnan tunnisteesta. Näistä yhdessä muodostuu 128-bittinen osoite, josta ensimmäinen 64 bittiä on verkon osaa ja viimeiset 64 bittiä verkkorajapinnan (interface) tunnistetta. IPv6-osoitteen verkon osan ei ole pakko olla 64 bittiä vaan se voi olla joko isompi tai pienempi. Yksi IPv6:n ominaisuuksista on kuitenkin osoitteen autokonfiguraatio mahdollisuus EUI-64-prosessilla, joka vaatii 64-bittisen

osuuden rajapinnan tunnisteelle ja on näin erittäin vahvasti suositeltu. (Hinden 2006, 8.)

Global Routing Prefix	Subnet ID	Interface ID
48-bittia	16-bittia	64-bittia
Verkko-osa – 64-bittia		Rajapinta-osa - 64-bittia
Koko osoite – 128-bittia		

Kuva 2. Julkisesti reititettävän IPv6-osoitteen rakenne (Hinden 2006, 9)

Kuvassa 2 on esitetty IPv6-osoitteen rakenne, jossa verkko-osa koostuu 48-bittisestä julkisesta prefiksistä ja 16-bittisestä aliverkon tunnisteesta. Jäljelle jäävät 64 bittiä käytetään rajapinnan tunnistamiseksi.

2.2 Osoitetyypit

Käyttötarkoitukseltaan IPv6-osoitteet voidaan jakaa kolmeen eri päätyyppiin. Nämä ovat unicast, multicast ja anycast. Tämän lisäksi osoitteet jakautuvat vielä useampiin alueellisiin ala-tyyppeihin (scope), joiden käyttö on rajattu tiettyyn verkon osaan. IPv6-laitteen interfacella voi olla samaan aikaan määriteltynä useita eri osoitteita (Graziani 2013, 83). Alueellisista alatyypeistä tärkeimmät ovat tietylle linkille (link-local scope) rajatut osoitteet ja internetin yli reititettävät julkisen (global scope) alueen osoitteet (Deering ym. 2005, 3).

2.2.1 Unicast

IPv6 unicast -osoitteet vastaavat luokattomia IPv4 CIDR -osoitteita (Hinden 2006, 5). Unicast-osoitteiden tarkoitus on määrittellä yhden laitteen yksi verkko-rajapinta ja olla käytetyn osoitteen käyttöalueesta riippuen uniikki. Esimerkiksi viestien lähdeosoitteena käytetään unicast-osoitteita. Verkkolaitte käyttää unicast-osoitteita kohdeosoitteena viestittäessään yhdelle tietylle kohdelaitteelle (Graziani 2013, 84).

2.2.2 Link-local unicast

Link-local-osoite on unicast-osoite, jonka käyttö rajoittuu yhdelle linkille. Link-local-osoite on ainoa pakollinen osoite IPv6-laitteen verkkorajapinnalle, jotta se pystyy toimimaan. Link-local-osoitteet ovat vain tietyn linkin sisällä uniikkeja

ja näin ollen ne eivät ole reititettävissä. IPv6-laitteiden on pystyttävä luomaan link-local-osoitteet verkkorajapinnoille automaattisesti. Link-local-osoitteille määritelty osoitealue on FE80::/10. (Graziani 2013, 107 - 109.)

2.2.3 Unique local unicast

Unique local- eli ULA-osoitteet ovat verrattavissa IPv4:n yksityisiin osoitteisiin ja niitä ei ole tarkoitus reitittää internettiin. IPv6 suuresta julkisten osoitteiden määrästä johtuen ULA-osoitteet eivät ole kuitenkaan samalla tavalla tarpeellisia kuin IPv4:ssä. Unique local -osoitteet ovat alueelta FC00::/7. (Graziani 2013, 119 - 120.)

2.2.4 Global unicast

Global unicast -osoitteet toimivat kuten IPv4:n julkiset osoitteet. Global unicast -osoitteita voidaan siis reitittää internetin yli ja ne ovat maailmanlaajuisesti uniikkeja. IPv6-laitteen yhdellä interfacella voi myös olla enemmän kuin yksi global unicast -osoite, yhdestä tai useammasta aliverkosta. Tällä hetkellä käytettävissä oleva global unicast -osoitteille varattu alue on 2000::/3. (Graziani 2013, 85 - 87.)

2.2.5 Multicast

Multicast-osoitteet ovat ennakkoon määriteltyjä osoitteita jotka voivat verkossa vastata useampaa laitetta. Laitteet voivat liittyä tarvittaviin multicast-ryhmiin ja näin vastaanottaa niihin lähetetyt viestit. Multicast-osoitteeseen lähetetty viesti voi siis päätyä useammalle laitteelle. IPv6 ei käytä levitysviestiosoitetta kuten IPv4, vaan se on korvattu kaikki IPv6-laitteet kattavalla, all-nodes multicast -osoitteella. Multicast-osoitteet ovat alueelta FF00::/8. (Graziani 2013, 124 - 125.)

2.2.6 Anycast

Anycast-osoitteet ovat osoitteita joita voidaan määrittellä useammalle kuin yhdelle verkkorajapinnalle. Näin saadaan aikaiseksi verkon redundanttisuutta. Anycast-osoitteet määritellään samalta osoitealueelta kuin global unicast -

osoitteet. Multicast- ja anycast-osoitteiden erona on, että anycast-osoitteeseen lähetetty viesti päätyy vain yhteen lähimpänä sijaitsevaan osoitteeseen. (Graziani 2013, 132.) Anycast-osoitteiden käyttökohteita ovat esimerkiksi palvelimet. Näin voidaan parantaa verkon redundanttisuutta laitevikojen varalta.

2.3 Neighbor discovery protocol

IPv6 tuo IPv6-laitteille naapuruuksia käsittelevän Neighbor Discovery Protocol -ominaisuuden (lyhenne NDP). NDP:n tehtävä on mahdollistaa IPv6-laitteiden tiedonvaihto toistensa kanssa. Protokollaan kuuluvien Neighbor Solicitation- ja Neighbor Advertisement -viestien yhtenä tehtävä on pitää kirjaa linkin muista IPv6-laitteista ja niiden tilasta (Graziani 2013, 169). Neighbor discovery hoitaa myös vastaavia tehtäviä kuin IPv4:n Address Resolution Protocol (ARP). IPv6 laitteen konfiguroidessa itselleen IPv6-osoitteen NDP lähettää neighbor solicitation -viestin samaan osoitteeseen varmistuakseen IPv6-osoitteen uniikkisuudesta (Cisco 2012).

Muita NDP:hen kuuluvia viestejä ovat Router Solicitation ja Router Advertisement, joilla on tärkeä rooli esimerkiksi IPv6-laitteiden autokonfiguraatiossa. Router solicitation- ja router advertisement -viestejä käytetään päätelaitteen ja reitittimen välisessä kommunikoinnissa. Reititin tavallisesti lähettää tietyin väliajoin router advertisement -viestejä omassa linkissään. IPv6-laite voi myös itse pyytää router solicitation -viestillä reitintä lähettämään välittömästi router advertisement -viestin. (Graziani 2013, 159.)

2.3.1 Router solicitation

Verkon laitteet lähettävät router solicitation -viestin tarvitessaan konfiguraatio-tietoja, kuten käynnistymisen yhteydessä. Router solicitation -viesti on isäntälaitteen pyyntö reitittimille router advertisement -viestin lähettämiseksi. Tyypillisesti isäntälaitte lähettää router solicitation -viestit kaikille reitittimille tarkoitettuun multicast-osoitteeseen FF02::2. Reitittimen vastaanottaessa router solicitation -viestin lähettää se vastauksena router advertisement -viestin. (Graziani 2013, 160.)

2.3.2 Router advertisement

Reitittimet lähettävät router advertisement -viestejä yleensä automaattisesti tietyin väliajoin sekä vastauksena IPv6-laitteilta tuleviin router solicitation -viesteihin. Router advertisement -viestin kohdeosoitteena on normaalisti all-nodes multicast -osoite, jolloin kaikki linkin IPv6-laitteet vastaanottavat viestin. Router advertisement -viestien tarkoitus on jakaa muille verkon laitteille konfiguraatioparametrejä, joiden avulla laitteet osaavat konfiguroida itsensä tai hakea lisätietoja esimerkiksi DHCP-palvelimelta. (Graziani 2013, 161.)

Router advertisementin sisältämistä parametreistä tämän työn kannalta huomionarvoisimmat ovat M- ja O-lippu sekä prefix-informaatio-optio. Kuvassa 3 on havainnollistettu router advertisement -viestin sisältämät kentät. Options-kentän sisältö voi vaihdella käytettävien lisäoptioiden mukaan.

ICMPv6 Router advertisement

Type	Code		Checksum
Cur hop limit	M	O	Rsrv.
Router lifetime			
Reachable time			
Retrans time			
Options (prefix information)			

Kuva 3. Router advertisement viestin sisältö (Narten ym. 2007,19)

M-lippu eli Managed Address Configuration flag on yhden bitin kokoinen kenttä router advertisement -viestissä. Kentän arvo voi siis olla joko 1 tai 0. Jos arvo on 1, se kertoo verkon laitteille, että IPv6-osoitekonfiguraatio on saatavilla DHCP-palvelimelta. Arvon ollessa 0 laitteiden on käytettävä tilattoman konfiguroinnin menetelmää (SLAAC). (Graziani 2013, 162.)

O-lippu eli Other Configuration flag on myös yhden bitin kokoinen kenttä router advertisement -viestissä. Kentän arvo voi olla joko 1 tai 0. Tämän lipun ollessa 1 verkon laitteet tietävät, että DHCP-palvelimelta on saatavilla myös muita konfiguraatietietoja, kuten nimipalvelimen osoite. (Graziani 2013, 162.)

Jos router advertisement -viesti kertoo laitteita konfiguroimaan itse oman osoitteensa, tarjoaa se siihen myös tarvittavat parametrit. Prefix-informaatio-optio sisältää tietoa linkillä käytettävästä prefiksistä. Näihin tietoihin kuuluvat itse IPv6-prefiksi eli osoitteen verkko-osa ja sen pituus. Tämän prefiksin avulla verkon laitteet osaavat luoda itselleen tarvittavat IPv6-osoitteet käyttämällä osoitteiden tilatonta autokonfigurointia. (Graziani 2013, 163.)

2.4 Osoitteiden dynaaminen konfigurointi

IPv6-kehityksen yksi tavoitteista on ollut tehdä laitteista mahdollisimman helposti verkkoon liitettäviä ja konfiguroitavia. Tähän tarkoitukseen IPv6 tarjoaa useita eri mahdollisuuksia. Osaa menetelmistä kutsutaan tilallisiksi (stateful) ja osaa tilattomiksi (stateless). Tilattomassa menetelmässä osoitteista ei pidetä kirjaa, vaan IPv6-laite tarkistaa osoitteen osoitteen uniikkiuden ennen sen käyttöönottoa. (Cisco 2006)

Tilattomana vaihtoehtona on Stateless Address Autoconfiguration (SLAAC). Tilattoman SLAAC:n myötä laitteet eivät ole riippuvaisia erillisestä DHCP-palvelimesta, vaan konfiguraatitiedot saadaan linkin reitittimeltä. Konfiguraation tilallisena vaihtoehtona on DHCPv6-palvelin. Tilallista menetelmää käytettäessä DHCP-palvelin ylläpitää jaettuja osoitteita ja muita konfiguraatitietoja. Mahdollista on myös käyttää tilallisen ja tilattoman menetelmän yhdistelmää, jossa esimerkiksi osoitteet konfiguroidaan tilattomasti ja muut konfiguraatitiedot haetaan DHCP-palvelimelta. (6deploy 2012)

2.4.1 Tilallinen konfigurointi

Tilattoman (stateless) SLAAC:n vaihtoehtona tilallinen (stateful) DHCPv6. Tilallisen osoitteenjaon hyötynä on osoitteiden tarkempi hallinta ja seuranta. Siinä missä SLAAC on erinomainen vaihtoehto esimerkiksi kuluttajan omassa lähiverkossa, operaattoreiden vaatimuksiin vastaa paremmin tilallinen DHCPv6. Yksittäisten osoitteiden lisäksi DHCPv6 voi jakaa myös prefix-delegaatiolla IPv6-prefiksejä reitittimille jaettavaksi edelleen eteenpäin. (6deploy 2012)

2.4.2 Tilaton konfigurointi

Stateless Address Autoconfiguration (SLAAC) on niin sanottu tilaton menetelmä, jolla laite määrittelee verkkorajapinnoilleen IPv6-osoitteita. Osoitteen verkko-osuuden SLAAC saa reitittimen router advertisement -viestistä ja interface identifier -osuuteen käytetään joko EUI-64-prosessia tai satunnais-generointia (Thomson ym. 2007, 8).

2.4.3 EUI-64

Extended Unique Identifier (EUI-64) on menetelmä, jolla IPv6-laite pystyy muodostamaan itse IPv6-osoitteen. Tähän prosessiin laite tarvitsee linkkinsä reitittimeltä IPv6-prefiksin. Tämän 64-bittisen prefiksin jatkoksi prosessi luo 64-bittisen rajapinnan tunnisteen (Interface-ID). Rajapinnan tunnisteen luomiseen EUI käyttää hyväkseen laitteen 48- tai 64-bittistä MAC-osoitetta. (6deploy 2012)

Joissakin tapauksissa laitteen MAC-osoitteen sisällyttämistä IP-osoitteeseen voidaan pitää tietoturvan kannalta ongelmallisena ja tällöin EUI-prosessin sijasta saatetaan käyttää prefiksin jatkona satunnaisesti luotua rajapinnan tunnistetta (Graziani 2013, 94).

2.5 DHCPv6

DHCPv6 on IPv6-protokollan vastine perinteiselle IPv4 DHCP:lle. DHCPv6 tarjoaa siis keskitetyn hallinnan IPv6-laitteiden dynaamiselle konfiguroinnille. DHCP:n avulla voidaan pitää yllä tietokantaa asiakkaille jaetuista konfiguraatio tiedoista, kuten IPv6-osoitteista. (Droms ym. 2003, 5.)

DHCPv6 on IPv6:ta käyttävä versio DHCP:stä. Perusperiaatteeltaan DHCPv6 toimii samoin kuin DHCPv4, siinä missä DHCPv4 palvelee IPv4-laitteita, DHCPv6 toimii IPv6-laitteiden parissa. DHCP:n eri versiot toimivat siis riippumatta toisistaan ja dual stack -verkossa on tarve molemmille versioille. DHCPv6 tuo myös mukanaan monia parannuksia ja muutoksia, jotka on nähty IPv6-maailmassa tarpeellisiksi. Operaattoriverkossa DHCP sijaisee yleensä keskitettynä ja erillään asiakasreitittimen linkistä. Jotta asiakasreititin voi kes-

kustella eri linkillä sijaitsevan DHCP-palvelimen kanssa, vaaditaan välittäjä (relay agent) DHCP-viesteille (Droms ym. 2003, 17). Tässä opinnäytetyössä käytetty malli perustuu välittäjän kautta toimivaan DHCP-palvelimeen.

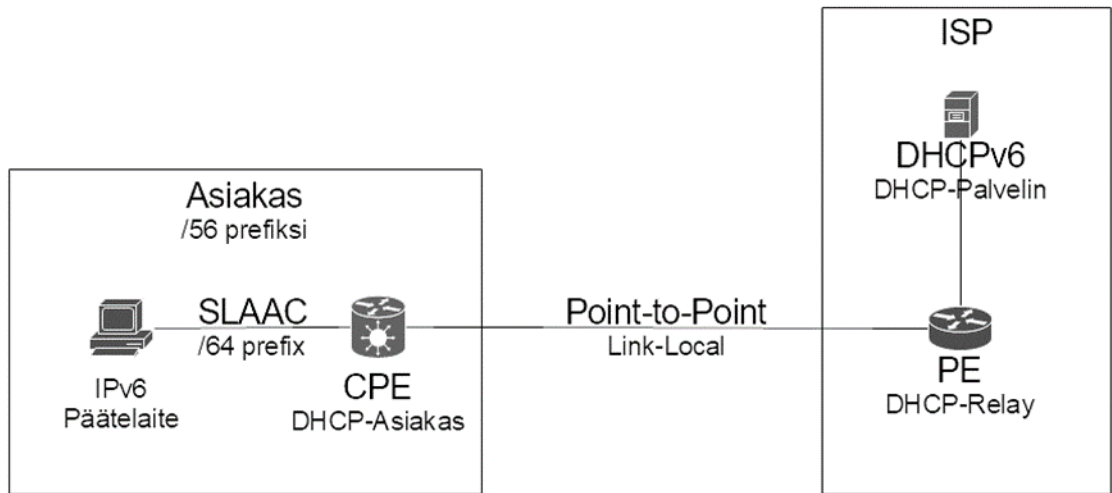
3 SUUNNITTELU

Suunnitelma rajattiin käsittämään asiakkaan reitittimen ja operaattorin reunareitittimen välistä toimintaa. Tähän kuului myös operaattorin sisäverkossa toimivan erillinen DHCPv6-palvelin. Esimerkkinä toteutettu verkko ja sen suunnitelma perustuu RFC3769:ssä kuvailtuun malliin. Tavoitteena oli suunnitella kuluttajakäytön vaatimuksiin soveltuva esimerkkitoeutus, joka keskittyy kuluttajan verkon ja palveluntarjoajan verkon väliseen toimintaan. Laitteiden osalta käsitellään operaattorin verkossa sijaitsevaa DHCPv6-palvelinta, operaattorin reunareititintä (PE) ja siihen yhteydessä olevaa kuluttajareititintä (CPE). Operaattorin reitittimen ja kuluttajan reitittimen välissä käytetään access-laitteena layer-3-kytkintä, johon voidaan kytkeä tarvittaessa useampia asiakkaita.

3.1 Arkkitehtuuri

Työn toteutuksen vaatimuksena oli, että loppukäyttäjille voidaan IPv6-periaatteiden mukaisesti jakaa helposti useita IPv6-osoitteita. Tätä tarkoitusta varten IPv6:n DHCPv6 tarjoaa prefix-delegaatio (DHCPv6-PD) mahdollisuuden. Suunniteltu access arkkitehtuuri perustuu siis DHCPv6:n tarjoamaan prefix-delegaatioon, jossa asiakkaan reitittimelle delegoidaan operaattorilta julkisen osoitealueen IPv6-prefiksi.

Prefix-delegaatiossa asiakasreititin saa siis itselleen käytettäväksi siis osan julkista IPv6-osoitealuetta. Delegoidusta prefiksistä asiakkaan päätelaite luo tarvittavat IPv6-osoitteet lähiverkon laitteille. Arkkitehtuurin kannalta oleelliset laitteet ja menetelmät on havainnollistettu kuvassa 4.



Kuva 4. Havainnollistus arkkitehtuurin kokoonpanosta

Asiakasreititin (CPE) toimii WAN-linkillä DHCPv6-asiakkaana. Jotta asiakas voi pyytää operaattorin verkossa toimivalta DHCPv6-palvelimelta prefiksiä, tarvitsee se välittäjäksi DHCPv6 relayn. Asiakasreititin keskustelee relayn kanssa link-local-osoitteilla. Vastaavasti relayn ja palvelimen välinen keskustelu tapahtuu global unicast -osoitteilla.

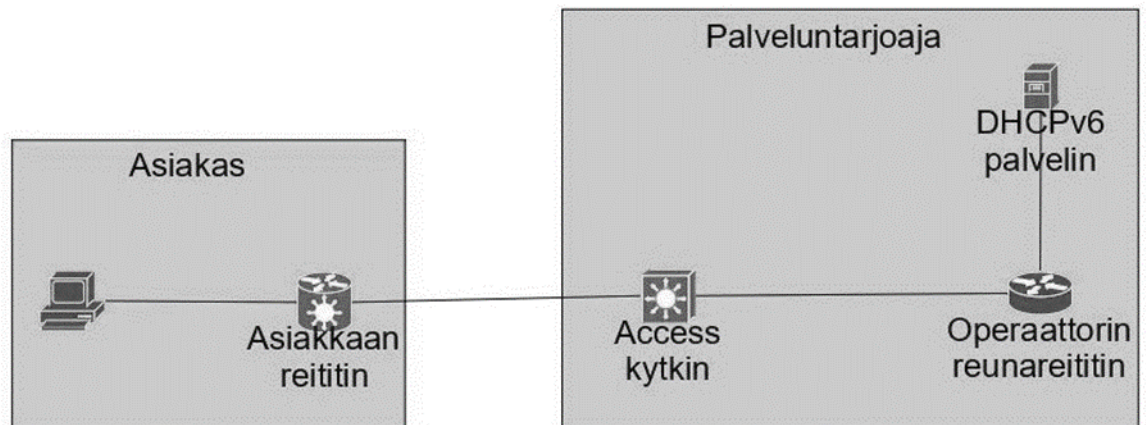
Asiakasreitittimen vastuulla on määrittää, miten se vastaanotettua prefiksiä käyttää. Lähiverkon laitteiden konfiguraatio tapahtuu tilatonta autokonfiguraatiota (SLAAC) käyttämällä, jolloin DHCP:n käyttö ei siis ole asiakkaan verkossa tarpeellista.

Operaattorin reunareititin (PE) on layer-3-yhteydessä asiakasreitittimeen ja osoittaa asiakasreitittimen hakemaan konfiguraatitietoja DHCPv6-palvelimelta.

Itse IPv6-prefiksien jakamisesta vastuussa on asiakkaan linkistä erillään sijaitseva DHCPv6-palvelin. Palvelin määrittää relayn lähettämien relay-forward- viestien sisällön perusteella asiakkaalle jaettavan prefiksin ja ylläpitää tietoja jaetuista prefikseistä.

3.2 Topologia

Suunnitelman verkkotopologia oli yksinkertainen malli operaattorin ja asiakkaan välisestä verkosta. Topologia sisälsi prefix-delegaatio arkkitehtuurin kannalta oleelliset laitteet. Mahdollisiin muihin operaattoriverkossa oleviin laitteisiin ei otettu kantaa.



Kuva 5. Suunnitelman verkkotopologia

Asiakkaan osalta topologiaan tarvittiin IPv6-päätelaite sekä asiakkaan reititin, joka hoitaisi yhteyden operaattorin suuntaan. Operaattoriverkon tarpeellisiksi laitteiksi katsottiin asiakaskeskittimenä toimiva access-kytkin, operaattorin reunareititin sekä operaattorin sisäverkossa toimiva DHCPv6-palvelin. Laitteiden kytkennät on nähtävillä kuvassa 5.

3.3 Asiakkaan tunnistus

Palveluntarjoajilla on viestintäviraston asettama velvoite säilyttää tiedot asiakkaalleen jakamistaan ip-osoitteista asiakkaan yksilöintiä varten. Näistä tiedoista on oltava tunnistettavissa, milloin tietyt osoitteet ovat olleet käytössä ja millä asiakkaalla (Viestintävirasto 2014). Tämän vuoksi tarvitaan DHCPv6:n lisäoptioita kuten optio 37, remote-ID. Optio 37 on vastine IPv4:n DHCP optio 82:lle. Näin asiakkaat pystytään erottamaan toisistaan ja voidaan pitää kirjaa asiakkaille milloinkin jaetuista prefiksistä vaatimusten mukaisesti.

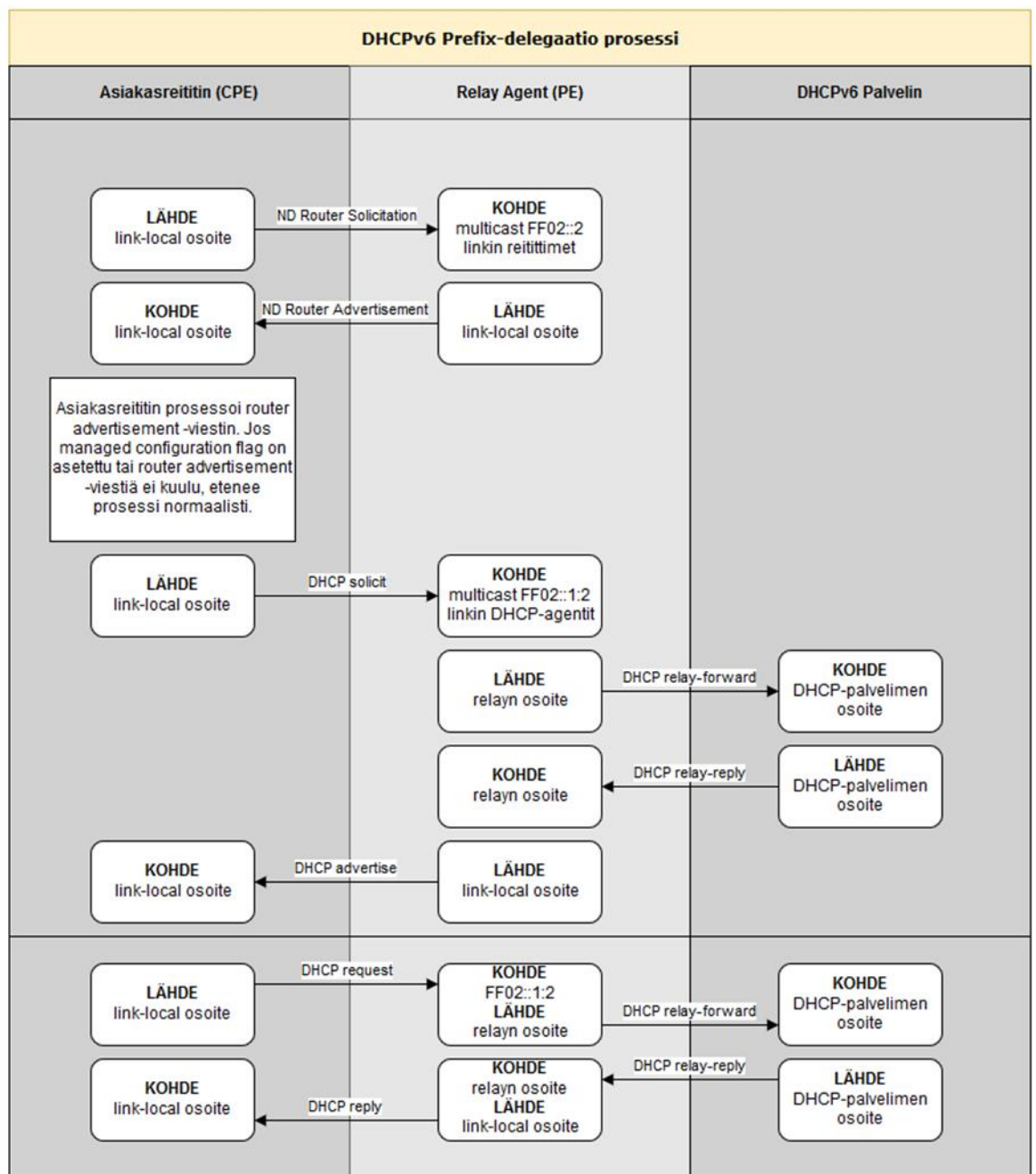
3.4 Prefix-delegaatio

DHCPv6-PD eli prefix-delegaatio on mekanismi, jolla DHCP-palvelin voi jakaa IPv6-prefiksin reitittimelle. Asiakasreititin toimii DHCPv6-asiakkaana ja käyttää

vastaanotettua prefiksiä jakaessaan osoitteita oman linkkinsä laitteille. Asiakkaan laite määrittelee, miten se prefiksiä käyttää router advertisement -viesteissä.

3.4.1 Prefix-delegaation kulku

Kun IPv6-laite verkossa on luonut itselleen link-local -osoitteen, voi se aloittaa prosessin muiden konfiguraatio-parametrien saamiseksi. Delegaatioon osallistuvien laitteiden välinen viestintä on kuvattuna kuvassa 6.



Kuva 6. Prefix delegaation viestienvaihto laitteiden välillä

Ensimmäisenä konfiguraatiota etsivä laite (CPE, kuva 6) lähettää neighbor discovery router solicitation -viestin (lyhenne ND RS) kaikille linkin reitittimille multicast-osoitteeseen FF02::02. Reititin (PE, kuva 6) vastaa solicitation-viestiin lähettämällä neighbor discovery router advertisement -viestin (lyhenne ND RA) siinä olleeseen lähdeosoitteeseen. Saatuaan ND RA -viestin, laite katsoo viestin sisältämää M-lippu-kentän bittiä ja jos se on asetettu, laite tietää hakea konfiguraatitietoja DHCP-palvelimelta. Seuraavaksi laite lähettää DHCP-pyyynnön (solicit) multicast-viestinä kaikille linkin DHCP-agenteille. Jos DHCP-palvelin ei sijaitse samalla linkillä, vaaditaan dhcp-relay vastaanottamaan viesti ja välittämään se eteenpäin DHCP relay-forward -viestinä yhdelle tai useammalle DHCP-palvelimelle. Palvelin vastaa lähettämällä relaylle konfiguraatitiedot DHCP relay-reply -viestinä. Viimeisenä DHCP relay lähettää tiedot eteenpäin niitä pyytäneelle laitteelle sen link-local-osoitteeseen DHCP-advertise -viestinä (Blanchet 2006, 91).

3.4.2 Asiakkaan prefiksi

IPv6-loppukäyttäjille jaettavan prefiksin pituudeksi on aikaisemmin suositeltu 48-bittistä prefiksiä, joka tarjoaisi asiakkaalle jopa yli 64 tuhatta 64-bittistä IPv6-aliverkkoa (Narten ym. 2011, 4). Täyden IPv6-osoitteen ollessa 128 bittiä, jokainen 64-bittinen aliverkko sisältää siis 2^{64} julkista IPv6-osoitetta. Uudempi IETF:n RFC6177 kuitenkin muutti tätä suositusta pienempään 56-bittiseen prefiksiin (Narten ym. 2011, 6).

Asiakkaalle 56-bittisestä prefiksistä jää käytettäväksi 256 kappaletta 64-bittisiä IPv6-aliverkkoja. Operaattorin alueelliselta IP-osoitteiden hallinnolta RIR:ltä (Regional Internet Registry) saama prefiksi on yleensä 32-bittinen, jolloin operaattorille jää käytettäväksi 96 bittiä. Tällaisesta prefiksistä operaattori saisi siis jaettua eteenpäin maksimissaan 64 tuhatta 48-bittistä prefiksiä tai vastavasti 16 miljoonaa 56-bittistä prefiksiä.

3.5 DHCPv6-palvelin

DHCPv6 palvelin käsittelee linkiltä tulleen asiakkaan DHCPv6 pyynnön ja pitää kirjaa jaetuista prefikseistä. Palvelimen sijainti on erillään asiakkaan linkistä, jolloin asiakkaan reititin ei pysty suoraan keskustelemaan DHCP-palvelimen kanssa itsenäisesti. Palvelimen osalta oleellista on, että se osaa jakaa

IPv6-prefiksejä. Tämän lisäksi palvelinohjelmiston on osattava käsitellä viesteihin relayn lisäämä optio 37 -kenttä eli remote-ID.

3.6 DHCPv6-relay agent

DHCP relay agent vaaditaan välittämään asiakkaan linkiltä tuleva DHCPv6-pyyntö operaattorin DHCP-palvelimelle. Relay agenttina toimiva laite myös lisää DHCP relay-forward -viesteihin remote-ID optiota käyttäen asiakkaan tunnistetiedot.

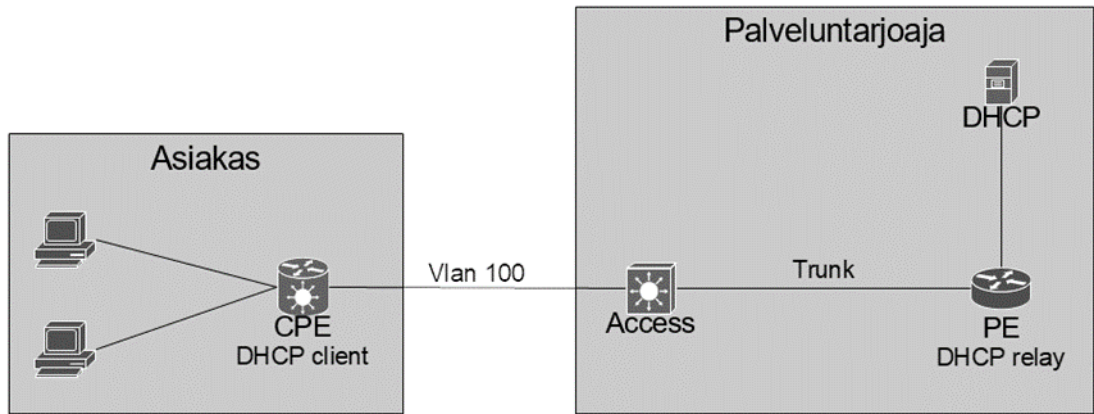
Remote-ID-option tarkoitus on siis välittää DHCP-palvelimelle tietoa konfiguraatiota pyytävästä asiakaslaitteesta ja sen linkistä. DHCPv6 remote-ID:n tunnus on optio 37. Sen sisältämää dataa ei ole tarkasti määritelty, vaan on laitteistovalmistajasta riippuvainen. Yleisesti remote-ID saattaa esimerkiksi sisältää asiakkaaseen yhteydessä olevan linkin verkkorajapinnan tunnisteeseen sekä VLAN-numeron. (Volz 2006.)

3.7 DHCPv6-asiakas

Kuluttajan reititin (CPE) toimii DHCP-asiakkaana, joka lähettää DHCP-pyyntöjä etsien DHCP-palvelimia omasta linkistään. Nämä pyynnöt ohjautuvat relay agentin kautta serverille. Kuluttajan reitittimen kannalta relay agentin toiminta on näkymätöntä, eikä vaikuta laitteiston konfiguraatioon.

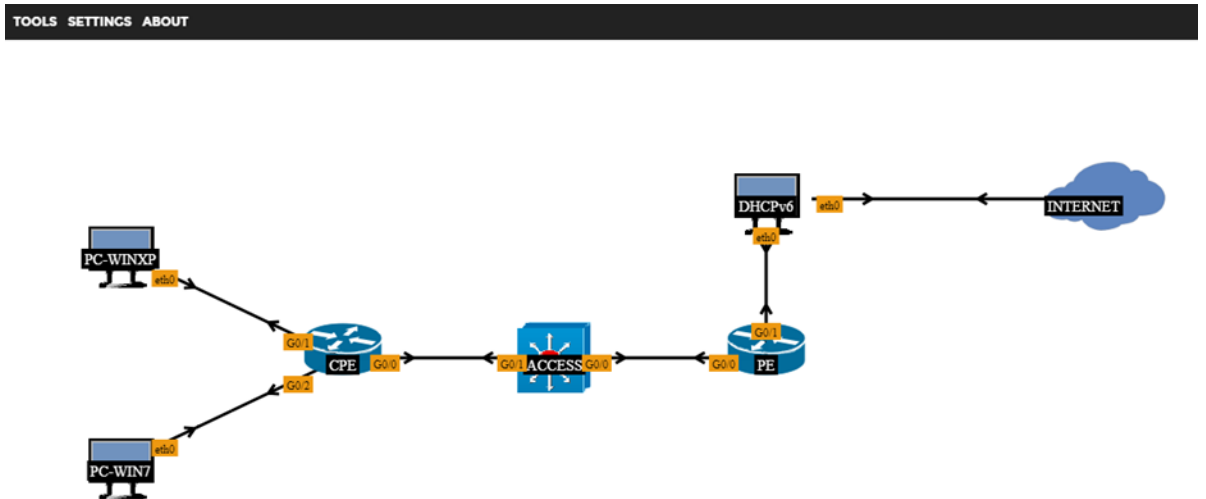
4 TOTEUTUS JA TESTAUS

Suunnitelman mukainen toteutus luotiin Kaakkois-Suomen Ammattikorkeakoulun virtuaalilaboratorio-alustalle. Virtuaalisen ympäristön etuna oli, ettei itse fyysisiä laitteita tarvittu, eikä toteutus niitä siis sisältänyt. Laitteisto-ohjelmistoina käytettiin vapaasti saatavilla olevia avoimen lähdekoodin ohjelmistoja.



Kuva 7. Toteutettavan verkon kokonaiskuva laitteistosta

Kuvassa 7 näkyvään toteutuksen kokoonpanoon kuului asiakkaan verkon osalta kaksi päätelaitetta ja asiakkaan reititin, joka nimettiin CPE:ksi. Asiakkaan reitittimeksi valittiin avoimen lähdekoodin OpenWRT-ohjelmisto. Operaattorin asiakaskeskittimen ja reunareitittimen osalta käytettiin laboratoriossa saatavilla olevia Cisco Systemsin virtualisointiin tarkoitettuja IOSv-ohjelmistoja. Operaattorin DHCP-palvelimena käytettiin ISC DHCP -palvelinohjelmistoa Xubuntu Linux -käyttöjärjestelmän päällä.

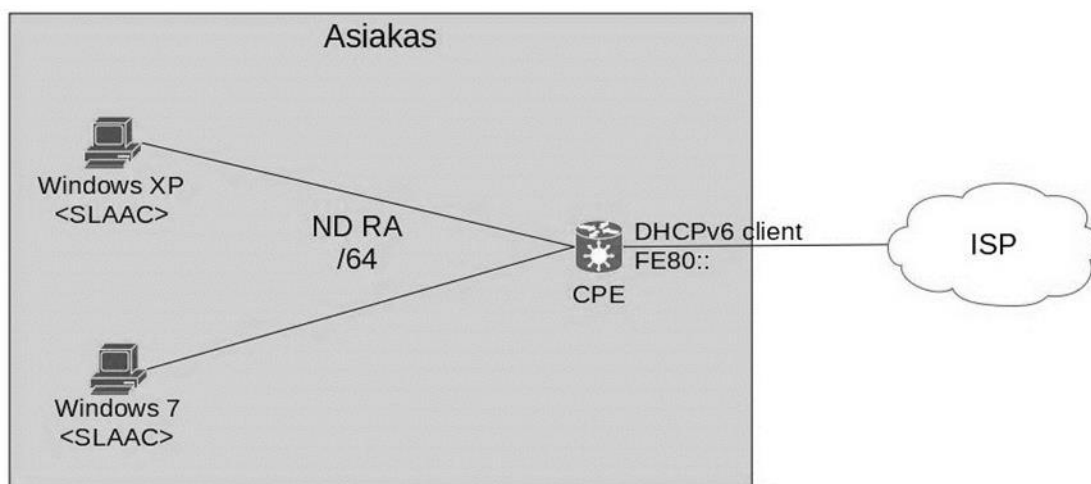


Kuva 8. Virtuaalilaboratorion laitteisto ja kytkennät

Ensimmäisenä toteutusta varten luotiin virtuaalilaboratorioon tarvittavat laitteet ja yhteydet (kuva 8). DHCPv6-palvelin liitettiin myös internettiin, jotta päivityksiä voitaisiin ladata.

4.1 Asiakastoteutus

Asiakkaan osalta testilaboratorioon kuului kaksi Windows-työasemaa, Windows 7 ja Windows XP, sekä asiakasreitittimenä OpenWRT-pohjainen reititin. OpenWRT on OpenWRT-projektin ylläpitämä Linux-käyttöjärjestelmään perustuva verkkolaitteohjelmisto (OpenWRT 2018).



Kuva 9. Asiakkaan verkon kuva

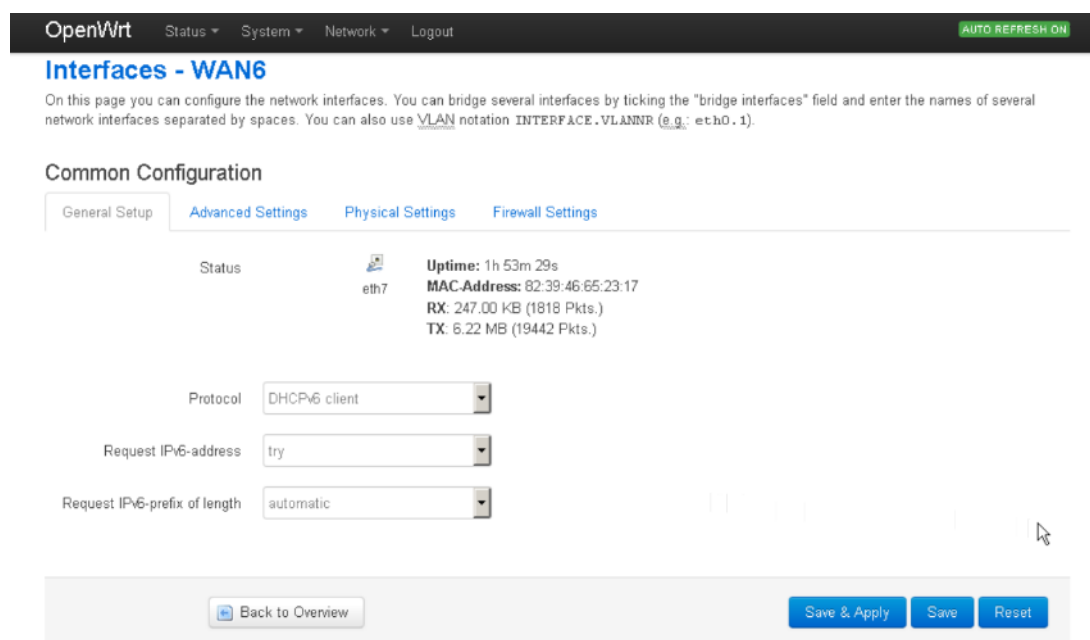
Asiakastoteutuksen tärkeimpänä tavoitteena oli konfiguroida asiakasreititin hakemaan IPv6-prefiksiä operaattoriin yhteydessä olevalta linkiltä. Operaattoriin asiakasreititin oli yhteydessä automaattisesti konfiguroimallaan FE80::/10-alueen link-local-osoitteella. Asiakkaan sisäverkon osalta asiakkaan reitittimen haluttiin jakavan 64-bittistä prefiksiä tilatonta autokonfiguraatiomenetelmää (SLAAC) käyttäen. Kuvassa 9 nähtävillä asiakkaan verkon kokoonpano.

4.1.1 Päätelaitteet

Ensimmäisenä asiakkaan verkkoon päätelaitteiksi asennettiin kaksi Windows-pohjaista virtuaalikonetta. Päätelaitteet toimivat IPv6-osoitteenjaon päätepisteinä ja onnistuneen prefix-delegaation vaatimuksena oli siis päätelaitteiden itsenäinen IPv6-konfiguraatio asiakasreitittimeltä saatavalla prefiksillä. Testin monipuolisuuden vuoksi toinen päätelaitteista edusti IPv6-ominaisuuksiltaan jo selvästi vanhempaa Windows XP -käyttöjärjestelmää ja toinen hieman uudempaa Windows 7 -käyttöjärjestelmää. Päätelaitteiden osalta mitään erillistä verkkokonfiguraatiota ei tarvittu eikä haluttu. Laitteet osaavat hakea itselleen IPv6-osoitteet automaattisesti verkkosovittimen oletusasetuksilla, kuten on tarkoituksenmukaista asiakasverkoissa.

4.1.2 Asiakasreititin

Asiakkaan reitittimeksi virtuaalilaboratorioon lisättiin OpenWRT-ohjelmiston versio 15.05.1. Reitittimen konfiguraatio tapahtui toiselta Windows-päätelaitteelta käsin käyttämällä OpenWRT:n tarjoamaa graafista LuCI-verkkokäyttöliittymää. Yhteys reitittimeen saatiin suoraan selaimella reitittimen oletusosoitteesta 192.168.1.1. Itse reitittimen konfigurointi oli graafisen käyttöliittymän ansiosta helppoa. IPv4 asetuksiin ei laitteessa puuttuttu. Jotta reititin osaisi pyytää operaattorin suunnalta IPv6-konfiguraatiota, konfiguroitiin se DHCPv6-asiakkaaksi. Kuvassa 10 asiakasreitittimen operaattoriin yhteydessä olevan "WAN6"-rajapinnan protokolla asetettiin "DHCPv6-Client"-tilaan. Pyydetävän prefiksin osalta laite jätettiin automaattiseen tilaan, sillä operaattorilta jaettaisiin vain yhden kokoista prefiksiä.



Kuva 10. WAN6-rajapinnan konfiguraationäkymä

Asiakkaan lähiverkon osalta reitittimen haluttiin jakavan konfiguraatitietoja tiilattomalla konfiguraatiomenetelmällä router advertisement -viesteissä. Tällöin asiakasreitittimeen ei siis tarvittu lähiverkon DHCPv6-toiminnallisuutta, joka myös oletuksena oli pois päältä. Lähiverkkoon kuului seitsemän liityntäporttia. Kaikki lähiverkon portit kuuluivat oletuksena samaan aliverkkoon, eikä tätä ollut tarpeellista muuttaa. Lähiverkon konfiguraation osalta valittiin haluttu lähiverkossa käytettävän IPv6-prefiksin pituus. Prefiksi asetettiin 64-bittiin "IPv6 assignment length" -valikosta, nähtävillä kuvassa 11.

The screenshot shows the OpenWrt web interface for configuring the 'br-lan' network interface. The 'Advanced Settings' tab is selected. The interface status is shown as 'br-lan' with an uptime of 2h 1m 55s. The MAC address is 82:39:46:65:23:10. The current IPv4 configuration is as follows:

Field	Value
Protocol	Static address
IPv4 address	192.168.1.1
IPv4 netmask	255.255.255.0
IPv4 gateway	
IPv4 broadcast	
Use custom DNS servers	
IPv6 assignment length	64

A note below the IPv6 assignment length field states: 'Assign a part of given length of every public IPv6-prefix to this interface'.

Kuva 11. Lähiverkon konfiguraationäkymä

Alustavasti operaattorin reunareitittimeen konfiguroitiin reitittimen oma DHCPv6-palvelin. Palvelin asetettiin jakamaan prefiksiä 2001:db8:beef::/56. Vaikka operaattorin reitittimen DHCP-palvelin oli ominaisuuksiltaan melko rajoitettu, oli se yksinkertainen konfiguroida ja näin voitiin nopeasti varmistua asiakasreitittimen toiminnallisuudesta. Ciscon DHCPv6-palvelin jakoi onnistuneesti /56-prefiksin asiakasreitittimelle, Asiakasreititin otti tästä itselleen lähiverkon oletusyhdyskäytäväksi 2001:db8:beef::1 osoitteen. Lisäksi reititin alkoi jakaa 2001:db8:beef::/64-prefiksiä lähiverkon muille laitteille.

The screenshot shows the OpenWrt web interface for the 'Interfaces' section. The 'Interface Overview' is displayed, showing the 'LAN' interface. The interface is highlighted in green, indicating it is active. The status and configuration details are as follows:

Network	Status	Actions
LAN br-lan	Uptime: 0h 28m 21s MAC-Address: 82:39:46:65:23:10 RX: 384.23 KB (3589 Pkts.) TX: 1.65 MB (3818 Pkts.) IPv4: 192.168.1.1/24 IPv6: 2001:db8:beef::1/64	Connect Stop Edit Delete

Kuva 12. Ciscon DHCPv6-palvelimelta saatu prefiksi käytössä

Kuvassa 12 on esillä verkkokäyttöliittymän näkymä lähiverkossa käytöstä olevassa prefiksistä 2001:db8:beef::/64 ja oletusyhdyskäytävän osoitteesta 2001:db8:beef::1.


```

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : lan
    IP Address. . . . .                : 192.168.1.101
    Subnet Mask . . . . .              : 255.255.255.0
    IP Address. . . . .                : 2001:db8:beef:0:9cc2:88a3:2f93:268e
    IP Address. . . . .                : 2001:db8:beef:0:623b:21ff:fec9:2710
    IP Address. . . . .                : fd2b:88b6:e473:0:9cc2:88a3:2f93:268e
    IP Address. . . . .                : fd2b:88b6:e473:0:623b:21ff:fec9:2710
    IP Address. . . . .                : fe80::623b:21ff:fec9:2710%4
    Default Gateway . . . . .          : 192.168.1.1
                                          fe80::8039:46ff:fe65:2310%4

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . :
    IP Address. . . . .                : fe80::ffff:ffff:fffd%5
    Default Gateway . . . . .          :

Tunnel adapter Automatic Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : lan
    IP Address. . . . .                : fe80::5efe:192.168.1.101%2
    Default Gateway . . . . .          :

C:\Documents and Settings\Administrator>

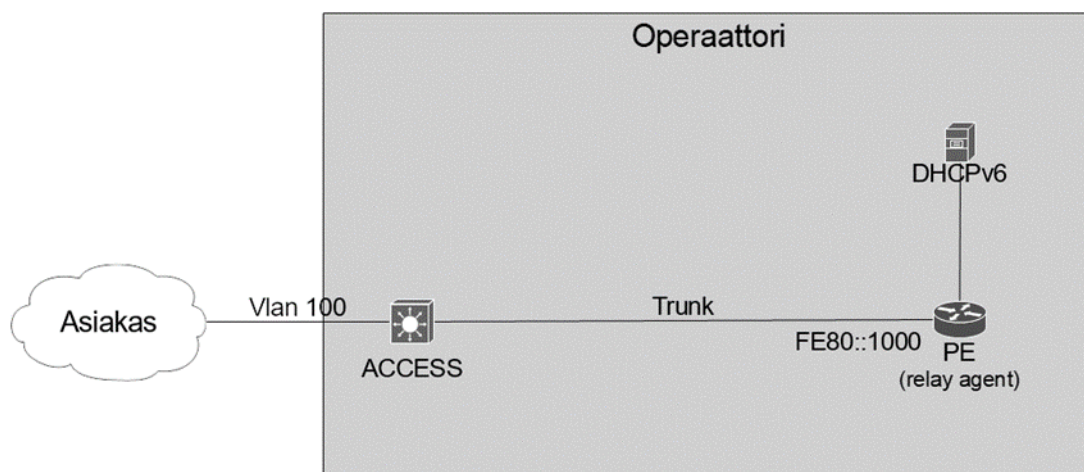
```

Kuva 13. Päätelaitteen luoma IPv6-konfiguraatio

Lähiverkon porteista jaettiin prefiksiä eteenpäin ND RA -viesteissä. Näistä viesteistä päätelaitteet osasivat onnistuneesti luoda omat julkiset IPv6-osoitteet. Kuvassa 13 Windows XP -koneen näkymä sen itselleen luomasta IPv6-osoitteesta. Windows XP:n tapa luoda IPv6-osoite EUI-64-prosessilla käyttäen verkkorajapintansa MAC-osoitetta oli myös nähtävissä.

4.2 Operaattoritoteutus

Operaattoritoteutuksen tavoitteina oli konfiguroida reunareitittimeen DHCP-viestejä välittävä relay agent -toiminnallisuus ja saada DHCPv6-palvelin jakamaan onnistuneesti osoitteita välittäjän ylitse. Kuvassa 14 havainnollistettuna operaattorin verkon osuuteen kuuluvat laitteet.



Kuva 14. Operaattorin verkon kuva

Operaattorin laitteina oli DHCPv6-palvelin, reunareititin ja asiakaskeskittimenä toimiva layer-3-kytkin. DHCP-palvelimena oli Ubuntu Linux -käyttöjärjestelmän päälle asennettu ISC DHCP:n uusin saatavilla oleva versio.

4.2.1 Asiakaskeskitin

Operaattorin reunareitittimen ja asiakkaan väliin luotiin asiakaskeskittimenä toimiva L3-kytkin nimeltä ACCESS.

```

3 ////////////////
4 //ACCESS
5 ////////////////
6 hostname ACCESS
7
8 line con 0
9 exec-timeout 60
10 exit
11
12 vlan 100
13 name ASIAKAS-1
14 exit
15
16 interface g0/0
17 description link to ISP
18 switchport trunk encapsulation dot1q
19 switchport mode trunk
20 no shutdown
21 exit
22
23 interface g0/1
24 description link to ASIAKAS-1
25 switchport mode access
26 switchport access vlan 100
27 no shutdown

```

Kuva 15. Asiakaskeskittimen konfiguraatio

Kuvassa 15 on nähtävillä kytkimessä käytetty konfiguraatio. Kytkimeen luotiin asiakkaalle oma VLAN ja asiakasreititin liitettiin yhteen kytkimen access -porttiin. Operaattorin suuntaan keskitin konfiguroitiin toimimaan trunk-porttina, jolloin useampi asiakas voisi olla tarvittaessa yhteydessä operaattoriin samalla fyysisellä linkillä käyttäen eri VLAN-tunnusta.

4.2.2 Reunareititin

Operaattorin reunareititin liitettiin olemaan yhteydessä asiakaskeskittimen kautta itse asiakkaan reitittimeen ja suoraan DHCPv6-palvelimeen. Reititimen tehtävä oli välittää asiakaskeskittimeltä tulevat DHCP-pyynnöt DHCPv6-palvelimelle. Tärkeimpänä oli välittäjänä toimivan relay agentin konfigurointi.

```

6 hostname PE
7 ipv6 unicast-routing
8
9 line con 0
10 exec-timeout 60
11 exit
12
13 interface l0
14 ipv6 address 2001:DB8::1000/128
15 exit
16
17 interface g0/0
18 description link to ACCESS
19 ipv6 address FE80::1000 link-local
20 no shutdown
21 exit
22
23 interface g0/0.100
24 encapsulation dot1q 100
25 ipv6 address fe80::100 link-local
26 ipv6 address 2001:db8:1000::100/48
27 ipv6 dhcp relay destination 2001:DB8:1::2 g0/1
28 ipv6 nd managed-config-flag
29 no shutdown
30 exit
31
32 interface g0/1
33 description link to DHCP
34 ipv6 address 2001:db8:1::1/64
35 ipv6 address fe80:1::1 link-local
36 no shutdown
37 exit
38

```

Kuva 16. Operaattorin reunareitittimen konfiguraatio

Reitittimeen konfiguroitiin (kuva 16) ensimmäisenä IPv6-toiminnallisuus *ipv6 unicast-routing* -komennolla. Tämän jälkeen konfiguroitiin liittymä asiakaskeskittimeen ja porteille tarpeelliset IPv6-osoitteet. Asiakkaan reitittimeen yhteydessä olevaan rajapintaan konfiguroitiin itse relay agent. Toiminto saatiin käyttöön komennolla *ipv6 dhcp relay destination 2001:db8:1::2 g0/1*, jossa parametreina käytettiin DHCPv6-palvelimen IPv6-osoitetta "2001:db8:1::2" ja palvelimeen yhteydessä olevaa porttia "g0/1". Relay agent ei tarvinnut toimiakseen muita komentoja, vaan reititin otti automaattisesti käyttöön muut relay

agentin toimintaan liittyvät ominaisuudet. Näihin kuuluivat remote-ID:n injektointi ja staattisen reitin luonti reititystauluun onnistuneen prefix-delegaation jälkeen.

4.2.3 DHCPv6-palvelin

Linux käyttöjärjestelmän päälle asennettavaa DHCPv6-palvelinta varten ladattiin ensimmäisenä käyttöjärjestelmäpäivitykset uusimpaan saatavilla olevaan versioon 16.04. Samalla ladattiin ja päivitettiin ISC DHCP -palvelinohjelmisto. Palvelimelle konfiguroitiin kiinteä IPv6-osoite `2001:db8:1::2`.

```

108 subnet6 2001:db8:1000::/64 {
109
110     option dhcp6.name-servers 2001:4860:4860::8888;
111     option dhcp6.domain-search "example.com";
112
113     prefix6 2001:db8:1000:ff00:: 2001:db8:1000:ff00:: /56;
114 }
```

Kuva 17. dhcpd6.conf -tiedoston osoitteenjaon konfiguraatio

DHCPv6-toiminnallisuutta varten luotiin palvelimelle konfiguraatitiedosto `dhcpd6.conf`, polkuun `/etc/dhcp/`. Käyttäjälle lisättiin myös luku- ja kirjoitusoikeus kyseiselle tiedostolle. Konfiguraatitiedostoon lisättiin jaettavaksi prefiksi `2001:db8:1000:ff00::/56` IPv6-aliverkosta `2001:db8:1000::/64` saapuville DHCP-pyyntöille (kuva 17).

Lopuksi palvelin asetettiin toimimaan operaattorin reunareitittimeen yhteydessä olevalla linkillä muokkaamalla käynnistys-skriptiin oletusrajapinnaksi `ens2`-liityntäportti. Tämän jälkeen itse DHCPv6-palvelu voitiin käynnistää komennolla `sudo dhcpd -6 -cf /etc/dhcp/dhcpd6.conf`, joka käynnistää palvelimen IPv6-tilassa käyttäen aikaisemmin määritettyä konfiguraatitiedostoa.

4.3 Delegoitu prefiksi

Delegaatio saatiin lopulta testattua onnistuneesti myös ISC DHCP -palvelimen ja asiakasreitittimen välillä. Palvelimen jakama `2001:db8:1000:ff00::/56`-prefiksi tuli asiakasreitittimelle käyttöön. Tästä asiakasreititin jakoi eteenpäin 64-bitin `2001:db8:1000:ff00/64`-prefiksiä muille lähiverkon laitteille ja asetti lähiverkon oletusyhdykäytävän osoitteeksi osoitteen `2001:db8:1000:ff00::1` kuvan 18 mukaisesti.



Kuva 18. Asiakkaan reitittimen saama prefiksi operaattorin DHCP-palvelimelta

Windows päätelaitteet loivat lopuksi omat IPv6 osoitteensa router advertisement -viesteistä saaduilla tiedoilla. Windows 7 -pätelaitteen luomat osoitteet on nähtävissä kuvassa 19. Uudemmallalla Windows 7 -laitteella prefiksin perään luotu rajapinnan tunniste on satunnaisgeneroitu, eikä se näin sisällä MAC-osoitteen tietoja.

```
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . : lan
IPv6 Address . . . . . : 2001:db8:1000:ff00:1588:1a3a:5d19:f7c5
Temporary IPv6 Address . . . . . : 2001:db8:1000:ff00:c1a3:fdcc:3a85:8da1
Link-local IPv6 Address . . . . . : fe80::1588:1a3a:5d19:f7c5%13
IPv4 Address . . . . . : 192.168.1.232
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::8039:46ff:fe65:2310%13
192.168.1.1
```

Kuva 19. Päätelaitteen luoma IPv6-osoite

Onnistuneen prefix-delegationin jälkeen myös operaattorin reunareititin oli lisännyt reititustauluunsa staattisen reitin jaetulle prefiksille.

5 JATKOKEHITYS

Työstä ei nimellisesti jäänyt jatkokehittävää. Laajuuden vuoksi aiheen käsittely kuitenkin jäi melko pintapuoliseksi. Esimerkiksi asiakkaalle jaettavien osoitteiden osoitesuunnitelmaan ei työssä otettu kantaa. Internet-operaattoreiden IPv6-osoitesuunnitelmiin suosituksia jakavat regional internet registry -organisaatiot (RIR), Euroopassa RIPE NCC. Myös syventävä katsaus operaattorin ja asiakkaan välisessä interaktiossa etenkin IPv6-ominaisuuksien tietoturvan osalta voisi toimia projekti- tai opinnäytetyöaiheena.

Mahdollisia seuraavan askeleen jatkokehityskohteita olisi ehkä itse toimeksiantajan verkon toteutuksessa. Tähän voisi sisältyä suunnitelman sovittaminen

toimeksiantajan laitteistolle. Työn toteutuksen virtuaalilaitteet eivät vastanneet operaattorilla käytössä olevia, joten heidän laitteensa konfigurointiin vaadittaisiin kuitenkin erillinen konfiguraatio ja selvitys tarvittavien ominaisuuksien löytymisestä laitteistolta.

6 POHDINTA

Työn tavoitteena oli selvittää internet-operaattorin IPv6-protokollan käyttöönottoa verkon asiakasosueella. Tarkoituksena oli löytää hyväksi havaittuja toimintatapoja ja malleja toteutukselle. Toimeksiantajalle näistä haluttiin saada dokumentti, joka toimisi heille ohjeena oman toteutuksensa yhteydessä. Työ rajattiin käsittämään asiakkaan ja operaattorin verkon välisen osuuden toiminta ja sen tärkeimmät laitteet. Tähän kuului asiakkaan verkkolaitteen toiminta asiakkaan omassa verkossa olevien laitteiden kanssa, sekä vuorovaikutus operaattorin laitteiston kanssa. Operaattorilta osuuteen kuului asiakkaan laitteen kanssa yhteydessä oleva reunalaite ja erillinen asiakkaiden tietoja hallitseva DHCP-palvelin. Suunnitelman perusteella luotiin toteutus laboratorioympäristössä ja testattiin onnistuneen prefix-delegaation toimivuus.

Työstä saatiin toimeksiantajalle haluttu palautus tehtyä vaikkakin se olisi voinut olla tarkemmin toimeksiantajan käyttöön kohdennettu ja kattavampi, kuin mitä se nykyisellään oli. Etenkin DHCP-palvelimen toimintaan liittyvät asiat olisivat vaatineet tarkempaa läpikäyntiä.

Työn alkuperäinen noin 6 kuukauden aikataulu oli jälkikäteen mietittynä liian tiukka, etenkin työssä ilmenneet haasteet huomioon ottaen. Työhön kuului paljon uutta opeteltavaa monelta eri alueelta ja tässä suhteessa rohkeampi rajaus olisi ollut työn kannalta hyvin oleellista. Vaikka IPv6:een liittyvää opetusta oli kursseilla ollut, oli pääpaino IPv4:ssä. Tämä lisäsi osaltaan uuden opittavan tiedon määrää. Lisäksi suunnitelman toteutuksessa tarvittavaan DHCP-palvelimen käyttöönottoon liittyi omat haasteensa. Monesta osasta ja ennestään tuntemattomista ohjelmistoista ja asioista johtuen aikaa kului myös osittain ylimääräisten asioiden selvittämiseen ja tiedon hankintaan, etenkin ongelmatilanteissa.

LÄHTEET

6deploy. 2012. IPv6 Autoconfiguration. Saatavilla: http://www.6deploy.eu/tutorials/080-6deploy_ipv6_autoconfiguration_mechs_v0_4.pdf [viitattu 23.5.2018].

Blanchet, M. 2006. *Migrating to IPv6: A practical guide to implementing IPv6 in mobile and fixed networks*. Chichester: J. Wiley & Sons.

Cisco. 2006. Internet Protocol Version 6 Q&A. Saatavilla: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/prod_gas0900aecd803715bf.html [viitattu 23.5.2018].

Cisco. 2011. DHCPv6 Based IPv6 Access Services. Saatavilla: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/whitepaper_c11-689821.html [viitattu 23.5.2018].

Cisco. 2012. IPv6 Neighbor Discovery. Saatavilla: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-15-2mt-book/ip6-neighb-disc.html> [viitattu 19.5.2018].

Deering & Hinden. 2017. Internet Protocol, Version 6 (IPv6) Specification. Saatavilla: <https://tools.ietf.org/pdf/rfc8200.pdf> [viitattu 8.5.2018].

Deering, ym. 2005. IPv6 Scoped Address Architecture. Saatavilla: <https://tools.ietf.org/pdf/rfc4007.pdf> [viitattu 21.4.2018].

Droms, ym. 2003. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Saatavilla: <https://tools.ietf.org/pdf/rfc3315.pdf> [viitattu 20.5.2018].

Graziani, R. 2013. *IPv6 fundamentals: A straightforward approach to understanding IPv6*. Indianapolis, IN: Cisco Press.

Hinden. 2006. IP Version 6 Addressing Architecture. Saatavilla: <https://tools.ietf.org/pdf/rfc4291.pdf> [viitattu 21.4.2018].

Miyakawa & Droms. 2004. Requirements for IPv6 Prefix Delegation. Saatavilla: <https://tools.ietf.org/pdf/rfc3769.pdf> [viitattu 16.5.2018].

Narten, ym. 2007. Neighbor Discovery for IP version 6 (IPv6). Saatavilla: <https://tools.ietf.org/pdf/rfc4861.pdf> [viitattu 14.5.2018].

Narten, ym. 2011. IPv6 Address Assignment to End Sites. Saatavilla: <https://tools.ietf.org/pdf/rfc6177.pdf> [viitattu 16.5.2018].

OpenWRT. 2018. Welcome to the OpenWrt Project. Saatavilla: <https://openwrt.org> [viitattu 28.5.2018].

Thomson, ym. 2007. IPv6 Stateless Address Autoconfiguration. Saatavilla: <https://tools.ietf.org/pdf/rfc4862.pdf> [viitattu 15.5.2018].

Viestintävirasto. 2014. Määräys teleyritysten tietojen säilytysvelvollisuudesta viranomaistarpeita varten. Saatavilla: <https://www.viestintavirasto.fi/attachments/maaraykset/Viestintavirasto53B2014.pdf> [viitattu 10.12.2017].

Volz. 2006. Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option. Saatavilla: <https://tools.ietf.org/pdf/rfc4649.pdf> [viitattu 14.5.2018].

KUVALUETTELO

Kuva 1. Esimerkki 60-bittisen prefiksin esitystavoista (Hinden. 2006, 5)

Kuva 2. Julkisesti reititettävän IPv6-osoitteen rakenne (Hinden 2006, 9)

Kuva 3. Router advertisement viestin sisältö (Narten ym. 2007,19)

Kuva 4. Havainnollistus arkkitehtuurin kokoonpanosta

Kuva 5. Suunnitelman verkkotopologia

Kuva 6. Prefix delegaation viestienvaihto laitteiden välillä

Kuva 7. Toteutettavan verkon kokonaiskuva laitteistosta

Kuva 8. Virtuaalilaboratorion laitteisto ja kytkennät

Kuva 9. Asiakkaan verkon kuva

Kuva 10. WAN6-rajapinnan konfiguraationäkymä

Kuva 11. Lähiverkon konfiguraationäkymä

Kuva 12. Ciscon DHCPv6-palvelimelta saatu prefiksi käytössä

Kuva 13. Päätelaitteen luoma IPv6-konfiguraatio

Kuva 14. Operaattorin verkon kuva

Kuva 15. Asiakaskeskittimen konfiguraatio

Kuva 16. Operaattorin reunareitittimen konfiguraatio

Kuva 17. dhcpd6.conf -tiedoston osoitteenjaon konfiguraatio

Kuva 18. Asiakkaan reitittimen saama prefiksi operaattorin DHCP-palvelimelta

Kuva 19. Päätelaitteen luoma IPv6-osoite