jamk.fi

IPv6 verkon suunnittelu ja toteutus operaattoriverkossa

Case: Haminan Energia

Joonas Tikkanen

Opinnäytetyö
Helmikuu 2016
Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala
Tietoverkkotekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Tikkanen, Joonas	Opinnäytetyö, AMK	2/2016
	Sivumäärä 66	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi

IPv6 verkon suunnittelu ja toteutus operaattoriverkossa
Case: Haminan Energia

Tutkinto-ohjelma

Tietotekniikka

Työn ohjaaja(t)

Saharinen Karo, Rantonen Mika

Toimeksiantaja(t)

Haminan Energia Oy

Tiivistelmä

Työn tavoitteena oli luoda suunnitelmallinen IPv6 -verkkototeutus, joka voidaan viedä Haminan Energian asiakkaille. Tehtävänä oli tutkia IPv6:n toiminnollisuuksia sekä toteuttaa toimiva kaksoispinoverkko Haminan Energian asiakkaille.

Opinnäytetyön toimeksiantajana toimi Haminan Energia Oy, joka toimittaa kuitu- sekä laajakaistayhteyksiä Haminan seudulla. Työ toteutettiin Haminan Energian asiakasverkkoon käyttäen apuna jo luotua DHCPv6 -palvelinta. Työ aloitettiin tekemällä muutossuunnitelma. Tämän jälkeen toteutettiin laboratorioverkko suunnitellun muutoksen pohjalta. Laboratorioverkon toteutusta käyttäen luotiin toimiva kaksoispinoverkko vapaaehtoisille kuituasiakkaille kokeilujaksoa varten.

Työn tuloksena luotiin toimiva kaksoispinoverkko, jossa pystyy käyttämään IPv4- sekä IPv6- standardin palveluita samanaikaisesti. Työtä voidaan käyttää soveltavana esimerkkinä muihin operaattoriverkkoihin, jotka miettivät IPv6 -standardin tuen tuomista omaan verkkoonsa.

Avainsanat (asiasanat)

IPv6, DHCPv6, Operaattoriverkko, kaksoispino, ICMPv6

Muut tiedot

jamk.fi

Description

Author(s)	Type of publication	Date
Tikkanen, Joonas	Bachelor's thesis	2/2016
		Language of publication: Finnish
	Number of pages 66	Permission for web publication: x

Title of publication

The IPv6 Plan and Implement in Carrier Network
Case: Haminan Energia

Degree programme
Information Technology

Supervisor(s)
Saharinen Karo, Rantonen Mika

Assigned by
Haminan Energia Oy

Abstract

The aim of this study was to create systematical IPv6 network implementation, which can be brought to customers of Haminan Energia Oy. The objective was to study the functions of IPv6 standard and implement a working Dual Stack data network.

This thesis was assigned by Hamina Energia Oy that delivers fiber and broadband connections inside Hamina region. The work was carried out into the company's customer network with usage of already implemented DHCPv6 server. The work was started by writing the transition plan. After that the laboratory network was implemented based on the plan. Using the implemented laboratory network the functional Dual Stack network was created, and it was used on a test period by volunteered fiber customers.

The thesis resulted in a fully working dual stack network, which is capable to use IPv4 and IPv6 services simultaneously. The work can be used as an adaptable example to other carrier networks where IPv6 standard is considered to be brought to their networks.

Keywords/tags (subjects)

IPv6, DHCPv6, Carrier Network, Dual Stack, ICMPv6

Miscellaneous

Sisältö

Kuviot

Taulukot

Lyhenteet

AH	Authentication Header
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BDR	Backup Designated Router
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 4
DNS	Domain Name System
DSLAM	Digital subscriber line access multiplexer
ESP	Encapsulating Security Payload
FNE	Fiber Network Eight
FTP	File Transfer Protocol
FTTB	Fiber to the Building
FTTH	Fiber to the Home
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
IoT	Internet of Things
IPSec	IP Security Architecture
IPTV	Internet Protocol television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
LACP	Link Aggregation Control Protocol
MAC	Media Access Control
MCT	Multi Cable Transits
MTU	Maximum transmission unit
NAT	Network address translation
NAT-PT	Network Address Translation Protocol Translation
NDP	Neighbor Discovery Protocol
OSI	Open Systems Interconnection
OSPFv3	Open Shortest Path First version 3
Oy	Osake Yhtiö
PPP	Point-to-Point Protocol
SFTP	SSH File Transfer Protocol
SLAAC	StateLess Address Auto Configuration
SNMPv2	Simple Network Management Protocol version 2
SSH	Secure Shell
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network
Wimax	Worldwide Interoperability for Microwave Access
VLAN	Virtual LAN
VRF	Virtual Routing and Forwarding

1 Työn lähtökohdat

1.1 Toimeksiantaja

Opinnäytetyön toimeksiantajana toimi Haminan Energia Oy. Haminan Energia tarjoaa markkinointinimellä Haminetti verkko-operaattoripalveluita Haminan lähialueella. Haminetin pääasialliset palvelut sijoittuvat laajakaistayhteyksiin. Haminetti tarjoaa myös langatonta Wimax -laajakaistayhteyttä, joka ylettyy Haminan haja-asutusalueille sekä saaristoon.

Ennen yrityksen alkua, vuonna 1901 se toimi Haminan kaupungin sähkölaitoksena. Hamina oli Suomen ensimmäinen kaupunki, joka aloitti maakaasun jakelun vuonna 1982. Maakaasun jakelun myötä sähkölaitoksen nimi muutettiin Haminan Energialaitokseksi. Energialaitos yhtiöitettiin vuonna 1994 alan murroksen sekä vaatimuksien muuttuessa. Yhtiöittämisen seurauksena perustettiin Haminan Energia Oy, jonka osakekanta on Haminan kaupungin omistuksessa. Haminan Energian päätoimisena liiketoimintana ovat sähkön ja maakaasun jakelu. Jakelun lisäksi toiminta kattaa kaukolämmön jakelun sekä tiedonsiirtopalvelut. (Historia)

1.2 Toimeksianto

Työn tarkoituksena oli tuoda IPv6 -osoitteistus kaksoispinotekniikkaa käyttäen Haminan Energian tietoverkkoasiakkaille. Toimeksiannon tarkoituksena oli käyttää jo aiemmin opinnäytetyönä tehtyä DHCPv6-palvelinta ja rakentaen IPv6 yhteensopiva tietoverkko jo olemassa olevaan verkkoinfrastruktuuriin.

Työssä esiteltiin IPv6 -protokolla sekä sen toimintoja. Lisäksi kerrottiin erilaisia transitiomekanismeja, miten voidaan siirtyä IPv4- verkosta IPv6- verkkoon. Työssä tehtiin toimeksiantajalle IPv6 -muutossuunnitelma sekä luodaan laboratorioverkko, jossa tutkittiin IPv6 -protokollan yhteensopivuutta verkkoinfrastruktuurissa. Lopuksi laboratorioverkon toteutus vietiin suunnitelmallisesti asiakasverkkoon ottaen huomioon verkkoon tehtävät muutokset. Työn lopussa pohdittiin, miten työ edistyi sekä mietitään tulevaisuuteen, kuinka kauan siirtymisvaihe uuteen IP-standardiin tietoverkko alalla kestää.

2 Internet Protocol version 6

2.1 Yleistä

Internet Protocol Version 6 eli lyhennettynä IPv6 -teknologian kehitys aloitettiin, kun huomattiin IPv4 -tekniikan rajallisuus. IPv6 on määritelty standardissa RFC2460, joka julkaistiin vuonna 1998. Suurin syy IPv6:n kehitykselle oli äkillinen julkisten IPv4-osoitteiden loppuminen. Jotta IPv6 -protokolla on kyvykäs skaalautumaan tulevaisuuden tarpeisiin, sen on tarjottava rajaton määrä IP-osoitteita sekä samalla tuotava liikkuvuutta. Nykyinen IPv6 sisällyttää laajennetun osoitteistustekniikan, joka on edeltäjäänsä tehokkaampi, tuoden enemmän ominaisuuksia pakettien otsikkoihin. (Teare ,& Paquet, 2007, 649) (Internet Protocol, Version 6 (IPv6) Specification, 2015)

2.2 IPv6:n ominaisuudet

IPv6-standardi tuo tietoverkkoon kehittyneempiä ominaisuuksia, kuin aiemmin käytetyssä IPv4-standardissa oli. IPv6 -standardin osoiteavaruus laajennettiin 32-bittisestä 128 bittiin. Tämä muutos toi useita hyötyjä verkkoon. Aiemmin IPv4-standardissa IP-osoitteita oli tarjolla 2^32 eli noin 4.3 miljardia, mutta nykyinen IPv6 verkko mahdol-listaa jopa 340 sekstiljoonaa IP-osoitetta (340 * 10^36). Laajemman osoiteavaruuden myötä esimerkiksi NAT-osoitteenmuutoksesta voitiin luopua. NAT-tekniikan luopumi-sen ansiosta tietoverkko yksinkertaistuu eikä osoitteita tarvitse uudelleen muodostaa. Isompi osoiteavaruus mahdollistaa myös niin sanotun ”plug and play” toiminallisuu-den päätelaitteiden automaattisen konfiguraation ansiosta. (Teare , & Paquet, 2007, 650)

IPv6 -standardin otsikointi on yksinkertaistettu verrattuna IPv4 -otsikoihin. IPv6-otsikointi parantaa mm. reitityksen tehokkuutta sekä edelleen lähetyksien suhdetta. Samalla IPv6 otsikointi poistaa pakettien tarkastussummaamisen. IPv6 -laajennusotsikoiden sekä vuon leiman avulla eri tietovirtoja ei tarvitse erikseen tunnistaa OSI -standardin kuljetus (transport) tasolla. (Teare , & Paquet, 2007, 650)

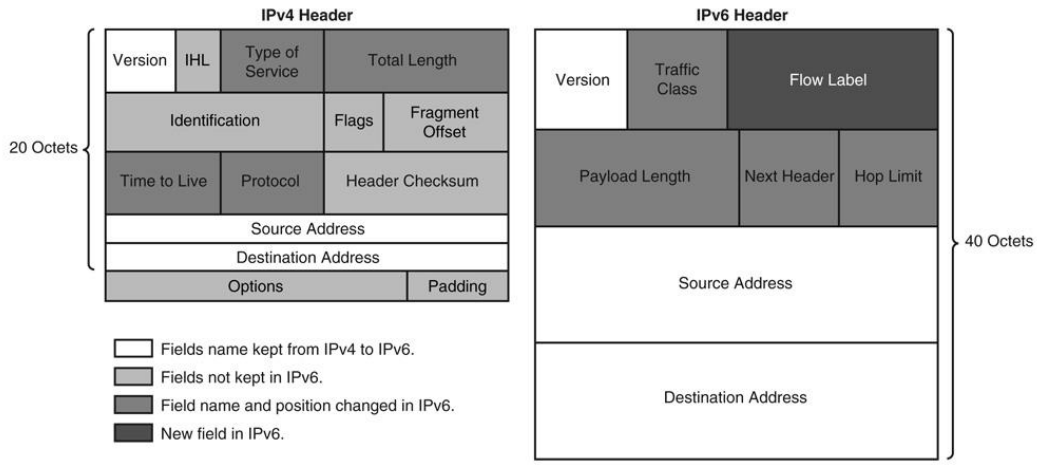
IPv6 standardi tuo tukea parempaan kannettavien älylaitteiden IP-verkkoon sekä tietoturvallisuuteen integroimalla IPSec-standardin suoraan IPv6 -protokollaan. Kannet-

tavuutta IPv6 -standardissa on ehostettu siten, että kannettava laite voi liikkua verkosta toiseen katkaisematta yhteyttä tai muuttamatta IP-osoitetta. IPv6:n laajennusotsikoiden avulla voidaan IPSec -yhteys muodostaa jokaisen verkon solmukohdan välille. kiteytettynä IPv6-standardi on tehokas edistys IPv4-standardista, joka muokkautuu paremmin nykyverkon vaatimuksiin. (Teare , & Paquet, 2007, 650)

3 IPv6:n osoitteet

3.1 IPv6-otsikko

Kuten kuviosta 1 voidaan havaita, IPv6 -standardin otsikko on noin tuplasti isompi verrattuna IPv4 -otsikkoon. IPv6 otsikossa on vähemmän kenttiä kuin IPv4 -otsikossa. IPv6 -rakenne on optimoitu 64-bittisille prosessoreille, jotka nopeuttavat pakettien purkua ja kokoamista suoraan rautatasolla. Koska osoitteet ovat 128 -bittisiä, IPv6 -osoitealueet ovat samalla neljä kertaa isompia kuin IPv4 -osoitealueet. IPv6- ja IPv4-standardissa on seitsemän samanlaista tai samaa tehtävää ajavaa aluetta. (Teare & Paquet, 2007, 653-655.)



Kuvio 1. Vertailu IPv4- ja IPv6 -standardin otsikoinnista (Overview of IPv6)

IPv6 otsikon ensimmäinen kenttä ”Version” kertoo heti paketin alussa, että kyseessä on IPv6-standardia käyttävä verkkopaketti. ”Traffic Class” -kenttä on sama asia kuin IPv4-otsikko kentän ”Type Of Service”. ”Traffic Class” -kenttä merkkaa paketin käyttämään haluttua palvelun laatu luokkaa (Quality of Service). Kenttä ”Flow Label” on 20 bittiä pitkä, joka on uusi IPv6-standardissa. Sitä voidaan käyttää, kun halutaan

merkitä jonkin paketin kuuluvan tiettyyn tietovirtaan. Tämä auttaa usean tason kytkimiä sekä reitittimiä käsittelemään liikennettä virroittain eikä paketti kerrallaan. Tämä toiminto nopeuttaa pakettien kytkentäprosesseja. ”Flow Label” -kenttää voi myös käyttää palvelun laadun tuottamisessa. ”Payload Length” -kenttä kertoo laitteelle, kuinka iso paketin tietosisältö on. IPv6-otsikkokenttä ”Next Header” on 8 bitin kokoinen kenttä, joka määrittelee, minkä tyyppistä tietoa on tulossa IPv6-otsikon jälkeen. Tieto voi olla OSI-mallin kuljetustason tietoa, esimerkiksi se voi kertoa, kuljetetaanko tieto TCP- vai UDP -protokollan mukaisesti. Kentän sisältämä tieto kertoo myös usein myöhemmin otsikkokentässä olevasta laajennusotsikosta. ”Hop Limit”-kenttä on 8 bittiä pitkä tieto, joka määrittelee paketin kulkeman enimmäismäärän, ennen kuin se pudotetaan tietovirrasta. Jokainen verkkojen välinen hyppy vähentää arvoa yhdellä. Jos arvo tippuu nollaan, lähetetään tieto lähettäjälle, että paketti hylättiin. Kentät ”Source Address” sekä ”Destination Address” sisältävät tiedot paketin lähde- ja kohdeosoitteista. Kentät ovat 16 oktettia pitkiä eli 128 bittiä. On huomattava, ettei IPv6 -otsikossa ole tarkastussumma(Checksum) otsikkoa, koska tarkastussumma sekä virheen hallinta suoritetaan kytkentätason teknologioissa. (Teare & Paquet, 2007, 653-655.)

3.2 IPv6-laajennusotsikot

IPv6 -standardin laajennusotsikot auttavat verkkolaitteita käsittelemään tietoa tehokkaammin luovuttamalla muille verkkolaitteelle olennaista prosessointitietoa. Koska IPv6 -standardin laajennusotsikot eivät ole vakiopituisia, ne sijoitetaan pakettiin ennen varsinaisen tietosisällön ”Payload” -kenttää. Tulevasta laajennusotsikosta ilmais-taan IPv6 -otsikkokentässä ”Next Header”. Yleisesti laajennusotsikoita ei prosessoida missään verkon solmukohdassa vaan ainoastaan sillä laitteella, mihin kyseinen paket-ti on tarkoitettu lähetettävän. Poikkeuksena on kuitenkin ”Hop-by-hop options header”, joka käsitellään verkon jokaisessa solmukohdassa. (Teare & Paquet, 2007, 655-657)

Jos IPv6 paketissa on useampi kuin yksi laajennusotsikko, otsikot lajitellaan seuraavan järjestyksen mukaisesti:

1. IPv6 header
2. Hop-by-hop options header
3. Destination options header
4. Routing header
5. Fragment header
6. Authentication Header and Encapsulating Security Payload header
7. Upper-layer header

Järjestyksessä ensimmäisenä on yleinen IPv6-otsikko ilman mitään laajennusotsikkoa. Seuraavaksi on mainittu ”Hop-by-hop options header”. Kun kyseistä laajennusotsikkoa käytetään, se prosessoidaan verkon jokaisessa solmukohdassa, jotka sijoittuvat mat-kalla päätelaitteelle. Tätä laajennusotsikkoa esimerkiksi käytetään jos käsitellään IPv6 jumbo paketteja eli siis niitä jotka ovat suurempia kuin verkkolaitteeseen määritelty paketin enimmäiskoko (MTU). Järjestyksessä kolmantena käsitellään laajennusotsikko ”Destination options header”. Tätä otsikkoa hyödynnetään kun paketissa on käytössä ”Routing header” laajennusotsikko. ”Next header” otsikko kentän arvolla 60 otsikko käsitellään päätelaitteessa sekä niissä kohteissa mitkä ovat määritelty ”Routing header”-laajennusotsikossa. Tätä laajennusotsikkoa käytetään usein päätelaitteen IPv6 kannettavuus toiminnoissa. ”Routing Header”-laajennusotsikkoa käytetään lähteen reitittämiseen IPv6 kannettavuus toiminnoissa. Otsikossa kerrotaan lähdelista tai tärkeimmät solmukohdat, joissa vieraillaan tiedon siirron aikana kohteeseen mentäessä. (Teare & Paquet, 2007, 655-657)

Laajennusotsikot ”Authentication header and Encapsulating Security Payload header” ovat tiedot, jota IPSec-protokolla käyttää voidakseen siirtää tietoa turvatusti. Otsikot sisältävät tietojen salaukseen tarvittavat AH sekä ESP-otsikkotiedot, jonka avulla muodostetaan yhteys joka on todennettu (Authentication), Eheä (Integrity) sekä luo-tamuksellinen(Confidentiality). Viimeisenä laajennusotsikkona on ”Upper-layer header”, jota tyypillisesti käytetään paketin merkitsemään tiedon kuljetusprotokollan. Merkintä yksinkertaisesti kertoo kuljetetaanko tieto käyttäen TCP(Next header-otsikkokentän arvo 6) vai UDP(Next header -otsikkokentän arvo 17) protokollaa. (Teare & Paquet, 2007, 655-657)

3.3 IPv6 osoitteen esitys

Normaali IPv6 osoite on 32 merkkiä pitkä heksadesimaali osoite. Osoitteessa on kahdeksan 4 heksadesimaali ryhmittymää, jotka eritellään toisistaan kaksoispisteellä. Normaali IPv6 osoite on siis muotoa X:X:X:X:X:X:X:X, jossa X kuvastaa 16-bittistä heksadesimaalia aluetta. Esimerkkiosoite voi olla alla olevassa muodossa:

```
2035:001:2BC5:0000:0000:087C:0000:0000A
```

IPv6-osoitteita voidaan myös lyhentää yksinkertaisempaan muotoon. Jos osoitteessa on kaksi nollan ryhmittymää, voidaan ne lyhentää merkitsemällä kaksi kaksoispistettä (::) peräkkäin osoitteessa. Tuplakaksoispistettä voidaan käyttää vain yhden kerran ja se merkitään osoitteen ensimmäiseen tuplanolla heksadesimaalikenttään. Tuplakaksoispisteen jälkeisen nollakentät voidaan merkitä vain yhdellä nollalla. Myös jos osoitteen heksadesimaali ryhmässä on numero 0 etummaisena, voidaan numero tiputtaa silloin pois. Täten edellä mainituilla osoitteen lyhentämissäännöillä, esimerkki osoite voidaan esittää muotoa:

```
2035:1:2BC5::87C:0:A
```

IPv6-standardin osoitteen aliverkon koko voidaan esittää prefiksillä. Se merkitään osoitteen perään vinoviivalla (/), jonka jälkeen merkitään verkon koko. Kun prefiksi lisätään osoitteeseen, se näyttää tältä:

```
1234:5678::/32
```

IPv6-osoitetta kirjoitettaessa, on huomioitava ettei heksadesimaali osoite ole merkkikokoriippuvainen. Toisin sanoen ei ole väliä onko osoitteen kirjaimet isoja vai pieniä. (Teare ,D. & Paquet, P. 2007. 657-658)

4 IPv6 osoitetyypit

4.1 Yleistä

IPv6-standardissa laitteen rajapinnoilla voi olla useita osoitteita. Jokaisella rajapinnalla on ainakin yksi looginen ”loopback” sekä yksi ”link-local” -osoite. ”Loopback”-rajapinnan osoite on aina ::1/128, jonka tarkoituksena on vastata kyselyihin heti takaisin. Vaihtoehtoisesti rajapinnalla voi olla useita uniikkeja paikallisia sekä julkisia osoitteita.

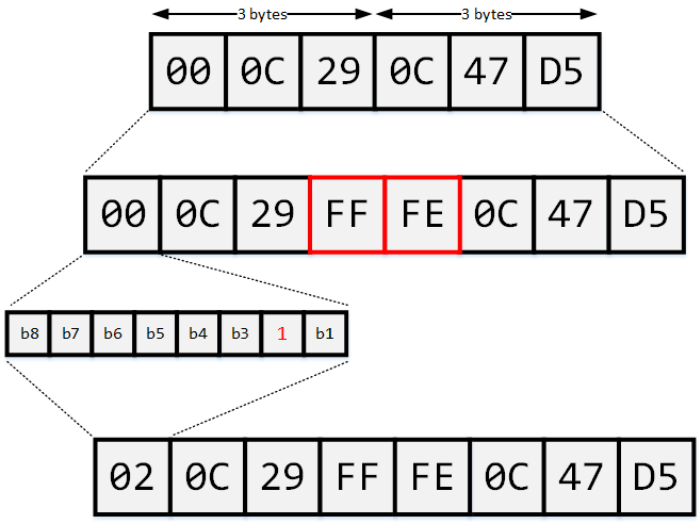
IPv6- osoitteet yleisesti jaotellaan kolmeen eri osoitetyyppiin: Unicast-, Anycast- sekä Multicast-osoitteisiin. Unicast-osoitetyyppi, jolla voidaan kohdentaa tieto menemään juuri yhdelle identifioidulle laitteelle. Anycast-osoitetyyppi on uusi IPv6-osoitetyyppi, jonka hyötynä on identifioida yksi osoite useaan rajapintaan. Anycast-osoitetta hyödynnetään esimerkiksi verkkoliikenteen kuormantasauksessa usean verkkolaitteen kesken. Multicast-osoitteen tarkoituksena on tavoittaa identifioituryhmä päätelaitteita yhdellä osoitteella. (Teare ,D. & Paquet, P. 2007. 658-659.)

4.2 Rajapinnan tunniste IPv6-osoitteissa

IPv6 -osoitteissa käytetään usein rajapinnan tunnisteita erottamaan verkon yksilölliset rajapinnat. Rajapinnan tunniste on yksilöllinen, joka muodostetaan alemman verkkokerroksen mediasta tai kapseloinnista. Rajapinnan tunnisteet ovat aina 64 bittiä pitkiä. Yleisesti rajapinnan tunnisteet luodaan käyttäen Ethernet -protokollan MAC osoitetta, mutta se voidaan luoda myös mm. ”PPP”, ”Token Ring” sekä ”ATM” verkkoprotokollien avulla. (Teare & Paquet, 2007, 658-661)

Ethernet -protokollan rajapinta tunniste muodostetaan MAC-osoitteen avulla sekä tekemällä tunnisteeseen EUI-64 -formaatin mukaiset muutokset. EUI-64 formaatin tunniste tehdään 48 bittisestä MAC osoitteesta, johon lisätään heksadesimaali FFFE kolmannen heksadesimaaliparin jälkeen. Lopuksi tunnisteen alusta seitsemäs bitti käännetään toisinpäin. Kyseinen bitti on ns. universaali/paikallinen bitti, jonka tarkoituksena tunnistaa uniikin osoitteen sijainti paikalliseksi tai universaaliksi osoitteeksi.

Bitin tarkoituksena on kertoa tulevaisuudessa protokollapinon ylemmälle tasolle yksilöllisestä yhteydestä vaikka osoitteen konteksti suurilta osin muuttuisikin. Kyseistä toimintoa ei kuitenkaan vielä ole yleisesti otettu käyttöön. Kuviossa 2. on havainnollistettu EUI-64 tunnisteformaatin muodostamisprosessi kokonaisuudessaan. (Teare & Paquet, 2007, 658-661)

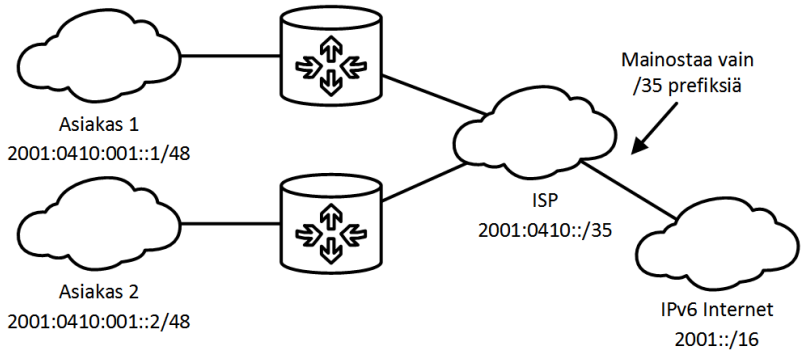


Kuvio 2. EUI-64 tunnisteformaatin muodostamisprosessi

4.2.1 Unicast

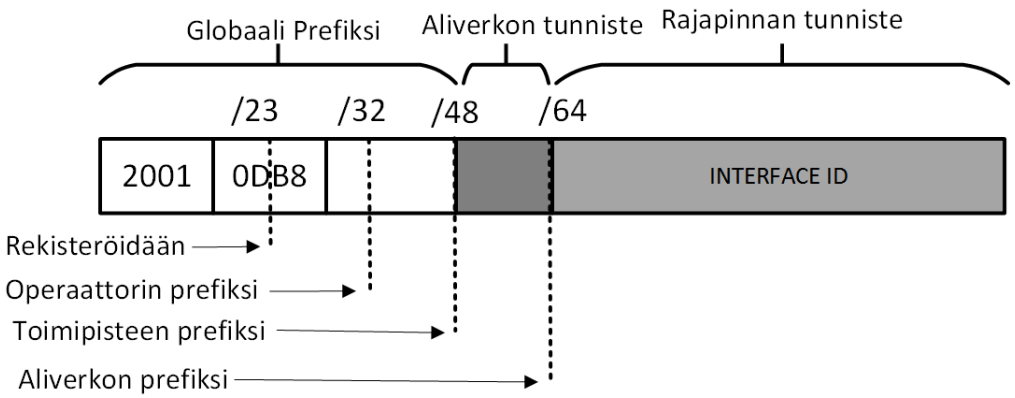
Unicast-osoitetyypillä on kaksi erilaista muotoa, jotka ovat ns. paikallinen osoite eli ”link local” -osoite sekä julkinen osoite eli ”global unicast”- osoite.

”Global Unicast”-osoite on toisin sanoen globaali osoite, joka on valittu universaalista Internetin osoiteavaruudesta. Osoitteen rakenne mahdollistaa pienemmän yleisen reititystaulun summaamalla yhä useampia osoitteita yhteen. Globaalien osoitteiden hierarkian avulla yhä isommat verkot voidaan summata yhteen, mikä nopeuttaa reitittin päätöksien laskemista. Kuviossa 3 on havainnollistettu IPv6-globaalien osoitteiden summautuminen. (Teare & Paquet, 2007, 661-662)



Kuvio 3. IPv6 globaalien osoitteiden summautuminen julkisissa reititystauluissa.

”Global Unicast” -osoite muodostuu 48 bitin suuruisesta globaalista reititysosasta eli prefiksistä, 16-bittisestä aliverkon tunnisteesta sekä aiemmin mainitusta rajapinnan tunnisteesta. Aliverkon tunniste on yksilöllisen organisaation tunniste, joka mahdollistaa sille luoda oman paikallisen osoitehierarkian. Tämä alue antaa kyvyn luoda yli 65 546 yksilöllistä aliverkkoa. Kuviossa 4 on kuvattu, kuinka ”Global Unicast” -osoite muodostetaan. (Teare & Paquet, 2007, 661-662)

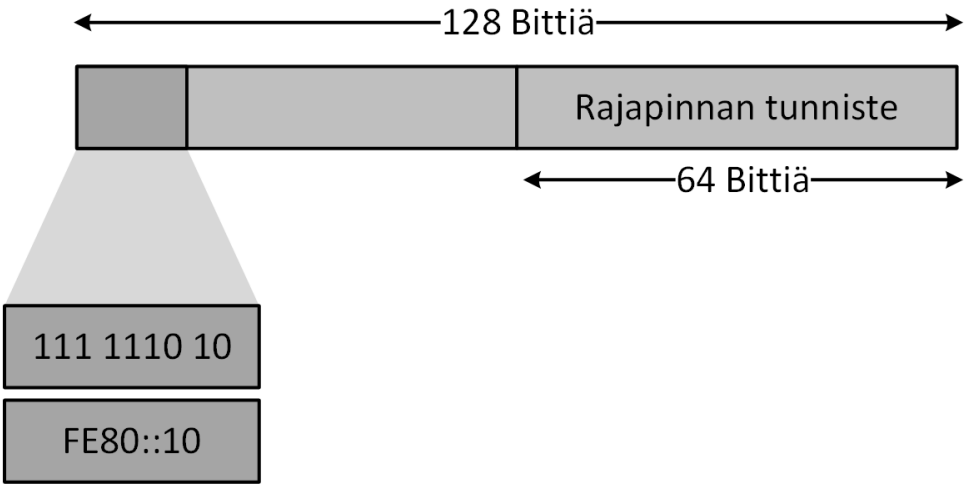


Kuvio 4. "Global Unicast" -osoitteen rakenne

Globaalit IPv6-osoitteen jakamisen hoitaa julkinen organisaatio nimeltä ”Internet Assigned Numbers Authority” eli lyhennettynä IANA. Se jakaa julkisia osoitteita osoitteesta 2001::/16 lähtien. Globaali osoiteavaruus kattaa verkot 2000::/3 verkkoon E000::/3. Osoiteavaruudesta on kuitenkin jätetty pois ”Multicast”-osoite FF00::/8. (Teare & Paquet, 2007, 661-662)

IPv6 -paikallinen osoite eli ”link-local” -osoite muodostetaan FE80::/10 prefiksistä, johon sisältyy EUI-64 standardin mukainen rajapinnan tunniste. ”Link-local” -osoitetta

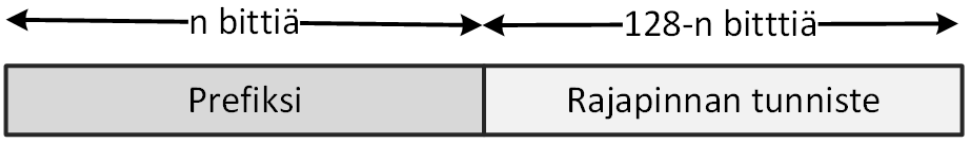
käytetään mm. automaattiseen osoitteen konfiguroimiseen, naapuriverkkojen havaitsemiseen sekä useisiin muihin reititysprotokolliin. Selvennettynä ”Link-Local Unicast”-osoitetta käytetään laitteiden yhdistämiseen lähiverkossa. Kun viestitään paikallisilla osoitteilla, on rajapintojen oltava yksilöllisiä sillä jokainen rajapinta on FE80::/10 prefiksissä. Kuviossa 5 on havainnollistettu ”Link-local” -osoitteen rakenne. (Teare & Paquet, 2007, 661-662)



Kuvio 5. "Link-local" -osoitteen rakenne

4.2.2 Anycast

IPv6 ”Anycast” -osoite on globaali ”Unicast” -osoite, joka on asetettu useammalle kuin yhdelle rajapinnalle. ”Anycast” -osoite on määritelty lähettävän paketin lähimmälle rajapinnalle, joka on asetettu ”Anycast” -osoiteryhmään. ”Anycast” -osoiteryhmä tarjoaa mekanismin, jolla löydetään lähin verkkosolmu. ”Anycast”-osoitteen rakenne on hyvin samanlainen kuin ”Unicast” -osoitteen. ”Anycast” -osoitteen rakenne on kuvattu kuviossa 6. (Teare & Paquet, 2007, 663-664)



Kuvio 6. "Anycast" -osoitteen rakenne

”Anycast” osoitteen toiminta menee seuraavalla tavalla:

- Lähettävä luo paketin missä ”Anycast” -osoite on kohdeosoitteena ja lähettää sen lähimmälle reitittimelle

- Reititin reitittää paketin lähimpään ”Anycast” -rajapintaan (lähin laite tai rajapinta joka jakaa kyseisen osoitteen).
- WAN -verkon reititystaulusta löytyy lähin rajapinta, joka on ensimmäinen naapuri, joka on oppinut kyseisen osoitteen.

”Anycast” -osoitteet jaetaan ”Unicast” -osoiteavaruudesta ja ne ovat samassa formaatissa kuin ”Unicast” -osoitteet, jolloin niitä ei voi erottaa toisistaan. Laitteissa, joihin ei ole asetettu ”Anycast” -osoitetta, nämä osoitteet näkyvät ”Unicast” -osoitteina. Kun ”Unicast” -osoite on asetettu useammalle kuin yhdelle rajapinnalle, se muuntautuu ”Anycast”-osoitteeksi. (Teare & Paquet, 2007, 663-664)

”Anycast” -osoitteita voidaan hyödyntää, kun halutaan kontrolloida liikenteen virtaan verkossa. Esimerkiksi ”Anycast” -osoitteita voidaan käyttää BGP-reitityksessä, kun asiakkaalla on monta yhteyttä eri verkko-operaattoreihin. Toinen käyttöesimerkki on kun verkossa on useampi reititin kytkettynä lähiverkkoon. Kaikki kyseiset reitittimet jakavat saman ”Anycast” -osoitteen. Tällöin etäällä olevien laitteiden tarvitsee tietää vain yksi ”Anycast” -osoitte ja ne voivat laskea sen avulla lähimmän reitin kyseiseen lähiverkkoon. (Teare & Paquet, 2007, 663-664)

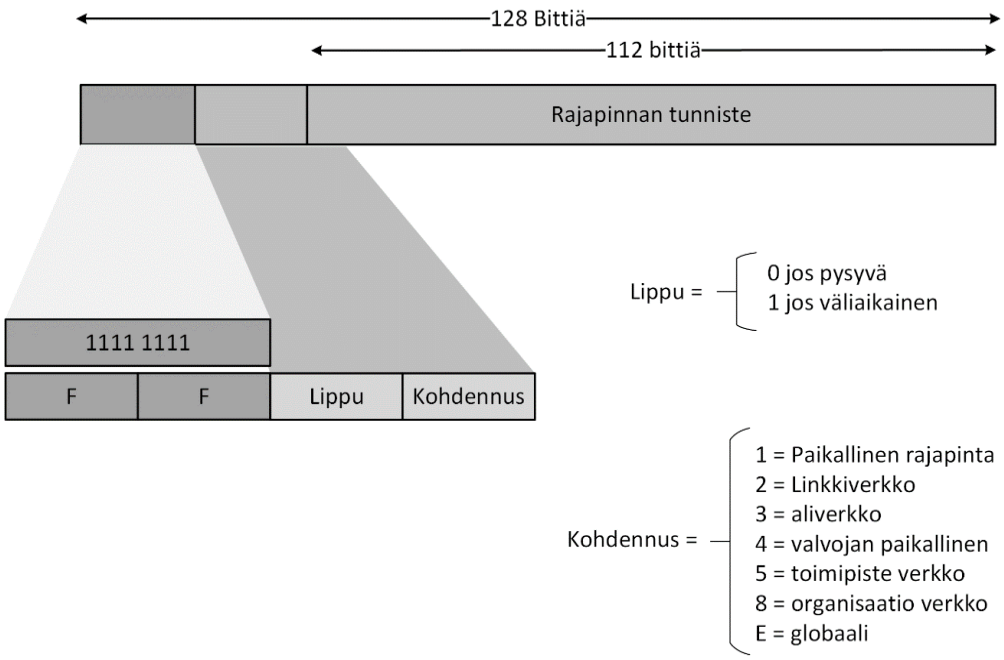
4.2.3 Multicast

”Multicast” -osoitteiden tarkoitus IPv6-standardissa on tavoittaa ryhmä verkon päätelaitteita yhdellä osoitteella. ”Multicast” -osoitteella liikennevirrassa paketti tavoittaa useat päätelaitteet yhtäaikaisesti. Multicast -toiminto on erittäin tärkeä IPv6-standardissa, sillä se toimii monien IPv6 -toimintojen ytimenä. ”Multicast” -toiminto korvaa vanhan IPv4-standardin Broadcast -toiminnon.

IPv6 ”Multicast” -osoitteet ovat valittu prefiksistä FF00::/8. Osoitteen toinen oktetti kertoo paketin eliniän lipun (flag) arvolla sekä mihin paketti kohdennetaan(scope). Jos lipun arvo on 0, on se yleisesti tunnettu ”Multicast”-osoite. Jos taas lipun arvo on 1, on se vain väliaikainen ”Multicast” -osoite. Kohdennusbitin arvolla on useampi eri määre. Määreet ovat selitetty taulukossa 1. ”Multicast” -osoitteen rakenne on esitetty kuviossa 7.

Taulukko 1. Selvennystaulukko "Multicast"-osoitteen kohdennusbitin arvolle

Kohdennus (scope) bi-tin arvo	**Selvennys**
1	Lähetys laitteen loopback rajapintoihin
2	Lähetys laitteeseen kytkettyihin linkkeihin (samanlainen kuin ”Unicast link-local scope”)
3	Lähetys laitteen aliverkkoon
4	Lähetys pääkäyttäjän asettamaan verkkoon (erikseen konfiguroitava)
5	Lähetys koko verkon toimipaikan laitteille
8	Lähetys koko organisaation laitteille (useita toimipaikkoja)
E	Lähetys globaalisti eli koko verkolle



Kuvio 7. "Multicast"-osoitteen rakenne

Osoitteen rakenteessa on 16 bitin etuliite, jossa sijaitsee osoitteen alkuoktetti FF, jonka jälkeen on osoitteen lippu- ja kohdennusbitit. Osoitteelle on jätetty 112 bitin alue, johon sijoitetaan ”Multicast”–ryhmän tunniste.

”Multicast” osoitteet alueesta FF00:: - FF0F:: , joiden lipun arvo on 0, on niille osoitteille varattu erityinen merkitys. IANA hallinnoi näitä erityisesti asetettuja ”Multicast”–osoitteita. Alla olevassa luettelossa on muutamia esimerkkejä erikoisista ”Multicast”–osoitteista:

- FF02::1-Viestin laitteille, jotka ovat suoraan yhdistetty kyseiseen laitteeseen.
- FF02::2-Viesti kaikille verkon reitittimille.
- FF02::9-Viesti kaikille reitittimille, jotka käyttävät RIP-reititysprotokollaa.
- FF02::1:FFXX:XXXX-Viesti tavoitetulle solmulle, missä XX:XXXX on vastaava 24 bitin osoite solmukohdassa, mihin viesti voidaan välittää.
- FF05::101-Viesti kaikille toimialueen NTP- palvelimille

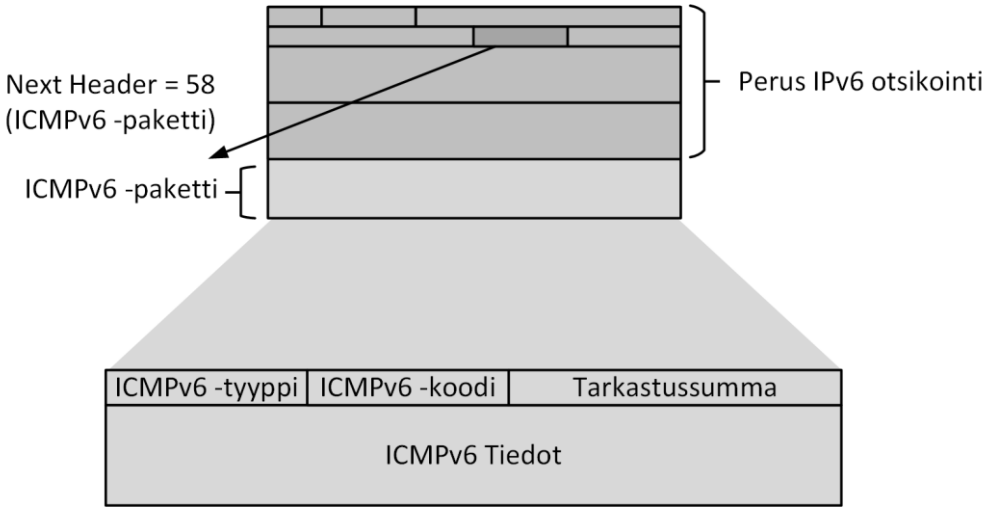
(Teare & Paquet, 2007, 664-666)

5 ICMPv6

5.1 Yleistä

ICMP -protokolla eli Internet Control Message Protocol on suunniteltu jo IPv4-standardiin, jonka jälkeen se myös suunniteltiin IPv6-verkkoon sopivaksi. ICMP-protokollan tarkoituksena on kerätä tietoa verkosta ja kertoa siitä päätelaitteelle. Protokolla ilmoittaa laitteelle, jos verkkopaketit eivät voida prosessoida päätelaitteelle, ja lähettää tiedon lähettäjälle. ICMP-protokollalla voidaan myös diagnosoida verkon laitteen toimivuutta lähettämällä ”ICMP Echo” ja ”ICMP request”-viestejä. Toiminto on paremmin tunnettu sanalla "Ping". (Silvia Hagen. 2014.)

IPv6–verkkoon soveltuva ICMPv6–protokolla on paljon tehokkaampi edeltäjäänsä ICMPv4-protokollaan. Esimerkiksi IGMP–toiminto hallinnoi paljon paremmin multicas-ryhmien jäsenyyksiä. Myös IPv4- standardin ARP/RARP viestit ovat korvattu paljon tehokkaammalla NDP-protokollalla. ICMPv6 -viestin sijoitus IPv6 -pakettiin on kuvattu kuviossa 8. (Silvia Hagen. 2014.)



Kuvio 8. ICMPv6 -viestin sisältö ja sijoitus IPv6 -pakettiin

ICMPv6 -protokollan tiedot sijoitetaan IPv6-otsikoinnen jälkeen ”Payload”-kenttään eli sinne mihin itse paketin tieto sijoitetaan. ”Next Header”-otsikon arvo 58 kertoo että tietosisällössä on ICMPv6 protokollan mukaista tietoa. ICMPv6- viestin ”Type”-kenttä määrittelee, minkä tyyppinen ICMPv6-viesti on. ”Code”-kentän tiedot riippuvat tyyppikentästä. Kentän tarkoituksena on tuoda lisäinformaatiota tietyissä tapauksissa. ”Checksum” eli tarkastussumma kentän tarkoituksena on huomata tietojen pirstaloituminen IPv6- sekä ICMPv6 -otsikoissa. Jotta tarkastussumma voidaan laskea, paketissa on oltava lähde- ja kohdeosoite merkittynä. Tyyppi sekä koodi kenttien tietojen perusteella rakennetaan ”Message Body”-kenttä. ”Message body”-kentän tiedot ei pitäisi ylittää 1280 bittiä. (Silvia Hagen. 2014.)

ICMPv6-viestejä on olemassa kahta eri luokkaa: ”Error Messages” sekä ”Infromational messages”. Häiriöviestit eli ”Error Messages” kertovat verkon häiriöistä, esimerkiksi, jos kohdeosoitetta ei tavoiteta tai paketin koko on liian iso lähetettäväksi. Häiriöviestien arvo tyyppikentässä on 0-127 välillä. ”Informational messages”-luokan tarkoituksena on kertoa tietoa verkon eri osista. Tyyppi kenttään sijoitetaan silloin arvot välillä 128-255. (Silvia Hagen. 2014.)

5.2 NDP

NDP eli Neighbor Discovery Protocol on määritelty alun perin standardissa RFC 4861. NDP:ssä on yhdistettynä monta eri IPv4-standardin tekniikkaa ja vähän enemmänkin. Esimerkiksi ARP ja ”ICMP Router Discovery and Redirect” on implementoitu suoraan

NDP-protokollaan. NDP protokollan avulla voidaan tehdä alla olevan listauksen mukaisia toimintoja:

- Tilaton autokonfiguraatio IPv6 osoitteisiin (SLAAC)
- Selvittää verkon prefixejä, reittejä sekä muita asetuksellisia tietoja.
- Varmentaa ettei verkossa ole kahta eri päätelaitetta samalla osoitteella (Duplicate IP Address Detection)
- Selvittää kytkentätason solmun osoitteita, jotka ovat samassa linkissä
- Etsiä naapuri reitittimiä, jotka voivat uudelleen välittää niiden paketit
- Selvittää mitkä naapuri reitittimet ovat saavutettavissa ja mitkä eivät
- Selvittää muutoksia linkki tason osoitteissa

Kaikki NDP-protokollan toiminnallisuudet perustuvat ICMPv6 ”Informational Messages”-viesteihin. (Silvia Hagen. 2014.)

5.3 NDP-Viestit

NDP-protokolla käyttää viittä eri ICMPv6 viestiä toiminnoissaan. ICMPv6 tyyppi kentän arvot 133-137 on varattu NDP tarvitsemille viesteille.

“Router Solicitation”- eli RS-viestin tarkoituksena on lähettää verkkoon viesti ”Multicast”-osoitteeseen, verkon jokaiselle solmukohdalle. RS-viestissä pyydetään tarvittavia tietoja yhteyden muodostamiseksi esim. oletusyhdyskäytävää ja verkon prefiksiä. Viestin tyyppiarvo paketin sisällä on 133. Viesti itsessään sisältää lähdelaitteen rajapinnan linkkitason MAC-osoitteen. (Functions of NDP, Neighbour Solicitation and Advertisement, Router Solicitation and Advertisement.)

”Router Advertisement”- eli RA-viesti on vastaus edelliseen RS-viestiin. RA-viestin lähettäjä on verkon lähin reititin. Viestin kohde-osoitteeksi tällöin merkitään edellisen viestin lähde osoite eli FF02::1 ”multicast”-osoite. RA-viestin sisältää verkon tietojen lisäksi erilaisia lippuja (flag), jotka kertovat muodostetaanko IPv6-osoite tilattomasti vai tilallisesti. Lyhyt kuvaus lipusta ja sen toiminnoista on kuvattu taulukossa 2. (Functions of NDP, Neighbour Solicitation and Advertisement, Router Solicitation and Advertisement.)

Taulukko 2. RA-Viestien liput ja niiden kuvaukset

Lipun nimi	Kuvaus
”Managed Address Configuration” -lippu	Kertoo päätelaitteelle, että se voi käytää osoitteen muodostukseen DHCPv6-protokollaa tilattoman autokonfiguraation lisäksi.
”Other Stateful Configuration”-lippu	Kertoo päätelaitteelle, että voi käyttää osoitteen muodostukseen vain DHCPv6-protokollaa.
”Home Agent”-lippu	Kertoo päätelaitteelle, että reititin toimii ns. kotiagenttina (”Home Agent”), joka toimii etänä olevien laitteiden rekisteröijänä.
”Default Router Preference”-lippu	Määrittää RA-viestin tärkeyden, jos verkosta tulee useita RA-viestejä eri reitittimiltä. Lipun tärkeysarvot: 01-Korkea 00-Keskitaso (oletusarvo) 11-Matala 10-Varattu
”Prx” -lippu	Välittää ND-viestit määriteltyyn verkkoon

Verkon perustietojen ja lippujen lisäksi RA-viesti sisältää aikamääreet, kuinka kauan naapuruus pidetään pystyssä ennen uutta keskustelua, sekä myös reitittimen lähiverkon rajapinnan MAC-osoite. (Functions of NDP, Neighbour Solicitation and Advertisement, Router Solicitation and Advertisement.)

”Neighbour Solicitation”- eli NS-viestejä käytetään silloin kun halutaan selvittää laitteen MAC-osoite toisesta IPv6- verkon laitteesta. NS-viesti lähetetään paikalliseen ”Multicast”-osoitteeseen, jonka sisällä on tietoa mm. lähettäjän MAC-osoite. ICMPv6-vietin tyyppi kentässä on tällöin arvo 135. (Functions of NDP, Neighbour Solicitation and Advertisement, Router Solicitation and Advertisement.)

”Neighbour Advertisement” eli lyhennettynä NA-viesti on vastaus NS-viestiin. Verkon jokainen laite viestii NS sekä NA viestejä, selvittääkseen laitteiden keskeisiä naapuruuksia. NA-viestin siis lähettää NS-viestin lähettäneen laitteen lähin toinen laite. NA-viestit voivat olla ns. pyydettyjä tai ei-pyydettyjä. Jos viesti on ei-pyydetty, on viesti lähetetty laitteelle jonka MAC-osoite on vaihtunut. Kuten RA-viestissä, niin myös NA-viesti sisältää lippuja. NA-viestissä voi olla kolme erilaista lippua:

- Jos ”Router”-lipun arvo on 1, on lähettäjälaite reititin.
- Jos ”Solicitated”-lipun arvo on 1, on NA-viesti vastaus saatuun NS-viestiin.
- ”Override”-lippua käytetään kun halutaan kertoa vastaanottavalle laitteelle, että sen täytyy tyhjentää paikallinen olemassa oleva naapuruus välimuisti (kun lipun arvo on 1).

NA-viestin lippujen lisäksi, viesti sisältää pyydetyn IPv6- osoitteen ja saman rajapinnan MAC-osoitteen. (Functions of NDP, Neighbour Solicitation and Advertisement, Router Solicitation and Advertisement.)

NDP-protokollan viimeinen viesti on ns. uudelleen lähetys viesti. Viestin ICMPv6 tyyppi kentän arvo on 137. Viesti lähetetään reitittimestä, kun se haluaa kertoa päätelaitteelle lyhemmästä polusta reitittimelle.

(Functions of NDP, Neighbour Solicitation and Advertisement, Router Solicitation and Advertisement.)

5.4 Autokonfiguraatio

5.4.1 Yleisesti

IPv6-standardissa on mahdollisuus käyttää kahta eri autokonfiguraatio tekniikkaa. Tekniikoita sanotaan ns. tilattomaksi sekä tilalliseksi autokonfiguraatioksi. Autokonfiguraatio tekniikoiden avulla voidaan määrittää päätelaitteiden verkko-osoitteet automaattisesti ennalta määritetystä osoiteavaruudesta. Kummassakin autokonfiguraatiossa ovat omat hyödyt sekä haitat, jotka ovat selvennettynä tarkemmin tulevissa alaotsikoissa. (Silvia Hagen. 2014.)

5.4.2 Tilaton

Tilaton autokonfiguraatio eli SLAAC (Stateless Address Autoconfiguration) toiminto on yksinkertainen muoto muodostaa IPv6 osoite. Se on suunniteltu niin, että laitteeseen ei tarvitse käsin tehdä mitään muutosta jotta laite voi saada yhteyden verkkoon. Tämä toiminto helpottaa ns. IoT(Internet of Things)-verkkoa, jossa on useita automatisoituja laitteita. Tilaton autokonfiguraatio on myös käytännöllinen yleisissä sekä tilapäisissä Ad-Hoc verkoissa, jossa halutaan minimoida järjestelmän hallintatyö.

Tilaton autokonfiguraatio on ainoastaan päätelaitteiden toiminto, eikä se toimi esimerkiksi reitittimissä. Kun päätelaite liitetään verkkoon, alkaa tilattoman autokonfiguraation prosessi, joka menee alla olevan järjestyksen mukaisesti:

1. Ensin laite muodostaa paikallisen ”link-local” -osoitteen käyttäen FE80::/64 prefiksiä sekä EUI-64 mukaista rajapinnan tunnistetta. Tämä toimii autokonfiguraatiossa ns. kokeellisena osoitteena ennen virallisen IPv6- osoitteen määrittämistä.
2. Laite liittyy kaikkien laitteiden (FF02::1) sekä alustavien osoitteiden ”Multicast” ryhmiin.
3. NDP-viesti ”Neighbor Solicitation”, jossa kohteena on kokeellinen osoite ja lähdeosoitteessa kaikki ovat nollia. Kohdeosoite kuuluu alustavien osoitteiden ”multicast”-ryhmään, joka aloittaa DAD prosessin, joka tarkista ettei verkossa ole laitetta samalla rajapinnan tunnisteella. Jos sama tunniste löytyy verkosta, ”Neighbor Advertisement” -vastausviesti lähetetään ja prosessi keskeytetään. Rajapinnan tunniste muodostetaan satunnaisella luvulla, jonka jälkeen DAD-prosessi viedään loppuun.
4. Voidakseen selvittää päätelaitteen oletusyhdyskäytävä, että verkossa on oltava IPv6 reititin. Se selvitetään lähettämällä NDP-viesti ”Router Solicitation” kaikille verkon solmuille multicast ryhmään kohteena FF02::2.
5. Kaikki verkon reitittimet vastaavat ”Router Advertisement”-viestillä, jossa on kunkin reitittimen oma prefiksi.
6. Tämän jälkeen päätelaite määrittää itselleen verkko-osoitteen yhdistämällä reitittimen prefiksin sekä rajapinnan tunnisteen.

Tilallisessa autokonfiguraatiossa verkko-osoitteet varmistetaan ennen asettamista, etteivät osoitteet ole kahdentuneet verkossa. (Silvia Hagen. 2014.)

6 DHCPv6

6.1 Yleistä

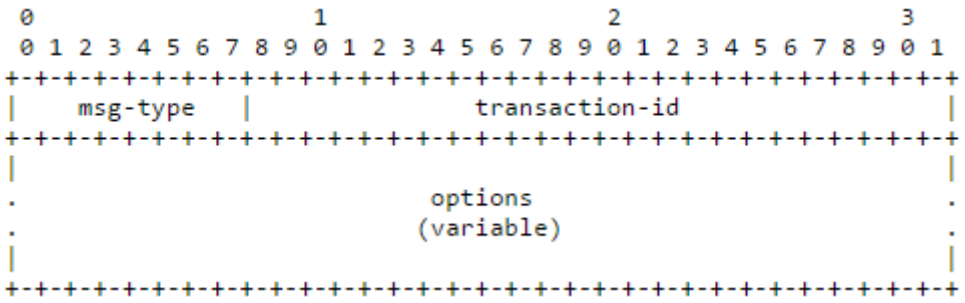
DHCPv6-palvelimen toiminnallisuudet ovat samankaltaiset kuin IPv4-verkoissa. DHCPv6 eli ”Dynamic Host Configuration Protocol for IPv6” on esitelty standardissa RFC3315. Lyhenteen lopussa oleva “v6” pääte ei kerro versiosta 6 vaan, että protokolla jakaa IPv6-standardin osoitteita. (Dynamic Host Configuration Protocol for IPv6 (DHCPv6))

6.2 DHCPv6 viestit ja sen sisältö

Päätelaiteen sekä DHCPv6-palvelin välisessä viestin vaihdossa tieto kulkee UDP-protokollan avulla. Viestejä vaihtaessa päätelaite käyttää UDP porttia 546 ja palvelin sekä ”DHCP Relay” porttia 547. Kun päätelaite lähettää DHCP pyynnön verkkoon, on sen kohdeosoitteena paikallinen ”link-local”-osoite. Pyynnön vastaanotettua palvelin vastaa viestiin lähettäen sen paikalliseen ”multicast”-osoitteeseen. Jos DHCP-palvelin ei ole samassa verkossa kuin päätelaite, asetetaan verkon reitittimeen välittäjä eli ”DHCP-relay”. Välittäjän tarkoituksena on välittää DHCP-pyynnöt suoraan palvelimen ”Unicast”-osoitteeseen. Jos palvelimen ja päätelaitteen välisessä keskustelussa tarvitaan vain kaksi sanomaa, tarkoittaa se että laitteeseen on asettanut IPv6-osoitteen jollain muulla tavalla. Tällöin laite tarvitsee vain lisätietoja mm. verkon NTP- sekä DNS-palvelimesta. DHCPv6 käyttää kahta erilaista ”Multicast” -osoitetta:

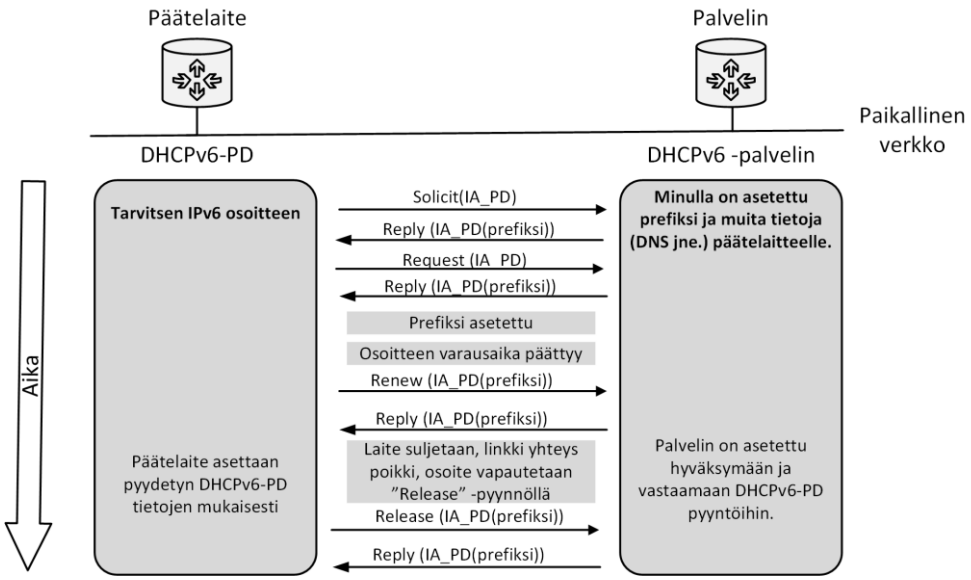
- ALL_DHCP_Relay_Agents_and_Servers (FF02::1:2): päätelaitteet käyttävät viestittäessä naapuri palvelimille sekä välittäjille.
- ALL_DHCP_Servers (FF05::1:3): Palvelimet käyttävät tätä osoitetta kun haluavat viestiä verkon palvelimille tai kun välittäjä ei tiedä palvelimen ”Unicast”-osoitetta.

Jokainen DHCPv6-viesti palvelimen sekä laitteen välillä jakavat identtisen otsikoinnin ja muuttuvan asetuskentän. DHCPv6-viestin otsikointi on nähtävissä kuviossa 9.



Kuvio 9. DHCPv6 -viestin otsikko kentät.

Viestin ensimmäinen kenttä ”msg-type” kuvaa DHCPv6-viestin tyypin. ”Transaction-ID”-kenttä on yksilöllinen viestimistunniste, jolla keskustelut eritellään. Viestin viimeinen ”Options”-kenttä on kooltaan muuttuva osio, jossa kuljetetaan asetustietoja. (Dynamic Host Configuration Protocol for IPv6 (DHCPv6))



Kuvio 10. DHCPv6 palvelimen sekä laitteen väliset viestit

Päätelaitteen ja palvelimen välinen keskustelu on nähtävissä kuviosta 10. Ensin päätelaite lähettää verkkoon ns. ”solicit”-pyynnön, missä se pyrkii löytämään lähimmän DHCPv6-palvelimen. Kaikki palvelimet joihin paikallinen ”multicast”-osoite saavuttaa, ne lähettävät vastauksena mainostus viestin (advertisement) verkkoon. Vastausviestin saatuaan päätelaite valitsee lähimmän palvelimen ja lähettää ”DHCP-request”-pyynnön. Pyynnössä laite haluaa sille ennalta määritellyn IPv6-osoitetteen, sekä muita verkkoyhteydelle olennaisia tietoja. Pyynnön saatuaan palvelin lähettää ”Reply” -viestin jossa ovat päätelaitteen haluamat tiedot. (Dynamic Host Configuration Protocol for IPv6 (DHCPv6).)

Kuviossa on myös nähtävissä, kuinka varattu IPv6-osoiteen aika purkautuu ja laitteet joutuvat keskustelemaan uuden osoitteen. Silloin päätelaite lähetettää ”Renew”-viestin, missä se pyyttää IPv6-osoitetta uudestaan. Palvelin vastaa tässä tapauksessa normaalista valitsemalla asetetusta IPv6-avaruudesta osoitteen ja lähettämällä se laiteelle. (Dynamic Host Configuration Protocol for IPv6 (DHCPv6).

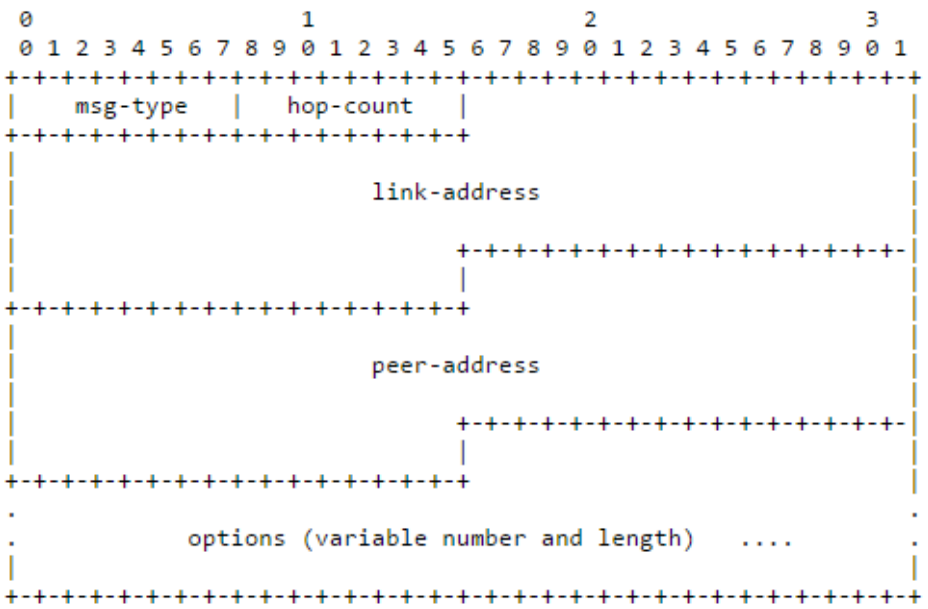
Kuvio myös havainnollistaa tapahtumasarjan jos laite sammutetaan, yhteys laitteeseen katkeaa tai se erikseen pyytää osoitteen vapauttamista. Kun päätelaite lähettää release pyynnön, palvelin vastaa antamalla vapaan osoitteen laitteelle.

(Dynamic Host Configuration Protocol for IPv6 (DHCPv6).)

(DHCPv6 Based IPv6 Access Services)

6.3 DHCP Relay

Välittäjä agentit eli ”Relay agents” välittävät DHCPv6-viestejä palvelimelle, kun palvelin sijaitsee eri verkossa päätelaitteiden kanssa. Asetus kentän tiedot ovat laitettu peräjälkeen ilman tyhjiä merkkejä asetusten välillä. Välittäjä agenttien viestin otsikkokentät on kuvattu kuviossa 11.



Kuvio 11. Välittäjä agenttien viestin otsikkokentät

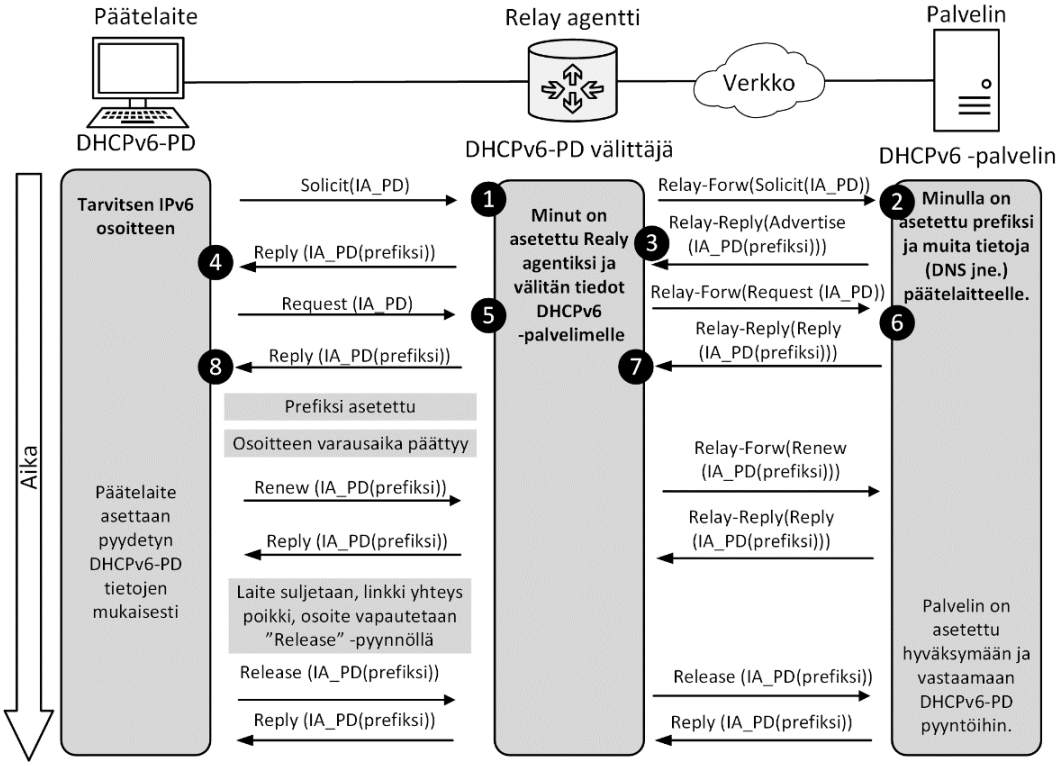
Relay-agentin ja palvelimen välillä kulkee kahta erilaista viestiä: ”Relay-forward”-viesti eli uudelleenlähetysviesti sekä ”Relay-Reply”-viesti eli vastaus välittäjän lähettämään viestiin. Otsikkokentät sekä niiden sisällöt viesteissä on havainnollistettu taulukossa 3. (Dynamic Host Configuration Protocol for IPv6 (DHCPv6)(DHCPv6 Based IPv6 Access Services)

Taulukko 3. Välitys agentin ja palvelimen väliset viestit sekä viestin otsikoiden sisältö havainnollistettuna

Otsikko-kenttä	*Välittäjä agentin viesti*	
	Relay-forward	**Relay-reply**
msg-type	RELAY-FORW	RELAY-REPL
hop-count	Viestin välittäjä agenttien määrä	Kopioitu ”Relay-forward”-kentästä
link-address	Globaali tai verkon paikallinen osoite, jota palvelin käyttää päätelaitteiden kytkennän havaitsemiseksi.	Kopioitu ”Relay-forward”-kentästä
peer-address	Osoite, mistä viesti oli välitetty	Kopioitu ”Relay-forward”-kentästä
options	Vastaanotettu viesti lähetetään kirjaimellisesti eteenpäin seuraavalle välittäjä agentille	Viesti kopioidaan ja välitetään välitysagentille tai laitteelle, jonka osoite on sijoitettu ”peer-address”-kenttään.

Jotta Relay agentit voivat välittää tietoja päätelaitteelta palvelimelle, sen on pakko sijaita linkkiyhteyden päässä päätelaitteesta. Kuitenkin Relay-agentin ja palvelimen välille ei tarvita linkki yhteyttä sillä tieto kulkee uniikilla IPv6- osoitteella. Agentin voi myös asettaa välittävän DHCP pyynnöt suoraan ”multicast”-osoitteeseen FF05::1:3 eli ” All_DHCP_Servers”. Silloin agentti asettaa viesteihin hyppyjen raja-arvoksi 32.

Kun DHCPv6-palvelin päättää vastata välitettyyn laitteen viestiin, se muodostaa vastauksen saatavilla olevista tiedoista sekä kopioimalla osan tiedoista agentin viestistä (esimerkiksi, rajapinnan tunnisteoption eli interface-id :n). Palvelin lähettää vastauksen lähdeosoitteeseen käyttämällä porttia 547. Relay agentti välittää viestin ”peer-address”-kentän osoitteeseen. Yksityiskohtaisempi selitys päätelaitteen, Relay-agentin sekä DHCPv6-palvelimen välisestä keskustelusta on selitettyä kuviossa 12. (Dynamic Host Configuration Protocol for IPv6 (DHCPv6)(DHCPv6 Based IPv6 Access Services)



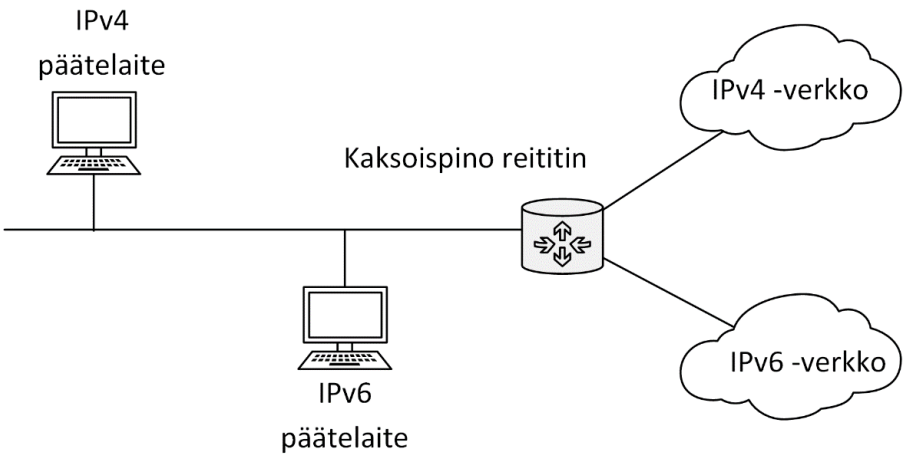
Kuvio 12. päätelaitteen, Relay agentin ja DHCPv6-palvelimen välinen keskustelu

7 Transitiomekanismit

7.1 Kaksoispino

Kaksoispino eli yleisemmin tunnettu ”Dual Stack” on metodi, jolla voidaan ottaa käyttöön IPv6-verkko samanaikaisesti IPv4- verkon kanssa. Kaikki verkon solmukohdat asetetaan tällöin olemaan yhteydessä IPv6- sekä IPv4-verkoissa. Solmukohdat reitittävät kummankin protokollan tietoja, jolloin rajapinnalla tai usealla rajapinnalla on

IPv6- sekä IPv4-osoitteet. Kaksoispinon toimintaperiaate on havainnollistettu kuviossa 13. (Teare & Paquet, 2007, 689-690)



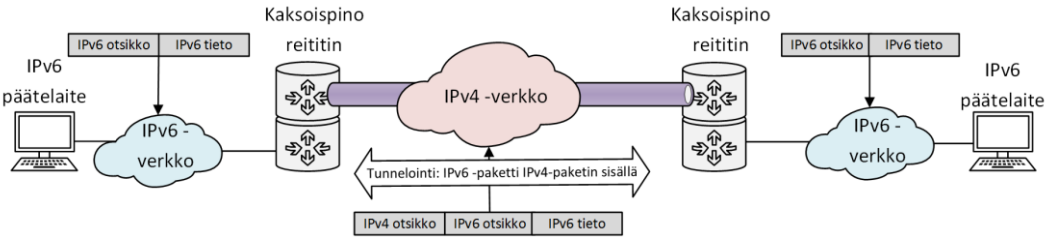
Kuvio 13. Kaksoispinon toimintaperiaate

Kaksoispinon reitittimet määrittelevät paketin kohdeosoitteen mukaan kumpaa protokollaa käyttää. Laitteen on kuitenkin suositeltavaa käyttää ipv6 pinoa jotta siirtyminen laajempaan verkko-osoitukseen on tulevaisuudessa mahdollista. Kaksoispino metodi on kaikista transitiomekanismeista käytetyin, sillä vanha IPv4-verkon sovellus toimii normaalisti, kun samanaikaisesti uudet ja modernit sovellutukset käyttää kumpaakin protokollapinoa. (Teare & Paquet, 2007, 689-690)

7.2 Tunnelointi

Tunnelointia usein käytetään silloin kun halutaan peittää yhteen sopimaton verkon alue jo tuotantoverkossa. IPv6-standardin tunnelointitekniikassa sisällytetään IPv6 paketti IPv4 protokollan tietokuorma kenttään. (Teare & Paquet, 2007, 689-694)

Tunnelointia tehdessä toimipisteen reunareititin kapseloi IPv6-paketin IPv4, paketin sisälle. Saatuaan paketin, kohde toimipisteen reunareititin purkaa kapseloinnin. Tiedon kapselointia ja sen purkamista tapahtuu toimipisteiden kummassakin päässä, johtuen liikenteen suunnasta. Tunneloinnin avulla voidaan yhdistää kaksi IPv6-verkkoa ilman että runkoverkkoa tarvitsee kääntää IPv6 yhteensopivaksi. Tunnelointitekniikan toimintaa on kuvattu kuviossa 14. (Teare & Paquet, 2007, 689-694)



Kuvio 14. Tunneloinnin toimintaperiaate

Tunnelia voidaan myös käyttää päätelaitteen sekä reunareitittimen välillä. Tällöin päätelaite voi saada yhteyden IPv6- verkkoon IPv4 yhteyden läpi. On kuitenkin hyvä huomioida ettei käsin asetettu tunnelin avulla voida välttää palomuureista sekä verkkosuodattimista. Täysin toimivan tunnelin pystyttämiksesi on siis asetettava tunnelin kummatkin reitittimet toimimaan kaksoispinolla. (Teare & Paquet, 2007, 689-694)

Kun tunnelointitekniikkaa käytetään, se pienentää verkkopaketin hyötykuorman kokoa vähentämällä MTU arvoa 20 oktetilla. Tunneloinnin rajoituksien takia tunnelointia ei suositella käytettävän verkon lopullisena ratkaisuna, sillä tunnelointiverkoista on vaikea etsiä vikoja. (Teare & Paquet, 2007, 689-694)

Tunnelointi tekniikoita on kehitetty useita, jolla jokaisella on hieman eri tarkoitus:

- Teredo-tunnelointi tekniikan avulla pystytään määrittelemään ”Unicast” -yhteystunneli kahden päätelaitteen välille käyttämällä Teredo-palvelinta sekä välittäjää. Teredo-tunneli onnistutaan tekemään myös NAT-tekniikan läpi. Teredo-tunnelointi tekniikka kuljettaa käyttämällä UDP siirto protokollaa portissa 3544.
- ISATAP eli ”Inter-Site Automatic Tunnel Addressing Protocol”-tunnelointi mekanismin tarkoituksena on luoda skaalautuva tunnelointi verkkojen sekä päätelaitteiden välille. ISATAP perustana toimii IPv4 infrastruktuurin NBMA linkki taso, jossa laitteet ovat yhdistetty vain suoraan toisiinsa eikä monilähetystä verkossa sallita. Automatisoinnin avulla ISATAP reitittimet ovat tietoisia toisistaan sekä niihin yhdistetyistä päätelaitteista. Tietoisuuden saatua ne muodostavat suoria tunneliyhteyksiä eri laitteiden kesken.
- ”Tunnel Broker” sekä ”Tunnel Server” muodostavat tunnelointimenetelmän, joka luo käsin luotuja tunnelointi yhteyksiä laitteiden välille. Menetelmä keskustelee tunnelit IPv4-verkon lävitse muodostaen ”Unicast” -yhteyksiä.
- 6to4 on automatosoitu tunnelointimekanismi, joka käyttää IPv4-runkoverkkoa apuna minimaalisilla konfiguraatiomuutoksilla. Mekanismissa muodostetaan tunneli yhteys,

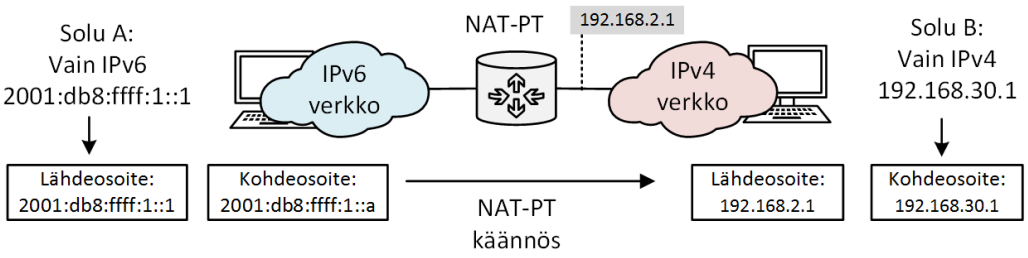
johon tietty kohdeosoitteen prefiksi reititetään. Reititysprosessissa kohdeosoite vaihtuu runkoverkkoon IPv4- osoitteeksi. Tunneliyhteyden toisessa päässä paketti uudelleen reititetään IPv6-sisäverkkoon.

(Teare & Paquet, 2007, 689-694)

(Grossetete, Levy-Abegnoli, Popoviciu, 2006, 120-124)

7.3 Käännösmekanismi

Joissain verkon tapauksissa on laitteistoja tai sovelluksia, jotka eivät koskaan saa päivitystä IPv6-standardiin. Tällöin on kätevä ottaa käyttöön käännösmekanismi, joka tunnetaan IPv6-tekniikassa paremmin nimellä NAT-PT. Käännösmekanismin ideana on kääntää IPv4-paketit IPv6-paketeiksi ja edestakaisin. NAT-PT käännöksessä tilaton IP/ICMP käännös algoritmi kääntää IP otsikko alueet, samalla kun NAT hoitaa IP-osoitteiden käännökset. Kuviossa 15 on esimerkki NAT-PT käännösmekanismin toiminnasta. (Teare & Paquet, 2007, 694-695) (Grossetete, Levy-Abegnoli, Popoviciu, 2006, 140-141)



Kuvio 15. Esimerkki NAT-PT käännösmekanismista

Esimerkki kuvio 15 havainnollistaa käännöksen, kun IPv6 paketti on lähetetty solmusta A solmuun B. Solmun A mielestä se on avannut yhteyden toiseen IPv6 solmuun vaikka solmu B onkin IPv4-verkossa. Tämä onkin yksi NAT-PT tekniikan eduista, sillä itse sovellutuksiin ei tarvitse muutoksia IPv6 toiminnallisuuden saamiseksi vaan sen solmu A tarvitsee vain tietää IPv6 kartan toiselle solmulle. IPv6 -osoite voidaan selvittää dynaamisesti käyttämällä DNS palvelinta. Dynaamisen NAT-käännöksen toiminta perustuu DNS kyselyihin, joka toimii käyttämällä ”DNS-ALG”-tekniikkaa. ”DNS-ALG”-tekniikka toimii kaksoispino menetelmällä, jossa mahdollistetaan IPv6-verkon päätelaite yhdistämään IPv4-verkon toimialueeseen. Tämä tekniikka vaatii että kaikki palvelimien sovellukset toimivat IPv6-protokollalla. (Teare & Paquet, 2007, 694-695)

8 IPv6:n muutossuunnitelma

8.1 Yleisesti

Muutossuunnitelman tavoitteena on luoda suunnitelmallinen malli, miten muutos IPv6-verkkoon tai sen osaan tapahtuu. Muutossuunnitelmassa määritellään ensin mihin osaan verkkoa halutaan muutossuunnitelman vaikuttavan, minkä jälkeen kartoitetaan verkon muutoksen yhteensopivuus. Muutossuunnitelman lopullisena tavoitteena on toimiva IPv6-verkko. (Lehtonen 2014.)

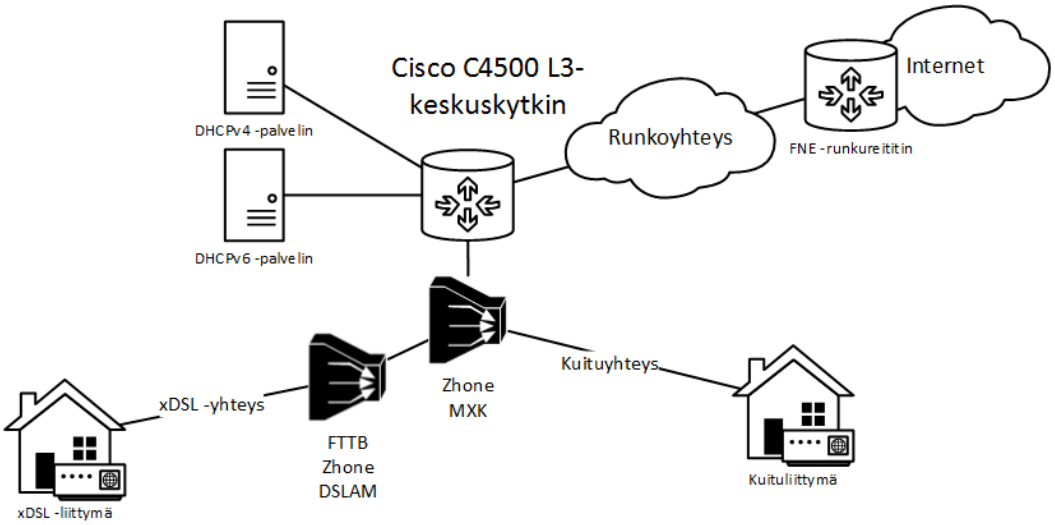
8.2 Verkkoinfrastruktuurin tila ennen muutosta

Ennen käytännön osuuden aloittamista kartoitettiin Haminan Energian verkon rakenne sekä mihin kyseinen IPv6 verkko kohdennetaan. Kartoituksessa ilmeni, että aiemmin oli tehty opinnäytetyönä DHCPv6-palvelin. Samalla selkiytyi RIPE -organisaatiolta haettu IPv6 prefiksi, johon verkko loppujen lopuksi toteutetaan. DNS-palvelu ostettiin ulkopuoliselta tarjoajalta. Runkoyhteyden Haminan Energian verkkoon tarjoaa FNE Finland Oy eli Fiber Network Eight Finland Oy.

Haminan Energian sisäverkko on jaettu eri segmentteihin käyttämällä virtuaalisia aliverkkoja eli VLAN-verkkoja. Verkon reunana toimi Cisco C4500 verkkotason 3 kytkin, joka osaa hyödyntää yhtäaikaisesti kytkentäverkkoa sekä IP-verkkoa. Laite siis osaa tehdä reititys- sekä kytkentäpäätöksiä. Asiakasverkko oli jaettu kahteen eri kytkentätason VLAN segmenttiin; kiinteistökuitu- sekä kuituliittymiin. Kiinteistökuituliittymissä eli lyhennettynä FTTB (Fiber To The Building), valokuitu tulee alueen lähistölle tai kerrostaloon, josta liittymät jaetaan DSLAM -laitteella. DSLAM-laitteesta yhteydet asiakkaille on toteutettu käyttämällä xDSL-tekniikkaa. Kuituliittymissä taas valokuitu on kytketty suoraan omakotitaloon. Kuituliittymät ovat lyhennetty FTTH (Fiber To The Home)-liittymiksi. Verkon osoitteiden jako toteutetaan DHCPv4- sekä DHCPv6-palvelimilla.

Verkossa käytetään kahta eri DSLAM-laitteiden valmistajaa; Zhone sekä Ericsson. Kummassakin laitevalmistajien laitteissa käytetään keskitettyä hallintajärjestelmää, jonka avulla voitiin muodostaa siltauksia eri päätelaitteille mihin tahansa verkkoa.

Asiakkaiden päätelaitteet olivat pääosin kahta eri valmistajaa: Inteno DG301AL-AC, VG50 sekä ZyXEL AMG1202-T10B. Haminan Energian verkko yksinkertaistettuna on nähtävissä kuviossa 16.



Kuvio 16. Haminan Energian asiakasverkko yksinkertaistettuna

8.3 Päivitettävän alueen rajaus

Muutossuunnitelmassa halutaan muuttaa asiakkaiden verkkoyhteys toimivan kaksoispino tekniikkaa käyttäen. Muutossuunnitelma siis vaikuttaa asiakasverkkoon. Muutossuunnitelman ulkopuolelle jätettiin kuitenkin WiMAX-asiakkaat. Muutosta ei nähty tarpeelliseksi kyseisille asiakkaille, sillä tekniikan tulevaisuus katsottiin päättyvän ennen kuin siirryttäisiin kokonaan käyttämään vain IPv6 -osoitteita.

8.4 Verkkolaitteiden sekä palveluiden IPv6-yhteensopivuus

Ennen kuin laboratorioverkkoa voitiin alkaa luomaan, täytyi selvittää kaikkien verkossa olevien laitteiden IPv6 yhteensopivuus. Testauksissa huomatiin että muut paitsi Ericssonin DSLAM-laitteet olivat IPv6 yhteensopivia. Ericssonin DSLAM-laitteiden yhteensopimattomuus johtui laitteiden vanhentuneista ohjelmistoversiosta. Verkossa oli kuitenkin menossa ns. siirtymävaihe Ericssonista Zhonen-laitteisiin, joten ohjelmistopäivitystä ei katsottu tarpeelliseksi. Päätelaitteet (ZyXEL sekä Inteno) pystyivät muodostamaan kaksoispino yhteyden oletusasetuksilla. Asiakkaiden päätelaitteita kartoittaessa oletetaan niiden olevan tehdasasetuksilla. Yhteensopivuus kar-

toituksessa huomattiin, että Ciscon L3-kytkimen järjestelmän ohjelmistoversio ei tukenut OSFPv3 reititystä, joten laite jouduttiin päivittämään yhteensopivuuden saavuttamiseksi. Taulukossa 4 on vedetty yhteen sisäverkon laitteiston yhteensopivuudesta.

Taulukko 4. Kartoitus verkkolaitteiden IPv6-yhteensopivuudesta

Laitteen nimi	*Tyyppi*	*Valmistaja*	*IPv6 -tuki*
Cisco C4500	L3 -kytkin	Cisco	Kyllä
Zhone	DSLAM	Zhone	Kyllä
Zhone	DSLAM	Zhone	Kyllä
Ericcson	DSLAM	Ericsson	Ei
ZyXEL	Asiakkaan päätelaite	ZyXEL	Kyllä
Inteno	Asiakkaan päätelaite	Inteno	Kyllä

Samalla kartoitettiin ulkoisten palveluiden IPv6 yhteensopivuus. Kartoituksessa huomattiin, että Elisan DNS palvelin oli IPv6 yhteensopiva, sen jälkeen kun Elisa oli tehnyt muutokset heidän palvelimelle. Muutoksien jälkeen voitiin tehdä IPv6 DNS pyyntöjä Haminan energian verkosta.

8.5 Muutoksen roolit, riskit sekä palautussuunnitelma

Muutossuunnitelman transitiomekanismiksi sovittiin kaksoispino-tekniikka, koska se katsottiin olevan sopivin menetelmä kyseiseen verkkoon. Kaksoispinotekniikka on laajasti tuettuna eri asiakasreitittimissä, joka helpottaa IPv6-standardin tuomista asiakkaille. Päärooli muutoksen toteuttamisessa on opinnäytetyön tekijällä. Toimeksiantajan verkkoasiantuntija toimii apuna muutoksen toteutuksessa.

Muutoksen riskit ovat pyritty minimalisoimaan muodostamalla laboratorioverkko ennen toteutuksen tuomista tuotantoon. Laboratorio verkossa voidaan testata kaikkien laitteiden IPv6 yhteensopivuus luomalla testausverkkoon tuotantoverkon kaltainen ympäristö. Suurimmat riskit muutoksessa ovat asiakkaiden sovelluksien IPv6 yhteensopivuus, sen jälkeen kun joskus tulevaisuudessa otetaan alkuperäinen IPv4 verkko pois käytöstä.

Konfiguraatio järjestys on hyvä määrittää, jotta muutos ei näkyisi asiakkaille palvelukatkoksena. Muutoksen konfiguraatio aloitetaan määrittelemällä DHCPv6 palvelimelle jaetavat prefiksit sekä osoitteet. Tämän jälkeen siirrytään keskusreitittimen konfigurointiin. Reititintä konfiguroitaessa on dokumentoitava tulevat asetukset asiakirjaan. Dokumentoimalla voidaan tarkistaa konfiguraation oikeellisuus ennen niitä laitteeseen asettamista. Asetukset on helpointa kopioida ja liittää asiakirjasta laitteen komentoriville, jolloin kirjotusvirheiden määrä minimoidaan. DSLAM laitteen konfiguraatiota ei tarvitse muuttaa, koska sen toiminta perustuu verkon kytkentätasoon.

Laboratorioverkon toteutusta siirrettäessä tuotantoverkkoon on hyvä määritellä palautussuunnitelma jos siirtymävaihe ei onnistu. Palautussuunnitelma on hyvä aloittaa verkon reitittimestä. Reitittimestä poistetaan asiakas VLAN -rajapinnoista IPv6 konfiguraatiot. Kyseinen toimenpide on nopea ja helppo sillä pieni muutos vaikuttaa kokonaisvaltaisesti asiakkaiden IPv6 toiminallisuuteen. Palautussuunnitelman konfiguraatiot on hyvä kirjoittaa asiakirjaan ylös, josta ne voidaan kopioida laitteen komentoriville.

Tärkeimpien laitteiden rajapintojen IPv6- osoitteista ylläpidetään taulukkodokumenttia, jotta ne voidaan tarkistaa. Samalla tehdään dokumentti missä on lueteltu tärkeimmät IPv6-konfiguraatiot eri laitteissa.

8.6 IP-osoitepolitiikka ja osotteiden jako

RIPE-organisaatiolta oli jo aiemmin haettu IPv6 prefiksiä. Prefiksi, joka organisaatiolta saatiin on 2A00:B9A0::/32. Prefiksin avulla osoitteet jaettiin kuuteen pääaliverkkoon. Jaetut aliverkot asetettiin FTTB- sekä FTTH- asiakkaille laboratorio- sekä tuotantoverkkoon, DHCP -palvelimelle sekä runkoyhteydelle. Aliverkot numeroitiin VLAN tunnisteen numeron mukaisesti. Jokaiselle pääaliverkolle jaettiin /48 prefiksi. Kohdassa

8.1. on kuvailtu miten asiakasverkkojen prefiksit ovat jaettu eri asiakkaille. Laboratorio verkossa toteutetaan kaksoispino yhteys, joten Haminan Energian IPv4 osoiteavaruudesta löytyi testaus verkkoon sopiva lohko. Taulukossa 5 on esitetty kuinka osoiteavaruudet ovat jaoteltu.

Taulukko 5. Verkon osoitteiden jaottelu

ALIVERKON NIMI	VLAN-TUNNISTE	PREFIKSI	ASIAKKAILLE JAETTAVA OSOITE WAN-PORTILLE	ASIAKKAIDEN JAETTTAVA ALIVERKKO
DHCPV6 - PALVELIN	401	2A00:B9A0:401::/48		
IPV6 RUNKOYHTEYS	100	2A00:B9A0:100::/48		
IPV6 LABORATORIO FTTB	801	2A00:B9A0:801::/48	2A00:B9A0:802:FFFF::/64 - 2A00:B9A0:802:FFFF:FFFF:FFFF :FFFF:/64	2A00:B9A0:802:0000::/64 - 2A00:B9A0:802:FFFE::/64
IPV6 LABORATORIO FTTH	802	2A00:B9A0:802::/48	2A00:B9A0:802:FFFF::/64 - 2A00:B9A0:802:FFFF:FFFF:FFFF :FFFF/64	2A00:B9A0:802:0000::/64 - 2A00:B9A0:802:FFFE::/64
IPV4 LABORATORIO FTTH	801	5.61.89.0/25	5.61.89.1 - 5.61.89.126	NAT
IPV4 LABORATORIO FTTB	802	5.61.89.128/25	5.61.89.129 - 5.61.89.255	NAT

9 Laboratorioverkko

9.1 DHCPv6-palvelin

Yritykselle vuonna 2014 tehtiin opinnäytetyönä DHCPv6-palvelin, joka toimi hyvänä pohjana palvelimen konfiguroinnissa laboratorioverkkoon. Konfiguraatiossa oli valmiiksi asetettu joitain prefiksejä jaettavaksi, mutta niitä piti muuttaa testiympäristöön sopivammaksi.

Palvelimen käyttöjärjestelmänä toimii 64-bittinen CentOS Linux jakelu. Palvelin pyörii VMware Sphere alustan päällä virtualisoituna, josta sitä voidaan hallita etäyhteyttä

käyttäen. Palvelinta käytettiin pääosin salatun SSH yhteyden läpi, sillä konfiguraatio tekstien kopioiminen ja liittäminen palvelimeen helpotti sen hallintaa. Palvelimessa on kaksi verkkorajapintaa. Ensimmäinen verkkorajapinta ”eth0” on ns. hallinta rajapinta, johon SSH yhteys otettiin. Samasta rajapinnasta päivitettiin asennuspaketteja. Toinen rajapinta ”eth1” on itse DHCPv6 rajapinta, joka keskustelee IPv6-osoitteiden allokoinnista päätelaitteiden kanssa. Kyseinen rajapinta on yhteydessä laboratorio verkkoon. Palvelimessa toimiva DHCP palvelu on nimeltään ISC-DHCP. Palvelu on laajasti käytössä oleva. Aiemmin tehdyssä opinnäytetyössä oli vertailtu eri DHCP palveluita. (Lampikari. 2014.)

Opinnäytetyön vertailussa päädyttiin ISC DHCP ohjelmistoon, sillä siinä oli parempi dokumentaatio sekä se pystyi käsittelemään suurempia määriä asiakkaista, lisäoptio kenttien kanssa. DHCPv6 -palvelimessa oli asetettu IPv6-pakettien reititys päälle sekä konfiguroitu ”iptables”-palomuuri päästämään läpi ICMPv6-viestit, jossa tyyppi kentässä ovat arvot väliltä 134-136.

Asetettu palvelimen konfiguraatio alkaa asettamalla palvelimen ”lease”-tiedoston sijainti, johon kaikki allokoidut IPv6 osoitteet dokumentoidaan. Tämän jälkeen asetetaan palvelin verkon toimivaltaisimmaksi DHCPv6 palvelimeksi. Tämä tarkoittaa, että jos verkossa on laite, joka on saanut väärät osoitetiedot, joltain muulta DHCP -palvelimelta, tiedot siinä tapauksessa korvataan toimivaltaisimman palvelimen antamilla tiedoilla. Toimivaltaisuus asetetaan konfiguraatiolla ”authoritative;”. Tämän jälkeen asetetaan ajat, jossa määritellään kuinka kauan osoite varataan ennen kuin laite keskustelee uuden osoitteen. Lopuksi vielä asetetaan ”log facility”, jotta palvelun lokit menisivät tiedostoon ”/var/log/dhcp6.log”. Palvelimen alku konfiguraatio kokonaisuudessaan on nähtävissä alapuolella.

```
dhcpv6-lease-file-name "/var/lib/dhcpd/dhcpd6.leases";

authoritative;
default-lease-time 86400;
max-lease-time 86400;
preferred-lifetime 86400;

log-facility local7;
```

Tämän jälkeen määritellään, miten lisäoptiot asetetaan lokiin sekä “lease”-tiedostoon. Opinnäytetyössä on asetettu palvelimelle vaatimukset, että DHCP lisäoptioiden

avulla pystytään määrittelemään tarkemmin päätelaite, johon osoite on annettu. Lisäoptiot on määritelty alla olevalla konfiguraatiolla.

```
on commit {
        if option dhcp6.ia-na = option dhcp6.ia-na{
                set iana = binary-to-ascii(16,16,":",substring(suffix(option dhcp6.ia-
                na,24),0,16));
        }
        if option dhcp6.ia-pd = option dhcp6.ia-pd{
                set iapd = binary-to-ascii(16,16,":", suffix(option dhcp6.ia-pd,16));
                set pdsize = binary-to-ascii(10,8,":",substring(suffix(option
                dhcp6.ia-pd,17),0,1));
        }

        set ifname = v6relay(1, option dhcp6.interface-id);
        set lla = (binary-to-ascii(16, 8, ":", suffix(option dhcp6.client-id, 6)));
        set remote-id = v6relay(1, option dhcp6.remote-id);
                if option dhcp6.ia-na = option dhcp6.ia-na{
                log(info, concat("ON COMMIT IA_NA: ", iana, " To: ", lla, " INT: ",
                ifname, " REMOTE-ID: ", remote-id));
        }
        if option dhcp6.ia-pd = option dhcp6.ia-pd{
                log(info, concat("ON COMMIT IA_PD: ", iapd, "/", pdsize, " To: ", lla,
                " INT: ", ifname, " REMOTE-ID: ", remote-id));
        }
    }
```

Yllä olevassa lisäoptioiden konfiguraatiossa ”commit”-käskyn alle kirjoitetut konfiguraatiot määrittelevät mitä tietoja asetetaan tiedostoon, kun DHCP-viestejä lähetetään sekä vastaanotetaan. Kahdessa ensimmäisessä ehtolauseessa määritellään palvelinta lukemaan DHCP-viestien sisältö kun optio kenttien arvot ovat 3 sekä 25. Viestit löytäessä se kirjoittaa tiedostoon muuttujien määrittelemät tiedot ascii-muodossa.

”commit”-käskyn loppu osassa on määritelty muuttujat ”ifname”, ”lla” sekä ”remote-id”. Muuttujat määritellään sisältävän tiettyjä DHCPv6 lisäoptioita. Jos konfiguraation viimeisin ehtolause täyttyy, asetetaan lisäoptioiden tiedot lokiin if -lauseen määrittelemällä tavalla.

”lease”-tiedoston sisällön määrittelemisen jälkeen on määriteltävä miten verkko-osoitteita jaetaan rekisteröidystä prefiksistä. Ensin määritellään DHCP-palvelimen prefiksi. Asetetusta alueesta ei kuitenkaan jaeta mitään osoitteita. Tämän jälkeen määritellään asetettujen VLAN tunnisteiden IP-osoiteavaruudet ”subnet6”-komennolla. Tämän jälkeen asetetaan tietty osoitteiden alku ja loppu, mistä jaetaan osoitteet päätelaitteille eli tässä tapauksessa reitittimien ”WAN”-rajapinnalle. Jaettujen osoitteiden määrittelemisen jälkeen asetetaan lisäoptiot, esimerkiksi DNS osoitteet. Komennolla ”ddns-update-style none;” määritellään, ettei dynaamisia nimikyselyitä

sallita. Rivit, jotka alkavat sanalla ”option”, määrittelevät DNS-palvelimien osoitteet, mitkä jaetaan päätelaitteille. ”prefix6”-komento asettaa jokaisen päätelaitteen oman aliverkon. Tällä tavoin jokainen päätelaite reitittimien takan oleva tietokone saa julkisten ”Unicast”-osoitteen. Tietokoneen IPv6-osoite muodostetaan tällöin reitittimen saadun prefiksin sekä rajapinnan tunnisteen mukaan. Tietokone ei siis keskustele DHCP-palvelimen kanssa vaan se määrittää osoitteen tilattomalla autokonfiguraatiolla. Asetetut osite määritykset kokonaisuudessaan on nähtävissä alapuolella.

```
subnet6 2a00:b9a0:401::/48 {
}

# VLAN801 osoitealue
subnet6 2a00:b9a0:801::/48 {
range6 2a00:b9a0:801:ffff:0000:0000:0000:0001 2a00:b9a0:801:ffff:ffff:ffff:ffff:fff0;
        # Lisäoptiot
        ddns-update-style none;
        option dhcp6.name-servers 2a00:1dd0:0:1::132, 2a00:1dd0:0:1::32;
        option dhcp6.domain-search "Haminetti.net";

        # Reitittimille jaettava prefix (eli reitittimen lan portille)
        prefix6 2a00:b9a0:801:: 2a00:b9a0:801:ffff:: /64;
}

# VLAN802 osoitealue
subnet6 2a00:b9a0:802::/48 {
        # Alue clienteille (esim. reitittimen wan portille)
range6 2a00:b9a0:802:ffff:0000:0000:0000:0001 2a00:b9a0:802:ffff:ffff:ffff:ffff:fff0;

        # Lisäoptiot
        ddns-update-style none;
        option dhcp6.name-servers 2a00:1dd0:0:1::132, 2a00:1dd0:0:1::32;
        option dhcp6.domain-search "Haminetti.net";

# Reitittimille jaettava prefix (eli reitittimen lan portille)
prefix6 2a00:b9a0:802:: 2a00:b9a0:802:ffff:: /64;

}
```

Konfiguraatioden asettamisen jälkeen palvelu käynnistettiin uudelleen käyttäen komentoa ”service dhcpd6 restart” tai ”dhcpd -6 -cf /etc/dhcp/dhcpd6.conf”. Tuloste palvelun uudelleen käynnistyksestä kummallakin komennolla on nähtävissä kuviosta 17. (Lampikari. 2014.)

```
[root@localhost ~]# service dhcpd6 stop
Stopping dhcpd6:                                           [  OK  ]
[root@localhost ~]# dhcpd -6 -cf /etc/dhcp/dhcpd6.conf
Internet Systems Consortium DHCP Server 4.3.3
Copyright 2004-2015 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/dhcp/dhcpd6.conf
Database file: /var/lib/dhcpd/dhcpd6.leases
PID file: /var/run/dhcpd6.pid
Wrote 3 NA, 0 TA, 3 PD leases to lease file.
Bound to *:547
Listening on Socket/5/eth1/2a00:b9a0:    ::/48
Sending on   Socket/5/eth1/2a00:b9a0:    ::/48

No subnet6 declaration for eth0 (fe80::250:56ff:fe88:6de4).
** Ignoring requests on eth0.  If this is not what
   you want, please write a subnet6 declaration
   in your dhcpd.conf file for the network segment
   to which interface eth0 is attached. **


No subnet6 declaration for eth2 (fe80::250:56ff:fe88:47bd).
** Ignoring requests on eth2.  If this is not what
   you want, please write a subnet6 declaration
   in your dhcpd.conf file for the network segment
   to which interface eth2 is attached. **

[root@localhost ~]# service dhcpd6 restart
Stopping dhcpd6:                                           [  OK  ]
Starting dhcpd6:                                           [  OK  ]
[root@localhost ~]#
```

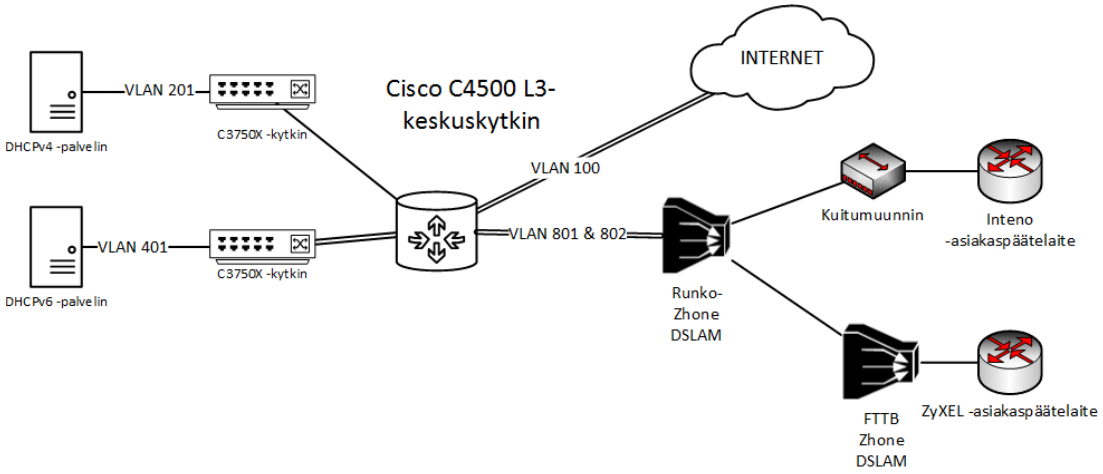
Kuvio 17. Tuloste DHCPv6 -palvelu uudelleen käynnistämisestä kahdella eri komennolla

9.2 Runkokytkimen konfiguraatiot

9.2.1 Laitteen kytkennät eripuolelle verkkoa

Verkon keskuskytkimenä toimii Cisco C4500 L3-tason kytkin, joka toimii samanaikaisesti kytkentä- sekä IP-verkko verkkotasoilla. Kytkimeen on yhdistetty DHCPv6-palvelin sekä runko yhteys Zhone DSLAM-laitteeseen. Kyseiset kytkennät ovat muodostettu yhdistämällä kaksi fyysistä porttia yhdeksi loogiseksi yhteydeksi. Tällöin yhteys jakaa kuorman kahden linkin välillä tasaisesti. Tällöin muodostuu ns. looginen ”Port Channel”-yhteys. Kyseisessä yhteydessä käytetään LACP(Link Aggregation Control Protocol)-protokollaa. DHCPv4-palvelin on yhdistetty sinne menevään kytkimeen yhdellä kuituyhteydellä.

Verkkolaitteessa eri verkot erotellaan virtuaalisien lähiverkkojen eli VLAN tunnisteiden avulla. Yhteys ulkoverkkoon on yhdistetty VLAN 100 kautta. DHCPv4- sekä DHCPv6-palvelimet ovat yhdistetty VLAN-tunnisteiden 201 sekä 401 kautta. Asiakasverkkojen VLAN-tunnisteet 801 sekä 802 ovat yhdistetty saman LACP linkin kautta. Kytkennät laboratorioverkon tärkeimpiin laitteisiin on havainnollistettu kuviossa 18.



Kuvio 18. Keskuskytkimen kytkennät laboratorioverkon eri laitteisiin.

9.2.2 VLAN-rajapinnat ja niiden kytkennät runkoverkkoon

Keskuskytkimen konfigurointi aloitettiin asettamalla IPv6-osoitteiden uniikki reititys päälle komennolla ”ipv6 unicast-routing”. Komennon avulla verkkolaite käynnisti palvelun, joka mahdollisti IPv6 viestin reitityksen. Laboratorioympäristölle luotiin oma virtuaalinen reititys prosessi eli ”VRF”. VRF reitititys prosessi luotiin, jonka jälkeen annettiin sille kuvaus. Lopuksi asetettiin numero, jolla reitti eroteltiin toisista reititys prosesseista.

```
ip vrf IPV6TESTIT
 description IPV6TESTIT
 rd 4:4
```

Seuraavaksi luotiin VLAN tunnisteet eri verkon osille. Sen jälkeen tunnisteille annettiin jokin kuvaava nimi. VLAN-tunnisteiden luonti tapahtui alla olevilla komennoilla.

```
vlan 100
 name FNE-runko

vlan 201
 name DHCPv4

vlan 401
 name DHCPv6

vlan 801
 name IPv6_FTTB_testvlan

vlan 802
 name IPv6_FTTH_testvlan
```

Tämän jälkeen luotiin asiakasverkkoken VLAN- tunnisteiden rajapinnat, jonka jälkeen niille annettiin kuvaus komennolla ”description”. Sitten liitetään aiemmin luotu VRF-

reititysprosessi VLAN-rajapintoihin. Seuravaksi määritellään rajapinnalle haluttu IP-osoite. Jotta asiakasreitittimet saisivat julkisen IPv4- sekä IPv6 -osoitteen on määriteltävä DHCP-viestien uudelleen lähettäjä eli ”Relay” kummallekkin IP-protokollalle. IPv4- standardin DHCP-relay määritellään komennolla ”ip helper-address” ja IPv6-standardin ”ipv6 dhcp relay destination” komennolla. Verkossa kulkee IPTV-liikennettä ,joten on asetettava rajapinta reitittämään multicast liikennettä komennolla ”ip pim sparse-mode”. Jotta rajapinta osaisi käsitellä IPv6 protokollaa, on se otettava käyttöön komennolla ”ipv6 enable”. Rajapintaan vielä asetettiin komento ” ipv6 nd managed-config-flag”, jolla kerrottiin päätelaitteille, että verkossa käytetään DHCPv6-palvelinta IP-osoitteiden määrittelyyn. Tämän jälkeen rajapintaan asetetaan IPv6-osoite, jonka jälkeen otetaan rajapinta pois ”shutdown” -tilasta. Asiakas VLAN-rajapintojen konfiguraatiot on nähtävissä alapuolella.

```
interface Vlan801
 description IPV6_FTTB_801
 ip vrf forwarding IPV6TESTIT
 ip address 5.61.89.1 255.255.255.128
 ip helper-address 5.61.88.XX
 ip pim sparse-mode
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 address 2A00:B9A0:801::1/48
 ipv6 dhcp relay destination 2A00:B9A0:401::2
 no shutdown

interface Vlan802
 description IPV6_FTTH_802
 ip vrf forwarding IPV6TESTIT
 ip address 5.61.89.129 255.255.255.128
 ip helper-address 5.61.88.XX
 ip pim sparse-mode
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 dhcp relay destination 2A00:B9A0:401::2
 ipv6 traffic-filter SALLITAAN_IPV6_VLAN802 in
 no shutdown
```

Seuraavaksi konfiguroidaan runkoverkon VLAN-tunnisteen rajapinta. Kuten asiakasverkkojenkin VLAN-rajapinnassakin, rajapinta luodaan, jonka jälkeen annetaan sille kuvaus. Tämän jälkeen asetetaan rajapintaan reititysprosessi sekä IPv4- sekä IPv6-osoitteet. Ulkoverkon VLAN-tunnisteen komennot kokonaisuudessaan on nähtävissä alapuolella.

```
interface Vlan100
 description Labra_IPv6_FNE-ulko
 ip vrf forwarding IPV6TESTIT
 ip address 5.61.88.XX 255.255.255.252
 ipv6 address 2A00:B9A0::2/32
 no shutdown
```

Runkoverkon VLAN-tunnisteen rajapinnaton asetettu, on vielä konfiguroitava DHCPv4- sekä DHCPv6-palvelimien VLAN-rajapinnat. DHCPv4-palvelimelle asetetaan IPv4-osoite ja DHCPv6- palvelimelle IPv6-osoite. Kummatkin VLAN-rajapinnat sijoitetaan samaan reititysprosessiin kuin muutkin VLAN -tunnisteet. Lopuksi kummatkin rajapinnat avataan käyttämällä komentoa ”no shutdown”.

```
interface Vlan201
 description DHCPv4
 ip vrf forwarding IPV6TESTIT
 ip address 5.61.88.X 255.255.255.252
 no shutdown


interface Vlan401
 description DHCPv6
 ip vrf forwarding IPV6TESTIT
 ip address 5.61.88.XX 255.255.255.248
 ipv6 address 2A00:B9A0:401::1/48
 ipv6 enable
 no shutdown
```

Tämän jälkeen asetetut VLAN-tunniste rajapinnat asetetaan loogisille ”port-channel”-rajapinnoille. ”Port-channel”-rajapinta 1 on asetettu runkoverkon yhteydelle ja 2 asiakasverkkojen ”Port-channel” yhteydelle. kolmas ”port-channel” on DHCPv6 liikenteelle.

```
interface Port-channel1
 description FNE-Runko-LACP
 switchport
 switchport trunk allowed vlan 100
 switchport mode trunk

interface Port-channel12
 description Zhone-DSLAM-LACP
 switchport
 switchport trunk allowed vlan 801,802
 switchport mode trunk

interface Port-channel3
 description FNE-Runko-LACP
 switchport
 switchport trunk allowed vlan 401
 switchport mode trunk
```

Sen jälkeen kun “Port-channel”-rajapinnat on luotu ja konfiguroitu, liitetään asetetut LACP-sekä VLAN rajapinnat fyysisiin yhteyksiin.

```
interface TenGigabitEthernet1/1
 description FNE_runko
 switchport trunk allowed vlan 100
 switchport mode trunk
 channel-group 1 mode active

interface TenGigabitEthernet1/2
 description FNE_runko
 switchport trunk allowed vlan 100
 switchport mode trunk
 channel-group 1 mode active

interface TenGigabitEthernet2/1
```

```
 description Zhone_Runko_DSLAM
 switchport trunk allowed vlan 801,802
 switchport mode trunk
 channel-group 2 mode active

interface TenGigabitEthernet2/2
 description Zhone_Runko_DSLAM
 switchport trunk allowed vlan 801,802
 switchport mode trunk
 channel-group 2 mode active

interface TenGigabitEthernet3/1
 description DHCPv6
 switchport trunk allowed vlan 401
 switchport mode trunk
 channel-group 3 mode active

interface TenGigabitEthernet3/2
 description DHCPv6
 switchport trunk allowed vlan 401
 switchport mode trunk
 channel-group 3 mode active
```

Asetettujen komentojen jälkeen keskuskytkin osaa reitittää IPv4-sekä IPv6 -otsikoituja paketteja sisäverkossa eri VLAN -tunnisteiden välillä eritellyssä. Liikenne jakautuu tasaisesti ”port-channel”-rajapintojen välillä. Asiakaspäätelaitteiden DHCP-kyselyt uudelleen lähetetään asetettuihin DHCP-palvelimin, jonka jälkeen ne saavat dynaamisesti vaihtuvat IP-osoitteet.

9.2.3 Pääsylistat

Pääsylistojen avulla voidaan suodataa verkkojen välistä liikennöintiä asettamalla sääntöjä sisään tai ulostulevalle liikenteelle. Kun asetetaan sääntöjä rajapintaan, sitä sääntöjä kutsutaan silloin pääsylistaksi.

Laboratorioverkossa halutaan asettaa pääsylistat sisään tulevalle liikenteelle. Rajapinnassa sallitaan vain tulevan vain sallitusta IP-osoite avaruudesta. Oletus sääntönä pääsylista estää liikennettä eli se liikenne mikä halutaan kieltää, on sallittava. Koska rajapinnassa kulkee kahta IP-protokollan liikennettä, on asetettava eri pääsylistat kummallekin standardille. IPv6 pääsylistat voidaan nimetä, mutta IPv4 listat merkitään numerolla.

IPv4 pääsylistassa sallitaan liikenne osoitetusta IP-osoite avaruudesta sekä sallitaan mikä tahansa liikenne ”Bootstrap Protocol” eli BOOTP-liikenne. Ennen sääntöjen asettamista asetetaan säännöille selitys ”remark” -komennolla. Pääsylistojen komennot ovat nähtävissä alapuolella.

```
access-list 100 remark Sallitaan_IPv4_FTTH_Labraverkosta
access-list 100 permit ip 5.61.89.0 0.0.0.127 any
access-list 100 remark Sallitaan_DHCP_liikenne_IP_avaruudesta
```

```
access-list 100 permit udp any eq bootpc any eq bootps

access-list 101 remark Sallitaan_liikenne_IP_avaruudesta
access-list 101 permit ip 5.61.89.129 0.0.0.127 any
access-list 101 remark Sallitaan_DHCP_liikenne_IP_avaruudesta
access-list 101 permit udp any eq bootpc any eq bootps
```

Ipv6-pääsylistassa toimintaperiaate on sama kuin Ipv4 säännöissäkin. Pääsylistassa sallitaan liikenne asetetusta prefiksistä sekä sallitaan DHCPv6 kyselyt. DHCPv6-palvelin vastaanottaa kyselyt portista 546 ja lähettää ne eteenpäin porttiin 547 käyttäen UDP siirto protokollaa.

```
ipv6 access-list SALLITAAN_IPV6_VLAN801
permit 2A00:B9A0:801::/48 any
remark SALLITAAN_DHCPV6_LIIKENNE
permit udp any eq 546 any

ipv6 access-list SALLITAAN_IPV6_VLAN802
permit 2A00:B9A0:802::/48 any
remark SALLITAAN_DHCPV6_LIIKENNE
permit udp any eq 546 any
```

Kun pääsylistat on luotu, on ne asetettava haluttuihin VLAN rajapintoihin komennoilla:

```
interface Vlan801
 ip access-group 100 in
 ipv6 traffic-filter SALLITAAN_IPV6_VLAN801 in
 exit

interface Vlan801
 ip access-group 101 in
 ipv6 traffic-filter SALLITAAN_IPV6_VLAN802 in
 exit
```

Asetettujen pääsylistojen lisäksi luodaan yksinkertainen pääsylista, jossa estetään kaikki IPv6-liikenne. Tämä pääsylista sijoitetaan jokaiseen hallinta rajapintaan. Pääsylista luodaan samanlaisilla komennoilla kuin aikaisempikin IPv6-pääsylista. Pääsylistan luonnin jälkeen se asetetaan ”line vty”-rajapintoihin sisään tulevalle liikenteelle. Alapuolisilla komennoilla luodaan pääsylista ja asetetaan ne ”telnet”-sekä ”SSH”-protokollalla hallittaviin rajapintoihin.

```
ipv6 access-list IPv6deny
deny ipv6 any any
exit

line vty 0 4
ipv6 access-class IPv6deny in
exit

line vty 5 15
ipv6 access-class IPv6deny in
exit
```

9.2.4 Reititys

Sisäverkon reititys ulkoverkkoon tapahtuu FNE Finland Oy:n tarjoaman runkoyhteyden kanssa. Yhteys runkokytkimestä sekä FNE:n verkkolaitteeseen on muodostettu kytkemällä useampi fyysinen yhteys yhdeksi loogiseksi yhteydeksi LACP-protokollaa käyttäen. Reititysprotokollana käytettiin OSFPv3-standardia.

Reititys aloitettiin luomalla OSPFv3-reititysprosessi sekä antamalla reititin tunniste alla olevilla komennoilla. Reitittimen tunniste eli ”router-id” arvo voi olla mikä tahansa, kuhan millään muulla ei ole samaa tunnistetta. Tässä tapauksessa käytettiin jo olemassa olevaa reitittimen tunnistetta, josta tunnisteen vaihdettiin viimeinen numero.

```
ipv6 router ospf XXXXX
 router-id 5.61.88.2
```

Tämän jälkeen reititysprosessi asetettiin niille rajapinnoille, mistä haluttiin tieto reitittää.

```
interface Vlan100
 ipv6 ospf 19889 area 0
 exit

interface Vlan801
 ipv6 ospf 19889 area 0
 exit

interface Vlan802
 ipv6 ospf 19889 area 0
 exit
```

OSPFv3-naapuruuksien määrittelemiseksi on vielä luotava looginen loopback-rajapinta alla olevilla komennoilla.

```
interface Loopback1
 ip vrf forwarding IPV6TESTIT
 ip address 5.61.88.X 255.255.255.255
 ipv6 address 2A00:B9A0:1::X/128
 ipv6 enable
```

Lopuksi asetettiin staattinen oletusreitti ulkoverkkoon alla komennolla:

```
ipv6 route ::/0 2A00:B9A0:100::1
```

Komennon avulla runkoverkko ohjaa IPv6 -liikenteen ulkoverkkoon osoitteeseen ” 2A00:B9A0:100::1”.

9.3 Yhteyksien luonti DSLAM-laitteeseen

9.3.1 Zhone DSLAM -laitteiden hallinta

Zhone:n DSLAM laitteita voidaan hallinnoida kolmella eri tavalla; perinteisesti SSH tunneliyhteyden kautta, Web-pohjaisten verkkosivujen kautta taikka keskitetysti virtualisoidun palvelimen kautta. Pääosin yhteyksien siltausprofiilit luotiin keskitetyn hallinnan kautta.

Laitteiden keskitetty hallinta eli ”ZMS Virtual Appliance” on virtualisoituhallinta järjestelmä, jonka avulla voidaan konfiguroida, valvoa sekä hallita verkkototeutuksia. Järjestelmä on suunniteltu ajettavan virtualisoituna ”VirtualBox”-ohjelmalla. Järjestelmää hallittiin ”ZMS NetHorizon”-käyttäjäohjelman kautta. Jokainen hallinta käsky viestittiin SNMPv2-protokollaa käyttäen. Järjestelmä tukee myös FTP,TFTP sekä SFTP-protokollia laitteiden hallinnassa. Järjestelmä voi hallita enintään:

- 32 kpl MXK-194/198-laitetta
- 16 kpl MXK319-laitetta
- 8 kpl MXK-819-laitetta
- 8 kpl MXK-823-laitetta
- 4096 ONT
- 256 kpl 1U:n Zhonen MX-laittetta
- 6144 kpl CPE yhteyttä

(ZMS Virtual Appliance, Zhone Technologies, 2014)

9.3.2 Uplink-profiilin luonti

DSLAM-laitteen uplink -profiili eli runko yhteys keskuskytkimeen luotiin SSH yhteyden kautta. Profiilia ei saatu luotua toimivasti keskitetyn hallinnan kautta, sillä laiteen LACP profiilin nimeämiskäytäntö oli erilainen laitteessa kuin ZMS VA-palvelimessa. Uplink-profiili luodaan kaikkiin muihinkin Zhonen DSLAM laitteeseen samalla komennolla.

Uplink-profiili luotiin ottamalla SSH-tunneliyhteys laitteen hallinta osoitteeseen. Tämän jälkeen uplink profiili luotiin alla olevalla komennolla.

```
bridge add 1/a/1/0/linkagg uplink vlan 801 tagged
```

Komennolla luodaan LACP-profiiliin uplink-yhteys, jossa kulkee vlan tunniste 801 merkittynä. Komennon suorittamisen jälkeen komentorivi antaa tulosteen, jossa kerrotaan laitteen luoneen profiilin onnistuneesti, sekä luonut siltauksen nimeltä ”C4510LACPRunko-801/bridge”. Tuloste on nähtävissä kuviossa 19.

```
zSH> bridge add 1/a/1/0/linkagg uplink vlan 801 tagged
Adding bridge on 1/a/1/0/linkagg
Created bridge-interface-record C4510LACPRunko-801/bridge
Bridge-path added successfully
zSH>
```

Kuvio 19. Tuloste Uplink -profiilin luonnista komentorivillä

Tämän jälkeen siltausta voidaan tutkia komennolla ”bridge showdetail C4510LACPRunko-801/bridge”. Komennon avulla huomataan, että yhteys on päällä, sehä sen tyyppinä on ”upl” eli uplink. Komennon tulosteesta huomattiin myös, että yhteydessä kulkee vlan tunniste 801 merkattuna, niin kuin pitääkin. Yhteyden fyysisenä rajapintana on LACP-profiili ”LACPRunko/linkagg”. Edellisen komennon tuloste on huomattavissa kuviosta 20.

```
zSH> bridge showdetail C4510LACPRunko-801/bridge
Bridge interface: C4510LACPRunko-801
        Administrative status: up         Operational status: up
        Blocked status: unblocked
        Type:upl          Tagged  801
        Data: S VLAN 801 default[U: 3600 sec, M: 250 sec, I: 0 sec]

Physical interface: C4510LACPRunko/linkagg
        Administrative status: up         Operational status: up
```

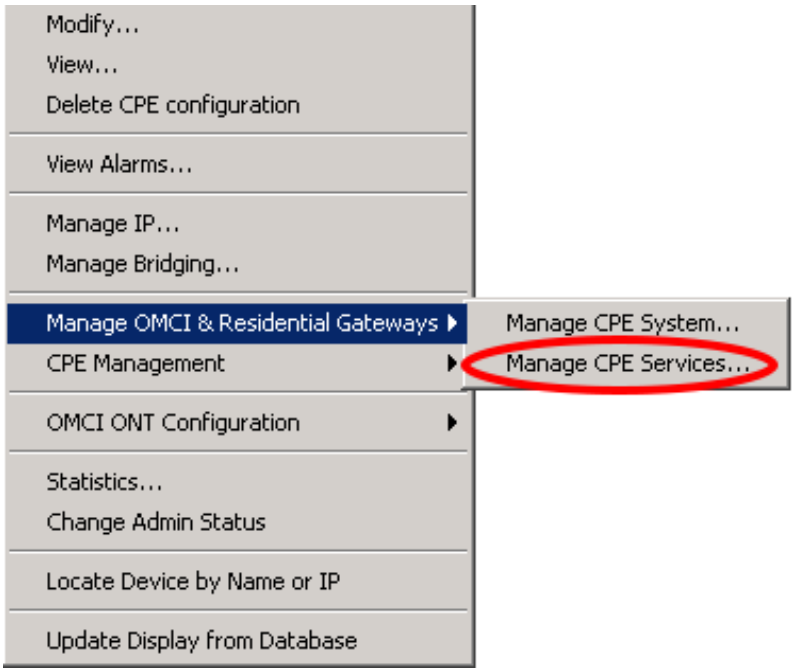
Kuvio 20. "bridge showdetail" -komennon tuloste juuri luodusta uplink -profiilista.

9.3.3 Downlink-profiilin luonti

Downlink-profiili eli keskittimen yhteys asiakkaan päätelaitteeseen luotiin graaffisen käyttöliittymän kautta. Yhteys luotiin vain kuituliittymiin, koska laajakaistaliittymien keskittimiin ei saatu luotua kaksoispino profiilia, johon sijoitettaisiin DHCPv6-standardin lisäoptio 82. Testauksissa huomattiin sen johtuvat laitteiston vajavaisesta ohjelmistosta.

Kuituliittymän yhteysprofiili luotiin NetHorizon-ohjelmiston avulla. Yhteyden luonti aloitettiin etsimällä ohjelmistosta haluttu keskitin laite sekä rajapinta, johon yhteys haluttiin luoda. Rajapinnan nimen kohdalta päästiin kuvion 21 näyttävään valikkoon

valikkoon painamalla hiiren oikeaa näppäintä, josta valittiin kohta ”Manage CPE Services”.

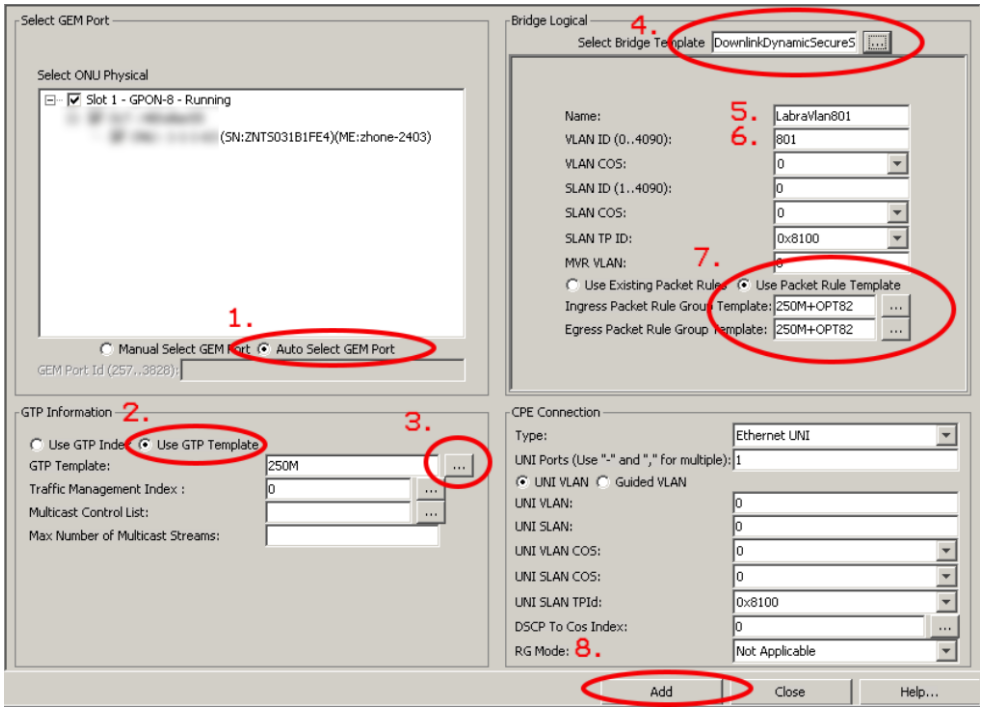


Kuvio 21. Valintanäkymä NetHorizon ohjelmiston yhteysprofiilin luonnissa laitteen asiakasrajapinnassa.

Valinnan jälkeen avautui ikkuna, jossa on kyseisen rajapinnan siltausprofiili. Profiilin alalaidasta painettiin ”Add” eli lisää painiketta. Painikkeen painamisen jälkeen avautui ikkuna, josta voitiin alkaa määrittelemään siltauksen asetuksia. Siltaus ikkunasta piti valita seuraavat kohdat:

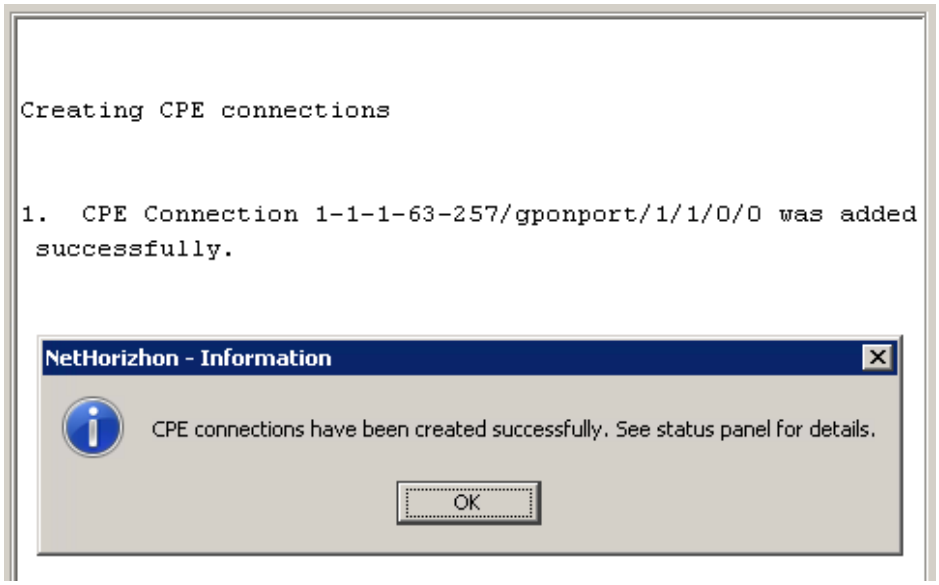
- ”Auto Select GEM Port”-Valitsee GEM portin automaattisesti eli GPON Encapsulation Method
- ”Use GTP Template”-GTP profiilin pohja eli toisin sanoen yhteyden nopeusprofiili
- ”Select Bridge Template: DownlinkDynamicSecureSingleTagged”-Siltaus profiilin pohja
- Name: ”LabraVlan801” - Nimi yhteydelle, joka lokitetaan DHCPv6 -palvelimelle
- VLAN ID: ”801”´- VLAN Tunnisteen numero
- Ingress Packet Rule Group Template: ”250M+OPT82”- Sisääntulevalle liikenteelle asetetaan 250 Megabitin rajoitus sekä DHCP viesteihin lisätään lisäoptio82.
- Egress Packet Rule Group Template: ”250M+OPT82”- Sisääntulevalle liikenteelle asetetaan 250 Megabitin rajoitus sekä DHCP viesteihin lisätään lisäoptio82.

Valintojen jälkeen asettamisen jälkeen painetaan ikkunan alaseuranasta ”Add”-painiketta, josta yhteys rakennetaan asetettujen valintojen mukaisesti. Kuvio 22 havainnollistaa, mitkä asetukset piti laittaa, kaksoispinoprofiilin rakentamiseksi.



Kuvio 22. Kuituyhteyden siltausprofiilin asetukset NetHorizon ohjelmistossa.

Add-painikkeen painamisen jälkeen ilmestyi kuvion 23 mukainen ilmoitus, josta nähdään yhteyden pystyttämisen onnistuneen.



Kuvio 23. Ilmoitus siltausyhteyden pystyttämisestä

10 Laboratorioverkon toimivuuden todentaminen

10.1 Runkokytkimen yhteys verkon eri alueisiin

Laboratorioverkon pystyttämisen jälkeen alettiin selvittämään verkon toimivuutta ja miten eri verkkolaitteet ovat vuorovaikutuksissa keskenään eri standardien kesken.

Kun kaikki verkon eri laitteet olivat asetettu toimintavalmiiksi, aloitettiin toimivuuden testaaminen selvittämällä IPv6-naapuruudet runkokytkimestä. Komennolla ”show ipv6 neighbors vlan 801” laite tulostaa kaikki IPv6-naapuruussuhteet ja niiden tilat vlan tunnisteesta 801. Mainittu komento suoritettiin ja sen tuloste on nähtävissä kuviosta 24.

```
C4510_Kellari#show ipv6 neighbors vlan 801
IPv6 Address                              Age Link-layer Addr State Interface
FE80::222:7FF:FE42:8F0                      0 0022.0742.08f0  REACH Vl801

C4510_Kellari#
```

Kuvio 24. "show ipv6 neighbors" -komennon tuloste vlan tunnisteesta 801

Tulosteesta huomataan että laite on havainnut verkossa asetetun asiakkaan päätelaitereitittimen. Kyseinen päätelaite on ”REACH”-tilassa, jonka ”link-local”-osoite on FE80::222:7FF:FE42:8F0. Tuloste kertoo myös laitteen MAC osoitteen, joka on eroteltu pisteillä.

IPv6-naapuruuksien selvittämisen jälkeen alettiin tekemään ”ping”-kyselyitä päätelaitteeseen. Kyselyissä runkokytkin lähetti viisi perättäistä kyselyä, josta on nähtävissä jokaisen kyselyn viive sekä saavutettavuus. Komennon tulosteesta nähdään myös kyselyiden viiveiden alin-, ylin- sekä keskiarvo. Verkon ensimmäinen kysely tehtiin reitittimen WAN-rajapinnan globaaliin ”unicast”-osoitteeseen. Kuviosta 25 on nähtävissä, että kysely saavuttaa päätelaitteen onnistuneesti.

```
C4510_Kellari#ping ipv6 2a00:b9a0:801:ffff:ffff:ffff:ffff:fff0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2A00:B9A0:801:FFFF:FFFF:FFFF:FFFF:FFF0, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
C4510_Kellari#
```

Kuvio 25. "Ping" -kysely päätelaitteen WAN-rajapintaan

Tämän jälkeen tehtiin seuraava yhteyskysely päätelaitereitittimen LAN-rajapintaan. Kuviosta 26 nähdään, että jokainen kysely meni verkkolaitteelle onnistuneesti.

```
C4510_Kellari#ping ipv6 2a00:b9a0:801:ffff::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2A00:B9A0:801:FFFF::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/8 ms
```

Kuvio 26. "Ping" -kysely päätelaitteen LAN-rajapintaan

Näiden kyselyiden jälkeen tehtiin vielä yhteyskokeilu DHCPv6-palvelimeen. Kyselyihin tuli vastauksena ”A” eli ” Administratively prohibited”. Tämä tarkoittaa, että ICMP-kyselyt ovat valvonnallisesti rajoitettu pääsylistalla tai palomuurilla. Kuviosta 27 on huomattavissa ”ping” -kyselyiden tuloste.

```
C4510_Kellari#ping ipv6 2a00:b9a0:    ::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2A00:B9A0:302::2, timeout is 2 seconds:
AAAAA
Success rate is 0 percent (0/5)
```

Kuvio 27. "Ping" -kysely DHCPv6 -palvelimelle

Tämän jälkeen tutkittiin DHCPv6-palvelimen ”ip6tables”-palomuurin sääntötaulua. Sääntötaulu oli nähtävissä suorittamalla komento ”ip6tables -L” palvelimen komentoriville. Komennon suoritettua oli nähtävissä, että sääntöketjuun on asetettu sääntö, jossa kaikki liikenne mistä tahansa estetään säännöllä ”icmp6-adm-prohibited”.

Yhteyskyselyiden jälkeen tutkittiin OSPFv3-reititysprotokollan toimivuutta. Ensimmäiseksi tutkittiin, onko runkoreititin saanut muodostettua naapuruutta ulkoverkon suuntaan. Naapuruus saatiin näkymiin suorittamalla reitittimeen komento ”show ipv6 ospf neighbors”. Komennon tulosteesta huomataan että asetettu reititin tunniste ”5.61.88.X” on muodostanut OSPFv3-naapuruuden täydellisesti rajapinnasta ”VlanXXX”. ´Tulosteesta on myös huomattavissa, että naapuruus käyttää asetettua prosessi tunnistetta. Kuviossa 28 nähdään komennon tuloste kokonaisuudessaan.

```
C4510_Kellari>show ipv6 ospf neighbor

            OSPFv3 Router with ID (5.61.88.  ) (Process ID      )

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
5.61.88.        128   FULL/DR         00:00:30    2               Vlan
```

Kuvio 28. OSPFv3 -naapuruudet ulkoverkkoon

OSPFv3-naapuruuksien jälkeen tutkittiin, mitä rajapinnat suorittavat reititystä. Komennolla ”show ipv6 ospf interface brief”, saatiin näkymään yhteenveto kaikista ospf -reititystä tekevää rajapintaa. Komennon tulosteesta nähdään että VLAN-rajapintoihin 802, 801 sekä 100 on konfiguroitu OSPFv3-reititys prosessitunnisteesta XXXXX. Asetetun komennon tuloste on näkyvissä kuviossa 30.

```
C4510_Kellari#show ipv6 ospf interface brief
Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
V1802              0               142        1     DR    0/0
V1801              0               141        1     DR    0/0
V1100              0               128        1     BDR   1/1
```

Kuvio 29. Tuloste IPv6 OSPFv3 naapuruuksista.

10.2 DSLAM-laitteen siltauksen tiedot

Kun siltaus oli saatu luotua laboratorioverkon DSLAM-laitteeseen, tutkittiin minkälaista tietoa laite näkee yhdistyneen vlan tunnisteeesta 801. Siltauksen tietoja tarkasteltiin SSH-yhteyden kautta. Yhdistettyä DSLAM-laitteeseen suoritettiin komento *”bridge show vlan 801”.* Komento tulosti kaikki siltaukset, jotka käsittelevtä VLAN-tunnisteen 801 tietoa. Tulosteesta huomataan, että laitteessa on kaksi siltausta, jotka käsittelevät vlan 801 tietoja. Toinen on Uplink-siltaus ja toinen on Downlink-siltaus. ”Downlink”-siltauksen taulukosta nähdään, että siltauksen kautta on yhdistettynä asiakasreititin, joka on saanut IPv4-sekä IPv6- osoitteet sekä IPv6-prefiksin. Siltaukseen on myös yhdistetty asiakasreitittimen ”link local”-osoite sekä MAC-osoite. Kummankin siltauksen tilan on ”up” eli niissä kulkee liikennettä. Komennon tuloste on näkyvissä alla olevassa liitteessä 2.

10.3 DHCPv6-palvelimen saadut kyselyt ja asetettujen osoitteiden todentaminen

Kun asiakasreititin kytkettiin verkkoon, se lähetti verkkoon DHCP-pyynnön. Kun runkoreititin sai kyseisen pyynnön, se uudelleen lähetti pyynnöt suoraan DHCPv6 sekä DHCPv4 palvelimelle. Runkoreititin toimii ”Relay”-roolissa eli uudelleen lähettäjänä. Käsiteltyä pyynnöt, DHCPv6-palvelin lähettää ne runkoreitittimelle, joka välittää viestit takaisin verkkoon.

Asiakkaan reitittimen DHCPv6-pyynnöt selityksineen on nähtävissä DHCP-lokissa. Lokia seurattiin suorittamalla komento ”tail-f 80 /var/log/dhcpd6”. Ennen komennon suorittamista ”dhcpd6”-palvelu käynnistetään uudelleen. Samalla päätelaitteen yhteys irrotettiin ja kytkettiin uudelleen, jolloin saadaan simuloitua IPv6-osoitteen uudelleen neuvottelu. Liitteessä 1 on näyttökuva DHCPv6-palvelimen lokista, jossa asiakasreititin saa onnistuneesti varattua itselleen IPv6-osoitteen sekä prefiksin.

Palvelimen loki alkaa ilmoituksella, jossa kerrotaan että DHCP palvelu versio 4.3.3 on käynnistetty ja että ohjelmisto on kopiosuojattu. Ilmoituksen jälkeen loki kertoo, että ”lease”-tiedostoon on kirjoitettu yksi varattu osoite sekä prefiksi. Sen jälkeen loki kertoo palvelun olevan liitetty TCP -porttiin 547, joka kuuntelee rajapintaa ”eth1”. Tämän jälkeen loki kertoo, että rajapintoihin ”eth0” sekä ”eth2” ei ole liitetty IPv6-aliverkkoa sekä kaikki pyynnöt kyseisistä rajapinnoista hylätään. Sen jälkeen loki kertoo palvelun olevan käynnistetty. Käynnistämisilmoituksen jälkeen palvelu saa uudelleen lähetetyn ”relay-forward”-viestin runkoreitittimen rajapinnalta. Viestin saatuaan, palvelu ottaa osoiteavaruudesta osoitteen sekä prefiksin, jonka se tarjoaa eteenpäin päätelaitereitittimelle. Tarjousviestin lähetettyä, palvelu vastaanottaa varmistusviestin päätelaitteelta. Vastaanotettua viestin palvelu hyväksyy neuvotellut IP-tiedot ja kirjoittaa ne ”lease”-tiedostoon. Hyväksymisen jälkeen palvelu päättää keskustelun päätelaiteen kanssa vastaamalla laitteelle, että osoitetiedot ovat varattu laitteelle seuraavan 24 tunnin ajan.

Lokin tarkastelun jälkeen tutkittiin ”lease”-tiedostoa, mihin palvelu kirjoitti varatut IPv6 -osoitetiedot. Tiedostosta huomattiin, että palvelu oli kirjoittanut tiedostoon asetettujen määreiden mukaisesti tarpeelliset liittymän tiedot. Kuviossa 30 nähdään

varattu IPv6-osoite, sekä prefiksi. Kuviosta on nähtävissä osoitetietojen tila, varauksen elinikä, päättymisaika, asetettujen lisäoptioiden tiedot (remote-id, lla, ifname), prefiksin suuruus, sekä varattu IPv6 -osoite sekä prefiksi.

```
ia-na "\001\000\000\000\000\003\000\001\000\"\007B\010\360" {
  cltt 4 2016/01/07 06:33:09;
  iaaddr 2a00:b9a0:801:ffff:ffff:ffff:ffff:fff0 {
    binding state active;
    preferred-life 86400;
    max-life 86400;
    ends 5 2016/01/08 06:33:09;
    set remote-id = "\000\000\025\200vlan801";
    set lla = "0:22:7:42:8:f0";
    set ifname = "Zhone MxK319 HE toimisto";
    set pdsize = "64";
    set iapd = "2a00:b9a0:801:ffff:0:0:0:0";
    set iana = "2a00:b9a0:801:ffff:ffff:ffff:ffff:fff0";
  }
}

ia-pd "\001\000\000\000\000\003\000\001\000\"\007B\010\360" {
  cltt 4 2016/01/07 06:33:09;
  iaprefix 2a00:b9a0:801:ffff::/64 {
    binding state active;
    preferred-life 86400;
    max-life 86400;
    ends 5 2016/01/08 06:33:09;
    set remote-id = "\000\000\025\200vlan801";
    set lla = "0:22:7:42:8:f0";
    set ifname = "Zhone MxK319 HE toimisto";
    set pdsize = "64";
    set iapd = "2a00:b9a0:801:ffff:0:0:0:0";
    set iana = "2a00:b9a0:801:ffff:ffff:ffff:ffff:fff0";
  }
}
```

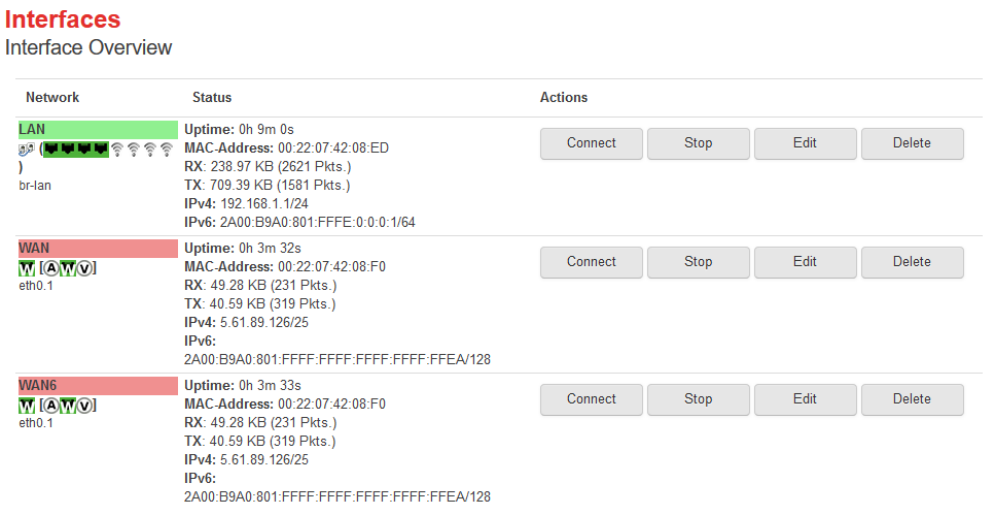
Kuvio 30. Ote varatusta osoitetiedoista "lease"-tiedostosta.

10.4 Asiakkaan reitittimen saamat tiedot

Asiakasyhteyden toimivuus tutkittiin Inteno:n päätelaite reitittimellä. Olettamuksena voitiin ajatella että asiakasreititin on oletusasetuksilla, joten laite palautettiin tehdasasetuksille ennen verkkoon kytkemistä. Verkkoon kytkettäessä huomattiin IPv4 tulleen laitteelle. Laite oli määritellyt DHCPv6 -palvelimelta asiakkaan lähiverkkoon ennalta määritellyn verkkoalue prefiksin, joka oli tässä tapauksessa ”2A00:B9A0:801:FFFE::/64”. DHCPv6-palvelimen lokitiedoista saadun viestien perusteella, tapahtuma huomattiin. WAN-rajapinta ei siis saanut globaalia IPv6-osoitetta. Laitteen asetuksia tarkkailtaessa huomattiin että ulkoverkon rajapinnan DHCPv6 -asiakkaan pyynnöt oli otettu pois käytöstä. Valinta asetettiin kuvion 31 mukaisesti ”try” tai ”force” asentoon, jolloin ulkoverkkokin sain globaalisesti uniikin IPv6-osoitteen.

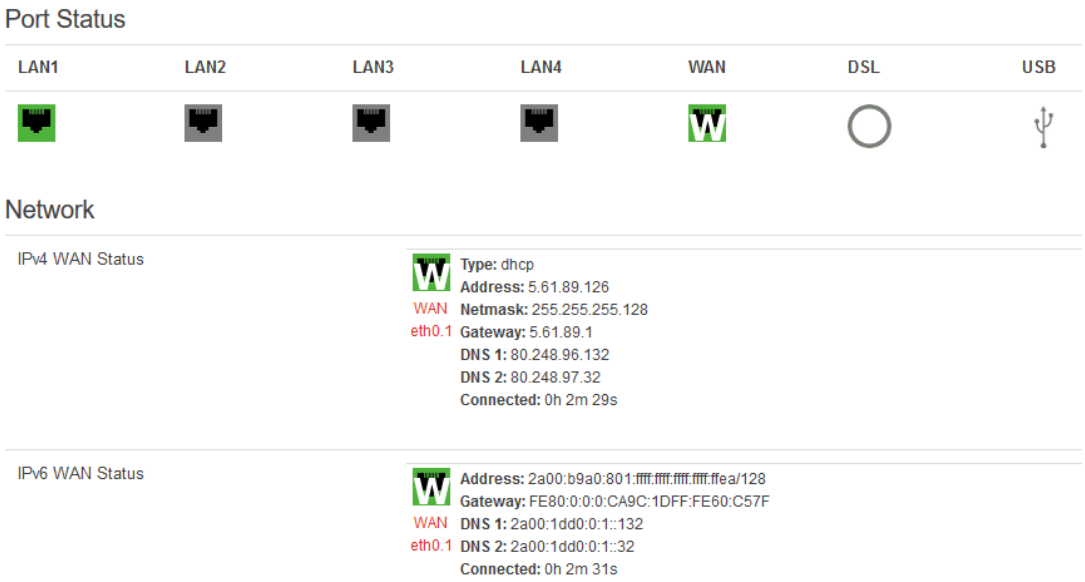
Kuvio 31. Inteno -reitittimen WAN-rajapinnan DHCPv6 asiakaspyyntöjen asettaminen

Verkkolaitteen asetuksien ”Interfaces”-sivulta (kuvio 32) on nähtävissä jokaisesta verkkorajapinnasta yhteenveto taulukko. Taulukosta nähdään lähiverkkoon määritelty prefiksi sekä ulkoverkon kummankin IP protokollan mukaiset osoitteet. Ulkoverkon rajapinta sai IPv4-osoitteeksi ”5.61.89.126/25” sekä IPv6 osoitteeksi ”2A00:B9A0:801:FFFF:FFFF:FFFF:FFFF:FFEA/128”. Lähiverkon rajapinta määritteli itselleen verkkoalueen ensimmäisen osoitteen eli ”2A00:B9A0:FFFE:0:0:0:1/64”. IPv4-verkossa asiakkaan lähiverkossa käytetään NAT -osoitteen käännösprotokollaa julkisen osoitteen vähäisyyden takia. Lähiverkon IPv4 verkkoprefiksi on siis standardin määrittelemä privaatti verkkoalue.



Kuvio 32. "Interface" -sivun rajapintatietojen yhteenveto taulukko

Laitteen ”Overview”-sivulta on nähtävissä, että rajapinnat saivat ensi- sekä toissijaiset DNS-palvelimien osoitteen kummallekkin protokollalle. Overview-sivun rajapinta tiedot ovat nähtävissä kuviossa 33.



Kuvio 33. laitteen "Overview" -sivun rajanpinta tiedot.

10.5 Asiakasreitittimen lähiverkossa olevan tietokoneen saamat osoitetiedot sekä yhteyden todentaminen

Reitittimen lähiverkkoon yhdistettiin Windows 10-käyttöjärjestelmällä varustettu tietokone. Yhdistämisen jälkeen avattiin tietokoneen komentokehote, johon kirjoitettiin komento ”ipconfig”. Komennolla ilmestyi tietoja laitteen verkkorajapinnasta. Tiedoista huomattiin, että tietokone oli asettanut itselleen globaalin IPv6-osoitteen. Osoite oli määritelty käyttämällä asiakasreitittimen saatua prefiksiä sekä EUI-64 rajapintatunnistetta. Tietokone oli määritellyt osoitteen käyttämällä autokonfiguraatiota. IP-osoitetiedoista huomattiin rajapinnan ”link-local”-osoite sekä IPv4-protokollan osoite sekä aliverkon peite eli ”Subnet Mask”. Tiedoista huomattiin myös, että laitteella oli kaksi oletusyhdyskäytävää kummallekin osoite protokollalle. IPv6-oletusyhdyskäytävä oli reitittimen paikallinen ”link-local”-osoite. IP-tietojen tarkastelun jälkeen tehtiin ”ICMP Echo”-kysely eli tutummin ”Ping”-kysely keskusreitittimen rajapintaan ”2A00:B9A0:801::1”. Kysely saavutti onnistuneesti runkoreitittimen rajapinnan. Tietokoneen rajapintatiedot sekä kyselyn tuloste on nähtävissä alapuolella olevasta kuviosta 34.

```
C:\WINDOWS\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : lan
   IPv6 Address. . . . . . . . . . . : 2a00:b9a0:801:fffe:8119:28f8:758d:485b
   Temporary IPv6 Address. . . . . . : 2a00:b9a0:801:fffe:99f7:1591:91a3:ebe7
   Link-local IPv6 Address . . . . . : fe80::8119:28f8:758d:485b%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.149
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::222:7ff:fe42:8ed%10
                                       192.168.1.1

C:\WINDOWS\system32>ping 2a00:b9a0:801::1

Pinging 2a00:b9a0:801::1 with 32 bytes of data:
Reply from 2a00:b9a0:801::1: time=2ms
Reply from 2a00:b9a0:801::1: time=2ms
Reply from 2a00:b9a0:801::1: time=2ms
Reply from 2a00:b9a0:801::1: time=2ms

Ping statistics for 2a00:b9a0:801::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\WINDOWS\system32>
```

Kuvio 34. Asiakasreitittimen lähiverkon tietokoneen IP-osoitetietojen sekä "Ping" -kyselyn tuloste

Tämän jälkeen testattiin saadun DNS-palvelimen toimivuutta tekemällä ”Ping”-kysely sekä nimikysely ”nslookup” kyseiseen osoitteeseen. Kuviosta 35 on huomattavissa, että ”Ping” kysely on ilmeisesti estetty, mutta nimikyselyt silti toimivat. Kyselyjen tulosteessa huomattiin, että asiakasreitittimen lähiverkossa DNS palvelimen osoite on verkon oletusyhdyskäytävä. Kysely reitietään lähiverkon kautta reitittimen saatuihin DNS-osoitteisiin, siksi lähiverkon privaatti IPv4– sekä ”link-local” IPv6 -osoite näkyy lähiverkon laitteissa nimipalvelimena.

```
C:\WINDOWS\system32>ping 2a00:1dd0:0:1::132

Pinging 2a00:1dd0:0:1::132 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 2a00:1dd0:0:1::132:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\WINDOWS\system32>nslookup 2a00:1dd0:0:1::132
Server:  Inteno.lan
Address:  192.168.1.1

Name:    ns1.kymp.net
Address:  2a00:1dd0:0:1::132
```

Kuvio 35. "Ping" - sekä nimi kysely DNS palvelimen osoitteeseen.

DNS-palvelimen testauksen jälkeen tutkittiin IPv6- verkon toimivuutta runkoverkossa. Toimivuus tutkittiin suorittamalla ”tracert” komento julkiseen ”ipv6.google.com” osoitteeseen. Kyselyn tulosteesta (Kuviosta 36) huomataan, kuinka viesti kulkee asiakasreitittimen sekä runkoreitittimen läpi ulkoverkkoon. Viesti 12 eri hypynjälkeen saavuttaa kysellyn domainin, jonka IPv6 osoite on ”2a00:1450:400f:804::200e.

```
C:\WINDOWS\system32>tracert ipv6.google.com

Tracing route to ipv6.l.google.com [2a00:1450:400f:804::200e]
over a maximum of 30 hops:

  1     2 ms     1 ms    <1 ms  2a00:b9a0:801:fffe::1
  2     3 ms     5 ms    23 ms  2a00:b9a0:801::1
  3     1 ms     1 ms     1 ms  2a00:b9a0:300::1
  4     5 ms     4 ms     4 ms  2a00:1d50:1:1d::5
  5     4 ms     4 ms     4 ms  2a00:1d50:1::1
  6     5 ms     5 ms     5 ms  2a00:1d50:1:e::2
  7     9 ms     9 ms     9 ms  2a00:5500:0:2::174
  8    11 ms    11 ms    11 ms  2a00:5500:0:2::208
  9    13 ms    13 ms    20 ms  2001:7f8:d:ff::115
 10    12 ms    12 ms    12 ms  2001:4860::1:0:26ec
 11    12 ms    12 ms    12 ms  2001:4860:0:1::e5
 12    12 ms    12 ms    12 ms  arn09s05-in-x0e.1e100.net [2a00:1450:400f:804::200e]

Trace complete.
```

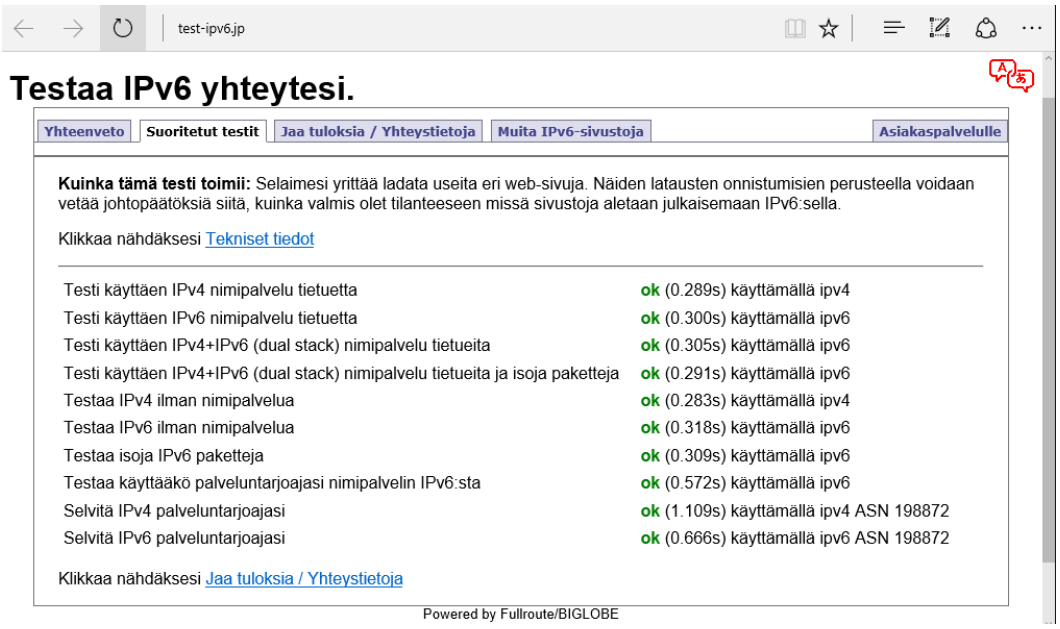
Kuvio 36. "tracert" kyselyn tuloste osoitteeseen "ipv6.google.com"

Tämän jälkeen tutkittiin miltä tietokone näyttää ulkoverkosta katsottuna. Internetissä on useita sivustoja, millä pystyy katsomaan onko tietokone IPv6 yhteensopiva.

Ensimmäinen sivusto, jolla vierailimme oli verkkohakupalvelu Google:n tekemä. Se sijaitsi osoitteessa ”ipv6test.google.com”. Selainikkunaan tuli kuvion 37 mukainen viesti, joka kertoi että IPv6 standardi on käytössä.

Kuvio 37. Googlen IPv6 -testin tuloste

Tämän jälkeen teimme toisen IPv6 testin sivustolla, joka antoi paljon enemmän tietoja yhteydestä. Sivusto erotteli jokaisen testin, joka varmisti IPv6 toimivuuden. Kuvissa 39 nähdään ”test-ipv6.jp”-sivuston antama tulos tietokoneen IPv6 toimivuudesta. Selain ikkunan tuloksen mukaan kaikki testit läpäistiin tuloksella ”ok”.



Kuvio 38. "test-ipv6.jp" -sivuston testitulokset

11 Laboratorio toteutuksen vienti tuotantoverkkoon

11.1 Tuotantoverkon suunnitelma

Laboratorioverkon toteutuksen tuominen tuotantoon aloitettiin kartoittamalla IPv6 yhteyden rajoitukset ja mahdollisuudet. Ainoa rajoitus kaksoispinoverkon käyttöönotossa oli liittymän yhteyden tyyppi. Kaksoispino verkkoon voitiin lisätä vain ne asiakkaat, joilla oli kuituliittymä sekä ei ollut IPTV-lisäpalvelua. IPTV käyttää IPv4-multicast liikennevirtaa videokuvan lähettämiseen. DSLAM-laitteen sekä GPON eli kuitukeskittimien siltaprofiiliasetukset eivät silti pystyneet muodostamaan kaksoispino yhteyttä, jossa kulkee IPTV-multicast liikennettä. Laitevalmistajan käyttöohjeessa on IPv6 vertailutaulukko IPv6 yhteensopivuuksista Zhonen verkkolaitteessa. Kuviossa 39 on kuvankaappaus käyttöohjeessa, josta huomataan ”Video Downlink”-profiilin toimivan vain IPv4-standardilla.

Table 20: IPv4 and IPv6 comparison

Feature/Configuration	Command	IPv4	IPv6		Comment
			Stateless	Statefull	
Video downlinks	bridge add … downlink-video	Yes	No	No	Currently mutlicast video (IPTV) is only supported with IPv4 and IGMP. Not in IPv6 and MLD. Conceptually, there is no requirement for bridge type downlinkvideo to have certain IP version. There is no related provisioning.

Kuvio 39. Kuvankaappaus Zhonen käyttöohjeen IPv6 yhteensopivuustaulukosta

Suunnittelussa päätettiin, että ilmenneiden ongelmien vuoksi järjestetään ilmainen kokeilujakso kaikille vapaaehtoisille kuituliittymäasiakkaille. Kaikki vapaaehtoiset kerättiin lähettämällä kirje kyseisille asiakkaille, jonka jälkeen halukkaat saivat osallistua pyrkiä kokeilujaksolle. Pyrkiminen kokeilujaksolle tapahtui vastaamalla lähetettyyn kirjeeseen, jonka tiedoissa on liittymän päätelaitteen mallimerkintä. Vastauskirjeen lähetettyä valittiin kokeilujaksolle sopeutuvat asiakkaat, jotka liitetään erilliseen IPv6-asiakasverkkoon. Tämän jälkeen asiakkaille lähetettiin ohjeistus reitittimen asetuksien säätämiseksi. Kokeilujakson aikana lähetetään kyselylomake verkon toimivuudesta, jonka tarkoituksena on selvittää yhteyden hyödyt sekä haitat. Kokeilujakson

päättymistä ei määritelty, sillä IPv6-osoitteistus haluttiin pitää pysyvänä ratkaisuna verkossa.

11.2 Tuotantoverkon toteutus

Suunnittelussa päätettiin, että tehdään erillinen IPv6-asiakasverkko johon halukkaat asiakkaat liitetään. Ennen tuotantoverkon toteuttamista päivitettiin MXK-runko DSLAM:n ohjelmisto, joka toi paranneltuja IPv6-ominaisuuksia laitteeseen. Verkkoon luotiin uusi VLAN-tunnistella merkitty verkko. Tunniste asetettiin yrityksen nimeämislogiikan mukaisesti. Verkossa käytettiin samaa IPv4-osoiteavaruutta kuin laboratorioverkossa yhteensä. IPv6- osoiteprefiksi asetettiin samalla kaavalla VLAN-tunnisteen mukaisesti. Verkossa käytettiin samoja konfiguraatioita, mitä laboratorioverkkoon oli asetettu. asetuksissa, muutettiin vain IP-osoitteet tuotantoverkon mukaisiksi. IPv6-asiakasverkkoa tehdessä poistettiin samalla laboratorioverkon konfiguraatiot sekä siltaukset eri verkkolaitteista. DHCPv6-palvelimessa muutettiin jaettavia verkkoalueita tuotantoverkon mukaisiksi. Palvelimelle myös asetettiin tallentumaan ”lease”-tiedostot sekä DHCPv6-palvelun lokit erilliselle lokipalvelimelle, josta tietoja voidaan paremmin hallita eikä tallennetut lokitiedostot kuormita palvelimen suorituskykyä. Runkoreitittimessä käytettiin samaa reititysprosessi tunnistetta kuin laboratorioverkossa. IPv4- sekä IPv6 pääsylistat luotiin uudelleen uusien osoitteiden mukaisiksi. Sen suurempia muutoksia ei laboratorioverkon toteutuksen viennistä tuotantoon tehty.

11.3 IPv6-asiakasverkon toiminta ja tulevaisuus

Tuotantoverkon rakentamisen jälkeen voitiin todeta, että IPv6-asiakasverkko toimi suunnitelmien mukaisesti. Siirtymävaihe oli kuitenkin vasta alussa, sillä vain osa asiakkaista sai kaksoispino yhteyden. Kokeilujakson tuloksien pohjalta voidaan tehdä päätös viedäänkö toteutus lopuille kuituasiakkaille. Kuituyhteyksien jälkeen seuraava etappi kaksoispino yhteyden siirrossa on odottaa, että Zhone:n laajakaista keskittimiin tulisi järjestelmäpäivitys, Päivityksen myötä voitaisiinmahdollistaa kaksoispino yhteys myös xDSL-asiakkaille.

Kun kuitu- sekä laajakaista-asiakkaat ovat saaneet kaksoispino yhteyden, voidaan aloittaa IPv4-standardin pois siirtymisestä. Arviolta tähän vaiheeseen on ainakin 10

vuotta aikaa. IPv4-protokollan puutteiden takia siirtymä kokonaan IPv6 -standardiin on tulevaisuudessa, on siitä hyvä luoda alustava aikataulu sen toteutukseen.

12 Yhteenveto

Työtä tehdessä ilmentyi useita ongelmia sekä onnistumisia. Jotkut ongelmat korjaantuivat yksinkertaisella konfiguraatiomuutoksella ja toiset vasta kuin verkkolaitteen järjestelmä oli saatu päivitettyä. Osa onnistumisisen hetket tapahtuivat usein ongelman ratkaisun jälkeen.

Työn suurin ongelma oli saada MXK-laitteen siltausprofiili luotua, niin että kaksoispinoyhteys olisi toimiva sekä että lisäoption sisältämä tieto-tulisi tallennettua kummankin protokollan DHCP-palvelimille. Usein siltaus saatiin muodostettua vain toisen kriteerin täyttyessä. MXK-laitteen Uplink-profiilin luonnissa ilmeni myös ongelma, sillä kun yhteyden loi graafisen käyttöliittymän kautta, yhteys ei toiminut. Uplink -profiili saatiin luotua SSH-yhteyden kautta kirjoittamalla erillinen komento laitteelle.

Pari ongelmaa, jäi vielä ratkaisua vaille. IPTV-toimimattomuus kaksoispinoyhteyden kanssa hämmensi, sillä IPTV-videovirrat toimii verkossa vain IPv4-standardilla. Useiden testauksien jälkeen myös jäi selvittämällä, miten lisäoptioiden lisäys siltaukseen voi aiheuttaa yhteyden toimimattomuuden. Useissa tilanteissa yhteys toimi ilman lisäoptio asetusta. Heti kun asetuksen lisäsi yhteyteen, laite ei voinut vastaanottaa palvelimen DHCPv6-viestejä. Vasta järjestelmäpäivityksen jälkeen yhteys alkoi toimimaan. Näiden ongelmien ratkaisemiseksi ei nähty oleelliseksi tutkia enempää, jotta työn tavoiteaika saavutettaisiin.

Työssä olleen onnistumisen hetket koostuivat osaksi ongelmien ratkaisujen löytämisestä. Yksi suurimmista onnistumisista oli MXK-laitteen järjestelmäpäivitys, jonka avulla laboratorioverkko voitiin julistaa toimivaksi. Työtä dokumentoidessa huomattiin, kuinka esitelty teoria tuki käytännön toteutusta. Hyvä esimerkki oli DHCPv6-viestit, jotka jälkeen todettiin protokollan toimivan teorian mukaisesti.

13 Pohdinta

Työtä tehdessä tapahtui kokonaisvaltainen oppimisprosessi, jonka lopputuloksena oli toimiva IPv6-ratkaisu operaattoriverkossa. Työ otti huomioon monipuolisesti verkon eri laitteen ja niiden rajoitteet. Työssä tehtiin muutossuunnitelma kaksoispinoyhteyden luomista varten. Suunnitelmassa otettiin huomioon riskit, verkko infrastruktuurin tila sekä rajaus mille verkko toteutettiin. Rajausta kuitenkin jouduttiin muuttamaan löydettyä puutos laajakaistaliittimien DSLAM:ien järjestelmästä, joka ei tukenut kunnolla kaksoispinoyhteyttä. Työssä olisi voinut paneutua enemmän aiemmin mainittuihin avoimiin ongelmiin.

Työn käytännön osuutta tehdessä huomattiin, kuinka että laitevalmistavat tehneet erilaisia toimintaratkaisuja IPv6-verkon suhteen. Testatut reitittimet tarjosivat hyvin IPv6 valmiutta asetussivuillaan. IPv6-standardi ei kuitenkaan yksinään ole vielä käyttökelvollinen, sillä IPv4 yhteyttä käytetään niin paljon alalla. Nykytilanteessa kaksoispino on helpoin ja käytetyin siirtymistapa IPv6 -standardiin.

Lähteet

DHCPv6 Based IPv6 Access Services. Viitattu 3.11.2015. http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/whitepaper_c11-689821.html

Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Viitattu 3.11.2015. https://tools.ietf.org/html/rfc3315

Grossetete, P., Levy-Abegnoli, E., Popoviciu, C. 2006. Deploying IPv6 Networks. Ciprian Cisco Systems.

Silvia Hagen, IPv6 Essentials, Third Edition. 2014. O'Reilly Media.

Functions of NDP, Neighbour Solicitation and Advertisement, Router Solicitation and Advertisement. Viitattu 3.11.2015. http://www.omnisecu.com/tcpip/ipv6/ndp-neighbour-discovery-protocol-functions-of-ndp.php

Historia, Viitattu 19.1.2016. http://www.haminanenergia.fi/fi/yritys/historia

Internet Protocol, Version 6 (IPv6) Specification. Viitattu 19.10.2015. https://www.ietf.org/rfc/rfc2460.txt

IPv6 - Auto Configuration vs DHCPv6. Viitattu 3.11.2015. http://ipv6.com/articles/general/Auto-Configuration-vs-DHCPv6.htm

Lampikari, J. 2014 DHCPv6-palvelin operaattorikäytössä. Opinnäytetyö. Kymenlaakson Ammattikorkeakoulu.

Lehtonen, J. 2014. IPv6-verkon suunnittelu ja implementointi yritysverkoissa. Opinnäytetyö. Metropolia Ammattikorkeakoulu.

Overview of IPv6. Viitattu 19.10.2015. http://www.cisco.com/c/en/us/td/docs/interfaces_modules/services_modules/ace/vA5_1_0/configuration/rtg_brdg/guide/rtbrgdgd/ipv6.html

Teare ,D. & Paquet, P. 2007. Authorized Self-Study Guide: Building Scalable Cisco Internetworks (BSCI0), third edition. Cisco Systems.

Zhone Technologies. Viitattu 3.11.2015. ZMS Virtual Appliance. http://www.zhone.com/products/ZMS_VA/ZMS_VA.

Liitteet

Liite 1. DHCPv6-palvelimen loki asiakasreitittimen liityttyä verkkoon

```
Jan  7 10:04:03 localhost dhcpd: Internet Systems Consortium DHCP Server 4.3.3
Jan  7 10:04:03 localhost dhcpd: Copyright 2004-2015 Internet Systems Consortium.
Jan  7 10:04:03 localhost dhcpd: All rights reserved.
Jan  7 10:04:03 localhost dhcpd: For info, please visit https://www.isc.org/software/dhcp/
Jan  7 10:04:03 localhost dhcpd: Wrote 2 NA, 0 TA, 2 PD leases to lease file.
Jan  7 10:04:03 localhost dhcpd: Bound to *:547
Jan  7 10:04:03 localhost dhcpd: Listening on Socket/5/eth1/2a00:b9a0:    ::/48
Jan  7 10:04:03 localhost dhcpd: Sending on   Socket/5/eth1/2a00:b9a0:    ::/48
Jan  7 10:04:03 localhost dhcpd:
Jan  7 10:04:03 localhost dhcpd: No subnet6 declaration for eth0 (fe80::250:56ff:fe88:6de4).
Jan  7 10:04:03 localhost dhcpd: ** Ignoring requests on eth0.  If this is not what
Jan  7 10:04:03 localhost dhcpd:    you want, please write a subnet6 declaration
Jan  7 10:04:03 localhost dhcpd:    in your dhcpd.conf file for the network segment
Jan  7 10:04:03 localhost dhcpd:    to which interface eth0 is attached. **
Jan  7 10:04:03 localhost dhcpd:
Jan  7 10:04:03 localhost dhcpd:
Jan  7 10:04:03 localhost dhcpd: No subnet6 declaration for eth2 (fe80::250:56ff:fe88:47bd).
Jan  7 10:04:03 localhost dhcpd: ** Ignoring requests on eth2.  If this is not what
Jan  7 10:04:03 localhost dhcpd:    you want, please write a subnet6 declaration
Jan  7 10:04:03 localhost dhcpd:    in your dhcpd.conf file for the network segment
Jan  7 10:04:03 localhost dhcpd:    to which interface eth2 is attached. **
Jan  7 10:04:03 localhost dhcpd:
Jan  7 10:04:03 localhost dhcpd: Server starting service.
Jan  7 10:04:37 localhost dhcpd: Relay-forward message from 2a00:b9a0:302::1 port 547, link address 2a00:b9a0:801::1, peer address fe80::222:7ff:fe42:8f0
Jan  7 10:04:37 localhost dhcpd: Client 00:03:00:01:00:22:07:42:08:f0 releases address 2a00:b9a0:801:ffff:ffff:ffff:ffff:fff0, which is not leased to it.
Jan  7 10:04:37 localhost dhcpd: Client 00:03:00:01:00:22:07:42:08:f0 releases prefix 2a00:b9a0:801:ffff::/64, which is not leased to it.
Jan  7 10:04:37 localhost dhcpd: Sending Relay-reply to 2a00:b9a0:    ::1 port 547
Jan  7 10:04:37 localhost dhcpd: Relay-forward message from 2a00:b9a0:    ::1 port 547, link address 2a00:b9a0:801::1, peer address fe80::222:7ff:fe42:8f0
Jan  7 10:04:37 localhost dhcpd: Picking pool address 2a00:b9a0:801:ffff:ffff:ffff:ffff:fff0
Jan  7 10:04:37 localhost dhcpd: Advertise NA: address 2a00:b9a0:801:ffff:ffff:ffff:ffff:fff0 to client with duid 00:03:00:01:00:22:07:42:08:f0 iaid = 1 valid for 86400 seconds
Jan  7 10:04:37 localhost dhcpd: Picking pool prefix 2a00:b9a0:801:ffff::/64
Jan  7 10:04:37 localhost dhcpd: Advertise PD: address 2a00:b9a0:801:ffff::/64 to client with duid 00:03:00:01:00:22:07:42:08:f0 iaid = 1 valid for 86400 seconds
Jan  7 10:04:37 localhost dhcpd: Sending Relay-reply to 2a00:b9a0:    ::1 port 547
Jan  7 10:04:38 localhost dhcpd: Relay-forward message from 2a00:b9a0:    ::1 port 547, link address 2a00:b9a0:801::1, peer address fe80::222:7ff:fe42:8f0
Jan  7 10:04:38 localhost dhcpd: Reply NA: address 2a00:b9a0:801:ffff:ffff:ffff:ffff:fff0 to client with duid 00:03:00:01:00:22:07:42:08:f0 iaid = 1 valid for 86400 seconds
Jan  7 10:04:38 localhost dhcpd: ON COMMIT IA_NA: 2a00:b9a0:801:ffff:ffff:ffff:ffff:fff0 To: 0:22:7:42:8:f0 INT: Zhone MxK319 HE toimisto REMOTE-ID:
Jan  7 10:04:38 localhost dhcpd: ON COMMIT IA_PD: 2a00:b9a0:801:ffff:0:0:0:0/64 To: 0:22:7:42:8:f0 INT: Zhone MxK319 HE toimisto REMOTE-ID:
Jan  7 10:04:38 localhost dhcpd: Reply PD: address 2a00:b9a0:801:ffff::/64 to client with duid 00:03:00:01:00:22:07:42:08:f0 iaid = 1 valid for 86400 seconds
Jan  7 10:04:38 localhost dhcpd: ON COMMIT IA_NA: 2a00:b9a0:801:ffff:ffff:ffff:ffff:fff0 To: 0:22:7:42:8:f0 INT: Zhone MxK319 HE toimisto REMOTE-ID:
Jan  7 10:04:38 localhost dhcpd: ON COMMIT IA_PD: 2a00:b9a0:801:ffff:0:0:0:0/64 To: 0:22:7:42:8:f0 INT: Zhone MxK319 HE toimisto REMOTE-ID:
Jan  7 10:04:38 localhost dhcpd: Wrote 5 NA, 0 TA, 4 PD leases to lease file.
Jan  7 10:04:38 localhost dhcpd: Sending Relay-reply to 2a00:b9a0:    ::1 port 547
```

Liite 2. ”Bridge show vlan 801”-komennon tuloste Zhone DLSAM-laitteessa

```
zSH> bridge show vlan 801
         Orig
Type     VLAN/SLAN  VLAN/SLAN      Physical                Bridge                          St  Table Data
-------------------------------------------------------------------------------------------------------------------------
dwn                 Tagged  801    1/1/1/63/gpononu        LabraVlan801/bridge             UP  S 00:22:07:42:08:f0 (Secure, TimeLeft: 86273 secs)
                                                                                                S 5.61.89.126 (Secure, TimeLeft: 5572 secs)
                                                                                                S fe80::222:7ff:fe42:8f0 (Secure, TimeLeft: 86273 secs)
                                                                                                S 2a00:b9a0:801:ffff:ffff:ffff:ffff:fff0 (Secure, TimeLeft: 86273 secs)
                                                                                                S 2a00:b9a0:801:ffff::/64 (Secure, TimeLeft: 86273 secs)
upl                 Tagged  801    1/a/1/0/linkagg         C4510LACPRunko-801/bridge       UP  S VLAN 801 default
2 Bridge Interfaces displayed
```