KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikka / Tietoverkkotekniikka

Kaisu Ahonen ja Niko Ingraeus

DHCPV6 OPERAATTORIKÄYTÖSSÄ

Opinnäytetyö 2012

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikka

AHONEN, KAISU &
INGRAEUS, NIKO

	DHCPv6 operaattorikäytössä
Opinnäytetyö	35 sivua + 3 liitesivua
Työn ohjaaja	Yliopettaja Martti Kettunen
Toimeksiantaja	KYMP OY
Huhtikuu 2012	
Avainsanat	IPv6, ICMPv6, DHCPv6, General Prefix, operaattoriverkko

Tämä opinnäytetyö on tehty KYMP OY:n toimeksiantona ja siinä on hyödynnetty Kymenlaakson ammattikorkeakoulun SimuNet-hankkeen testiverkkoa ja ICT-laboratorion opetuskäyttöön tarkoitettuja laitteita.

Työn keskeisenä tavoitteena oli tutkia DHCPv4- ja DHCPv6-verkkoprotokollien välisiä eroja sekä tutustua siihen, miten DHCPv6-ominaisuuksia hyödynnetään operaattorikäytössä. Lisäksi työssä perehdyttiin IPv4- ja IPv6-protokollien välisiin eroihin. Huomioon otettiin myös ICMPv6-virheviestit sekä Neighbor Discovery -protokolla.

Käytännön osuudessa SimuNetissä sijaitsevaan operaattorireitittimeen konfiguroitiin DHCPv6-palvelin, jonka tarkoituksena oli jakaa verkkotunnukset DHCPv6-asiakasreitittimelle. IPv6-tilaajan asiakasreitittimen tehtävänä oli jakaa reitittimeen kytketyille loppukäyttäjille verkkotunnus ja sen pohjalta IPv6-osoitteet ja muut verkon asetukset, kuten nimipalvelimen IP-osoite. Toteutus tapahtui käyttämällä hyväksi DHCPv6-protokollan uutta verkkotunnusten jakoa eli Prefix Delegation – toimintoa.

Työn tuloksena saatiin aikaiseksi toimiva kytkentä, jossa verkkotunnukset kulkevat SimuNetissä sijaitsevalta DHCPv6-palvelimelta ICT-laboratoriossa sijaitsevalle työasemalle. Työn käytännön osuudessa suurena apuna toimivat Kymenlaakson ammattikorkeakoulun tietoverkkotekniikan erikoistumisopintojen opiskelijat, jotka avustivat merkittävästi käytännön osuuden toteutuksessa.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Information Technology

AHONEN, KAISU &
INGRAEUS, NIKO

Bachelor's Thesis	ISP using DHCPv6
Supervisor	35 pages + 3 pages of appendices
Commissioned by	Martti Kettunen, Principal Lecturer
April 2012	KYMP OY
Keywords	IPv6, ICMPv6, DHCPv6, General prefix, Provider Network

This thesis work was commissioned by KYMP OY and it utilized the ICT-laboratory environment and the test network of the SimuNet project, which is a co-project of Kymenlaakso University of Applied Sciences.

The main objective was to go through the differences between DHCPv4 and DHCPv6 network protocols and explore how to use DHCPv6 in an ISP network. Another goal was to investigate the differences between IPv4 and IPv6 protocols. ICMPv6 error messages and Neighbor Discovery protocol was also taken into account.

In the practical part of this thesis work, a DHCPv6 server was configured to the ISP router in the SimuNet network. The purpose of the server was to assign network prefixes to the DHCPv6 client router. The job of the IPv6 client router was to hand out the IPv6 addresses and other settings like a DNS address based on the network prefix. This was done by using DHCPv6 protocol's new function, which is called Prefix Delegation.

As a result of this work, a functional connection was achieved where the prefixes travel from the DHCPv6 server, which is located in SimuNet to the end-user, which is stationed in the ICT laboratory. A great amount of assistance was received from the students of Information Technology specialization studies of Kymenlaakso University of Applied Sciences, who helped substantially in the practical part of this thesis work.

SISÄLLYS

LYHENNELUETTELO

AAAA	Authentication, Authorization, Accounting and Auditing; *DNS -palvelimen resurssitietue.*
ARP	Address Resolution Protocol; *Osoitteenselvitysprotokolla.*
DAD	Duplicate Address Detection; *Päällekkäisten IP-osoitteiden tunnistus.*
DHCP	Dynamic Host Configuration Protocol; *Verkkoon kytkeytyville laitteille osoitetietoja jakava protokolla.*
DHCPv6	Dynamic Host Configuration Protocol version 6; *Protokolla, jolla määritellään laitteiden verkkoasetuksia.*
DNS	Domain Name System; *Nimipalvelujärjestelmä, joka muuntaa verkkotunnukset IP-osoitteiksi.*
DSLAM	Digital Subscriber Line Access Multiplexer; *Laite, joka erottelee puheliikenteen dataliikenteestä tilaajaliitännässä.*
ICMPv6	Internet Control Message Protocol version 6; *Virhetilanteista raportoimiseen käytettävä protokolla.*
IETF	The Internet Engineering Task Force; *Internet-protokollien standardoinnista vastaava organisaatio.*
IPng	Internet Protocol next generation; *IPv6:n nimitys varhaisessa kehitysvaiheessa.*
IPv4	Internet Protocol version 4; *Internet-protokollan versio 4.*
IPv6	Internet Protocol version 6; *Internet-protokollan versio 6.*

ISP	Internet Service Provider; *Internet-palveluntarjoaja.*
MAC-osoite	Media Access Control; *Ethernet-verkon laitteita yksilöivä Layer 2-tason osoite.*
MTU	Maximum Transmission Unit; *Suurin käytettävissä oleva siirtoyksikkö.*
NA	Neighbor Advertisement; *Naapurin mainostus.*
NAT	Network Address Translation; *Verkon osoitteenmuunnos.*
NDP	Neighbor Discovery Protocol; *Verkkosolmujen ylläpitoa varten käytettävä protokolla.*
Node	*IPv6-verkon solmupiste.*
NS	Neighbor Solicitation; *Naapuruuskysely.*
NUD	Neighbor Unreachability Detection; *Tavoittamattomien jäsenten tunnistus.*
PE	Provider Edge; *Palveluntarjoajan reunareititin.*
RA	Router Advertisement; *Reititinmainostus.*
RS	Router Solicitation; *Reititinkysely.*
VDSL	Very high rate Digital Subscriber Line; *Tekniikka, joka mahdollistaa laajakaistaisen symmetrisen tiedonsiirtoyhteyden toteuttamisen loppukäyttäjälle.*
VMware	*Ohjelma, jonka avulla voidaan simuloida virtuaalitietokonetta.*

1 JOHDANTO

IPv4-osoitteiden vähäinen määrä on aiheuttanut sen, että IP-osoitteet eivät enää riitä kaikille. Tämän vuoksi on pitänyt kehittää uusi Internet-protokolla, IPv6. IETF aloitti uuden protokollan kehittämisen jo 1990-luvulla ja IPv6-osoitteet ovat olleet yleisessä käytössä jo vuodesta 1998, jolloin kyseinen protokolla standardoitiin. Myös IPv6-protokollaperheen muut protokollat ovat muuttuneet ja kehittyneet, koska IPv6-yhteyskäytäntö ei ole yhteensopiva IPv4-yhteyskäytännön kanssa. Tässä työssä paneudutaan erityisesti DHCP:n kehittyneemmän version, DHCPv6:n, toimintaan ja eroihin aiempaan verrattuna sekä sen toimintaan operaattoriverkossa.

DHCPv6 on kehitetty juuri IPv6-osoitteiden vuoksi, koska ennen käytössä ollut DHCPv4 ei pysty käsittelemään IPv6-paketteja. Uusi DHCP versio tuo mukanaan uusia ominaisuuksia ja päivitettyjä versioita vanhoista ominaisuuksista.

Tämä opinnäytetyö on tehty Kotkassa toimivalle ICT-palveluyritys KYMP OY:lle. KYMP on valtakunnalliseen Finnet-ryhmään kuuluva yritys, joka tarjoaa kattavia tietoliikenne- ja telekommunikaatioratkaisuja asiakkailleen Kymenlaaksossa ja Etelä-Karjalassa. KYMP työllistää noin 200 henkilöä.

Työ on osa Kymenlaakson ammattikorkeakoulun SimuNet-hanketta, joka on operaattoriverkko pienoiskoossa. Se sijaitsee Kymenlaakson ammattikorkeakoulun ICTLAB-opetusympäristössä ja on tarkoitettu testaus-, tutkimus- ja tuotekehitysympäristöksi. SimuNet-verkon avulla voidaan mallintaa niitä haastavia tilanteita, joita tietoverkko-operaattoreilla ja Internet-palveluntarjoajilla on tietoverkon uusien ratkaisujen toteuttamisessa. (Kettunen 2009, 11.)

Tämä opinnäytetyö keskittyy käsittelemään DHCPv6:n toimintaa operaattorikäytössä. Työssä käsitellään teoriassa IPv6- ja IPv4-protokollien välisiä eroja sekä DHCPv6:n ja DHCPv4:n eroja. Käytännön kokeilujen avulla on havainnollistettu uusien protokollien toimintaa käytännössä.

Osa työssä käytetyistä laitteista on SimuNet-laboratoriosta ja osa koulun Tietoverkkotekniikan laboratoriosta. Käytetyistä laitteista yksi oli Nokia Siemensin ja loput Cisco Systemsin, joten työssä esiintyvä konfiguraatiosanasto on lähestulkoon Cisco System-

sin termistöä. Tietoverkkotekniikan erikoistumisopintojen opiskelijat avustivat merkittävästi käytännön osuuden toteutuksessa.

2 INTERNET-PROTOKOLLA VERSIO 6

Internet-protokolla versio 6 (IPv6) on poistumassa olevan IPv4:n seuraajaksi kehitetty protokolla. IPv6:n kehitys alkoi jo 1990-luvun alussa, kun huomattiin, että tarvittaisiin uusi Internet protokolla. Alkuvaiheessa sitä kutsuttiin nimellä IPng (Internet Protocol next generation). Kehittämisen aloitti IETF (Internet Engineering Task Force), joka oli kehittänyt myös aiemman, IPv4:n. IPv6 standardoitiin vuonna 1998 ja on ollut siitä lähtien käytettävissä. (Hogg & Vyncke 2009, 3.)

IPv6 tarjoaa useita merkittäviä muutoksia IPv4:n verrattuna. Merkittävimmät muutokset ovat osoitteiden pituus ja osoiteavaruuden laajuus. Osoitteiden pituus kasvoi vanhasta 32 bitistä 128 bittiin, joka tarkoittaa sitä, että kaiken kaikkiaan verkossa voi olla 2^{128} osoitetta. (Hogg & Vyncke 2009, 4.)

IPv6:ssa on pyritty siihen, että pakettien välittäminen päätelaitteelta toiselle olisi mahdollisimman yksinkertaista. Kasvaneen osoiteavaruuden myötä on tullut uusia verkko-ominaisuuksia. Ylimääräisistä verkon osoitteenmuunnoksista (NAT) on luovuttu, koska jokaiselle verkon solmupisteelle (node) on oma osoite ja sitä voidaan käyttää sisäiseen ja ulkoiseen kommunikointiin. (Hogg & Vyncke 2009, 5.) Muita uusia ominaisuuksia on IP-osoitteiden tilaton autokonfiguraatio (stateless autoconfiguration) sekä multihoming-ominaisuus. Tilaton autokonfiguraatio mahdollistaa IP-osoitteen ja muiden asetusten automaattisen konfiguroinnin niin, että asiakkaan täytyy vain kytkeä laite kiinni verkkoon. Multihoming-ominaisuus sallii laitteille monta eri IPv6-osoitetta. Näin saadaan parannettua laitteiden yhteyksien luotettavuutta. (RFC 2185)

2.1 IPv6-osoitteen muodostuminen

IPv6-osoitteet muodostuvat kahdeksasta 16 bitin kentästä. Jokaisessa kentässä on kaksi tavua, eli kokonaisessa osoitteessa on 16 tavua. Kentät erotetaan toisistaan kaksoispisteellä, kun taas IPv4:ssa kentät erotetaan toisistaan pisteellä. Kentät esitetään neljän merkin mittaisella heksadesimaaliluvulla, ja jos osoitteessa on useampi nolla peräkkäin, voidaan ne lyhentää kahdella kaksoispisteellä, mutta vain kerran yhdessä osoit-

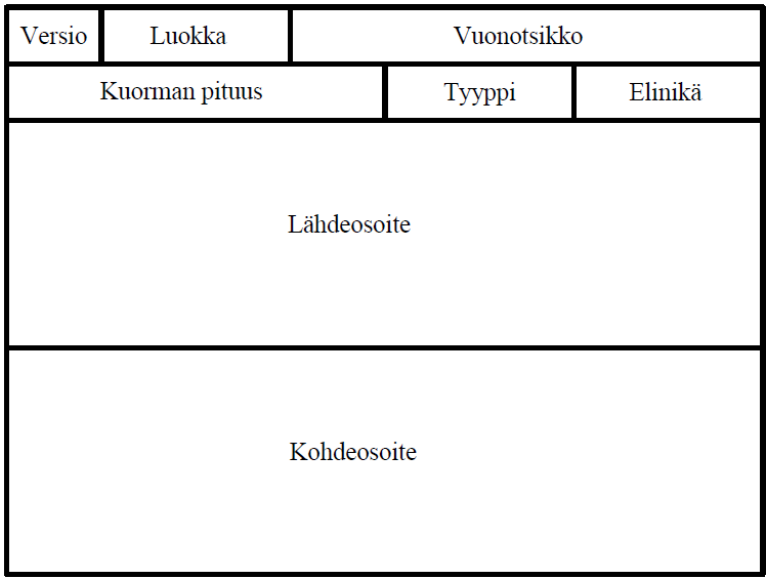
teessa. Esimerkiksi IPv6-osoite *2001:0DB8:0000:0000:0000:0000:1420:57AB* voidaan täten lyhentää muotoon *2001:DB8::1420:57AB.* (RFC 2185)

IPv6-osoitteet voidaan jakaa unicast-, multicast- ja anycast-osoitteisiin. Unicast-osoitteita ovat julkisesti käytettävät osoitteet ja linkkikohtaiset link-local-osoitteet, joita ei voi reitittää mihinkään, eli ne voivat olla samoja eri verkoissa. Link-local-osoitteissa käytettävä prefiksi eli verkkotunnus on *FE80::/10*. IPv6:n multicast-osoitteet korvaavat IPv4:n broadcast-osoitteet, ja niillä liikennöidään tietyn multicast-ryhmän jäseniin samanaikaisesti. Näiden verkkotunnus eli prefiksi on *FF00::/8*. Anycast-osoite lähetetään lähimmälle anycast-vastaanottajalle, joka vastaa reititysprotokollan mukaista liityntäporttia. (RFC 2185)

2.2 Otsikkokentät ja paketin rakenne

IPv6-osoitteiden otsikot (kuva 1) koostuvat kahdeksasta kentästä ja niiden koko on 40 tavua eli 320 bittiä, näistä 8 tavua käytetään yleisille attribuuteille ja loput 32 tavua on jaettu lähde- ja kohdeosoitetta varten. Vertauksena IPv4:ssa otsikkokenttiä oli 14, mutta osoitteiden otsikoiden koko oli vain 20 tavua eli 160 bittiä. (IPv6, juniper.net) Vaikka IPv6-otsikon kenttien määrä on pienempi kuin IPv4-otsikossa, on IPv6-otsikko suurempi kuin version 4 otsikko. IPv6-pakettien prosessointi ei hidastu suuren otsikkokoon takia, vaan nopeutuu, koska IPv6 otsikkokenttä pudottaa pois joitakin IPv4-otsikkokenttiä, kuten otsakkeen pituus, tunniste, liput, pirstaleen aloituskohta ja otsakkeen tarkistesumma, tai siirtää ne otsikon lisäkenttiin. Näin otsikosta tulee helpommin käsiteltävä ja samalla lähettämisen tehokkuus paranee. Tavoitteena on, että otsikoita käsiteltäisiin enemmän raudalla kuin ohjelmallisesti. Näin parannetaan laitteiden suorituskykyä. (Hogg & Vyncke 2009, 133.)

Aiemmin reitittimet pilkkoivat IP-paketteja, mutta versiossa 6 pirstalointi tapahtuu päätelaitteissa, joiden tehtävä on selvittää polussa käytettävissä oleva suurin mahdollinen paketin koko (MTU). Tämä sisältää mahdolliset kehykset, joten ne vievät osan käytettävissä olevasta tilasta. Päätelaite sijoittaa pirstaloinnissa käytettävät kentät (tunnisteet, liput ja pirstaleen aloituskohta) IPv6:n otsikon lisäkenttiin. Linkin MTU:n koon ylittävät paketit pudotetaan ja lähettäjälle lähetetään ICMPv6-virheviesti. Linkin pienin mahdollinen MTU on 1280 tavua. Tämä määritellään standardissa. (Hagen 2006, 18.)



Kuva 1. IPv6-otsikkokenttä (Rinne 1998, 11)

IPv6-otsikkokenttiä on kahdeksan erilaista tyyppiä:

Versio: Kenttä on 4-bittinen versionumero, joka on IPv6:ssa 6 ja IPv4:ssa 4.

Liikenneluokka: Kenttä, joka on kahdeksan bittiä pitkä. IPv4:ssa vastaava on ToS-kenttä. Kenttä antaa paketille liikenneluokka-merkinnän, jota käytetään Differentiated Services – palveluissa.

Vuonotsikko: 20 bitin kokoinen kenttä, joka sallii vain tietynlaisen liikenteen, johon lisätään labelit eli liput. Kenttää käytetään esimerkiksi multilayer-kytkimissä pakettien siirtoon ja siirron nopeuttamiseen.

Kuormanpituus: Kenttä määrittää otsikoidun paketin kuorman pituuden tavuina. Pituus lasketaan otsikkokentän jälkeisestä osasta.

Tyyppi: Kenttä joka kertoo, mikä otsikko tulee seuraavana IPv6-paketin otsikon jälkeen. Otsikko voi olla kuljetuskerroksen paketti tai jokin lisäotsikko.

Elinikä: Määrittää, kuinka monta hyppyä IPv6-paketti voi maksimissaan edetä. Jokainen hyppy vähentää paketin hop limit -arvoa yhdellä. Paketti hylätään, jos arvo saavuttaa nollan. IPv4:ssa tätä kenttää vastaa Time To Live -kenttä.

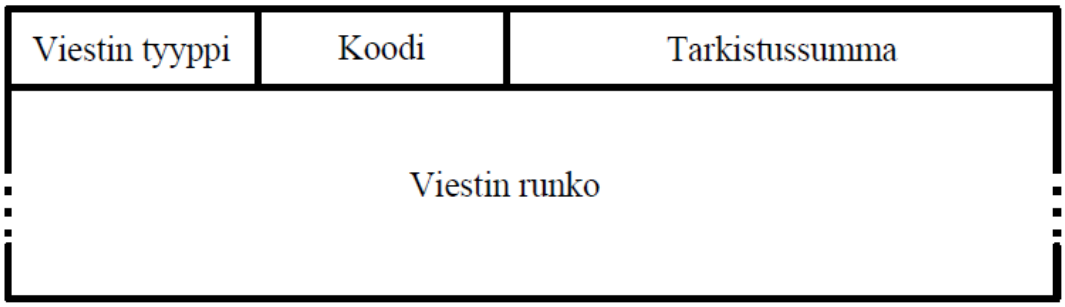
Lähdeosoite: 128 bittiä pitkä kenttä kertoo, mistä paketti on lähtöisin.

Kohdeosoite: Myös 128 bittiä pitkä ja kertoo, minne paketti on menossa.

(Rinne 1998, 11.)

2.3 ICMPv6-yhteyskäytäntö

Internet Control Message Protocol version 6:sta (ICMPv6) käytetään virhetilanteista raportoimiseen, IP-kerroksella tapahtuvien diagnoosien tekemiseen ja suorittamaan Neighbor Discovery -toimintaa. ICMPv6 viestit (kuva 2) kuljetetaan IPv6-pakettien sisällä ja viestin tunnistaa siitä, kun IPv6:n tyyppi-kentän arvo on 58. (Gai 1998, 84.) Kaikkien IPv6-solmujen täytyy tukea ICMPv6-protokollaa. (Rinne 1998, 34.)



Kuva 2. ICMPv6-viestin yleinen rakenne (Rinne 1998, 34)

Protokollassa käytetään kahta viestityyppiä 8-bittisen viestin tyyppi - kentän avulla. Jos kentän eniten merkitsevän bitin arvo on nolla (arvot väliltä 0-127), on kyseessä virheilmoitus. Jos arvo on yksi (arvot väliltä 128–255), on kyseessä informaatioviesti. Koodi-kenttä on 8-bittinen ja sen sisältö riippuu viestin tyypistä. Sillä kerrotaan tarkemmin viestin sisältö. Tarkistussumma-kenttä on 16-bittinen, ja sitä käytetään mahdollisen korruptoituneen datan havaitsemiseen. Viestin runko sisältää eri viesteille kuuluvan datan. (Gai 1998, 84.)

2.4 Neighbor Discovery -protokolla

Neighbor Discovery eli ND-protokolla vastaa IPv4:n ARP-osoitteenselvitysprotokollaa ja osittain se korvaa myös aiemman DHCPv4-protokollan toimintoja. ND yhdistää reitittimen etsinnän ja uudelleenohjauksen sekä verkon jäsenien osoitteiden selvittämisen ICMPv6:ssa. Päivitetty menetelmä tarjoaa myös Neighbor Unreachability Detectionin (NUD) eli tavoittamattomien jäsenten tunnistuksen sekä päällekkäisten IP-osoitteiden tunnistamisen eli Duplicate IP address Detectionin

(DAD). ND-protokollaa tarvitaan, kun konfiguroidaan automaattisesti verkkoliitännän osoite, määritettäessä prefiksejä ja reittejä, DAD-menetelmässä, etsittäessä vaihtoehtoisia reitittimiä sekä selvitettäessä naapurien tavoitettavuutta. ND toimii ICMPv6:n informatiivisten- ja virheviestien avulla. (Hagen 2006, 73–74.)

2.5 Naapurikyselyt ja -mainostukset

Neighbor Solicitation (NS) eli naapurikysely- ja Neighbor Advertisement (NA) eli naapurimainostusviestien tarkoitus on toimia ARP-protokollan tavoin ja yhdistää IPv6-osoite laitteen linkkikerroksen MAC-osoitteeseen. Lisäksi näiden viestien avulla selvitetään naapurin saatavuutta. Vertailuna ARP:ssa kohteen MAC-osoitetta ei välttämättä saada selville, joten naapuri todetaan kuolleeksi ja liikennöinti siihen estyy. (Hagen 2006, 79.)

Verkossa oleva laite lähettää NS-viestin, kun sen tarvitsee ratkaista IPv6-osoite linkkikerroksen osoitteeksi ja varmistaakseen, onko sen naapuri olemassa ja tavoitettavissa. NA-viestillä voidaan varmistaa päätelaitteen tai reitittimen olemassaolo ja sen avulla voidaan myös tarjota Layer 2-tason osoitetietoa tarvittaessa. (Hagen 2006, 79.)

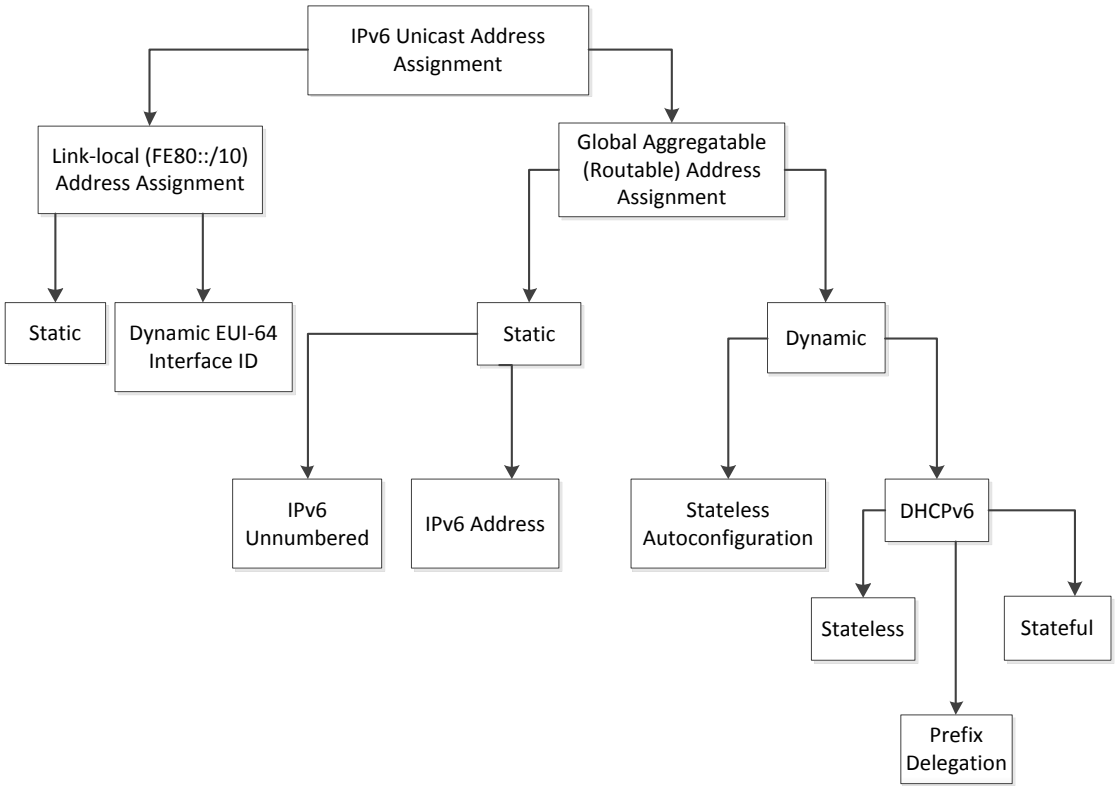
2.6 Nimipalvelujärjestelmä

Domain Name System on Internetin nimipalvelujärjestelmä, jonka tärkein tehtävä on muuntaa verkkotunnuksia IP-osoitteiksi. Nimipalvelun toteuttavia palvelintyyppejä on kahdenlaisia: resolverit eli koneet, jotka hakevat vastauksia nimipalvelukyselyihin ja autoritääriset nimipalvelimet, joiden tehtävänä on antaa nimipalvelukyselyihin vastauksia. (RFC 1101)

IPv6-osoitteiden käyttöönotto on aiheuttanut muutoksia myös DNS-palvelimeen. Kolme huomattavinta muutosta ovat uusi resurssitietue AAAA, uusi käänteisresolverihierarkia ja muutokset kyselytyyppeihin ja resoluutio proseduuriin. Tavallinen DNS-osoiteresurssitietue on määritelty 32-bittiselle IPv4-osoitteelle, joten luotiin uusi joka toimii 128-bittisten IPv6-osoitteiden kanssa. (DNS, The TCP/IP Guide)

3 IPV6 UNICAST -OSOITTEIDEN JAKAMINEN

Tässä osuudessa käsitellään, kuinka unicast-osoitteita voidaan jakaa verkossa oleville päätelaitteille. Päätelaitteet voivat saada unicast-osoitteen joko staattisesti tai dynaamisesti. IPv6 tuo mukanaan useita menetelmiä unicast-osoitteiden jakamiseen. Tärkeimmät näistä menetelmistä ovat tilallinen DHCP, tilaton autokonfiguraatio ja staattinen konfiguraatio. Kuva 3 havainnollistaa IPv6 unicast -osoitteiden jakoa.



Kuva 3. IPv6 unicast -osoitteiden jakamistavat (Teare 2010, 716)

3.1 Linkkikohtaiset unicast-osoitteet

Linkkikohtaista (link-local) osoitetta on suunniteltu käytettävän yksittäisen linkin sisäiseen osoitteistukseen eri tilanteissa, kuten automaattisessa osoitteen konfiguroinnissa, naapurin määrittelemisessä ja tilanteessa, joissa ei ole reititintä mukana. Reitittimet eivät lähetä eteenpäin muille linkeille paketteja, joissa lähettäjänä tai vastaanottajana on linkkikohtainen osoite. Linkkikohtaisissa osoitteissa käytettävä verkkotunnus eli prefiksi on FE80::/10. (Teare 2010, 707.)

Ensimmäisenä, kun laite kytketään verkkoon, se selvittää itselleen linkkikohtaisen osoitteen, joka muodostuu yleisesti tiedossa olevasta linkkikohtaisen osoitteen etuliitteestä sekä yksikäsitteisestä laitteen tunnuksesta muodostetusta EUI-64-tunnuksesta.

Tuo tunnus muodostetaan yleensä linkkikerroksen Ethernet-osoitteesta, joka on 48-bittinen, lisäämällä siihen kaksi oktettia osoitteen keskelle. Tätä menetelmää kutsutaan dynaamiseksi osoitteenmuodostumiseksi. Toisaalta osoite voidaan myös luoda manuaalisesti eli staattisesti. (Teare 2010, 707.)

3.2 Julkiset unicast-osoitteet

Globaalien eli julkisten unicast-osoitteiden periaate on se, että ne ovat skaalautuvia ja mahdollistavat täten hierarkkisen reitityksen. Ideana on se, että TLA (Top-Level Aggregation) muodostuu ylimmän tason keskuksista, jotka tarjoavat Internetin yleisiä siirtopalveluja, ja ne saavat omat TLA ID-tunnuksensa kansainvälisiltä osoitteiden jakamisesta vastaavilta rekisteröintielimiltä. Ylimmän tason keskukset tarjoavat siirtopalveluja pienemmille palvelujen tarjoajille, jotka muodostavat NLA (Next-Level Aggregation) joukon. TLA-keskukset siis jakavat osoitteet omista osoitealueista alemman tason palvelujen tarjoajille. NLA-keskuksissa olevat palvelujen tarjoajat voivat olla joko tavallisia tai pitkien siirtopalvelujen tarjoajia. Jos NLA:ssa olevat palvelun tarjoajat ovat tavallisia, jakavat ne vuorostaan osoitteet tilaajilleen osoitealueestaan. SLA (Site-Level Aggregation) eli aluetason tunnus identifioi yhden alueen sisältämät linkit. Saman keskuksen ja palvelujen tarjoajien tilaajilta löytyy sama osoitteen alkuosa, joka taas helpottaa ja nopeuttaa pakettien reititystä. (King 1998)

3.3 Stateless autoconfiguration

Uusi ominaisuus IPv6-protokollassa on tilaton autokonfiguraatio, missä solmupisteet konfiguroivat itsensä automaattisesti, kun ne liitetään verkkoon. (Blanchet 2008, 79.) Tilattoman autokonfiguraation avulla verkkolaitteelle luodaan uniikki osoite verkkolaitteen omaa MAC-osoitetta käyttäen ja reitittimeltä saatavaa tietoa. MAC-osoite muunnetaan käyttäen EUI-64-formaattia ja yhdistetään reitittimen tietoihin. Näin päätelaite saa täysin uniikin IPv6-osoitteen helposti. (Hagen 2006, 87.)

Tilattomassa autokonfiguraatiossa liityttyään verkkoon laite liittyy kaikkien solmujen multicast-ryhmään. Laite on ohjelmoitu vastaanottamaan kaikkien solmujen multicast-ryhmälle lähetettyjä paketteja. Tämän ryhmän IPv6-osoite on FF02::1. Tämän jälkeen laite lähettää Router Solicitation - eli reititinkyselyviestin. Viesti lähetetään multicast-osoitteelle FF02::2, joka käsittää kaikki reitittimet verkossa. IP-pakettien, jonka sisällä viesti kulkee, laitetaan lähdeosoitteeksi oma linkkikohtainen osoite. Saadessaan tämän kyselyviestin, reitittimet vastaavat siihen Router Advertisement – eli reititinmainos-

tusviestillä. Kyseinen viesti lähetetään kyselyssä mukana tulleeseen linkkikerroksen osoitteeseen. (Teare 2010, 725.)

Oppiakseen kaikki tarvittavat tiedot, tilaton autokonfiguraatio käyttää hyödykseen Neighbor Discovery -protokollan RA- ja RS-viestejä, joiden avulla se oppii verkkotunnuksen ja sen pituuden sekä oletusreitittimen. Seuraavaksi se johtaa itselleen IPv6-osoitteen isäntäosan käyttäen EUI-64-formaattia. Lopuksi tilaton autokonfiguraatio käyttää tilatonta DHCP:tä (Stateless DHCP) oppiakseen DNS-palvelimen IPv6-osoitteen. Reititinmainostus-viesteissä on kaksi konfiguroitavaa lippua, jotka liittyvät osoitteiden autokonfigurointiin. Nämä liput ovat Managed Address Configuration Flag eli M-lippu ja Other Stateful Configuration Flag eli O-lippu. (Teare 2010, 725.)

4 DHCP-VERKKOPROTOKOLLA

Dynamic Host Configuration Protocol on verkkoprotokolla, jonka avulla voidaan määrittää automaattisesti laitteiden verkkoasetuksia. Näitä asetuksia ovat muun muassa IP-osoite, lähiverkon peite ja nimipalvelimen IP-osoite. DHCP toimii verkko-osoitteiden hallintapaikkana, eli jos verkon tiedoissa tapahtuu muutos, tietoja ei tarvitse päivittää jokaiselle päätelaitteelle erikseen. Riittää, että muutokset päivitetään DHCP-palvelimelle. (RFC 2131)

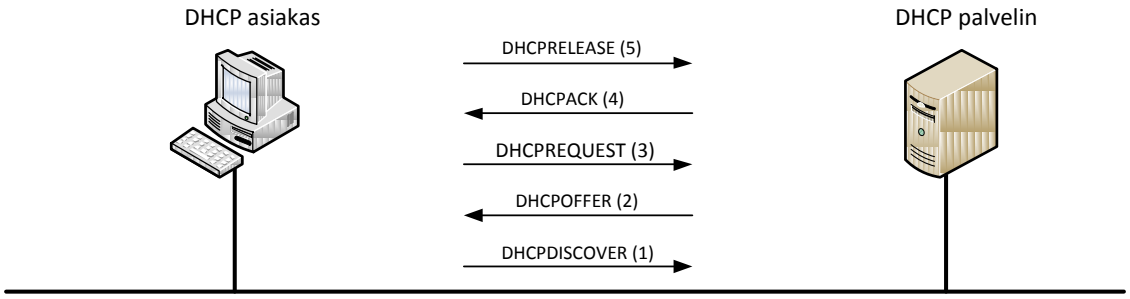
DHCP perustuu asiakas-palvelinarkkitehtuuriin. Normaalisti DHCP toimii omassa aliverkossaan, jossa DHCP-asiakas (client) lähettää broadcast-viestin omaan fyysiseen aliverkkoonsa. Lisäksi voidaan käyttää myös DHCP-välityspalvelinta (relay), jonka avulla voidaan laajentaa toimintaa aliverkon ulkopuolelle. Välityspalvelin määritetään reitittävän laitteen konfiguraatioon ja sen toiminnosta voidaan käyttää myös nimitystä DHCP-helper tai IP-helper-address. DHCP-helper nimitystä käytetään silloin, kun on kyse toiminnosta joka nimenomaan käsittelee DHCP-pyynnöt eteenpäin. IP-helper käsitettä käytetään silloin, kun DHCP-relay on yksi useista käsitellyistä toiminnoista. (RFC 2131)

DHCP:llä on kolme tapaa jakaa IP-osoitteita: automaattinen, dynaaminen ja manuaalinen. Automaattisessa tavassa palvelin antaa käyttäjälle pysyvän osoitteen. Dynaamisella tavalla käyttäjä taas saa lainaksi osoitteen ennalta määritellyksi ajaksi. Manuaali-

sesti jaettu osoite on verkon ylläpitäjän määrittelemä ja se jaetaan DHCP:tä hyväksi käyttäen. (RFC 2131)

4.1 DHCP-viestit

DHCP:n ja DHCPv6:n viestit eroavat toisistaan lähinnä vain kirjoitusasultaan ja prosessin pituudessa (kuva 5). DHCPv6:ssa kirjoitusasu on aiempaa lyhyempi ja edestakaisin lähetettävien kyselyiden määrä on pienempi. DHCP:ssä asiakasohjelma etsii aluksi palvelinta *DHCPDISCOVER*-viestillä ja palvelin tarjoaa asiakkaalle osoitetta viestillä *DHCPOFFER*. Tämän jälkeen asiakas pyytää käyttöönsä osoitetta *DHCPREQUEST*-viestillä, palvelin hyväksyy sen *DHCPACK*-viestillä. Asiakas luopuu halutessaan osoitteesta *DHCPRELEASE*-viestillä. Tällöin palvelin vapauttaa osoitteen, minkä jälkeen palvelin voi jakaa kyseisen osoitteen jollekin muulle asiakkaalle. (RFC 2131) Kuva 4 havainnollistaa DHCP-viestin liikennettä asiakkaan ja palvelimen välillä.



Kuva 7. Uuden osoitteen kysyminen ja siitä luopuminen (RFC 2131)

DHCPv6:n asiakas-palvelinkonsepti on hyvin samanlainen kuin DHCPv4:ssä. Jos asiakas haluaa saada verkkoasetukset, se lähettää pyynnön lähiverkossa olevalle DHCPv6-palvelimelle viestillä *SOLICIT*, palvelin vastaa pyyntöön *ADVERTISE*-viestillä. Seuraavaksi asiakas lähettää *REQUEST*-viestin pyytääkseen itselleen osoitetta. Tämän palvelin hyväksyy *REPLY*-viestillä.

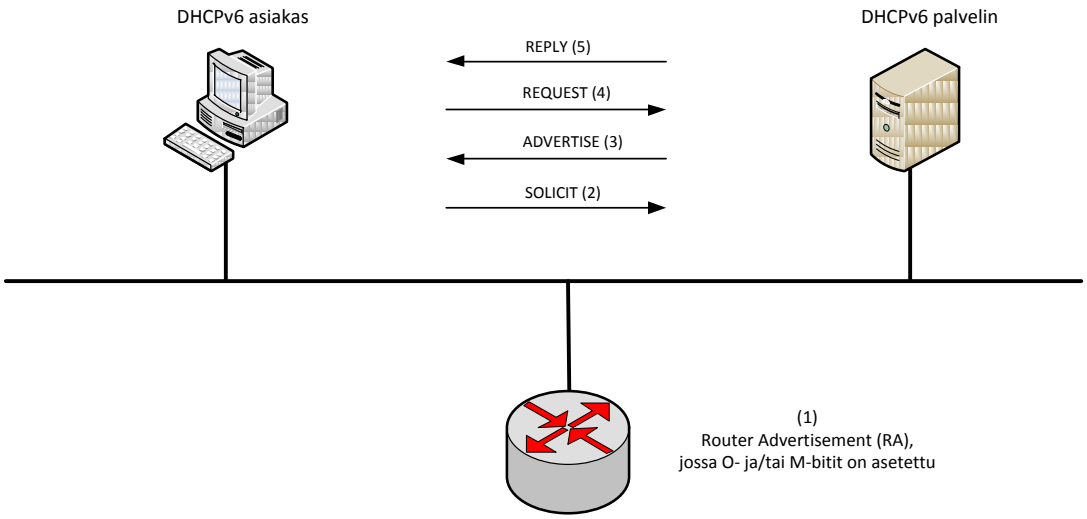
DHCPv6 Message Type	DHCPv4 Message Type
SOLICIT (1)	DHCPDISCOVER
ADVERTISE (2)	DHCPOFFER
REQUEST (3), RENEW (5), REBIND (6)	DHCPREQUEST
REPLY (7)	DHCPACK/DHCPNAK
RELEASE (8)	DHCPRELEASE
INFORMATION-REQUEST (11)	DHCPINFORM
DECLINE (9)	DHCPDECLINE
CONFIRM (4)	none
RECONFIGURE (10)	DHCPFORCERENEW
RELAY-FORW (12), RELAY-REPLY (13)	none

Kuva 5. DHCPv6:n ja DHCPv4:n viestikenttien vertailu (RFC 3315)

DHCPv6 on tuonut tullessaan kolme uutta viestityyppiä, joille ei ole vastaavuutta aiemmassa nelosversiossa. Uudet viestit ovat *CONFIRM*, *RELAY-FORW* ja *RELAY-REPLY*. Confirm-viestillä asiakas varmistaa palvelimelta, että sille annetut osoitteet ovat vielä yhteensopivia asiakkaan käyttämälle linkille. Relay-forw-viestin välityspalvelin lähettää palvelimelle, joko suoraan tai toisen välityspalvelimen kautta. Relay-reply-viestin palvelin lähettää välityspalvelimelle. Viesti sisältää sanoman, jonka välityspalvelin toimittaa asiakkaalle. (RFC 3315)

4.2 DHCPv6:n toimintaperiaate

DHCPv6:n asiakas-palvelinkonsepti on hyvin samanlainen kuin IPv4:n DHCP. Jos asiakaskone haluaa saada itselleen konfiguraatioparametrejä, lähettää se pyynnön omaan lähiverkkoonsa etsien näin DHCPv6-palvelimia. Tämä tehdään viesteillä *Solicit* ja *Advertise*. Tunnettuja Multicast-osoitteita käytetään DHCP-palvelimien etsimiseen. Nämä Multicast-osoitteet ovat *FE02::1:2* ja *FE05::1:3*. Seuraavaksi DHCPv6-asiakas pyytää itselleen parametrejä *Request*-viestin avulla, johon saatavilla oleva palvelin vastaa pyydetyillä tiedoilla *Reply*-viestillä. Alla oleva kuva 6 havainnollistaa kyseistä tapahtumaa. (RFC 3315)



Kuva 6. DHCPv6 pyynnöt ja vastaukset (RFC 3315)

4.3 M- ja O-liput

Jos M- ja O-liput ovat molemmat asetettu arvoon 0, on kyseessä tilaton autokonfiguraatio (stateless autoconfiguration). Tällöin verkkotunnus eli prefiksi ja oletusreititin haetaan reitittimeltä RS- ja RA-viestien avulla. Muut asetukset saadaan jotenkin muuten, esimerkiksi käsin kirjoittamalla. Jos molemmat liput ovat asetettu arvoon 1, on kyseessä tilallinen DHCPv6 (DHCPv6 stateful). Tällöin käyttäjät käyttävät DHCPv6:sta saadakseen osoitteet ja muut asetukset. Oletusreititin haetaan reitittimeltä samoilla viesteillä kuin edellisessä, mutta kaikki muut tiedot saadaan DHCPv6-palvelimelta, jonka tulee olla asennettu stateful-tilaan. Tällöin palvelin pitää kirjaa osoitelainoista. Jos O-lippu on arvossa 1 ja M-lippu on arvossa 0, on kyseessä taas tilaton DHCPv6 (DHCPv6 stateless), jolloin käyttäjät saavat DHCPv6:n avulla itselleen vain muut asetukset. Läheiset reitittimet on konfiguroitu mainostamaan globaaleiden osoitteiden prefiksejä josta päätelaite johtaa itselleen tilattoman osoitteen. DHCPv6-palvelin toimii tässä tapauksessa stateless-tilassa, jolloin se ei pidä kirjaa jakamistaan tiedoista. Jos M-lippu on arvossa 1 ja O-lippu on arvossa 0, tällöin käyttäjät saavat vain osoitteen DHCPv6-palvelimelta. Muut asetukset saadaan jotenkin muuten. Tämä on kuitenkin hyvin epätodennäköinen tila. (Microsoft, techdays.fi)

4.4 IPv6-osoitteiden takaisinvetäminen

Jo jaetut IPv6-osoitteet on mahdollista vetää takaisin hyödyntämällä IPv6-osoitteiden elinaikamäärityksiä. Esimerkiksi konfiguroitaessa verkon yhdyskäytäväreititintä voi IPv6-osoitteita kirjoittaessa voi epähuomiossa kirjoittaa yhdyskäytävän osoitteen väärin. Tällöin ei pelkkä osoitteen korjaus riitä, sillä sen hetken aikana, kun virheellinen osoite käy liityntäportissa, verkossa olevat päätelaitteet ovat jo ehtineet oppia väärän osoitteen. IPv6-maailmassa laitteen yhdellä liityntäportilla voi olla useita IPv6-osoitteita. Jos väärinkirjoitettua osoitetta ei poisteta päätelaitteelta, ovat väärät osoitteet voimassa oman elinaikansa (oletuksena 7 vuorokautta) päätelaitteessa ja ne saattavat sekoittaa verkon toiminnan. (Kettunen 2012)

5 IPV6 VERKKOTUNNUKSET ELI PREFIKSIT

IPv6-prefiksit eli verkkotunnukset ilmaisevat reittejä, osoiteavaruutta tai osoitealueita. IPv6-osoitteiden prefiksit esitetään muodossa: IPv6-osoite / prefiksin pituus. Prefiksin pituus on desimaaliarvo, joka määrittää, kuinka moni vierekkäisistä biteistä määrittää prefiksin. Esimerkiksi jos operaattorin prefiksi on 2001:DB8*::/32*, niin silloin suuremman organisaation prefiksi voisi olla *2001:DB8:100::/48*. Pienemmän organisaation prefiksi olisi *2001:DB8:100:4000::/56* ja aliverkon prefiksi *2001:DB8:100:4001::/64*. (Microsoft, techdays.fi)

5.1 General prefix -tunnukset

IPv6:n myötä useat Internet-palveluntarjoajat ovat ajatelleet tapaa, jolla voitaisiin tehokkaasti jakaa prefiksejä asiakkaille. IPv6 tarjoaa tähän tehokkaan menetelmän, josta käytetään nimeä Prefix Delegation. Prefix Delegation -menetelmän avulla asiakkaiden reunareitittimille voidaan automaattisesti lähettää verkkotunnuksia eli prefiksejä, josta asiakasreitittimet sitten jakavat IPv6-osoitteita päätelaitteille.

Jotta osoitteiden jakamisprosessi olisi kivuttomampaa, on ainakin testissä olleissa Cisco Systemsin laitteissa tapa jolla prefiksiin voidaan viitata myös nimellä. Tätä tapaa kutsutaan nimellä General Prefix. Prefiksi *2001:db8:42::/48* voidaan korvata nimellä ja siihen voidaan viitata liityntäporttia konfiguroidessa. Alla oleva esimerkki selventää tapahtumaa.

Ensiksi määritellään General Prefix:

Router(config)#ipv6 general-prefix OmanPrefiksinNimi 2001:db8:42::/48

Kun halutaan antaa liityntäportille IPv6-osoite, voidaan viitata äsken luotuun General Prefiksiin, jolloin ei tarvitse kirjoittaa koko osoitetta:

Router(config)#interface FastEthernet0/0
Router(config-if)#ipv6 address OmanPrefiksinNimi 0:0:0:10::1/64

Show ipv6 interface brief -käskyn avulla varmistetaan vielä, että liityntäportti on saanut itselleen IPv6-osoitteen.

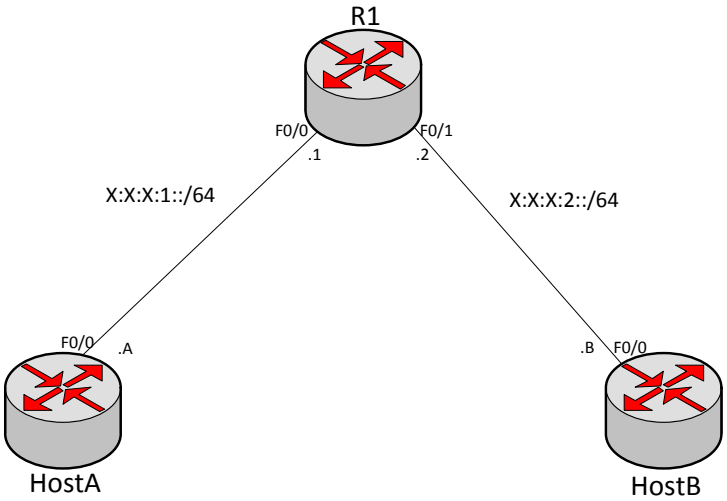
Router(config-if)#show ipv6 interface brief
FastEthernet0/0 [up/up]
2001:DB8:42:10::1

Kuten on huomattavissa, osoitteen alkuosa (*2001:db8:42::/48*) on saatu General Prefiksin avulla ja loppuosa osoitteesta (*10::1*) tulee liityntäporttiin äsken määritellyn komennon avulla.

5.2 General Prefix operaattoreiden käytössä

Internet-palveluntarjoajat (ISP) voivat käyttää General Prefix -toimintoa hyödykseen. Palveluntarjoajan reitittimeen kytketty asiakasreititin saa palveluntarjoajalta automaattisesti tiedon siitä mitä prefiksejä verkossa käytetään ja josta asiakasreititin sitten jakaa IPv6-osoitteita päätelaitteille. Tämän toiminnon avulla osoitteiden uudelleen numerointi helpoittuu huomattavasti; jos esimerkiksi palveluntarjoajan prefiksi muuttuu, voidaan se hetkessä ilmoittaa palveluntarjoajan reitittimeen kytketyille asiakasreitittimille.

Alla olevassa kuvassa 7 asiakasreititin R1 on saanut palveluntarjoajalta /48 prefiksin jota kutsutaan myös nimellä site prefix. Tähän prefiksiin reititin liittää oman 16-bittisen aliverkko ID:n. Näin saadaan aikaan /64 prefiksi josta IPv6-osoitteita voidaan alkaa jakamaan päätelaitteille HostA ja HostB, jotka ovat omassa aliverkossaan.



Kuva 7. General Prefix – esimerkkikytkentä (Cisconinja´s Blog)

Ensiksi konfiguroidaan link-local - osoitteet jokaiseen laitteeseen:

R1(config)#interface FastEthernet0/0
R1config-if)#ipv6 address FE80::1 link-local

R1config)#interface FastEthernet0/1
R1(config-if)#ipv6 address FE80::2 link-local

HostA(config)#interface FastEthernet0/0
HostA(config-if)#ipv6 address FE80::A link-local

HostB(config)#interface FastEthernet0/0
HostB(config-if)#ipv6 address FE80::B link-local

Oletetaan, että ISP on määrännyt prefiksin *2001:db8:aaaa::/48*. Seuraavaksi määritellään kyseisen prefiksi General Prefiksiksi komennolla:

R1(config)#ipv6 general-prefix ISP-prefix 2001:DB8:AAAA::/48

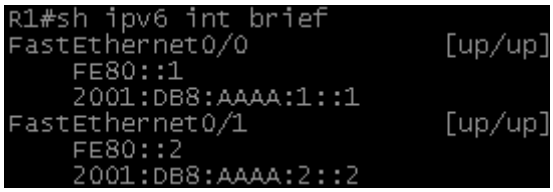
Seuraavaksi konfiguroidaan globaali unicast-osoite R1:een käyttämällä ISP:ltä saatua prefiksiä, joka juuri määriteltiin:

R1(config)#interface FastEthernet0/0
R1(config-if)#ipv6 address ISP-prefix ::1:0:0:0:1/64

Komennolla *debug ipv6 nd* havainnollistetaan kuinka R1 saa itselleen osoitteen General Prefiksin avulla.

R1#debug ipv6 nd
**Mar 1 00:59:51.019: ICMPv6-ND: Adding prefix 2001:DB8:AAAA:1::1/64 to FastEthernet0/0*

**Mar 1 00:59:51.019: ICMPv6-ND: Sending NS for 2001:DB8:AAAA:1::1 on FastEthernet0/0*
**Mar 1 00:59:52.019: ICMPv6-ND: DAD: 2001:DB8:AAAA:1::1 is unique.*
**Mar 1 00:59:52.019: ICMPv6-ND: Sending NA for 2001:DB8:AAAA:1::1 on FastEthernet0/0*
**Mar 1 00:59:52.023: ICMPv6-ND: Address 2001:DB8:AAAA:1::1/64 is up on FastEthernet0/0*



Kuva 8. R1-reitittimen *show ipv6 interface brief* – komento (Cisconinja´s Blog)

Oletuksena IPv6 prefiksejä mainostetaan RA-viesteissä Valid Lifetime arvolla 30 päivää ja Preferred Lifetime arvolla 7 päivää. Vaikka prefiksi poistetaan RA-viesteistä, käyttävät R1-asiakasreitittimeen kytketyt reitittimet silti osoitetta, jonka he ovat oppineet autokonfiguraation avulla, kunnes prefiksin elinaika loppuu. Muutetaan Valid Lifetime arvo 300 sekuntiin ja Preferred Lifetime arvo 200 sekuntiin. Vaihdetaan myös RA-viestien lähetysväli 200 sekuntista 60 sekuntiin.

R1(config)#interface FastEthernet0/0
R1(config-if)#ipv6 nd ra-interval 60
R1(config-if)#ipv6 nd prefix-default 300 200

R1(config)#interface FastEthernet0/1
R1(config-if)#ipv6 nd ra-interval 60
R1(config-if)#ipv6 nd prefix-default 300 200

Seuraavaksi käynnistetään IPv6 reititys ja RA-viestien lähetys R1-asiakasreitittimessä:

R1(config)ipv6 unicast-routing

Tämän jälkeen R1-reititin alkaa lähettää RA-viestejä eteenpäin.

R1#debug ipv6 nd
**Mar 1 01:24:42.007: ICMPv6-ND: Sending RA to FF02::1 on FastEthernet0/0*
**Mar 1 01:24:42.007: ICMPv6-ND: MTU = 1500*
**Mar 1 01:24:42.007: ICMPv6-ND: prefix = 2001:DB8:AAAA:1::/64 onlink autoconfig*
**Mar 1 01:24:42.011: ICMPv6-ND: 300/200 (valid/preferred)*
**Mar 1 01:24:42.011: ICMPv6-ND: Sending RA to FF02::1 on FastEthernet0/1*

**Mar 1 01:24:42.011: ICMPv6-ND: MTU = 1500*

**Mar 1 01:24:42.011: ICMPv6-ND: prefix = 2001:DB8:AAAA:2::/64 onlink autoconfig*

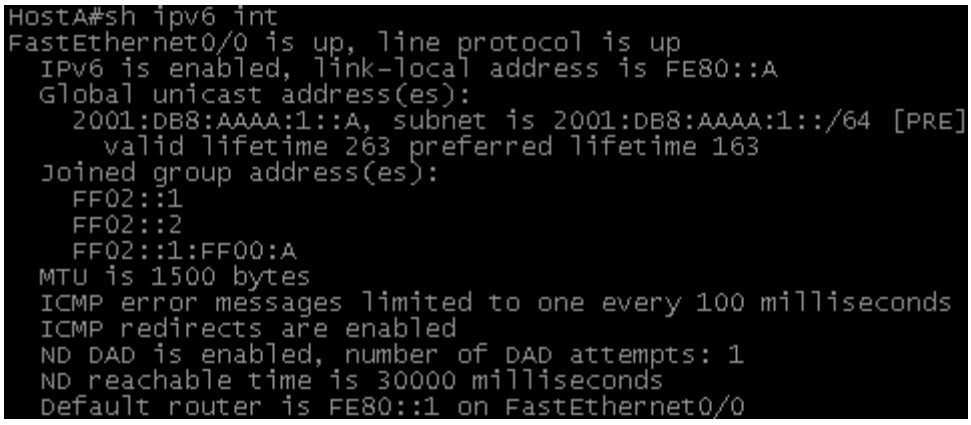
**Mar 1 01:24:42.015: ICMPv6-ND: 300/200 (valid/preferred)*

Seuraavaksi konfiguroidaan HostA ja HostB käyttämään tilatonta autokonfiguraatiota:

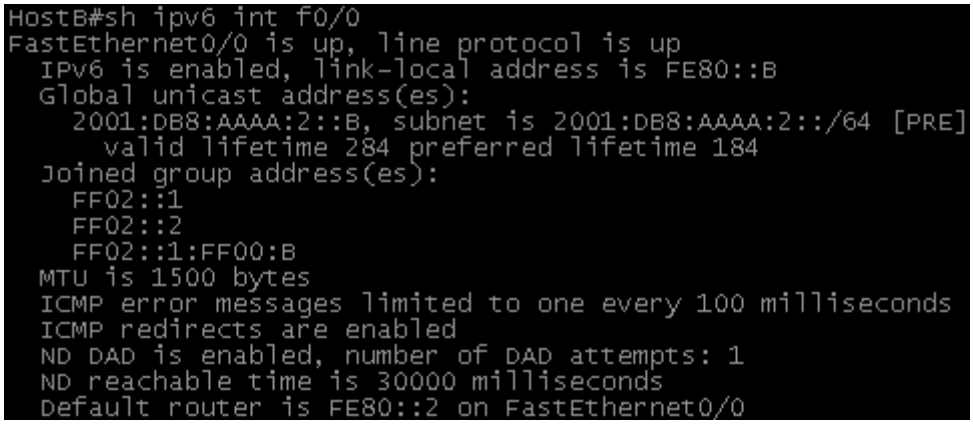
HostA(config)#interface FastEthernet0/0
HostA(config-if)#ipv6 address autoconfig

HostB(config)#interface FastEthernet0/0
HostB(config-if)#ipv6 address autoconfig

Tämän jälkeen HostA ja HostB saavat itselleen määrätyt osoitteet ja oppivat samalla prefiksin elinajan.



Kuva 9. HostA-reitittimen *show ipv6 interface* – komento (Cisconinja´s Blog)



Kuva 10. HostB-reitittimen komento *show ipv6 interface f0/0* (Cisconinja´s Blog)

Oletetaan, että palveluntarjoajamme prefiksi muuttuu ja uusi prefiksi on *2001:db8:bbbb::/48.* Lisätään uusi prefiksi General Prefiksiksi komennolla:

R1(config)#ipv6 general-prefix ISP-prefix 2001:DB8:BBBB::/48

R1-reititin oppii uuden prefiksin ja konfiguroi sen pohjalta itselleen uuden osoitteen. R1-reititin alkaa mainostamaan molempia prefiksejä RA-viesteissä.

Kuva 11. R1-reitittimen s*h ipv6 int brief-komento* (Cisconinja's Blog)

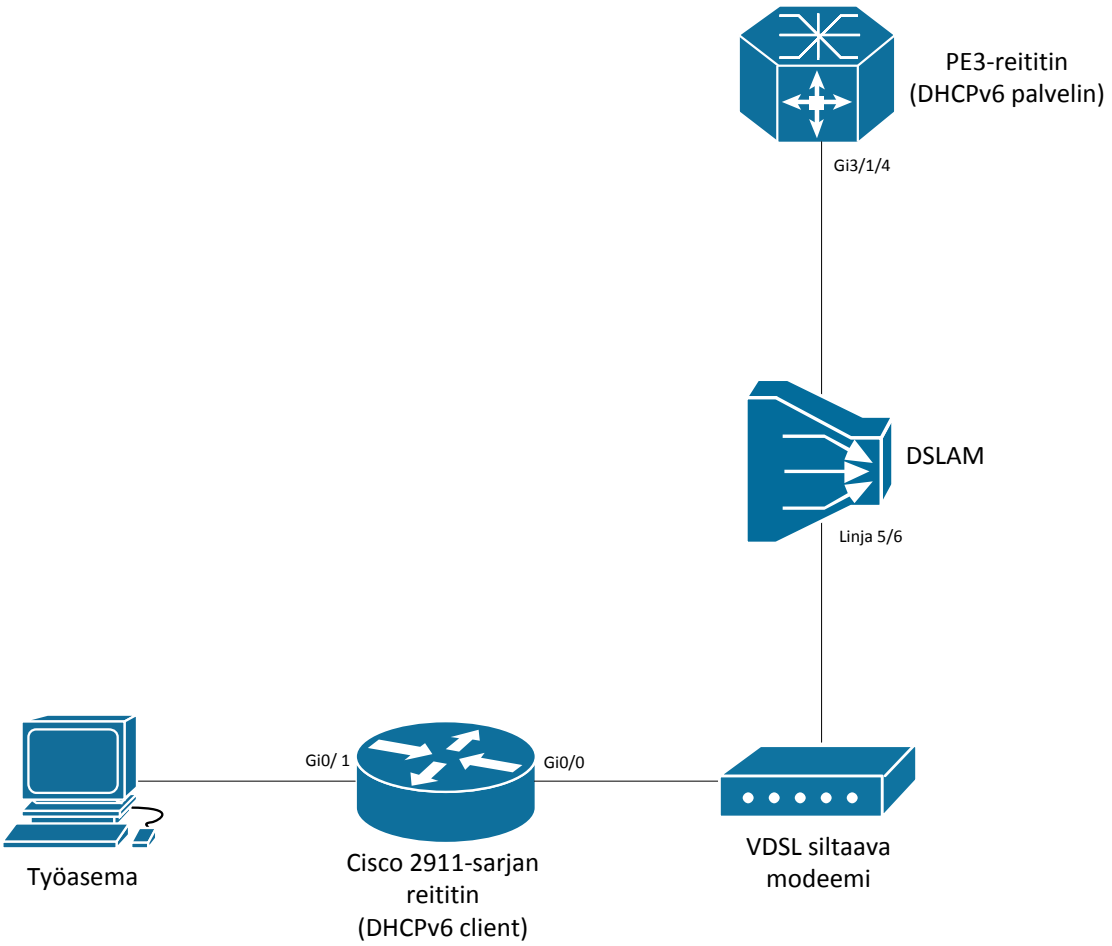
RA-viestin kuultuaan kumpikin päätelaite konfiguroi itselleen osoitteen perustuen uuteen prefiksiin. Tämän jälkeen kummallakin päätelaitteella on kaksi eri osoitetta. Seuraavaksi poistetaan vanha prefiksi R1-reitittimestä:

R1(config)#no ipv6 general-prefix ISP-prefix 2001:DB8:AAAA::/48

R1 poistaa osoitteen ja lakkaa sen mainostamisen RA-viesteissä. 200 sekunnin jälkeen prefiksin suositellun elinajan laskuri menee nollaan, jolloin osoite merkitään vanhentuneeksi (deprecated). Tämä tarkoittaa sitä, että osoitetta ei voida käyttää enää uusien yhteyksien lähdeosoitteena. 300 sekunnin kuluttua osoitteen kelvollinen elinaika päättyy, jolloin osoite poistuu käytöstä.

6 TYÖN TOTEUTUS

Työssä tarkoituksena oli rakentaa testitilanne, jossa on mukana operaattori ja kuviteltu IPv6-asiakas. Tarkoituksena oli saada DHCPv6-palvelin jakamaan prefiksi-tiedon, domain-nimen ja DNS-palvelimen IPv6-osoitten. DHCPv6-palvelin sijaitsi SimuNetin PE3-reitittimen portissa GigabitEthernet3/1/4.2000 ja DHCPv6-asiakas laitteena toimi ICT-laboratorion reititin Cisco 2911 (kuva 12). Työ koostui kahdesta erillisestä osasta: DHCPv6-palvelimesta ja -asiakkaasta sekä DSLAM:sta ja VDSL-sillasta. DSLAM:nä käytettiin SimuNetissä sijaitsevaa Nokia Siemens Hix5625 ja VDSL-siltana toimi ZyXelP870HN.



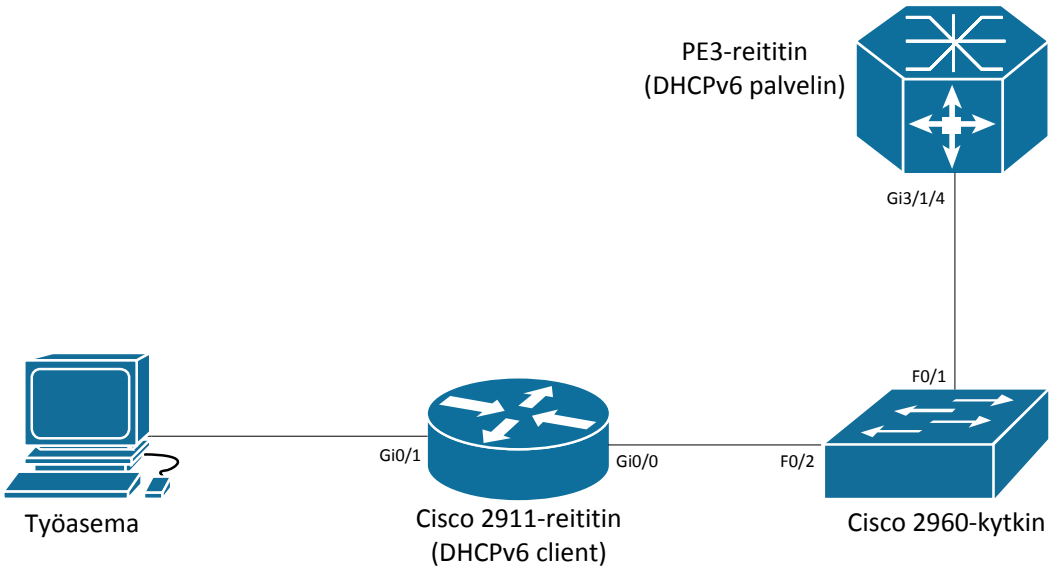
Kuva 12. Työssä käytetty kytkentä

6.1 Pohjustusta työhön

Ennen varsinaisen kytkennän aloittamista tutustuttiin IPv6:n toimintaan ICT-laboratorion verkkolevyllä olevan harjoitustyön avulla. Ensin tehtiin kytkentä IPv4-osoitteiden avulla ja vaihdettiin ne sitten IPv6-osoitteiksi, jotta tulisi selkeästi näkyviin 4- ja 6-versioiden välinen ero. Seuraavaksi kytkentään alettiin vähitellen lisätä DHCPv6-konfiguraatiota. Nämä pienet harjoitukset tehtiin useampaan otteeseen alusta loppuun, että varmasti olisi peruskonfiguraatio hallussa. Näiden jälkeen löytyi cisco.com-sivuilta (DHCPv6 Example, cisco.com) DHCPv6-harjoitus, jonka avulla saatiin tuntumaa siihen, miten DHCPv6-palvelimen ja -asiakkaan konfiguraatiot eroavat toisistaan. Myös tämä tehtiin useamman kerran, jotta olisi varmuus osaamisesta varsinaista työtä ajatellen.

6.2 Alustava kytkentä

Kun kaikki edeltävät harjoitukset oli saatu kunnolla menemään läpi, niin että useammalla kerralla kaikki toimii, siirryttiin hahmottelemaan varsinaista työtä. Ensimmäinen versio ei sisältänyt DSLAM:iä ja VDSL-siltaa, vaan ne korvattiin Cisco 2960-kytkimellä (kuva 13).



Kuva 13. Alustava kytkentä

Kytkimestä tarvittiin kaksi porttia: FastEthernet0/1 ja FastEthernet0/2. Portti 0/1 oli kytkettynä PE3-reitittimen porttiin GigabitEthernet3/1/4, portti 0/2 oli kytkettynä DHCPv6-asiakkaana toimivaan Cisco 2911-reitittimeen. PE3-laitteelle päin oleva portti konfiguroitiin trunk-portiksi ja toinen portti access-portiksi.

Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport mode trunk

Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport mode access

Cisco 2911-reititin konfiguroitiin DHCPv6-asiakkaaksi. Portti GigabitEthernet0/0 vastaanotti tietoa DHCPv6-palvelimelta ja portti GigabitEthernet0/1 välitti tiedot työasemalle. Ensin otettiin käyttöön reitittimen staattiset ja dynaamiset reititysominaisuudet komennolla:

Router(config)#ipv6 unicast-routing

Tämän jälkeen konfiguroitiin portit Gi0/0 ja Gi0/1 ja määritettiin ne käyttämään IPv6:sta. Lisäksi Gi0/0-portti määriteltiin käyttämään tilatonta autokonfiguraatiota komennolla *ipv6 address autoconfig default*, jolloin portti sai itselleen julkisen IPv6-osoitteen ja link-local – osoitteen ilman käsin luotuja määrityksiä:

Router(config)#interface GigabitEthernet0/0
Router(config-if)#description runko
Router(config-if)#ipv6 address autoconfig default
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 dhcp client pd ISP

ipv6 dhcp client pd ISP komennolla annetaan DHCP-asiakasreitittimelle prefix delegation – toiminnan avulla General Prefix nimeltä ISP.

Router(config)#interface GigabitEthernet0/1
Router(config-if)#description client
Router(config-if)#ipv6 address ISP ::1/64
Router(config-if)#ipv6 nd other-config-flag
Router(config-if)#ipv6 dhcp relay destination 2A00:1DD0:100:4100::1

ipv6 address isp ::1/64 käskyllä kerrotaan liityntäportille GigabitEthernet0/1 sen julkinen IPv6-osoite, jonka alkuosa saadaan prefix delegationin avulla. Komennolla *ipv6 nd other config flag* asetetaan Other stateful configuration -lippu päälle RA-viestissä. Tämä kertoo sen, että DNS-palvelimen osoite ja domainin nimi haetaan DHCP:n avulla.

SimuNetissa sijaitseva PE3-reititin konfiguroitiin DHCPv6-palvelimeksi. Porttiin GigabitEthernet3/1/4 luotiin aliliityntäportti 2000, johon konfiguroitiin tarvittavat asetukset, jotta DHCPv6 toimii. Aluksi käynnistettiin reitittimeen IPv6-reititys komennolla:

Router(config)#ipv6 unicast-routing

Seuraava vaihe oli luoda local pool määrittämällä sille nimi ja IPv6-osoite. Local pool on IPv6-osoitteiden alue, josta DHCPv6:n prefix delegation – toiminnon avulla jaetaan asiakkaan reitittimiin verkkotunnukset eli prefiksit. Jaettavien verkkotunnusten verkkomaskin pituus on 64 bittiä ja koko osoitealueen verkkomaski on 56 bittiä.

Router(config)#ipv6 local pool VLAN2000ipv6 2001:DB8:100:4000::/56 64

Luotiin IPv6 DHCP pool, jolle määritettiin nimipalvelimen IPv6-osoitteet ja annettiin domainin nimeksi testidomain.net sekä kerrottiin, mistä local pool – osoitealueesta verkkotunnukset eli prefixit jaetaan asiakasreitittimille.

Router(config)#ipv6 dhcp pool vlan2000
Router(config-dhcpv6)#prefix-delegation pool VLAN2000ipv6
Router(config-dhcpv6)#dns-server 2001:DB8:1::32
Router(config-dhcpv6)#dns-server 2001:DB8:0:1::132
Router(config-dhcpv6)#domain-name testidomain.net

Lopuksi konfiguroitiin aliliityntäportti 2000 porttiin Gi3/1/4 ja siihen tarvittavat määritykset, kuten IPv4- ja IPv6-osoitteet. Käynnistettiin IPv6-protokolla ja määritettiin käytettävä DHCP-palvelin.

Router(config)#interface GigabitEthernet3/1/4.2000
Router(config-subif)#encapsulation dot1Q 2000
Router(config-subif)#ip address 10.10.10.1 255.255.255.0
Router(config-subif)#ipv6 address 2001:DB8:100:4100::1/64
Router(config-subif)#ipv6 enable
Router(config-subif)#ipv6 nd managed-config-flag
Router(config-subif)#ipv6 dhcp server vlan2000

Komennolla *ipv6 nd managed-config-flag* asetetaan Managed configuration – lippu päälle RA-viesteissä. Käskyllä *ipv6 dhcp server vlan 2000* käynnistetään IPv6:n DHCP-palvelu liityntäportissa ja kerrotaan, että IPv6-osoitteita jaetaan poolista valn2000.

6.3 Lopullinen kytkentä

Kun alustava kytkentä toimi juuri niin kuin pitikin, otettiin kytkin pois kytkennästä. Kytkimen tilalle laitettiin Nokia Siemensin Hix5625 DSLAM ja ZyXelin P870HN - VDSL-silta. DSLAM:iin piti konfiguroida muutamia muutoksia, jotta laite päästäisi PE3-reitittimeltä tulevat DHCPv6-paketit lävitseen. Ensin Bridgeport 5/6/1 piti saada käyttämään virtuaalilähiverkkoa (vlan) 2000. Tämän jälkeen luotiin vlan 2000.

KYAMK_DSLAM(bridge)#create vlan 2000

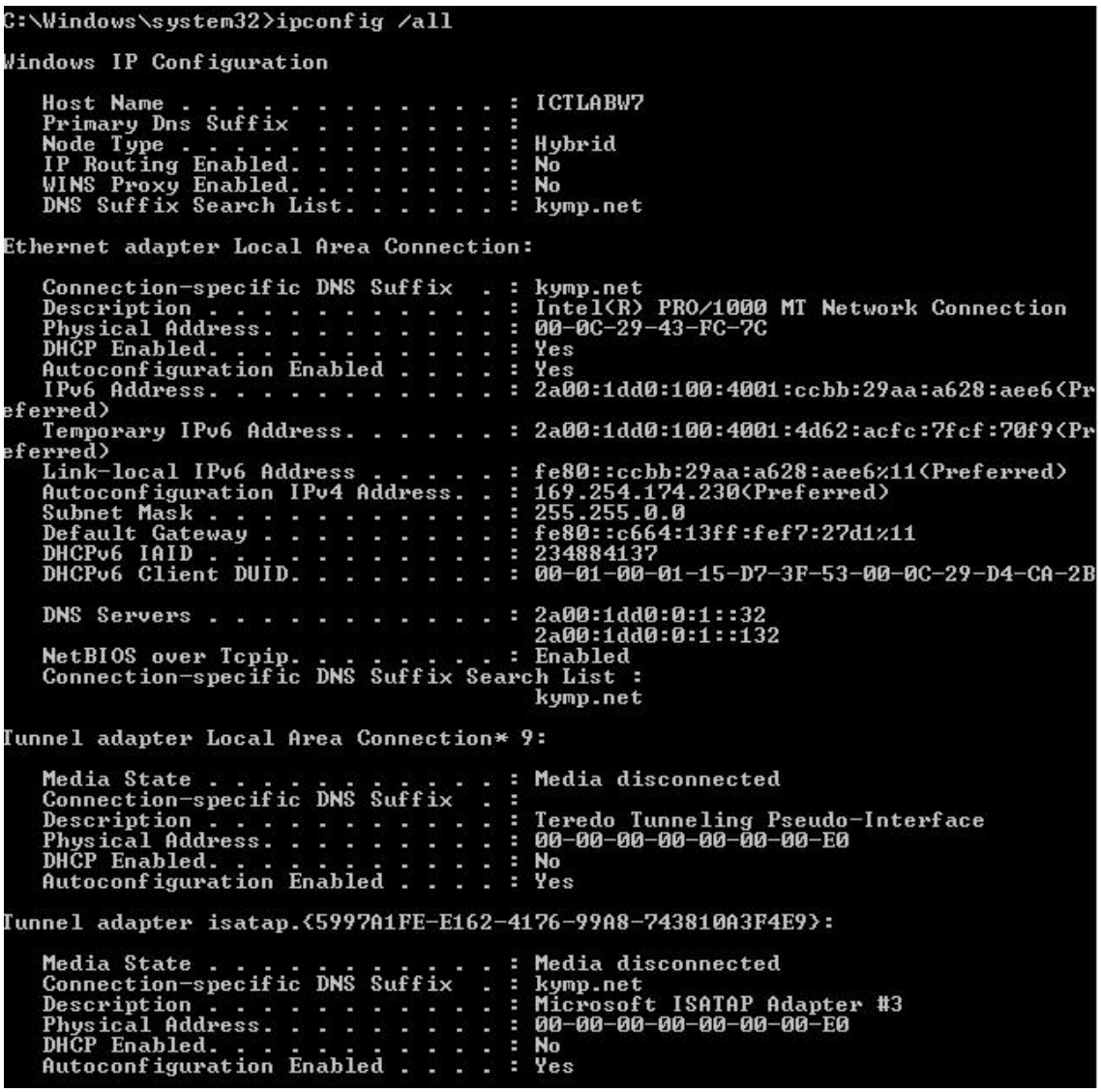
Tämän jälkeen lisättiin joukko määrityksiä, joilla saatiin DSLAM toimimaan halutulla tavalla. Komennolla *vlan add 2000 0/2 tagged 5/6/1 untagged* liitettiin portit 0/2 ja 5/6/1 vlaniin 2000 ja tehtiin portista 0/2 trunk-portti ja 5/6/1-portista linjaportti. Komennolla *vlan cross-connect 2000 on* sallitaan kaikkien multicast-, broadcast- ja unicast-kehyksien pääsy vlan 2000:n. Multicast-komennoilla laitetaan IP-reititys päälle. Lisäksi kytkettiin pois päältä arp-viestien edelleen lähetys ja konfiguroitiin portti 5/6/1 päästämään *untagged*-kehykset läpi ja pudottamaan *tagged*-kehykset.

KYAMK_DSLAM(bridge)#vlan add 2000 0/2 tagged 5/6/1 untagged
KYAMK_DSLAM(bridge)#vlan cross-connect 2000 on
KYAMK_DSLAM(bridge)#vlan multicast-flooding 2000 on
KYAMK_DSLAM(bridge)#vlan multicast-permission 2000 enable
KYAMK_DSLAM(bridge)#ip arp-reply vlan-forward 2000 disable
KYAMK_DSLAM(bridge)#bridgeport 5/6/1 taggingmode untagged

VDSL-sillalle ei tarvinnut tehdä mitään muutoksia. Tämän jälkeen laitettiin kaapelit paikalleen kuvan 10 osoittamalla tavalla.

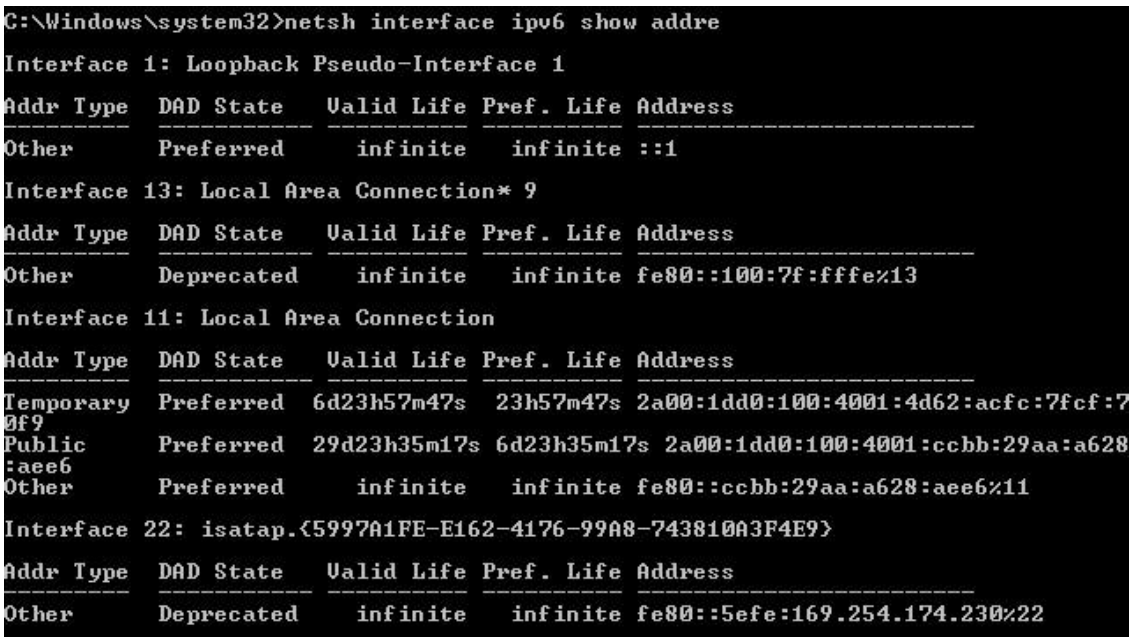
6.4 Kytkennän testaus

Kytkennän toiminta testattiin avaamalla työasemalle VMware-työasema Windows 7 – käyttöjärjestelmällä. Työasemalla avattiin komentorivi ja vapautettiin osoitteet komennolla *ipconfig /release6* ja haettiin osoitteet uudelleen komennolla *ipconfig /renew6.* Kuvassa 14 näkyy, kuinka työasema on saanut IPv6-osoitteen, DNS-palvelimen osoitteen sekä DNS-nimen testidomain.net.



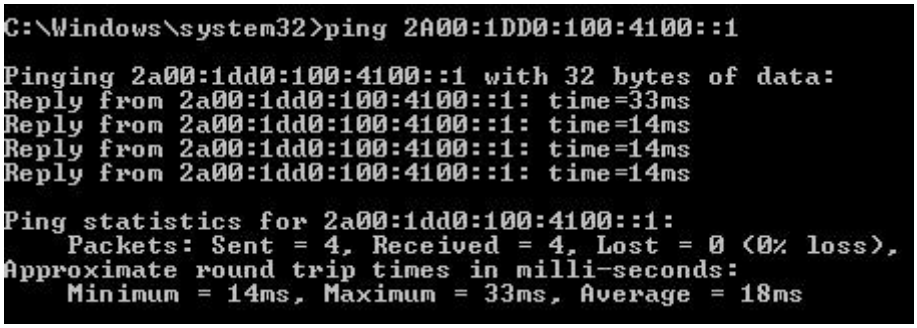
Kuva 14. Työaseman ipconfig

Seuraavaksi työaseman komentoriville syötettiin käsky *netsh interface ipv6 show addresses.* Kuvassa 15 näkyy, että osoitteen voimassaoloaika on lähtenyt pienenemään seitesemästä vuorokaudesta alaspäin, ja siitä voi päätellä, että osoitteet on juuri saatu, eli ne eivät ole aikaisemmin opittuja.



Kuva 15. Työaseman IPv6-osoitteiden voimassaoloajat

Lopuksi vielä testattiin yhteyden toimintaa PE3-reitittimelle saakka *ping*-komennon avulla. Ping-toiminnon kohdeosoite oli PE3-reitittimessä sijaitseva oletusyhdyskäytävän osoite. Ping-toiminnon tulokset näkyvät kuvassa 16 ja siitä voidaan päätellä, että työasemalta on pääsy PE3-reitittimelle.



Kuva 16. Ping PE3-reitittimelle

7 TULOKSET

Tämän opinnäytetyön tarkoituksena oli tarkastella DHCPv6:n toimintaa operaattorikäytössä. Ensimmäisenä aiheeseen tutustuttiin tekemällä harjoituksia aluksi IPv4-osoitteiden avulla ja sitten sama harjoitus IPv6-osoitteilla. Harjoitusten vaativuustasoa nostettiin jokaisen harjoituksen jälkeen. Näin saatiin hyvä perusta lopullisen työn suorittamiseen.

Teoriapuolella perehdyttiin DHCPv6:n lisäksi IPv6:n muutoksiin ja sen aiheuttamiin muutoksiin muihin protokolliin, kuten nimipalveluun. Työssä myös vertailtiin IPv4:n ja IPv6:n eroja. Todettiin, että IPv6:n käyttöönotto aiheuttaa suuriakin muutoksia joihinkin protokolliin. Muun muassa uuden ja vanhan DHCP:n ero on valtaisa. Kaikki DHCP-viestit ovat muuttuneet kirjoitusasultaan ja uusia ominaisuuksia on tullut lukuisa määrä lisää. Merkittävin uusi ominaisuus DHCPv6:ssa on M- ja O-lippujen mukaan tulo. Niiden avulla määritellään, onko osoitteiden konfigurointi tilallinen vai tilaton sekä onko määrittely automaattinen vai ei.

Työssä tuli eteen muutamia pieniä ongelmia. Suurin yksittäinen ongelma oli DSLAM:n konfigurointi. Laitteeseen oli jonkin aiemman projektin yhteydessä konfiguroitu muutama komento, jotka eivät olleet yhteensopivia DHCPv6:n kanssa. Kun ylimääräiset komennot poistettiin, alkoi kytkentä toimia niin kuin pitääkin. Ylimääräisten komentojen aiheuttamaa umpikujaa ei havaittu heti, vaan ensin epäiltiin, että vika on VDSL-sillassa ja se vaihdettiinkin useaan otteeseen.

Työn tuloksena oli toimiva, pienimuotoinen operaattoriverkko, joka käytti DHCPv6:sta. DHCPv6-palvelin jakoi osoitteet DSLAM:n kautta DHCPv6-asikasreitittimelle ja siitä eteenpäin asiakkaan päätelaitteelle.

Jatkokehityksenä työlle voisi tehdä samanlaisen kytkennän, mutta PE3-reititin, joka toimi DHCPv6-palvelimena, vaihdettaisiin Linux- tai Windows-palvelimeksi. Näin saataisiin jollain tapaa helpommin hallittava operaattoriverkko.

LÄHTEET

Blanchet, M. 2007. Migrating to IPv6. West Sussex, England: John Wiley & Sons, Ltd.

DHCP for IPv6. Cisco. Saatavissa: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6554/ps6600/ps6641/aag_C45-456070_v2.pdf. [Viitattu 23.2.2012]

DHCPv6 using the Prefix Delegation Feature Configuration Example. Cisco Systems. Saatavissa: http://www.cisco.com/image/gif/paws/113141/DHCPv6-00.pdf. [Viitattu 23.2.2012]

DNS. The TCP/IP Guide. Saatavissa: http://www.tcpipguide.com/free/t_DNSChangesToSupportIPVersion6.htm. [Viitattu 29.3.2012]

Gai, S. 1998. Internetworking IPv6 with Cisco Routers. Texas, USA: McGraw-Hill.

Hagen, S. 2006. IPv6 Essentials. Kalifornia, USA: O´Reilly Media.

Hogg, S. & Vyncke, E. 2009. IPv6 Security. Indianapolis, USA: Cisco Press.

IPv6 General Prefixes. Cisconinja´s Blog. Saatavissa: http://cisconinja.wordpress.com/2009/03/10/ipv6-general-prefixes/ [Viitattu 6.5.2012]

IPv6 Packet Headers. Juniper Networks. Saatavissa: http://www.juniper.net/techpubs/software/erx/erx50x/swconfig-routing-vol1/html/ipv6-config4.html. [Viitattu 15.3.2012]

Kettunen, M. 2012. IPv6 osoitteiden poisto. Saatavissa: http://www.ictlab.kyamk.fi/index.php?option=com_content&view=article&id=111:ipv6-osoitteiden-poisto&catid=34:tietoverkkotekniikka-yleinen&Itemid=96. [Viitattu 9.5.2012]

Kettunen, M. 2009. Tietoverkkotekniikan uudet haasteet SimuNet-hankkeen lähtökohtana. Saatavissa: http://papaya.ictlab.kyamk.fi/~amake/SimuNet/SimuNet%20artikkeliv6a.pdf. [Viitattu 2.5.2012]

King, S., Fax, R., Haskin, D., Ling, W., Meehan, T. & Fink, R. 1998. The Case for IPv6. Saatavissa: http://wiki.tools.ietf.org/group/iab/draft-ietf-iab-case-for-ipv6/draft-ietf-iab-case-for-ipv6-02-from-01.diff.html. [Viitattu 9.5.2012]

RFC 1101, DNS Encoding of Network Names and Other Types. IETF. Saatavissa: http://tools.ietf.org/html/rfc1101. [Viitattu 29.3.2012]

RFC 2131, Dynamic Host Configuration Protocol. IETF. Saatavissa: http://www.ietf.org/rfc/rfc2131.txt. [Viitattu 23.2.2012]

RFC 2185, Routing Aspects of IPv6 Transition. IETF. Saatavissa: http://tools.ietf.org/html/rfc2185. [Viitattu 23.2.2012]

RFC 2461, Neighbor Discovery for IP Version 6 (IPV6). IETF. Saatavissa: http://www.ietf.org/rfc/rfc2461.txt. [Viitattu 29.3.2012]

Rinne, J. 1998. IPv6 – uusi Internet-protokolla. Opinnäytetyö. Tampereen teknillinen korkeakoulu.

Teare, D. 2010. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide. Indianapolis, USA: Cisco Press.

Vuola, J. & Bergius, J. 2012. IPv6 statuspäivitys ITPron näkökulmasta. Microsoft tech-days Helsinki 2012 tapahtuman kalvosarja. Saatavissa: https://www.techdays.fi/Portals/0/LiiteTiedostot/34..pdf. [Viitattu 20.4.2012]

```
hostname PE3
!
ip dhcp pool VLAN2000
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
!
ipv6 unicast-routing
ipv6 dhcp pool vlan2000
 prefix-delegation pool
!
VLAN2000ipv6
 dns-server 2A00:1DD0:0:1::32
 dns-server 2A00:1DD0:0:1::132
 domain-name testidomain.net
!
vlan 2000
 name g4
!
interface GigabitEthernet3/1/4.2000
 encapsulation dot1Q 2000
 ip address 10.10.10.1 255.255.255.0
 ipv6 address 2A00:1DD0:100:4100::1/64
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 dhcp server vlan2000
!
ipv6 local pool VLAN2000ipv6 2A00:1DD0:100:4000::/56 64
!
end
```

```
hostname Router
!
ipv6 unicast-routing
!
ip domain list testidomain.net
!
interface GigabitEthernet0/0
 description runko
 no ip address
 duplex auto
 speed auto
 ipv6 address autoconfig default
 ipv6 enable
 ipv6 dhcp client pd ISP
!
interface GigabitEthernet0/1
 description client
 no ip address
 no ip route-cache cef
 duplex auto
 speed auto
 ipv6 address ISP ::1/64
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination 2A00:1DD0:100:4100::1
!
end
```

```
bridgeport 5/6/1,6/5/1 taggingmode untagged
!
bridgeport 5/3/1,5/4/1,5/5/1,5/6/1,5/7/1,5/8/1 pvid 403,404,405,2000,407,408
!
!  Vlan creation
vlan create 69,2000
! Management Vlans
!  Vlan assigned ports
vlan add 69 0/1,0/2,0/3,0/4 tagged
vlan add 2000 0/2 tagged 5/5/1,5/6/1,6/5/1 untagged
!  Vlan attributes
!   vlan agingtime
!   vlan names
!   vlan mcast permission
vlan multicast-permission 2000 enable
!   vlan service type
!   vlan cross mode
vlan cross-connect 2000 on
!   vlan ip routing
!   vlan multicast-flooding
vlan multicast-flooding 2000 on
!   vlan mac-address-translation
!   vlan xlation
!
ip arp-reply vlan-forward 2000 disable
ip dhcp mode snoop
ip pppoe mode snoop
ip dhcp option82 policy drop
!
ip dhcp provider DHCP2000
 index 1
 option82 all
 simplified on
 commit exit
!
end
```