

IPv6-verkot

Jarkko Kuosmanen

Opinnäytetyö

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma Tietotekniikan koulutusohjelma	
Työn tekijä(t) Jarkko Kuosmanen	
Työn nimi IPv6-verkot	
Päiväys 15.5.2013	Sivumäärä/Liitteet 32/0
Ohjaaja(t) laboratorioinsinööri Pekka Vedenpää	
Toimeksiantaja/Yhteistyökumppani(t) Savonia-ammattikorkeakoulu	
Tiivistelmä <p>Tämän opinnäytetyön aihe oli IPv6-verkot ja se tehtiin Savonia-ammattikorkeakoululle. Työn tavoitteena oli selvittää Savonian tietoverkon IPv6:n käyttöönoton valmiudet.</p> <p>IPv6-käyttöönotto alkaa olla ajankohtaista, koska IPv4-osoitteet ovat loppumassa Euroopassa. Yrityksillä joilla on olemassa tietoverkko, ei ole kiirettä aloittaa käyttöönottoa, mutta uuteen protokollaan olisi hyvä tutustua.</p> <p>Työhön etsittiin tietoa Ciscon sivuilta Savonian tietoverkossa käytettävien laitteiden IPv6-tuesta. Savonian verkossa käytettävien mallien dokumenteista etsittiin tukevatko ne IPv6-ominaisuuksia, kuten IPv6 käyttöoikeuden tarkistusluetteloita. Selvityksen perusteella Savonian tietoverkossa IPv6-käyttöönoton voi tehdä ilman suuria laitehankintoja ja päivityksiä. Lisäksi työssä tarjotaan ehdotuksia link local -osoitteiden ja Internet-palveluntarjoajasta riippumattoman osoiteavaruuden käyttöön.</p>	
Avainsanat IPv6, IPv4, tuplapino, tunnelointi, tilaton autokonfiguraatio	

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Jarkko Kuosmanen			
Title of Thesis IPv6 Networks			
Date	15 May 2013	Pages/Appendices	32/0
Supervisor(s) Mr Pekka Vedenpää, Laboratory Engineer			
Client Organisation/Partners Savonia University of Applied Sciences			
<p>Abstract</p> <p>The subject of this thesis was IPv6 networks. The object was to research the readiness of the network of Savonia University of Applied Sciences for the introduction of IPv6.</p> <p>Some enterprises already need IPv6 because IPv4 addresses have almost run out, at least in Europe. Enterprises that already have an existing network do not need IPv6 yet, but they should familiarize themselves with the new protocol.</p> <p>Cisco's web site was used to research the IPv6 readiness of the networking equipment that is used in Savonia's network. The documentations of models used in Savonia's network were used to see if they support IPv6 features, such as IPv6 Access Control Lists. The research showed that Savonia's network is IPv6 ready and does not need many equipment purchases or upgrades. In addition, the thesis provides suggestions on how to use link local addresses and provider independent address space in Savonia's network.</p>			
<p>Keywords IPv6, IPv4, dualstack, tunnelling, stateless autoconfiguration</p>			

SISÄLTÖ

SANASTO	7
1 JOHDANTO.....	8
2 IPv6-KÄYTTÖÖNOTON HYÖTYJÄ.....	9
2.1 IPv6:n ominaisuudet.....	9
2.1.1 IPv6-osoitteiden ominaisuudet	10
2.1.2 IPv6-paketin otsikko.....	11
2.1.3 Laajennusotsikot	13
2.1.4 MTU:n selvitys	14
3 IPV6-OSOITTEET	16
3.1 Osoitteen esitysmuoto.....	16
3.2 Verkkorajapinnan tunniste IPv6-osoitteissa	17
3.3 Osoitetyypit.....	18
3.3.1 Globaalit kohdelähetysosoitteet	19
3.3.2 Link local -osoitteet	20
3.3.3 Ryhmäosoitteet.....	21
3.3.4 Solicited-node-ryhmäosoitteet	22
3.3.5 Anycast-osoitteet	23
4 IPV6-OSOITTEIDEN JAKAMINEN YRITYSVERKOSSA.....	24
5 SIIRTYMÄVAIHEEN TEKNIIKAT	26
5.1 Tuplapino.....	26
5.2 Tunnelointi.....	27
6 SAVONIAN TIETOVERKKO	28
6.1 IPv6-käyttöönoton vaatimukset.....	28
6.2 Osoitteiden käyttö	28
6.2.1 Link local -osoitteet	28
6.2.2 Yksiköt ja aliverkot	29
6.3 Siirtymävaihe	30
7 YHTEENVETO	31
LÄHTEET	32

SANASTO

CIDR – Classless Inter-Domain Routing, osoite jolla on luokkaansa pienempi prefiksi, eli se edustaa useampaa sen luokan ali-/verkkoa

DHCP - Dynamic Host Configuration Protocol on verkkoprotokolla, jonka tehtävä on jakaa IP-osoitteita lähiverkon laitteille

DiffServ – Differentiated Services eli erotellut palvelut on yksi palvelun laadun takaamisessa käytettävistä malleista

MTU - Maximum Transmission Unit eli suurin lähetysyksikön koko

NAT – Network Address Translation, osoitteenmuunnostekniikka

QoS – Quality of Service eli palvelun laatu

1 JOHDANTO

Tämän opinnäytetyön aihe on IPv6-verkot ja työ on tehty Savonia-ammattikorkeakoululle. Tavoitteena on selvittää Savonian tietoverkon IPv6:n käyttöönoton valmiudet.

Aluksi vertaillaan IPv6:ta ja IPv4:ää, minkä jälkeen tutustutaan IPv6:n uusiin ominaisuuksiin ja osoitteisiin. Lisäksi tutustutaan siirtymätekniikoihin ja IPV6-osoitteiden tilattomaan autokonfiguraatioon. Lopuksi käsitellään Savonian tietoverkossa käytettävien laitteiden IPv6-tukea, sekä annetaan ehdotuksia link local -osoitteiden käytöstä ja Internet-palveluntarjoajasta riippumattoman osoiteavaruuden aliverkotuksesta.

Savonia-ammattikorkeakoulu toimii kolmella paikkakunnalla: Iisalmessa, Kuopiossa ja Varkaudessa. Savoniaa ylläpitää Savonia-ammattikorkeakoulun kuntayhtymä, jonka jäsenkunnat ovat Iisalmi, Kiuruvesi, Kuopio, Lapinlahti ja Varkaus. Kuntayhtymän johtajana ja Savonia-ammattikorkeakoulun rehtorina toimii Veli-Matti Tolppi.

2 IPv6-KÄYTTÖÖNOTON HYÖTYJÄ

Suurin syy IPv6-osoitteiden käyttöönottoon on IPv4-osoitteiden loppuminen, joka on käytännössä tapahtunut jo ainakin Euroopassa. Euroopan Internet-rekisteriä ylläpitävä RIPE NCC ilmoitti 14.9.2012 laittavansa viimeisen /8 prefiksiä olevan osoiteavaruuden jakoon paikallisille Internet-palveluntarjoajille. Tämä tarkoittaa sitä, että jokainen paikallinen Internet-palveluntarjoaja saa vain yhden /22 prefiksiä (1 024 osoitetta) olevan osoiteavaruuden, mikäli ne ovat ottaneet IPv6-osoiteavaruuden jaettavaksi. IPv4-osoitteita kuitenkin vapautuu yrityksiltä, jotka ottavat IPv6-osoitteen käyttöön. (RIPE NCC 2012.)

IPv4:llä on muitakin heikkouksia, kuin osoitteiden vähäinen määrä, joita IPv6:ssa on yritetty korjata. IPv4-osoitteiden vähäisyyden vuoksi joudutaan käyttämään yksityisiä osoitteita ja NAT-osoitteenmuunnosta julkiseksi osoitteeksi. Tällöin todellinen lähettäjä jää piiloon, mikä toisaalta antaa anonymiteetin käyttäjälle. Heikkoutena on myös IPv4-osoitteiden huono ryhmitettävyys CIDR-reitiksi, koska jokaisen luokan osoitteita jaetaan ympäri maailmaa. Tästä syystä Internetin reititystaulu kasvaa aina kun verkkoon lisätään laitteita. Suuret reititystaulut vaativat paljon muistia ja suoritustehoa Internet-palveluntarjoajien reitittimiltä. Internetin reititystaulussa oli tammikuun 2013 loppupuolella jo yli 442 000 reittiä. Reititystaulu on kasvanut vuoden 2010 alkupuolen 310 000:sta yli 130 000 reitillä. (CIDR Report 2013; Teare 2010.)

2.1 IPv6:n ominaisuudet

Lukujen 2.1 - 2.1.4 kaikki tieto pohjautuu D. Tearen teokseen Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide (Teare 2010).

IPv6:n ominaisuudet tukevat nykyisiä ja ennakoitavissa olevia verkon vaatimuksia paremmin kuin IPv4:n ominaisuudet. Tässä luvussa eritellään lyhyesti näitä ominaisuuksia.

IPv4:n 32-bittinen osoiteavaruus tarjoaa hieman alle 4,3 miljardia osoitetta. Osoiteavaruus on NAT-osoitteenmuunnoksesta huolimatta riittämätön maailman hieman yli 7 miljardille ihmiselle. IPv6:n 128-bittinen osoiteavaruus tarjoaa $3,4 \cdot 10^{38}$ osoitetta eli $5 \cdot 10^{28}$ osoitetta jokaiselle maailman ihmiselle. Isompi osoiteavaruus tarjoaa useita etuja, kuten parannettu globaali saavutettavuus ja joustavuus.

IPv6:ssa NAT on jätetty pois, koska päästä päähän -yhteydet saavutetaan ilman osoitteiden loppumista. Aluksi suunniteilla olleet yksityiset IPv6-osoitteet hylättiin, koska olisi tarvittu NAT-osoitteenmuunnosta. Myös yleislähetysosoitteet on jätetty pois. Niiden sijaan käytetään ryhmäosoitteita ja uusia anycast-osoitteita. Yleislähetykset saattavat aiheuttaa levitysviestimyrskyn eli toimintahäiriön, joka voi tukkia koko verkon.

IP-paketin otsikkoa on yksinkertaistettu reititystehokkuuden parantamiseksi. Otsikosta on poistettu varmistussumma ja lisätty virtausleima, jolla pakettiliikenteen virtauksia voidaan tunnistaa lukematta sitä kuljetuskerroksen tiedoista, kun reititetään virtauksen perusteella. Valinnat käsitellään yksinkertaisemmin ja tehokkaammin IPv6:ssa kuin IPv4:ssä. IPv4:ssä valinnat olivat osana otsikkoa, kun taas IPv6:ssa ne käsitellään omilla erillisissä laajennusotsikoissaan. IPv6-paketin otsikosta ja laajennusotsikoista kerrotaan tarkemmin seuraavissa alaluvuissa.

IPv6 tukee liikkuvuutta Mobile IP:n ja turvallisuutta IPsec:n muodossa. Mobile IP on Internet Engineerin Task Forcen (IETF) kehittämä standardi kummallekin IP:n versiolle, mikä mahdollistaa mobiililaitteiden liikkumisen ilman yhteyden katkeamista. Koska IPv4 ei tarjoa automaattisesti tämäntapaista liikkuvuutta, sen tukeminen vaatii ylimääräistä konfigurointia. IPv6:ssa liikkuvuus on sisäänrakennettuna, eli mikä tahansa IPv6-päätelaite voi käyttää sitä tarvittaessa. IPv6:n reititysotsikot tekee mobile IPv6:sta paljon tehokkaamman kuin IPv4. IPsec on IETF:n kehittämä IP-verkkojen turvallisuusstandardi, joka on saatavilla kummallekin IP:n versiolle. IPsec on käytävissä kaikilla IPv6-päätelaitteilla, mikä tekee IPv6-Internetistä turvallisemman.

IPv6:n käyttöönottoon on monia tapoja, ja sen voi ottaa käyttöön IPv4:n rinnalle. Yleisin tapa on tuplapino: samassa verkkorajapinnassa on sekä IPv4- että IPv6-osoite. Tällöin kumpikin protokollan versio toimii yhtä aikaa ja ne käyttävät omia reititystaulujaan. Toinen väliaikainen tapa on tunnelointi: IPv6-paketti kuljetetaan IPv4-paketin sisällä. Tunnelleita on erilaisia, joista jokainen sopii eri käyttötarkoitukseen.

2.1.1 IPv6-osoitteiden ominaisuudet

IPv6-osoitteiden ominaisuudet tarjoavat joustavuutta, toisin kuin IPv4:n ominaisuudet. Tässä luvussa on lyhyesti kuvailtu näitä ominaisuuksia.

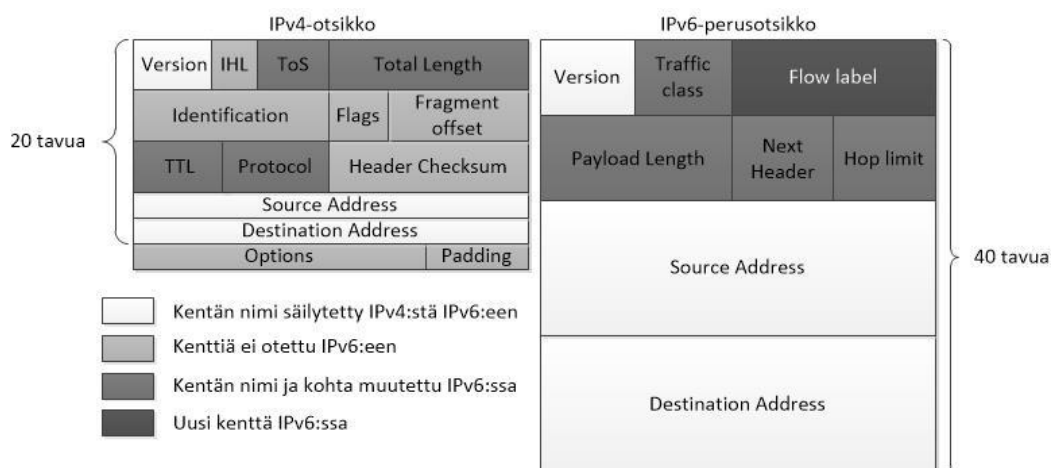
Tilaton autokonfiguraatio tarjoaa IPv6-osoitteen automaattisen konfiguroinnin, joka liittää laitteen siirtokerroksen osoitteen IPv6-osoitteeseen. IPv6:ssa on yksinkertaistettu mekanismi osoitteen ja prefiksin uudelleennumerointiin. Reititin mainostaa uutta prefiksiä, ja verkon muut laitteet voivat alkaa heti hyödyntää uutta tietoa.

Verkkorajapinnoille voidaan antaa monta erityyppistä osoitetta ja niitä voidaan käyttää yhtä aikaa. IPv6-laitteet luovat automaattisesti jokaiselle verkkorajapinnalle link local -osoitteen. Näitä osoitteita käytetään moneen tarkoitukseen, esimerkiksi reititysprotokollat käyttävät link local -osoitteita seuraavana hyppynä vaihtaessaan reitityspäivityksiä.

Koska osoitteita on tarjolla niin paljon, yritykset voivat valita joko Internet-palveluntarjoajan osoiteavaruuden tai oman tarjoajasta riippumattoman osoiteavaruuden. Oma osoiteavaruus helpottaa verkkoyhteyksien kahdentamista ja Internet-palveluntarjoajan vaihtamista, kun verkkoa ei tarvitse numeroida uudelleen. Palveluntarjoajasta riippumattomat osoitteet eivät kuitenkaan ole ryhmitettävissä palveluntarjoajien osoitteiden kanssa.

2.1.2 IPv6-paketin otsikko

IPv6-perusotsikko on 40 tavun kokoinen, kun vastaavasti IPv4-otsikko on 20 tavun kokoinen. IPv4-otsikossa on 12 peruskenttää ja vaihtelevan kokoinen vaihtoehtokenttä, joka kasvattaa otsikon kokonaispituutta. IPv6-otsikossa on 7 samantapaista kenttää kuin IPv4:ssä ja yksi kokonaan uusi kenttä. Kuviossa 1 on esitetty vierekkäin kumpikin IP-otsikko.



KUVIO 1. IP-pakettien perusotsikot vertailussa

IPv6-otsikossa ei ole varmistussummakenttää, koska luotettavina pidettävät siirtokerrosteknologiat laskevat varmistussumman ja suorittavat virheiden valvonnan, joten IP-otsikon varmistussummaa pidetään tarpeettomana.

IPv6-perusotsikon kahdeksan kenttää ovat versio, liikenteen tyyppi (Traffic Class), virtausleima (Flow Label), hyötykuorman pituus (Payload Length), seuraava otsikko (Next Header), hyppyraja (Hop Limit) sekä lähde- ja kohdeosoite.

Versiokenttä on 4-bittinen ja se on sama kuin IPv4:ssä. Kentän arvona on 6 IPv6-paketissa ja 4 IPv4-paketissa.

Liikenteen tyyppi -kenttä on 8-bittinen ja se on samantapainen kuin Type of Service (ToS) -kenttä IPv4:ssä. Tähän kenttään merkitään liikenteen tyyppi, jota käytetään erotettujen palveluiden palvelun laatuun (DiffServ QoS). Nämä toiminnallisuudet ovat samat IPv6:ssa ja IPv4:ssä.

IPv6:een on lisätty 20-bittinen virtausleimakenttä. Paketin lähde voi merkitä tähän kenttään paketin kuuluvan tiettyyn virtaukseen. Reitittimien on mahdollista käsitellä liikennettä mieluummin virtausten perusteella kuin jokainen paketti erikseen, jolloin pakettien välittäminen on nopeampaa. Virtausleimakenttää voidaan käyttää myös palvelun laadun takaamiseen.

16-bittinen hyötykuorman pituus -kenttä, joka mahdollistaa 64 kilotavun hyötykuorman, on samantapainen kuin IPv4:n kokonaispituuskenttä.

Seuraava otsikko -kenttä on 8-bittinen, ja sen arvo määrittelee IPv6-perusotsikon jälkeisen tiedon tyyppin. Perusotsikon jälkeinen tieto voi olla kuljetuskerroksen TCP- tai UDP-paketti tai laajennusotsikko. Seuraava otsikko -kenttä on samantapainen kuin protokollakenttä IPv4:ssä.

8-bittinen hyppyrajakenttä määrittelee hyppyjen maksimimäärän, jonka IPv6-paketti voi kulkea. Tämä kenttä on samantapainen kuin IPv4:n Time to Live (TTL) -kenttä. Jokainen reititin vähentää kentän arvoa yhdellä. Koska IPv6-otsikossa ei ole varmistussummaa, IPv6-reitittimet voivat vähentää arvoa laskematta uutta varmistussummaa, kun taas IPv4-reitittimissä uudelleen laskenta vie prosessointiaikaa. Jos arvoksi tulee nolla, lähetetään viesti takaisin lähettäjälle ja paketti hylätään.

128-bittiset, eli 16-tavuiset lähde- ja kohdeosoitekentät tunnistavat paketin lähettäjän ja kohteen IPv6-osoitteet.

Perusotsikon kahdeksaa kenttää seuraa joko laajennusotsikkoketju tai paketin dataosuus. Seuraava otsikko -kenttä kertoo seuraavan laajennusotsikon tyyppin. Laajennusotsikoiden määrää ei ole määrätty, joten laajennusotsikkoketjun kokonaispituus voi vaihdella.

2.1.3 Laajennusotsikot

IPv6:ssa käytetään laajennusotsikoita, jotka käsittelevät vaihtoehdot tehokkaasti ja nopeuttaa käsittelyä päätelaitteilla. Seuraava otsikko -kenttä osoittaa ketjun seuraavaan otsikkoon; aivan kuten c-ohjelmoinnissa käytettävässä yksisuuntaisessa linkityssä listassa.

Useimmat laajennusotsikot tutkitaan ja käsitellään vasta paketin kohteena olevassa laitteessa. Laitte tutkii ensimmäisen laajennusotsikon, mikäli sellainen löytyy. Laajennusotsikon sisältö määrittelee täytyykö laitteen lukea seuraava otsikko. Siitä syystä laajennusotsikot täytyy käsitellä siinä järjestyksessä kuin ne ovat paketissa.

Vaikka laajennusotsikoita on monenlaisia, ainoastaan hop-by-hop-laajennusotsikko pitää tutkia reitin jokaisessa laitteessa, jos se paketista löytyy. Hop-by-hop-laajennusotsikko täytyy tulla heti IPv6-perusotsikon jälkeen ja se ilmaistaan seuraava otsikko -kentän arvolla nolla.

Kun useaa laajennusotsikkoa käytetään samassa paketissa, niiden tulee olla oikeassa järjestyksessä: IPv6-perusotsikko, hop-by-hop-otsikko, määränpään vaihtoehdot -otsikko, reititysotsikko, hajautusotsikko, autentikointiotsikko ja Encapsulating Security Payload (ESP) -otsikko.

IPv6-perusotsikon jälkeen tulevaa hop-by-hop-otsikkoa käytettäessä, se käsitellään reitin jokaisessa reitittimessä. Esimerkki käyttötilanteita ovat Router Alertit, joihin kuuluu Resource Reservation Protocol (RSVP) ja Multicast Listener Discovery (MLD) viestit.

Kolmantena tulee määränpään vaihtoehdot -otsikko, silloin kun käytetään reititysotsikkoa. Tätä otsikkoa tarkoittava seuraava otsikko -kentän arvo on 60. Tämä otsikko

seuraa mahdollista hop-by-hop-otsikkoa, jolloin määränpään vaihtoehdot -otsikko käsitellään paketin määränpäässä, kuin myös jokaisessa reititysotsikon määrittelemässä kohteessa. Vaihtoehtoisesti määränpään vaihtoehdot -otsikko voi seurata mitä tahansa ESP-otsikkoa, jolloin määränpään vaihtoehdot -otsikko käsitellään vain paketin määränpäässä. Esimerkiksi mobile IPv6:ssa käytetään tätä otsikkoa.

Neljäntenä tulevaa reititysotsikkoa, jonka seuraava otsikko -kentän arvo on 43, käytetään lähdereititykseen ja mobile IPv6:ssa. IPv6-lähde luetteloi tähän otsikkoon yhden tai useamman välilaitteen, joissa paketin pitää käydä matkalla kohteeseen.

Viidentenä tulevaa hajautusotsikko, jonka seuraava otsikko -kentän arvo on 44, käytetään kun lähteen pitää pilkkoa paketti, joka on isompi kuin reitin suurin lähetysyksikön koko (MTU). Hajautusotsikkoa käytetään jokaisessa pilkotussa paketissa.

Kuudentena tulevat IPsec:ssä käytettävät autentikointiotsikko (AH), jonka seuraava otsikko -kentän arvo on 51 ja ESP-otsikko, jonka seuraava otsikko -kentän arvo on 50. Näitä otsikoita käytetään tuomaan autentikointi, eheys ja tietosuoja paketille. Nämä otsikot ovat identtiset IPv4:ssä ja IPv6:ssa.

Viimeisenä tulee dataosuus, eli kuljetuskerroksen otsikko. Kaksi pääprotokollaa ovat TCP, jonka seuraava otsikko -kentän arvo on 6 ja UDP, jonka seuraava otsikko -kentän arvo on 17.

2.1.4 MTU:n selvitys

IPv4:ssä reitittimet suorittavat paketin pilkkomisen aiheuttaen erilaisia käsittelyongelmia. IPv6-reitittimet eivät enää suorita pilkkomista vaan IPv6-lähdelaite käyttää selvitysprosessia, joka määrittelee sopivan MTU:n käytettäväksi kyseisellä istunnolla. Selvitysprosessissa lähdelaite yrittää lähettää ylemmän kerroksen määräämän kokoisen paketin. Jos lähdelaite vastaanottaa Internet Control Message Protocol for IPv6 (ICMPv6) ”paketti liian iso” -viestin, se lähettää uudelleen MTU:n selvityspaketin pienemmällä MTU:lla. Tätä prosessia jatketaan kunnes laite vastaanottaa vastauksen siitä, että paketti pääsi perille ehjänä. Sen jälkeen laite asettaa MTU:n istunnolle.

ICMPv6 ”paketti liian iso” -viesti sisältää reitille sopivan MTU:n koon. Jokainen laite seuraa MTU:n kokoa jokaiselle istunnolleen. Yleisesti seuraus tapahtuu luomalla vä-

limuisti kohdeosoitteen mukaan tai lähdeosoitteen mukaan, jos käytetään lähdereititystä. Vaihtoehtoisesti seurannan voi tehdä myös virtausleiman avulla.

Selvitysprosessi on hyödyllinen, koska jos reititysreitti muuttuu, voi olla sopivampaa käyttää uutta MTU:a. Laitteet suorittavat MTU:n selvityksen viiden minuutin välein katsoakseen onko MTU kasvanut matkalla. IPv6-sovellus- ja kuljetuskerrokset hyväksyvät MTU:n pienennysilmoitukset IPv6-kerrokselta. Mikäli ylemmät kerrokset eivät hyväksy ilmoituksia, löytyy IPv6:sta mekanismi, jolla lähdelaitte voi pilkkoa liian isot paketit. Ylempiä kerroksia kuitenkin kehoitetaan välttämään pilkkomista tarvitsevien pakettien lähettämistä.

3 IPV6-OSOITTEET

Lukujen 3 - 3.3.5 kaikki tieto pohjautuu lähteeseen (Teare 2010).

Kuten jo mainittu, IPv6-osoitteen koko on 128 bittiä ja sen mahdollistaman osoiteavaruuden loppuun kuluttamisen pitäisi olla mahdotonta. Osoitteen bittien määrän kasvattaminen kasvattaa myös otsikon kokoa. Jokaisen IP-otsikon lähde- ja kohdeosoitteet lisäävät jokaiseen IPv6-otsikkoon 256 bittiä kun taas IPv4-otsikkoon ne lisäävät 64 bittiä.

Isompi osoiteavaruus kuitenkin mahdollistaa kookkaat osoitevaraukset Internet-palveluntarjoajille ja organisaatioille. Internet-palveluntarjoaja voi ryhmittää kaikki asiakkansa prefiksit yhdeksi prefiksiksi, jonka ilmoittaa IPv6-Internetiin. Asiakkaiden prefiksien ryhmittäminen johtaa tehokkaaseen ja skaalautuvaan reititystauluun. Isompi osoiteavaruus tarkoittaa myös sitä, että organisaatioille voidaan myöntää tarpeeksi iso prefiksi, joka riittää määrittelemään kyseisen organisaation koko verkon.

3.1 Osoitteen esitysmuoto

IPv4-osoitteesta tuttu pisteillä erotettu desimaalimuoto on vaihtunut kaksoispisteillä erotettuun heksadesimaalimuotoon. Uusi esitysmuoto on 16 bitin eli neljän heksadesimaalin ryhmät erotettuna kaksoispisteellä. Tämänlaisia ryhmiä osoitteessa on siis kahdeksan kappaletta. Vanhalla esitysmuodolla esitettyä osoitteessa olisi 16 kappaletta desimaaleja pisteillä erotettuna.

Osoite voi olla esimerkiksi FE80:0000:0234:2001:0000:0000:0001, mutta onneksi osoitteet voidaan lyhentää tiettyjen sääntöjen avulla. Alla olevassa taulukossa 1 on esitetty kolmessa vaiheessa osoitteen lyhennyssäännöt.

Taulukon ensimmäisessä kohdassa jokaisen ryhmän aloittavat nollat on jätetty kirjoittamatta. Toisessa kohdassa neljän nollan ryhmä on kirjoitettu yhtenä nollana. Kolmannessa kohdassa useamman peräkkäisen neljän nollan ryhmä on kirjoitettu kahdella kaksoispisteellä.

TAULUKKO 1. IPv6-osoitteen lyhentämissäännöt

Osoitteen lyhentämissäännöt		
Sääntö	Täysi osoite	Lyhennetty osoite
1.	FE80:0000:0234:2001:0000:0000:0COD:0001	FE80:0000:234:2001:0000:0000:COD:1
2.	FE80:0000:0234:2001:0000:0000:0COD:0001	FE80:0:234:2001:0:0:COD:1
3.	FE80:0000:0234:2001:0000:0000:0COD:0001	FE80:0:234:2001::COD:1

Laitteet täydentävät kahden kaksoispisteen väliin nollia, kunnes osoite on 128-bittinen. Kahta peräkkäistä kaksoispistettä ei saa käyttää osoitteessa kuin kerran, koska muuten olisi mahdotonta määrittää, kuinka monta nollaa mihinkin väliin pitäisi tulla.

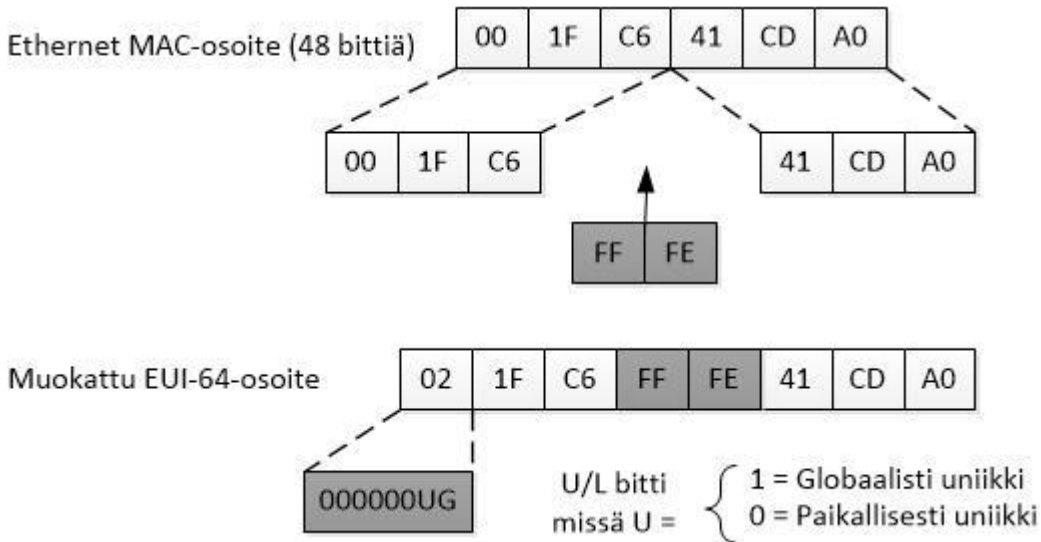
Aliverkon maski voidaan kirjoittaa samalla tavalla kuin IPv4:ssä prefiksinä, esimerkiksi /24. IPv6 käyttää prefiksiä ilmaisemaan verkon tai aliverkon bittien määrän.

3.2 Verkkorajapinnan tunniste IPv6-osoitteissa

IPv6-verkoissa linkki määrittellään verkon mediaksi, jonka yli laitteet kommunikoivat käyttäen siirtokerrosta. Verkkorajapinnan tunnisteita (Interface Identifier, ID) käytetään IPv6-osoitteissa tunnistamaan uniikki verkkorajapinta linkissä. Niitä voi ajatella myös IPv6-osoitteen isäntäosana. Tunnisteiden tulee olla uniikit linkissä, ja ne voivat olla uniikkeja myös laajemmin, kuten globaalisti.

Kun verkkorajapinnan tunniste on johdettu suoraan verkkorajapinnan siirtokerroksen osoitteesta, tunnisteeseen oletetaan olevan uniikki globaalisti. Verkkorajapinnan tunniste on aina 64 bittiä, ja se voidaan luoda dynaamisesti siirtokerroksen median ja kapseloinnin perusteella.

Siirtokerros määrittelee, kuinka IPv6-verkkorajapinnan tunniste luodaan ja kuinka naapurin tunnistus käsittelee siirtokerroksen osoitteen selvittämisen. Ethernet-tekniikassa tunniste perustuu verkkorajapinnan mac-osoitteeseen ja on ”Extended Unique Identifier 64-bit” (EUI-64) -muodossa. EUI-64-muotoinen tunniste johdetaan 48-bittisestä mac-osoitteesta lisäämällä 16-bittinen heksadesimaali FFFE kolmen ylemmän tavun ja kolmen alemman tavun väliin. Seitsemänneksi ylin bitti asetetaan ykköseksi osoittamaan verkkorajapinnan tunnisteiden uniikkiutta. EUI-64-muotoisen tunnisteiden johtaminen on esitetty kuviossa 2.



KUVIO 2. EUI-64-muotoisen verkkorajapinnan tunnisteiden johtaminen mac-osoitteesta

IPv6-verkkorajapinnan tunnisteiden seitsemättä bittiä käytetään tunnistamaan osoitteen uniikkisuus paikallisesti tai maailmanlaajuisesti. Koska mac-osoitteiden oletetaan olevan maailmanlaajuisesti uniikkeja, myös niistä johdettujen tunnisteiden oletetaan olevan maailmanlaajuisesti uniikkeja. Ylempien kerrosten protokollien on tulevaisuudessa tarkoitus tunnistaa uniikit yhteydet tämän bitin avulla. Tämä toiminto ei vielä ole käytössä. IPv6-verkkorajapinnan tunnisteiden kahdeksatta bittiä, G-bittiä, käytetään ryhmien hallinnassa.

Yksityisyys- ja turvallisuushuolien takia isäntäkoneet voivat luoda satunnaisen verkkorajapinnan tunnisteiden käyttäen mac-osoitetta pohjana. Näillä osoitteilla on lyhyt elinikä, ja ne generoidaan uudestaan aika ajoin. Tämä prosessi on määritelty RFC:ssä 2941, Privacy Extensions for Stateless Autoconfiguration in IPv6. Esimerkiksi Microsoft Windows -käyttöjärjestelmissä tämä toiminto on ollut käytössä jo Windows XP:ssä.

3.3 Osoitetyypit

IPv6:ssa on kolme pääosoitetyppiä, jotka ovat kohdelähetys, ryhmälähetys ja uusi anycast. Kohdelähetys- ja ryhmäosoitteet ovat samanlaiset kuin IPv4:n vastaavat. Kuten jo mainittu, IPv6:ssa yleislähetykset on jätetty pois.

Käyttötavan puolesta IPv6-kohdelähetysosoitteet eivät eroa IPv4-kohdelähetysosoitteista; aliverkon prefiksi ja kohdelähetysosoite liittyvät yhteen verkkorajapintaan. Paketti, joka lähetetään kohdelähetysosoitteeseen, menee verkkoraja-

pintaan, jolla on kyseinen osoite. IPv6-kohdelähetysosoiteavaruus kattaa koko IPv6-osoitejoukon lukuun ottamatta ryhmälähetysosoiteavaruutta, joka on FF00::/8-osoitejoukko.

Myös IPv6-ryhmälähetykset toimivat samaan tapaan kuin IPv4:ssä: paketti joka lähetetään ryhmäosoitteeseen, menee sitä ryhmää kuunteleville verkkorajapinnoille. Ainut poikkeus on huomattavasti suurempi osoiteavaruus.

Uudet anycast-osoitteet toimivat niin, että sama osoite annetaan usealle eri laitteen verkkorajapinnalle eli laitteiden ryhmälle. Paketti, joka lähetetään anycast-osoitteeseen, menee lähimpänä olevan laitteen verkkorajapintaan. Lähimpänä olevan laitteen määrää reititysprotokolla. Siksi kaikkien samaa anycast-osoitetta käyttävien laitteiden tulisi tarjota samaa palvelua. Anycast-osoitteita voi käyttää esimerkiksi kuorman jakamiseen.

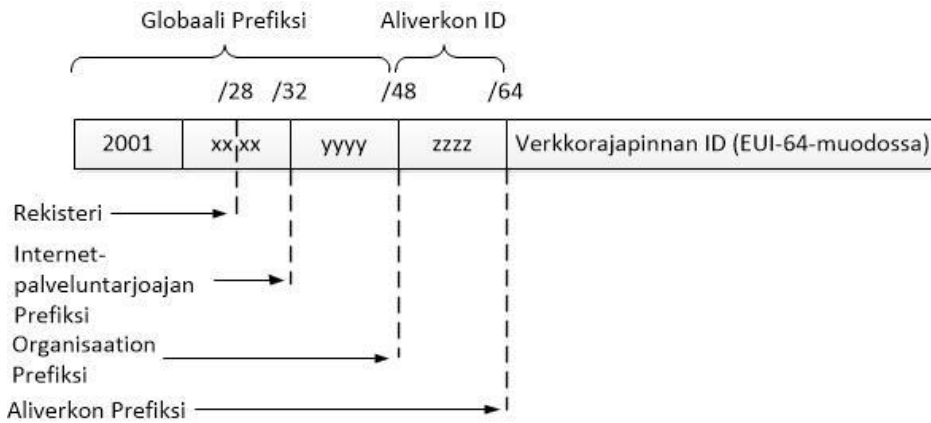
Yhdelle verkkorajapinnalle voi antaa useamman mitä tahansa tyyppiä olevan IPv6-osoitteen. Jokaisessa IPv6:ta käyttävässä verkkorajapinnassa tulee olla vähintään yksi loopback-osoite (::1/128) ja yksi link local -osoite.

3.3.1 Globaalit kohdelähetysosoitteet

Internet Assigned Numbers Authority (IANA) jakaa globaalit kohdelähetysosoitteet eli Internetissä käytettävät ja reititettävät osoitteet. IANAn nykyinen globaalien kohdelähetysosoitteiden luovutus käyttää osoitejoukkoa, joka alkaa binäärillä 001 tai toisin ilmaistuna 2000::/3. Rekisterit saavat osoitteita arvoalueelta 2001::/16. Globaalit kohdelähetysosoitteet ovat vastine IPv4:n julkisille IP-osoitteille.

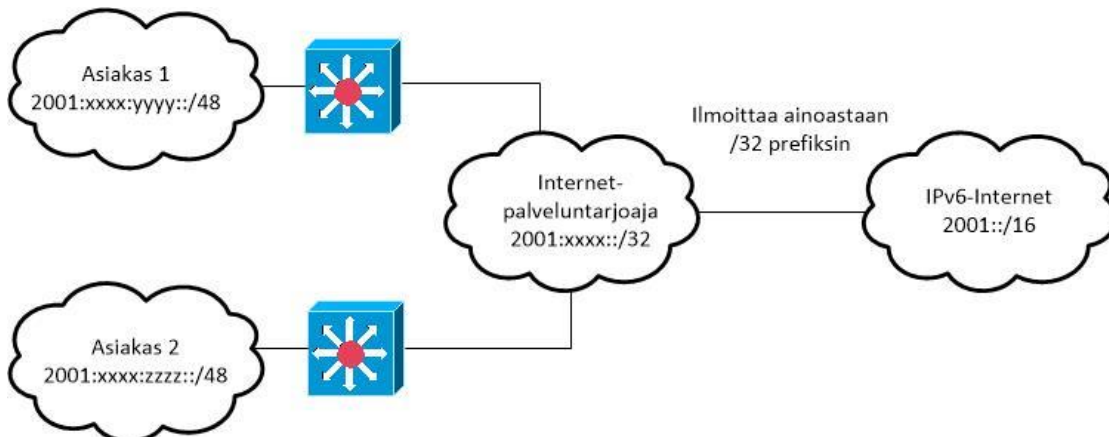
Osoitteiden joiden prefiksi on väliltä 2000::/3 - E000::/3 mukaan lukematta ryhmälähetysosoiteavaruutta FF00::/8 edellytetään käyttävän EUI-64-muotoa 64-bittisissä verkkorajapinnan tunnisteissa.

Globaali kohdelähetysosoite koostuu tyypillisesti 48-bittisestä globaalista reititysprefiksistä, 16-bittisestä aliverkon tunnisteesta ja 64-bittisestä verkkorajapinnan tunnisteesta. Osoitteen rakenne on esitetty kuviossa 3.



KUVIO 3. Globaalin IPv6-kohdelähetysosoitteen rakenne

IPv6-osoitteen rakenne mahdollistaa reititysprefiksien ryhmittämisen niin, että globaalien reititystaulujen merkintöjen määrää voitaisiin vähentää. Linkeissä käytettävät globaalit kohdelähetysosoitteet ryhmitetään ylöspäin organisaatiossa ja lopulta Internet-palveluntarjoajalle. Tämä on esitetty kuviossa 4.



KUVIO 4. IPv6-kohdelähetys prefiksien ryhmittäminen

Individuaaliset organisaatiot voivat käyttää aliverkon tunnistetta oman paikallisen osoitehierarkian luomiseen. 16-bittinen aliverkon tunniste -kenttä mahdollistaa organisaation käyttöön 65536 aliverkkoa.

3.3.2 Link local -osoitteet

Link local -osoitteiden laajuus on rajoitettu paikalliseen linkkiin. Link local -osoitteet luodaan automaattisesti jokaisessa IPv6-verkkorajapinnassa käyttämällä link local -prefiksiä FE80::/10 ja 64-bittistä verkkorajapinnan tunnistetta. Link local -osoitteet

voidaan konfiguroida myös itse, jolloin käsin syötetty osoite korvaa dynaamisesti luodun osoitteen. Link local -osoitteita ei voi olla kuin yksi linkkissään.

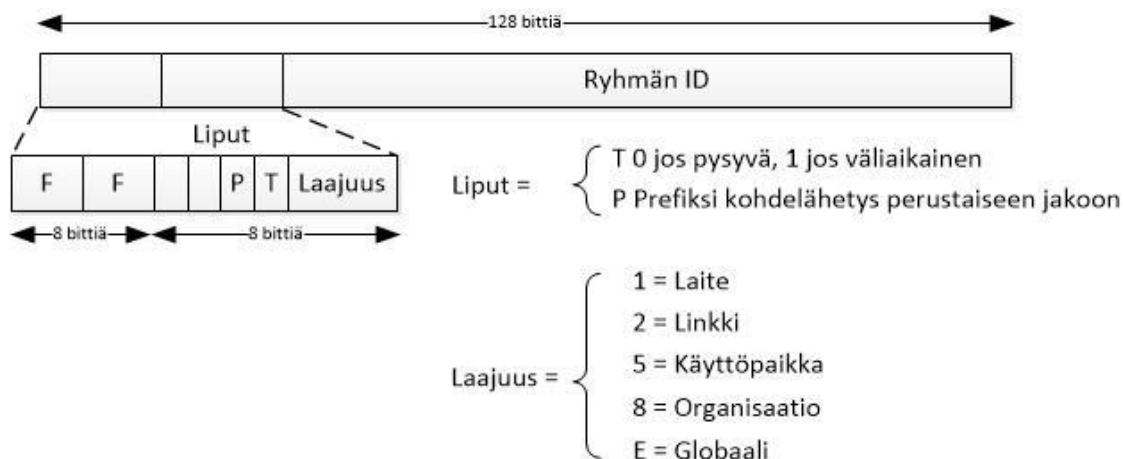
Link local -osoitteita käytetään osoitteiden automaattiseen konfigurointiin, naapurin selvitykseen, reitittimen selvitykseen ja monessa reititysprotokollassa. Link local -osoitteita voidaan käyttää yhdistämään laitteita samassa paikallisessa verkossa ilman globaaleja kohdelähetysosoitteita. Kun kommunikoidaan link local -osoitteilla, pitää ulosmenoverkkorajapinta määritellä, koska kaikki verkkorajapinnat on yhdistetty FE80::/10-verkkoon.

3.3.3 Ryhmäosoitteet

Yksittäinen verkkorajapinta voi liittyä useaan ryhmälähetysryhmään, eikä ryhmälähetysryhmien määrää ole rajoitettu. Ryhmälähetystyksiä käytetään paljon IPv6:ssa, koska sillä korvataan yleislähetykset. Ryhmäosoitteet ovat tehokkaampia kuin yleislähetysosoitteet, koska liikenne lähetetään vain niille tietyille vastaanottajille: jotka ovat liittyneet ryhmälähetysryhmään.

IPv6-ryhmäosoitteet on määritelty prefiksillä FF00::/8. Osoitteen toinen tavu sisältää prefiksi- ja tilapäisyysliput sekä ryhmäosoitteen laajuuden ilmaisevat bitit. Tilapäisyyslippu (T) on nolla pysyvillä eli tunnetuilla ryhmäosoitteilla ja yksi tilapäisillä eli dynaamisilla ryhmäosoitteilla. Prefiksilippu (P) asetetaan ykköseksi, kun lähdeverkon kohdelähetysprefiksi liitetään ryhmälähetysryhmän osoitteeseen.

4-bittisen laajuusparametrin arvot ovat: 1 laite laajuudelle (loopback), 2 linkin laajuudelle (samaan tapaan kuin link local -osoitteet), 5 käyttöpaikan laajuudelle, 8 organisaation laajuudelle (useampi käyttöpaikka) ja E globaalille laajuudelle. IPv6-ryhmäosoitteen rakenne on esitetty kuviossa 5.



KUVIO 5. IPv6-ryhmäosoite

Ryhmäosoite, joka alkaa esimerkiksi prefiksillä FF02::/16 on pysyvä ryhmäosoite, jonka laajuus on linkki. IPv6-ryhmäosoiteissa ei ole TTL-kenttää, koska laajuus määrittellään osoitteessa. Osoitteen alimmat 112 bittiä jää ryhmälähetysryhmän tunnisteelle. Osoitteet väliltä FF00::/16 - FF0F::/16 ovat varattuja, koska niiden T-lippu on nolla.

3.3.4 Solicited-node-ryhmäosoitteet

Solicited-node-ryhmäosoitteita käytetään Neighbor Solicitation (NS) -viesteissä eli naapurin selvitys -viesteissä, jotka lähetetään paikalliseen linkkiin, kun halutaan selvittää toisen laitteen siirtokerroksen osoite. IPv6:n naapurin selvitys toimii siis samaan tapaan kuin Address Resolution Protocol (ARP) IPv4:ssä eli selvitetään IP-osoitetta vastaava mac-osoite.

Solicited-node-ryhmäosoite käyttää muotoa FF02:1::FFXX:XXXX eli se toimii linkissä ja paketti lähetetään kaikille linkissä oleville laitteille. Osoitteen XX:XXXX osuus on selvittävän kohdelähetysosoitteen tai anycast-osoitteen 24 oikean puoleista bittiä. Harvinaisissa tapauksissa samassa linkissä olevien kohdelähetysosoitteiden 24 oikean puoleista bittiä eivät ole uniikkeja. Siitä ei siltikään aiheudu ongelmaa, sillä NS-viestissä lähetetään mukana myös kokonainen IPv6-osoite, jota ollaan selvittämässä. Joten vaikka kahdella samassa linkissä olevalla laitteella olisikin sama solicited-node-ryhmäosoite, ainoastaan laite, jonka IPv6-osoite löytyy paketin sisältä, vastaa pyyntöön.

3.3.5 Anycast-osoitteet

Anycast-osoitteet jaetaan kohdelähetysosoiteavaruudesta ja ovat samassa formaatissa, joten niitä ei voi tunnistaa toisistaan osoitteen perusteella. Anycast-osoite ei saa olla paketin lähdeosoitteena, vaan laitteella tulee olla myös globaali kohdelähetysosoite. Tästä syystä laitteet, joille annetaan anycast-osoite, täytyy konfiguroida tunnistamaan osoite anycast-osoitteeksi.

Anycast on määritelty tavaksi, jolla lähettää paketti lähimpään verkkorajapintaan, joka kuuluu anycast-ryhmään. Lähin verkkorajapinta määräytyy reititysprotokollan metriikan mukaan.

Vaikka anycastia ehdotettiin jo vuonna 1993 osaksi Internet-protokollaa, on IPv6-anycast-osoitteita jaeuttu vain muutamia. Näihin kuuluu esimerkiksi router-subnet-anycast ja Mobile IPv6 home agent -anycast.

Anycast-osoitteiden mahdollinen tulevaisuuden käytötapa on liikennevirtojen reittien hallinta. Anycast on hyödyllinen esimerkiksi "multihomed" -verkoissa, joissa asiakkaalla on käytössään useampi Internet-palveluntarjoaja ja useampi yhteys jokaiseen niistä. Jokaiselle Internet-palveluntarjoajalle voi antaa oman anycast-osoitteen, jota käytetään kyseisen palveluntarjoajan reitittimillä. Näin kaikki asiakkaan verkosta lähetetyt paketit menevät lähimmän pisteen kautta Internetiin.

4 IPV6-OSOITTEIDEN JAKAMINEN YRITYSVERKOSSA

IPv6-osoitteita voidaan jakaa joko staattisesti tai dynaamisesti. Dynaamiseen jakoon on kaksi tapaa: DHCPv6 ja tilaton autokonfiguraatio. DHCPv6 toimii samalla tavalla kuin IPv4-verkoissa käytettävä DHCP. DHCPv6 tarvitsee käyttöjärjestelmäksi vähintään Microsoft Windows Server 2008:n (Davies, J. 2008). Tilaton autokonfiguraatio on selitetty seuraavassa luvussa. Nimipalveluun osoitteet lisätään uudella AAAA-tietueella (IPv6 Friday. 2012).

Aina kun laite saa uuden IPv6-osoitteen, se suorittaa Duplicate Address Detection (DAD) -prosessin, jolla selvitetään onko osoite uniikki paikallisessa linkissä. DAD-prosessi käyttää NS-viestiä selvittääkseen, onko samassa linkissä olevalla toisella laitteella käytössä sama IPv6-osoite. Laite lähettää NS-viestin omaan solicited-node-ryhmäosoitteeseen. Tämän viestin lähdeosoite on :: eli täsmentämätön osoite. Jos viestiin vastataan, se tarkoittaa että IPv6-osoite on jo käytössä ja pyytävän laitteen ei tulisi käyttää sitä. (Teare 2010.)

IPv6-reititin, jossa on IPv6-reititys kytkettynä päälle, voi lähettää verkon tietoja paikallisen linkin kaikille laitteille. Tietoja lähetetään joko ajoittain tai isäntäkoneen pyynnöstä. Tietoihin kuuluu linkin 64-bittinen verkon prefiksi ja oletusreitti. Isäntäkoneet voivat konfiguroida itsensä automaattisesti liittämällä IPv6-verkkorajapinnan tunnisteeseen EUI-64-muodossa linkin 64-bittiseen verkon prefiksiin. (Teare 2010.)

Tilaton autokonfiguraatio käyttää naapurin selvitystä. Naapurin selvitys toimii kaikilla IPv6-laitteilla, mukaan lukien isäntäkoneet. Selvitys alkaa lähettämällä ICMPv6 viesti tyyppiä 135 (NS) linkkiin. Viestin lähdeosoite on lähdelaitteen IPv6-osoite ja kohdeosoite on kohdelaitteen IPv6-osoitetta vastaava solicited-node-ryhmäosoite. Viesti sisältää myös lähdelaitteen siirtokerroksen osoitteen, jotta kohdelaite voi käyttää osoitetta välittömästi. (Teare 2010.)

NS-viestiin vastataan ICMPv6 viestillä tyyppiä 136, Neighbor Advertisement (NA). Tämän viestin lähdeosoite on vastaajan IPv6-osoite ja kohdeosoite on alkuperäisen lähteen IPv6-osoite. Viesti sisältää myös vastaajan siirtokerroksen osoitteen. Vastauksen jälkeen laitteet pystyvät kommunikoimaan keskenään, koska tuntevat toistensa siirtokerroksen osoitteet. (Teare 2010.)

Kun laitteet pystyvät kommunikoimaan, isäntäkone voi kysyä autokonfiguraatio tietoja. Tilaton autokonfiguraatio käyttää Router Advertisement (RA) -viestien tietoja konfiguroidakseen isäntäkoneet automaattisesti ilman ihmisen väliintuloa. RA-viestejä lähetetään ajoittain, mutta isäntäkone voi lähettää Router Solicitation (RS) -viestin käynnistyessään, ettei sen tarvitse odottaa seuraavaa RA-viestiä. Reititin vastaa välittömästi RS-viestiin RA-viestillä, joka lähetetään linkin kaikki laitteet -ryhmäosoitteeseen. (Teare 2010.)

Tilatonta autokonfiguraatiota voidaan käyttää myös laitteiden uudelleennumerointiin; koko käyttöpaikan uudelleennumerointiin tarvitsee uudelleennumeroida vain reitittimet. Tässä tapauksessa RA-viestit sisältävät sekä uuden että vanhan prefiksin. Vanhan prefiksin elinaikaa vähennetään ilmaisemaan, että isäntäkoneiden tulisi käyttää uutta prefiksiä, mutta pitäisivät auki nykyiset yhteydet, jotka käyttävät vanhaa prefiksiä. Laitteilla on kaksi kohdelähetysosoitetta kunnes vanhan prefiksin elinaika on umpeutunut. Tämän jälkeen RA-viestit sisältävät ainoastaan uuden prefiksin. (Teare 2010.)

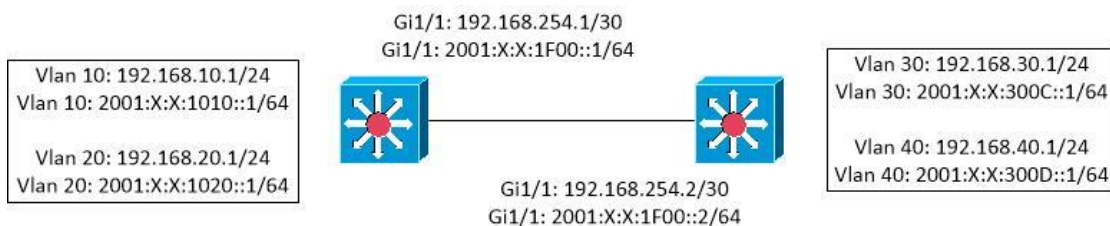
5 SIIRTYMÄVAIHEEN TEKNIIKAT

Lukujen 5 - 5.2 kaikki tieto pohjautuu D. Tearen teokseen Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide (Teare 2010).

IPv4:stä IPv6:een siirtymisessä on käytännössä kaksi päätyyliä: tuplapino ja tunnelointi. Kumpaakin suositellaan käytettävän väliaikaisena ratkaisuna. Näistä eniten käytetty tyyli on tuplapino.

5.1 Tuplapino

Tuplapinossa laite on liitetty sekä IPv4- että IPv6-verkkoon; laitteella on kaksi protokollapinoa. Nämä kaksi pinoa voivat olla laitteen yhdessä verkkorajapinnassa tai erillisissä verkkorajapinnoissa. Kuviossa 6 on esitetty esimerkki tuplapinosta, jossa kumpikin pino on samassa verkkorajapinnassa.



KUVIO 6. Tuplapinottu verkko

Tuplapinottu laite valitsee kohdeosoitteen perusteella, kumpaa pinoa tulisi käyttää. Laitteen tulisi suosia IPv6:ta. Tuplapino tulee olemaan yleisin lähestymistapa IPv6-käyttöönnotossa. Vanhat pelkästään IPv4:llä toimivat ohjelmat toimivat kuten ennenkin, kun taas uudet ja muokatut ohjelmat hyödyntävät kumpaakin pinoa. Ohjelmien tekijät voivat lisätä uuden Application Programming Interface:n (API), joka tukee IPv4- ja IPv6-osoitteita ja Domain Name System (DNS) -kyselyitä.

Tämän tekniikan huono puoli on laitteiden muistivaatimukset, kun laitteen pitää ylläpitää kahden IP protokollan reititystaulut, naapuritaulut ja kaikki muu. Lisäksi se mutkistaa hieman vianetsintää ja verkon valvomista.

5.2 Tunnelointi

Tunnelointia voidaan käyttää, kun liitetään kaksi IPv6-verkkoa IPv4-verkon yli. On olemassa monenlaisia tunneleita, joista jokainen käy erilaiseen käyttötarkoitukseen. Joissain tunnelointitekniikoissa verkkorajapinnan julkinen IPv4-osoite muunnetaan IPv6-osoitteeksi ja liitetään kyseisellä tunnelilla käytettävään prefiksiin.

Kun IPv6-liikennettä tunneloidaan IPv4-verkon yli, reunalaitteet kapseloivat IPv6-paketit IPv4-paketin sisään. Tunnelin toisessa päässä reunalaite purkaa kapseloinnin ja toisin päin. Tämä mahdollistaa erillään olevien IPv6-verkkojen yhdistämisen ilman välitysverkon muuntamista IPv6:een.

6 SAVONIAN TIETOVERKKO

6.1 IPv6-käyttöönnoton vaatimukset

Savonian tietoverkossa käytettävien laitteiden IPv6-tukea tutkittiin Ciscon sivuilta. Savonian tietoverkossa paljon käytetyt Cisco Catalyst 2960 -sarjan kytkimet tukevat IPv6:ta LAN Base -levykuvalla. Cisco Catalyst 2960-S -sarjan kytkimet tukevat oletuksena kaikkia IPv6-ominaisuuksia, mutta muut Catalyst 2960 -sarjan kytkimet tarvitsevat päivityksiä tai vaihdon uudempaan laitteeseen. (Cisco a.)

Reitittävistä laitteissa Cisco Catalyst 4500 -sarjan kytkimet tukevat IPv6:n ominaisuuksia, mutta reititystä varten tarvitaan Enterprise-tason levykuva (Cisco b). Catalyst 3560 -malli tarvitsee Advanced IP Services levykuvan reititystä varten, lisäksi vain tietyt mallit tukevat IPv6-ominaisuuksia, joten laitteen saattaa joutua vaihtamaan (Cisco c).

IPv6-osoitteiden tuki löytyy palvelimilla Microsoft Windows Server 2003 ja työpöydissä Microsoft Windows XP -käyttöjärjestelmistä (Microsoft 2005). Mikäli Savonia haluaa käyttää DHCPv6:ta osoitteiden jakamiseen, pitää palvelimissa olla vähintään Microsoft Windows Server 2008 ja työpöydissä Microsoft Windows Vista -käyttöjärjestelmät (Davies 2008).

6.2 Osoitteiden käyttö

Seuraavissa alaluvuissa käsitellään link local -osoitteiden käyttöä ja Internet-palveluntarjoajasta riippumattoman osoitevaruuden aliverkottamista.

6.2.1 Link local -osoitteet

Link local -osoitteille on ainakin kolme erilaista käyttötapaa. Ensimmäinen tapa on jättää ne dynaamisiksi, jolloin niitä ei tarvitse itse konfiguroida. Tämä tarkoittaa EUI-64-muodossa olevaa mac-osoitteesta johdettua osoitetta. Tämä saattaa silti olla paras vaihtoehto.

Toinen tapa on keksiä jokaiselle kytkimelle tunniste, joka konfiguroidaan jokaiseen IPv6-liitäntään, koska link local -osoitteiden ei tarvitse olla uniikkeja kuin yhdessä linkissä. Esimerkiksi huoneessa C-3010 olevan kytkimen link local -osoite voisi olla FE80::C:3010.

Kolmas tapa on lisätä edelliseen käyttötapaan vielä verkkorajapintakohtainen tunniste. Esimerkiksi vlan-rajapinnat olisivat paljaita numeroita (vlan 10: 0010), fastethernet-rajapinnat (fa0/10: 0f10) ja gigabitethernet-rajapinnat (gi1/1: 00b1). Myös korttipaikkoja voi yrittää ottaa mukaan, esimerkiksi Gi1/0/1 => b101. Esimerkki kokonaisuudesta osoitteesta FE80::C:3010:b101.

Jälkimmäisten tapojen huono puoli on, että osoitteet joudutaan konfiguroimaan itse laitteille ja tilatunnuksia on vain a-f.

Reititysprotokollat käyttävät link local -osoitteita, joten näiden osoitteiden tuntemisesta voi olla hyötyä vikatilanteissa.

6.2.2 Yksiköt ja aliverkot

Mikäli Savonia haluaa käyttää Internet-palveluntarjoajasta riippumatonta osoiteavaruutta, olisi /48 prefiksiä oleva osoiteavaruus sopiva. Tällaisella prefiksillä saa 16 bittiä käyttöön aliverkoille, mikä tarkoittaa 65 536 aliverkkoa. Ensimmäiset 4 bittiä eli ensimmäinen hexadesimaali voisi ilmaista yksikön; Kuopiolle, Iisalmeille ja Varkaudelle on omat /52 prefiksinsä. Tällöin osoitteet ovat helposti tunnistettavissa. Jäljelle jää vielä 13 mahdollista yksikköä. Jokaisella yksiköllä voi olla 4 096 aliverkkoa.

Yhden yksikön voisi käyttää myös videoneuvottelulaitteille. Näin niillekin olisi yksilöllinen osoitteen alkuosa.

Havainnollistetaan asiaa vielä osoitteiden avulla:

- Kuopio: 2001:X:X:1000::/52
 - Vlan 10: 2001:X:X:1010::/64
- Iisalmi: 2001:X:X:2000::/52
 - Vlan 20: 2001:X:X:2200::/64
- Varkaus: 2001:X:X:3000/52
 - Vlan 30: 2001:X:X:3003::/64

- Videoneuvottelu: 2001:X:X:F000::/64
 - Laite 1, Kuopio: 2001:X:X:F000:Y:Y:Y:Y/64
 - Laite 2, Iisalmi: 2001:X:X:F000:Z:Z:Z:Z/64

Internet-palveluntarjoajasta riippuvia osoitteita käytettäessä jokainen käyttäjä saa oman osoiteavaruuden.

6.3 Siirtymävaihe

Savonian tietoverkossa on vähän reitittäviä laitteita, joten tunnelointiin ei ole tarvetta. Koska tunnelin kummassakin päässä ainakin yhden reitittimen pitää olla tuplapinottu, jää tuplapino ainoaksi käyttökelpoiseksi siirtymävaiheen tekniikaksi. Siirtymävaiheen voi aloittaa Kuopiosta, kun IPv6-verkko toimii ja sitä osataan ylläpitää, voidaan aloittaa käyttö myös muualla.

7 YHTEENVETO

Opinnäytetyön tavoitteena oli Savonia-ammattikorkeakoulun tietoverkon IPv6-valmiuden selvittäminen. IPv6-valmiutta tutkittiin Ciscon sivuilta Savonian tietoverkossa käytettävien laitteiden osalta. Saatujen tietojen perusteella Savonian tietoverkko on IPv6-valmis, eikä sen käyttöönotto aiheuta suuria laitehankintoja tai päivityksiä. Lisäksi opinnäytetyö tarjosi ehdotuksia link local -osoitteiden ja Internet-palveluntarjoajasta riippumattoman osoiteavaruuden käyttöön, joita Savonia voi hyödyntää tarvittaessa.

LÄHTEET

CIDR Report. 2013. *CIDR RERPORT for 25 Jan 13* [WWW-sivu]. CIDR Report [viitattu 25.1.2013]. Saatavissa: <http://www.cidr-report.org/as2.0/>

Cisco a. *Cisco Catalyst 2960 and 2960-S Series Switches* [WWW-sivu]. Cisco Systems [viitattu 25.3.2013]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/qa_c67-577519.html

Cisco b. *Cisco Catalyst 4500 E-Series* [WWW-sivu]. Cisco Systems [viitattu 25.3.2013]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps4324/prod_gas0900aec806d8b06.html

Cisco c. *Cisco Catalyst 3560 Series Switches Data Sheet* [WWW-sivu]. Cisco Systems [viitattu 25.3.2013]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/product_data_sheet09186a00801f3d7d.html

Davies, J. 2008. *The Cable Guy, The DHCPv6 Protocol* [WWW-sivu]. Microsoft Technet Magazine [viitattu 25.3.2013]. Saatavissa: [http://technet.microsoft.com/fin/magazine/2007.03.cableguy\(en-us\).aspx](http://technet.microsoft.com/fin/magazine/2007.03.cableguy(en-us).aspx)

IPv6 Friday. 2012. *IPv6 and DNS – AAAA !* [WWW-sivu]. IPv6 Friday [viitattu 25.3.2013]. Saatavissa: <http://ipv6friday.org/blog/2012/01/ipv6-and-dns/>

Microsoft. 2005. *IPv6 configuration items* [WWW-sivu]. Microsoft Technet [viitattu 21.3.2013]. Saatavissa: <http://technet.microsoft.com/en-us/library/cc783049%28v=ws.10%29.aspx>

RIPE NCC. 2012. *RIPE NCC Begins to Allocate IPv4 Address Space From the Last /8* [verkköjulkaisu]. RIPE NCC [viitattu 25.1.2013]. Saatavissa: <https://www.ripe.net/internet-coordination/news/announcements/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8>

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