Jukka-Pekka Hautanen

IPv6-protokolla

Opinnäytetyö

Kevät 2012

Tekniikan yksikkö

Tietotekniikan koulutusohjelma

Seinäjoen ammattikorkeakoulu
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Koulutusohjelma: Tietotekniikan koulutusohjelma

Suuntautumisvaihtoehto: Tietoverkkotekniikat

Tekijä: Hautanen Jukka-Pekka

Työn nimi: IPv6-protokolla

Ohjaaja: Anttonen Alpo

Vuosi: 2012 Sivumäärä: 70 Liitteiden lukumäärä: 2

Tämän työn tarkoituksena on tutkia IPv6-protokollaa ja IPv6-protokollan yhteensopivuutta IPv4-protokollan kanssa. Työn alussa tarkastellaan IPv6-protokollan historiaa ja tämän hetkistä levinneisyyttä.

Työssä paneudutaan tarkemmin IPv6-protokollan pääpiirteisiin: IPv6-protokollan osoitetyypit ja niiden esitystavat, aliverkotus, IPv6-protokollan uudistetun otsikon rakenne ja uudet lisäotsikot. Edellä mainittuja pääpiirteitä verrataan tarvittaessa IPv4-protokollaan, jotta nähdään parannukset, joita uuteen protokollaan siirryttäessä on tehty.

Näiden lisäksi työssä tutkitaan IPv6-protokollan mukanaan tuomia uusia ominaisuuksia ja tärkeimpiä palveluita: autokonfiguraatio, DHCPv6, Path MTU Discovery ja Neighbor Discovery Protocol.

Työssä paneudutaan myös IPv6-protokollaa uhkaaviin tietoturvauhkiin ja miten ne ovat mahdollisesti muuttuneet protokollan vaihdoksen takia. Läpi käydään IPSec ja sitä koskevat tietoturva-lisäotsikot ja tunnelointiin liittyvät tietoturvauhat.

Tärkeänä osana työssä tutkitaan IPv6- ja IPv4-protokollan yhteiseloa ja käydään siihen liittyvät tekniikat läpi. Tekniikoista käydään läpi Dual Stack, tunnelointi ja Network Address and Protocol Translation. Näiden tekniikoiden avulla tehdään myös käytännön työ. Työn lopussa rakennetaan IPv6-protokollaa tukeva verkko ja tutkitaan sen yhteentoimivuutta IPv4-protokollan kanssa.

Avainsanat: IPv6, IPv4, Dual Stack, tunnelointi, Protocol Translation

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Information Technology

Specialisation: Information Network Technology

Author: Hautanen Jukka-Pekka

Title of thesis: IPv6-protokolla

Supervisor: Anttonen Alpo

Year: 2012 Number of pages: 70 Number of appendices: 2

The main purpose of this thesis was to study IPv6 protocol and its compatibility with IPv4 protocol in depth. Both the history and the current distribution of IPv6 protocol are presented.

The main features including: different address classes, address class representation, sub networks, new construction of IPv6 header and, additional headers are studied more profoundly and then compared with IPv4 protocol in order to see the improvements of IPv6 protocol.

Beside these new characteristics and services of IPv6 protocol other important features are studied in this thesis: autoconfiguration, DHCPv6, Path MTU Discovery and, Neighbor Discovery Protocol.

Lastly, the most critical data protection threats are examined. Data protection threats have changed in IPv6 protocol and those are compared with IPv4 protocol. IPSec, the additional headers of data protection, and different tunneling threats are examined, as well.

The most important aspect of this thesis was to study the migration of IPv6 and IPv4 protocol. Three different techniques were contemplated: Dual Stack, Tunneling and, Network Address and Protocol Translation. One of these techniques was tested in practice when IPv6 network was built and its compatibility was examined with IPv4 protocol.

Keywords: IPv6, IPv4, Dual Stack, tunneling, Protocol Translation

SISÄLTÖ

Kuvio- ja taulukkoluettelo

Käytetyt termit ja lyhenteet

802.11-laite	802.11-laite on IEEE:n standardien mukainen laite langattomille WLAN-lähiverkoille.
API	Application Programming Interface, toimii eri ohjelmien yhtymäkohtana.
ARP	Address Resolution Protocol, on Internet-protokolla, jonka avulla osoitetaan oikea IPv4-osoite oikealle MAC-osoitteelle.
CIDR	Classless Interdomain Routing, on tekniikka, jonka avulla reitittimet pystyvät luomaan ryhmäreittejä, jotta keskusreittimille ei jaettaisi niin paljoa reititysinformaatiota.
CRC	Cyclic Redundancy Check, on tarkisteavaimen luontiin tarkoitettu tiivistealgoritmi.
DAD	Duplicate Address Detection, IPv6-protokollan mekanismi, joka tarkastaa osoitteen uniikkiuden.
DHCPv6	Dynamic Host Configuration Protocol version 6, on IPv6-protokollan kanssa yhteen sopiva versio DHCP-palvelusta. Sen tehtävänä on jakaa IPv6-osoitteita verkkolaitteille.
DNS	Domain Name System, nimipalvelu, jonka tehtävänä on muuttaa verkkotunnukset IP-osoitteiksi.
FQDN	Fully Qualified Domain Name, on verkkoalueen nimi, joka sisältää myös IPv6-osoitetiedot.
HTTP	Hypertext Transfer Protocol, on verkkoprotokolla, joka on World Wide Webin datakommunikaation perusta.

IANA	Internet Assigned Numbers Authority, on organisaatio joka vastaa maailmanlaajuisesti IP-osoitteista.
ICMP	Internet Control Message Protocol, on TCP/IP-pinon kontrolliprotokolla, jolla lähetetään nopeasti viestejä koneesta toiseen.
IETF	Internet Engineering Task Force, Internetin standardeiden luonnista vastaava organisaatio.
IPSec	IP Security, protokolla, joka mahdollistaa mm. käyttäjien aidonnuksen ja verkkoliikenteen salauksen.
IPv4	Internet Protocol version 4, Internet-protokolla, jonka avulla liikennöidään Internetissä.
IPv6	Internet Protocol version 6, uudistettu Internet-protokolla, jonka avulla liikennöidään Internetissä.
IS-IS	Intermediate System to Intermediate System, on reitityksprotokolla, joka tukee IPv4-, IPv6- ja muita Internet-protokollia.
MTU	Maximum Transmission Unit, on arvo, joka ilmaisee verkon valitun reitin suurimman mahdollisen paketin koon.
NAT	Network Address Translation, IPv4-protokollassa käytetty osoitteenmuutosmekaniikka.
NAT-PT	Network Address Translation Protocol Translation, on muunnostekniikka, jonka avulla IPv6-laitteet pystyvät keskustelemaan IPv4-laitteiden kanssa.
NDP	Neighbor Discovery Protocol, on protokolla, joka määrittelee muutamia tärkeitä sisäänrakennettuja mekanismeja IPv6-protokollaan.

OSPFv3	Open Shortest Path First version 3, on IPv6-protokollan vastaava reititysprotokolla OSPFv2.
PMTUD	Path MTU Discovery, on mekaniikka, jonka avulla pystytään määrittelmään suurimman mahdollisen lähetettävän IP-paketin koko verkkolaitteiden välillä.
RFC	Requests For Comments, IETF-organisaation julkaisemia, Internetiä koskevia standardeja.
RPF	Reverse Path Forwarding, moderneissa reitittimissä käytetty tekniikka, jonka tarkoituksena on tarjota silmukaton multicast-pakettien reititys, sekä auttaa estämään IP-osoitteiden urkintaa.
SA	Security Association**,** on järjestelmä jaettuja turvallisuutta koskevia ominaisuuksia kahden verkon välillä.
TCP	Transmission Control Protocol, tietoliikenneprotokolla, jonka avulla voidaan luoda yhteys kahden isäntälaitteen välille.
UDP	User Datagram Protocol, on protokolla, jonka avulla kaksi isäntälaitetta voivat siirtää dataa keskenään ilman yhteyden luomista.

1 JOHDANTO

1.1 Työn tausta

Työn lukijalta odotetaan tuntemusta IPv4-protokollasta, joten tässä työssä ainoastaan viitataan uusiin ja paranneltuihin osioihin.

Tällä hetkellä käytössä oleva IPv4-osoiteavaruus on loppumaisillaan maailmasta. NRO:n mukaan viimeisetkin IPv4-osoitealueet on jaettu pois. Maailmanlaajuisesti osoitteista vastaa IANA, joka ilmoitti kolmas helmikuuta jakavansa loput viisi osoitealuetta AfriNIC:n, ARIN:n, APNIC:n, LACNIC:n ja RIPEN:n kesken. IPv4-protokollan mukaisia IP-osoitealueita ei ole enää jaettavaksi RIReille. IPv4-osoitteiden arvioidaan loppuvan vuoden kuluttua. (Nikulainen 2011.)

IPv6-osoiteavaruuteen siirtyminen on vääjäämätöntä ja tämän on huomannut myös Seinäjoen koulutuskuntayhtymä, jonka toimeksiannosta tämä tutkimus tehdään. IPv6 on seuraavan sukupolven Internetprotokolla, jossa on paljon suurempi IP-osoiteavaruus kuin IPv4-protokollassa. Tämä mahdollistaa tulevaisuudessa verkkojen lisääntymisen ja kasvun.

IPv6-protokollaan siirtyminen täysin vie vuosia ja sen takia tässä opinnäytetyössä tutkitaan IPv4- ja IPv6-protokollien yhteensopivuutta ja eri toimintoja näiden kahden protokollan välillä.

1.2 Työn tavoite

Työn päällimmäisenä tavoitteena on tutustua IPv6-protokollaan ja verrata sitä IPv4-protokollaan. Lähemmin tarkasteltuna tähän kuuluvat IPv6-osoitteistus, IPv6-protokollan mukanaan tuomat uudet palvelut, sekä IPv6-protokollan IPv4-yhteensopivat tekniikat.

Työssä tutustutaan kolmeen erilaiseen yhteensopivuusmenetelmään: Dual Stack, tunnelointi ja Protocol Translation. Lopullinen käytännön testaus tehdään käyttäen tunnelointitekniikkaa.

Työn lopputavoite on ymmärtää ja osata käyttää IPv6-protokollan mukanaan tuomia uudistuksia ja hallita niiden vaikutus nykyisiin verkkoihin. Näiden kolmen edellä mainitun yhteensopivuusmenetelmän lisäksi niiden käytön osaaminen IPv4- ja IPv6-verkkojen välillä.

1.3 Työn rakenne

Työn alussa käydään läpi IPv6-protkollan historia ja tämän hetkinen tilanne. IPv6-protokollan kuitenkin jo suhteellisen pitkää historiaa valotetaan jo ensimmäisten standardien luonnista nykyhetkeen saakka. Levinneisyydessä tarkastellaan IPv6-protokollaa tukevien laitteiden laajenemista, eri maanosien tilannetta IPv6-protokollan käyttöön otossa ja varsinaista implementoitujen IPv6-verkkojen määrää.

Kappaleessa kolme käydään läpi IPv6-protokollan uudistetut osoitteet ja mitä ne pitävät sisällään. Laajennetun osoiteavaruuden lisäksi tarkastellaan IPv6-protokollan mukanaan tuomia kolmea uutta osoitetyyppiä ja niiden alatyyppejä. Kappaleessa keskitytään myös uuden pitkän ja monimutkaisen osoitteen esitystavan helpottamiseen ja aliverkotukseen. Lopuksi käydään läpi IPv6-protokollaan uudistettu otsikko ja lisäotsikot.

Kappaleessa neljä käydään läpi IPv6-protokollan uudet ja tärkeimmät palvelut. Näihin palveluihin lukeutuu autokonfiguraatio, joka on yksi tärkeimmistä uuden protokollan palveluista, helpottaen osoitteistusta huomattavasti. Muita läpikäytäviä on uudistettu DHCPv6, pakettien osioitumista estävä Path MTU Discovery ja Neighbor Discovery Protocol.

Kappaleessa viisi tutustutaan erilaisiin IPv6-protokollan migraatiomenetelmiin. Näitä ovat Dual Stack, tunnelointi ja Network Address and Protocol Translation. Tunnelointi-tekniikoita on monenlaisia ja tärkeimmät niistä käydään tässä kappaleessa läpi.

Kappaleessa kuusi keskitytään IPv6-protokollan tietoturvauhkiin. Kappaleessa tutustutaan IPv6-protokollassa mukana tulleeseen IPSec-standardiin ja sen arkkitehtuuriin. Kappaleessa käydään läpi myös erilaisia hyökkäysmenetelmiä ja

miten ne ovat mahdollisesti muuttuneet IPv4-protokollan vastaavista hyökkäysmenetelmistä. Lopuksi tutkitaan vielä tunneloinnin aiheuttamia tietoturvauhkia.

Kappaleessa seitsemän keskittyy käytännön työhön. Työssä perustetaan kaksi IPv6-verkkoa ja näiden väliin IPv4-verkko. IPv6-verkot kommunikoivat keskenään tunneloimalla. Kappaleessa käydään läpi tarkka tunneloinnin konfiguroiminen ja testaus.

2 IPV6-PROTOKOLLAN HISTORIA JA LEVINNEISYYS

2.1 IPv6-protokollan historia

IPv4-protokollan osoiteavaruus huomattiin suureksi rajoittavaksi tekijäksi, Internetin kasvaessa hurjaa vauhtia, jo vuonna 1992. Vuonna 1995 IPv4-osoiteavaruudesta oli käytetty jo yksi neljäsosa ja siirryttäessä kohti 2000-lukua oli osoiteavaruuden kapasiteetista käytetty jo puolet. Internetin valtava kasvupyrähdys ei jäänyt kuitenkaan huomaamatta ja jo vuonna 1994 IETF ryhtyi kehittämään uutta Internet-protokollaa, Internet Protocol version 6. (Kaushik 2008a.)

Ensimmäiset IPv6-standardit IETF julkaisi joulukuussa 1995. Tuolloinen Deeringin ja Hindenin julkaisema RFC 1883 piti sisällään vasta muutamia parannuksia, joista tärkein oli laajennettu osoiteavaruus. Muita merkittäviä kategorioita oli yksinkertaistettu otsikko, paranneltu tuki lisäotsikoille ja vuon käsittelylle. (Deering & Hinden 1995.)

IPv6-protokollan kehittäminen ei kuitenkaan ollut helppoa. Yritysmaailmalla oli negatiivinen asenne uutta protokollaa kohtaan, koska se tiesi suuria lisäkustannuksia. Laitevalmistajille tilanne oli epämieluisa, koska he olisivat joutuneet uusimaan monia komponentteja laitteissaan. Operaattoreille tilanne oli vielä tukalampi heidän joutuessaan uusimaan koko verkon laitteet, sen lisäksi olivat vielä siitä aiheutuvat työkustannukset. (Anttila 2001, 110-111.)

Toinen IPv6-protokollan kehitystä hidastava tekijä oli uudet ja tehokkaat tavat säästää osoitteita IPv4-osoiteavaruudessa. Tärkeimpiä näistä olivat CIDR, NAT ja DHCP. CIDR:n ansioista uudet sivustot saivat käyttöönsä huomattavasti vähemmän osoitteita kuin aikaisempina vuosina. Tästäkin menetelmästä huolimatta pyynnöt uusille osoitealueille olivat kasvussa, vaikka osoitealueiden koko pienentyi CIDR:n myötä. NATin osoitteenmuutostekniikka mahdollisti monen isäntälaitteen käyttävän vain yhtä julkista osoitetta, sen sijaan, että jokaisella isäntälaitteella olisi oma kiinteä IPv4-osoite. Lisäksi DHCP mahdollisti osoitteiden

vuokraamisen isäntälaitteille tietyksi ajaksi. Näin osoitteet kiersivät aina niitä tarvitseville. (Dunmore 2005, 3-4.)

Osoitteiden säästämistoimista huolimatta IPv6-protokollan kehitys jatkui. Vuoden 1998 joulukuussa IETF julkaisi uudelleen arvioidut standardit IPv6-protokollalle. (Deering & Hinden 1998.)

Kehitystoimia nopeuttivat muutamat kokeilulliset ja käytännölliset testit, joiden tulosten pohjalta myös standardeja päiviteltiin. Kehitystä avustivat akateemiset verkot, jotka olivat valmiina tutustumaan ja kehittämään uutta teknologiaa. 2000-luvun alkupuoliskon aikana erinäisten IPv6-käyttöönottojen määrä lisääntyi niin valtavasti, että myös laite- ja ohjelmistovalmistajat ryhtyivät lisäämään IPv6-tukea tuotteisiinsa. Erityistä kiinnostusta IPv6-protokolla herätti Aasian Internet-palvelujentarjoajissa. Aasian myöhäisen Internetin vallankumouksen takia heillä on suurempi pula IPv4-osoitteista kuin länsimailla. Tämä johti siihen, että jopa osa Aasian hallituksista antoi virallisen tukensa IPv6-protokolalle. Euroopassa IPv6-protokollan käyttöönottoa vauhditti Euroopan komission Framework Programmes, joka rahoitti projekteja kuten 6NET ja Euro6IX. Näiden projektien tehtävänä oli hankkia käytännön kokemusta protokollasta. (Dunmore 2005, 3-4.)

IPv4-protokollan osoiteavaruuden oletettiin loppuvan 2000-luvun puolivälin tienoilla, mutta säästökeinojen ansioista osoitteita riitti hiukan pidemmäksi aikaa. Aasian ja Välimeren verkon informaatiopalvelukeskus sai 31. tammikuuta 2011 viimeisimmän suuren osoitealueen. Tämän jälkeen osoitteita oli jäljellä enää viisi osoitealuetta, jotka jaetaan säännön mukaisesti jokaiselle maailman viidelle alueelliselle Internet-rekisterille. Vielä tämän jälkeen muutamia osoitealueita on varattu multicast-osoitteille, mutta käytännössä katsoen kaikki osoitteet on jo jaettu. (Lawson 2011.)

2.2 IPv6-protokollan levinneisyys

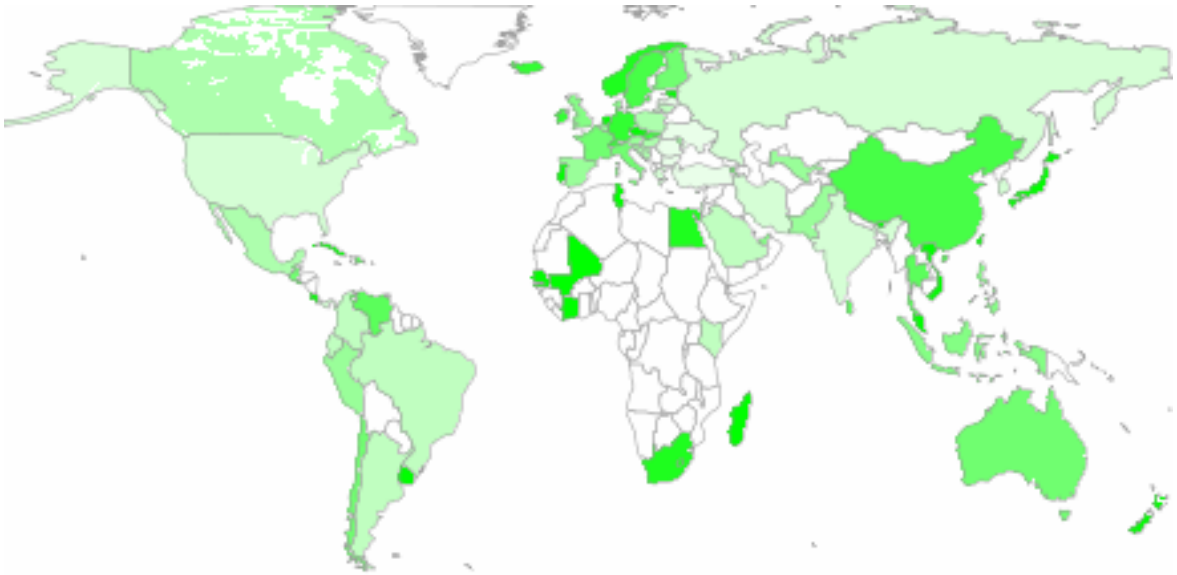
IPv6-protokollan leviäminen maailmanlaajuisesti ei ole vielä ollut merkittävää vasta hiljattain loppuneiden IPv4-osoitteiden takia. IPv6-protokollaa varten perustettiin jo vuonna 1999 IPv6 Forum -organisaatio, joka tukee IPv6-protokollan leviämistä ja

informoi sen hyödyistä. Kyseinen organisaatio myös auttaa valmistajia testaamaan tuotteidensa IPv6-valmiuksia ja jakaa sertifikaatteja testien läpäisseille tuotteille. Samoja palveluja tarjotaan myös muille IPv6-osa-alueille, kuten Internet-sivustoille. (IPv6 Forum 2008.)

Eri maanosissa IPv6-protokollan vastaanotto on ollut erilaista. IPv6-protokolla on saanut hyvän lähdön Pohjois-Amerikassa. Yhdysvaltojen hallitus on vaatinut, että kaikki verkkolaitteiden toimittajat siirtyvät tukemaan IPv6-protokollaa laitteissaan kesään 2008 mennessä. Kanadassa on pystytetty julkinen tunnelointiserveri, jonka avulla kuka tahansa IPv4-protokollan käyttäjä voi liittyä 6Bonen luomaan IPv6-verkkoon. Kanada on muodostanut pysyvän yhteyden natiivilla IPv6-protokollalla ja IPv4-tunneleiden avulla esim. Yhdysvaltojen kanssa. (Kaushik 2008b.)

Aasiassa IPv6-protokolla nauttii suurinta suosiota. Japanissa hallitus tukee suuresti IPv6-protokollan kehitystä, ja osa Internetin palveluntarjoajista on aloittanut jo IPv6-palvelujen jakamisen. Japanin suurimmat reititinvalmistajat ovat hankkineet kaikille tuotteilleen ”v6-ready” -statuksen ja monet elektroniikan valmistajat ovat aloittaneet testauksen omille laitteilleen. Kiinan hallitus on aloittanut projektin, jonka avulla se tekee aikaisen nurkanvaltauksen IPv6-maailmaan. Beijingin vuoden 2008 Olympialaisten verkkoyhteydet järjestettiin myös pelkästään IPv6-protokollaa käyttäen. Etelä-Korealla on käynnissä projekti nimeltään KOREAv6, joka tähtää IPv6-valmiuksilla varustettuihin verkkoihin eri sektoreilla, laitteiden kaupallistamisen nopeuttamiseen ja yleiseen IPv6-protokollan tietouteen. (Kaushik 2008b.)

IPv6-protokollan tukeminen Euroopassa on ollut myös merkittävää. Ranskassa perustettiin The IPv6 Task Force -organisaatio jo vuoden 2002 syyskuussa. Organisaatiolla on omat keskuksensa eri euroopan maissa, mm. Portugalissa, Espanjassa, Italiassa, Ruotsissa ja Suomessa. Organisaatio johtaa IPv6-tutkimus- ja kehitystyötä. Monet maista ovatkin jo järjestäneet sisäisiä IPv6-verkkoja tai muunlaisia palveluja, kuten IPv6-protokollalla toimivia WLANeja. (Palet 2004.)



Kuvio 1. IPv6-protokollan levinneisyys maailmalla. (BGPmon 2009a.)

Kuvio 1 havainnollistaa IPv6-protokollan levinneisyyden maailmalla. Tummempi väri tarkoittaa suurempaa levinneisyyttä. Maailmanlaajuinen levinneisyys on tällä hetkellä n. 4 % (2009) ideaalin ollessa 100 %, joten paljon on vielä tehtävää. Kuvion värityksen perusteet on tehty vertaamalla kuinka monessa autonomisessa järjestelmässä on IPv6-prefix käytössä. (BGPmon 2009b.)

Kesäkuun kahdeksas 2011 Internet Society järjesti World IPv6 Day -tapahtuman, jonka aikana monet suuret yritykset, organisaatiot ja Internet-sivustot mahdollistivat palveluidensa käytön IPv6-protokollaa käyttäen. Merkittäviä nimiä olivat mm. Cisco, Microsoft, Google, Facebook ja Youtube. Tapahtuma oli onnistunut, eikä kukaan osallistuneista organisaatiosta tehnyt valituksia IPv6-protokollan käyttöönotosta johtuneista ongelmista. IPv4- ja IPv6-protokollien yhteiselo näkyi kuitenkin piikkinä Internetin kasvaneessa liikenteessä, joka saattaa operaattoreiden mukaan tuottaa ongelmia IPv6-protokollaan käyttöön siirtymisessä. Tapahtumalla oli myös pidempiaikaisia hyötyjä, joidenkin organisaatioiden luvatessa parempaa IPv6-tukea tuotteilleen. (Dornan 2011.)

3 IPV6-PROTOKOLLAN OSOITTEET

3.1 Yleistä

IPv6-protokolla on paranneltu versio vanhasta IPv4-protokollasta. Tärkeimpänä ominaisuutena se esittelee laajennetun osoiteavaruuden. IPv4-protokollan osoiteavaruus on 2^{32} osoitetta laaja. IPv6-protokollan osoiteavaruus on 2^{128} osoitetta laaja, mikä on todella suuri harppaus vanhaan protokollaan nähden. IPv6-protokollan ansioista jokaisella maapallon maaperäiselle neliömetrille riittää n. 1500 uniikkia osoitetta. (Anttila 2001, 110-111.)

Uusi laajempi osoiteavaruus mahdollistaa uusien erityyppisten laitteiden saavan oman uniikin osoitteensa, kuten kämmentietokoneiden, matkapuhelinten ja 802.11-laitteiden. Tämän lisäksi laajennettu osoiteavaruus mahdollistaa hierarkkisen järjestelyn osoiteavaruuden sisällä. Hierarkkinen osoitteiden jakaminen mahdollistaa uudenlaisen toiminnallisuuden ja joustavuuden uuden protokollan kanssa. IPv6-protokolla mahdollistaa myös useiden osoitteiden käytön eri palveluntarjoajilta. Tämä ei ole ollenkaan yksinkertainen prosessi IPv4-protokollalla, toisin kuin IPv6-protokollassa. Tämä tekniikka mahdollistaa suuren luotettavuuden Internet-yhteydelle ja on hyödyllinen varsinkin suurille yrityksille ja organisaatioille. (Desmeules 2007, 18-20.)

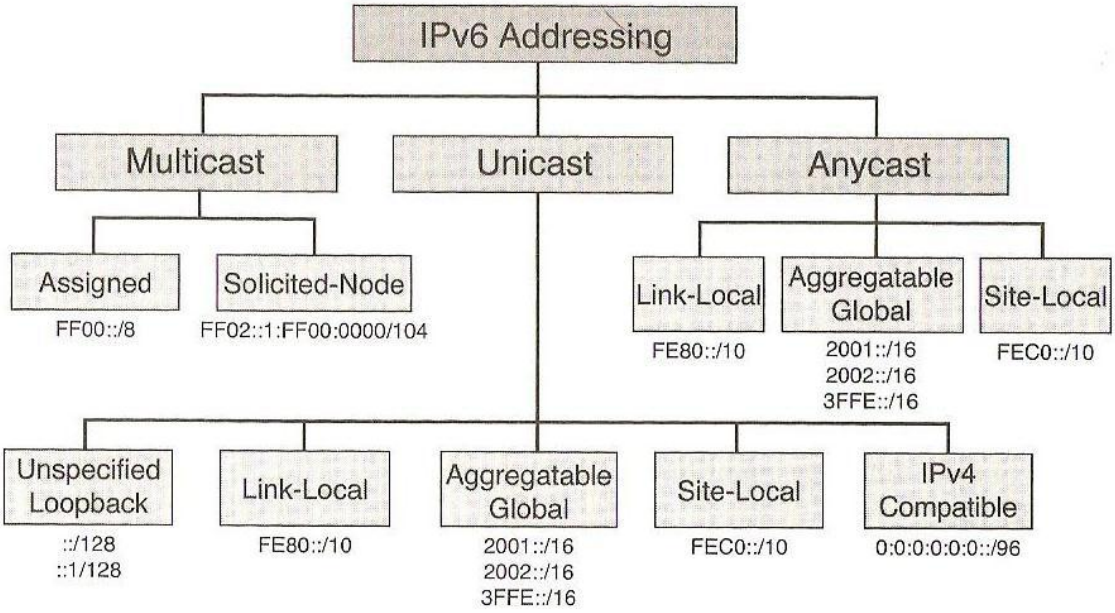
Multicast-osoite on korvannut IPv4-protokollan broadcast-osoitteen. Tästä johtuen IPv4-protokollasta tuttua ARP-taulua ei käytetä IPv6-protokollassa. ARP on korvattu erillisillä ryhmillä, jotka määritellään käyttäen multicast-osoitetta. Pakettia lähetettäessä paketti ohjautuu vain multicast-ryhmän jäsenille, eikä kaikille kuten broadcast-lähetyksissä. Broadcastiin verrattuna multicast käyttää täten verkkoa paljon tehokkaammin, kuormittaa vähemmän laitteiden CPU:ta, sekä estää erinäisiä ongelmia kuten ”broadcast stormin”. (Desmeules 2007, 24.)

3.2 IPv6-protokollan osoitetyypit

IPv6-osoitteet osoitetaan erikseen jokaiselle portille, eikä niitä osoiteta laitteille yksinään. Jokaisella portilla on monta osoitetta, esim.: aggregatable global, link-local, site-local. IPv6-osoitteet jakautuvat kolmeen eri pääryhmään, multicast-, unicast- ja anycast-osoite. Näillä jokaisella päätyypeillä on kaksi tai useampi osoitetyyppi. (Desmeules 2007, 61.)

Multicast-osoite jakautuu assigned- (FF00::/8) ja solicited-node-osoitteiksi (FF02::1:FF00:0000/104). Unicast-osoitteella on viisi erilaista alatyyppiä: Unspecified loopback (::/128, 1::/128), link-local (FE80::/10), aggregatable global (2001::/16, 2002::/16, 3FFE::/16), site-local (FEC0::/10) ja IPv4-yhteensopiva (0:0:0:0:0:0::/96). (Desmeules 2007, 61.)

Anycast-osoitteet jakautuvat kolmeen ryhmään, jotka ovat tyypiltään samanlaisia kuin unicast-osoitteen alatyypit. Anycast-osoitteet ovat: link-local (FE80::/10), aggregatable global (2001::/16, 2002::/16, 3FFE::/16), site-local (FEC0::/10). (Desmeules 2007, 61.)

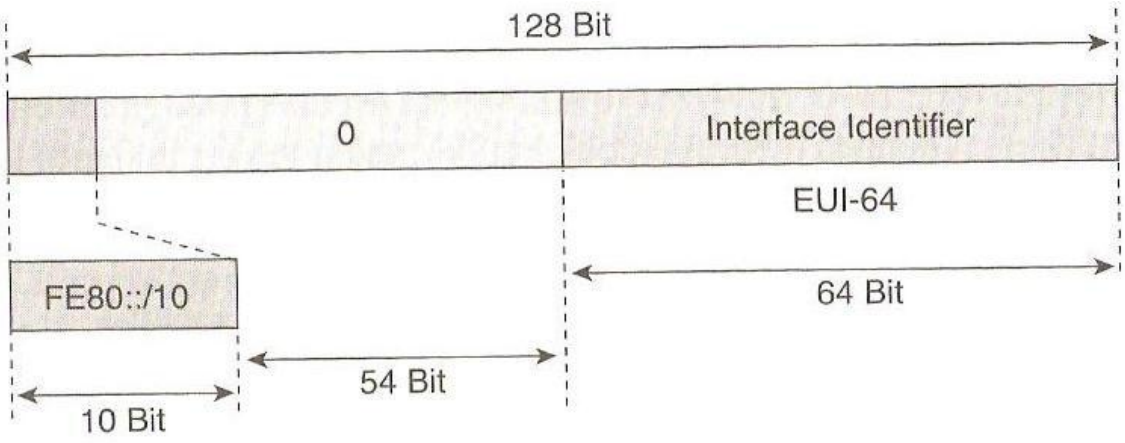


Kuvio 2. IPv6-osoiteryhmien rakenne. (Desmeules 2007, 61.)

3.2.1 Unicast-osoitteet

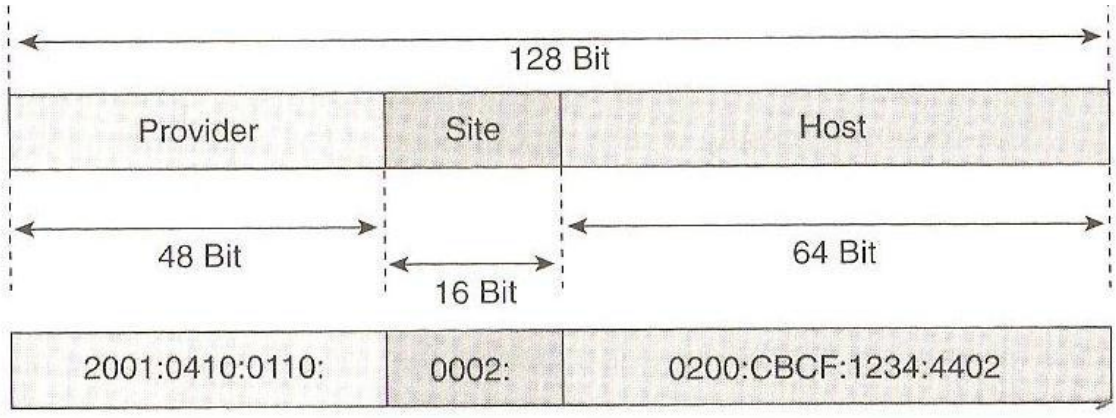
Jokaisella laitteella on IPv6-protokollassa oma loopback-osoite. Osoite on 1::/128. Unspecified-osoite on unicast-osoite, jota ei ole nimetty millekään portille. Sen osoitteen arvo on ::/128. (Desmeules 2007, 74.)

Link-local-osoite on kehitetty paikallisen linkin verkkolaitteiden välistä liikennöintiä varten. Link-local-osoitteita ei koskaan reititetä aliverkkojen välisessä liikenteessä. Monet IPv6-protokollan mekanismit käyttävät link-local-osoitetta, kuten esim. NDP-protokolla. Laitteen jokainen portti saa automaattisesti oman link-local-osoitteen, kun IPv6-protokolla otetaan käyttöön. Kuten kuviosta 3 näkyy, link-local-osoite saa FE80::/10-prefixin ja EUI-64-formaatti muodostaa osoitteen loppuosan. (Desmeules 2007, 62.)



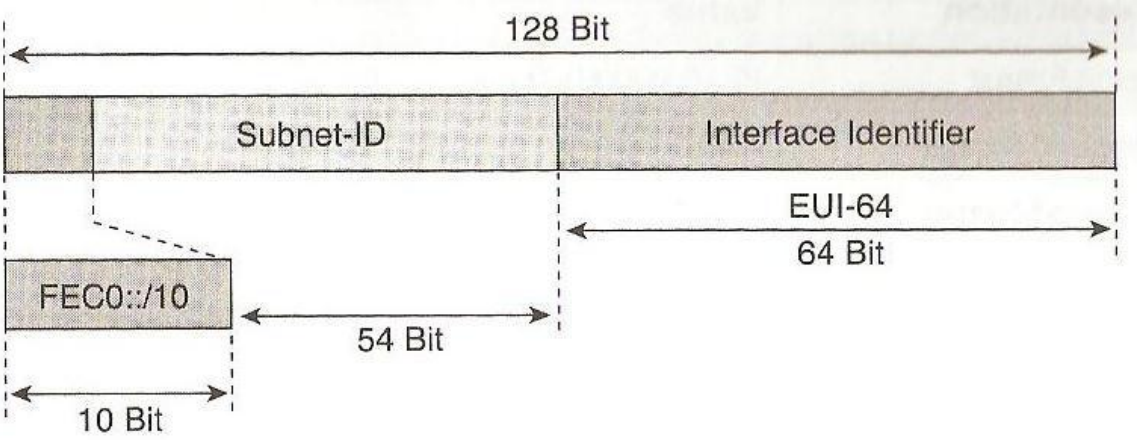
Kuvio 3. Link-local-osoitteen rakenne. (Desmeules 2007, 62.)

Aggregatable global unicast -osoite on pääosoitetyyppi IPv6-liikenteessä ja se on tärkein osa IPv6-osoitteistusarkkitehtuuria. Aggregatable global unicast -osoite on jaettu kolmeen osaan: prefixiin, joka saadaan palveluntarjoajalta; site-osan, jolla organisaatio voi luoda aliverkkoja ja host-osan, joka määrittelee verkkolaitteen portin ID-numeron. (Desmeules 2007, 65-66.)



Kuvio 4. Aggregatable global unicast -osoitteen rakenne. (Desmeules 2007, 66.)

Site-local-osoite on myös paikallisen verkon sisällä toimiva osoite. Näitä osoitteita ei jaeta automaattisesti, vaan ne joudutaan konfiguroimaan manuaalisesti. Site-local-osoitteet vastaavat IPv4-protokollan yksityisiä osoitteita (192.168.0.0/16). Site-local-osoitteita voivat käyttää organisaatiot, jotka eivät ole saaneet aggregatable global unicast -osoitteita palveluntarjoajalta. Näitäkään osoitteita ei saa reitittää Internettiin. Site-local-osoite muodostuu FEC0::/10-prefixistä, 54 bittisestä aliverkon ID:stä ja EUI-64-formaatilla luodusta loppuosasta. (Desmeules 2007, 62.)



Kuvio 5. Site-local-osoitteen rakenne. (Desmeules 2007, 64.)

Viides unicast-osoitetyyppi on IPv4-yhteensopiva osoite. Sitä käytetään tunnelointiin eli kuljettamaan IPv6-paketteja IPv4-verkossa. (Desmeules 2007, 74.)

3.2.2 Multicast-osoitteet

RFC 2373:ssa määritellään ja varataan muutama IPv6-osoite multicast käyttöön. Näitä varattuja osoitteita kutsutaan multicast assigned -osoitteiksi. Alla olevassa taulukossa määritellään varatut osoitteet. (Desmeules 2007, 70.)

Taulukko 1. Multicast-osoitteet.

Multicast-osoite	Laajuus	Tarkoitus	Kuvaus
F01::1	Verkkolaite	Kaikille verkkolaitteille	Kaikki verkkolaitteet porttien alueella
F01::2	Verkkolaite	Kaikille reitittimille	Kaikki verkkolaitteet porttien alueella
F02::1	Link-local	Kaikille verkkolaitteille	Kaikki verkkolaitteet link-local alueella
F02::2	Link-local	Kaikille reitittimille	Kaikki reitittimet link-local alueella
F05::1	Verkkoalue	Kaikille reitittimille	Kaikki reitittimet verkkoalueen alueella

Jokaista unicast- ja anycast-osoitetta kohti luodaan automaattisesti oma solicited-node multicast -osoite. Tämän osoitteen laajuus ulottuu local-link-tasolle. Osoitetta käytetään korvatessa ARP:ia ja DAD-mekanismin apuna. (Desmeules 2007, 71.)

3.2.3 Anycast-osoitteet

Anycast-osoitteen ideana on lähettää paketti lähimmälle, samaan anycast-ryhmään kuuluvalle verkkolaitteelle. Tämän takia verkon reititys on tärkeä osa anycast-mekanismia ja anycast aktivoi löytämismekanismin lähimmille laitteille. Anycast-osoitteet käyttävät osoitteita: aggregatable global unicast, site-local tai link-local. Tämän takia anycast-osoitteita ei voida erottaa normaalista unicast-osoitteesta. Anycast-osoitteita varten on varattu yksi osoite. Kyseinen osoite on nimeltään subnet-router anycast. Kaikkien IPv6-reitittimien täytyy tukea kyseistä osoitetta kaikille aliverkon portille. (Desmeules 2007, 73.)

3.3 Osoitteen esitystapa

IPv6-protokollan IP-osoitteet ovat neljä kertaa pidempiä kuin IPv4-protokollan osoitteet. Tästä johtuen ne ovat hankalia muistaa ulkoa ja sen takia IPv6-osoitteita varten on kehitetty useampi erilainen esitystapa. Nämä esitystavat on määrätty RFC 2373:ssa ja näiden eri esitystapojen avulla osoitteen muistaminen ja lukeminen helpottuu.

RFC 2373:ssa määritellään kolme erilaista esitystapaa. Suositeltu muoto on pisin muoto. Tässä muodossa osoitteesta esitetään kaikki IPv6-osoitteen kolmekymmentäkaksi hex-desimaaliarvoa. Osoite koostuu kahdeksasta 16 bitin kentästä, jotka erotellaan kaksoispisteellä. Jokainen 16 bitin kenttä esitetään neljällä hex-desimaaliarvolla. (Deering & Hinden 1998.)

Esimerkkejä:

2001:0410:0000:1234:FB00:1400:5000:45FF

3ffe:0000:0000:0000:1010:2a2a:0000:0001

FE80:0000:0000:0000:0000:0000:0000:0009

Monesti IPv6-osoitteissa on pitkä rivi nollia. Tällaisten osoitteiden kirjoittamista ja muistamista on helpotettu esitystapasäännöllä. IPv6-osoitteet, jotka sisältävät yhdessä tai useammassa peräkkäisessä 16 bitin kentässä pelkkiä nollia voidaan

lyhentää poistamalla pelkkiä nollia sisältävät kentät ja lisäämällä toiset tuplapisteet niiden tilalle. Kuitenkin vain yhdet ylimääräiset tuplapisteet ovat sallittu yhtä IPv6-osoitetta kohti. (Deering & Hinden 1998.)

Esimerkkejä:

2001:0410::1234:FB00:1400:5000:45FF

3ffe::1010:2a2a:0000:0001

FE80::0009

Toinen esitystapa koskee IPv6-osoitteita joiden 16 bitin kentän aloittaa yksi tai useampi nolla. Nämä aloittavat nollat voidaan poistaa IPv6-osoitteen yksinkertaistamiseksi. Kuitenkin jos kentän kaikki 16 bittiä ovat nollia, täytyy ainakin yksi nolla näistä säilyttää.

Esimerkkejä:

2001:410:0:1234:FB00:1400:5000:45FF

3ffe:0:0:0:1010:2a2a:0:1

FE80:0:0:0:0:0:0:9

Nämä kaksi aiempaa supistusmuotoa voidaan myös yhdistää, jotta IPv6-osoitetta voidaan yksinkertaistaa entisestään.

Esimerkkejä:

2001:410::1234:FB00:1400:5000:45FF

3ffe::1010:2a2a:0:1

FE80::9

IPv6-osoitteen kolmas esitystapa koskee IPv4-osoitteen esittämistä IPv6-osoitteessa. Ensimmäinen osio IPv6-osoitteessa käyttää hex-desimaaliarvoa ja IPv4-osa on desimaalimuodossa. Kahden tyyppisillä IPv6-osoitteilla on upotettu IPv4-osoite sisässään. Ensimmäinen niistä on IPv4-yhteensopiva IPv6-osoite. Sitä

käytetään automaattisen tunneliyhteyksien luomiseen, joiden avulla voidaan lähettää IPv6-paketteja IPv4-verkoissa. Toinen osoite on IPv4-kartoitetut IPv6-osoitteet. Nämä osoitteet ovat käytössä vain paikallisesti laitteilla, jotka käyttävät IPv4- ja IPv6-protokollapinoja, eikä niitä reititetä mihinkään. (Desmeules 2007, 58.)

Molemmat näistä osoitetyypeistä käyttävät samanlaista esitystapaa, joten osoitteiden erottamiseksi ne käyttävät erilaista prefixä. IPv4-yhteensopivassa IPv6-osoitteessa yhdeksänkymmentäkuusi ensimmäistä bittiä asetetaan nollaksi, jonka jälkeen seuraa 32-bittinen IPv4-osoite. IPv4-kartoitetut IPv6-osoitteen kahdeksankymmentä ensimmäistä bittiä asetetaan nollaksi, jonka jälkeen seuraavat 16 bittiä asetetaan ykkösiksi. Vasta näiden jälkeen tulee 32-bittinen IPv4-osoite. Myös näitä osoitemuotoja voidaan supistaa ja tehdä osoite yksinkertaisemmaksi. (Desmeules 2007, 58-59.)

Esimerkkejä:

0000:0000:0000:0000:0000:0000:206.123.31.2 tai ::206.123.31.2

0000:0000:0000:0000:0000:FFFF:206.123.31.2 tai ::FFFF:206.123.31.2

3.4 Aliverkotus

IPv4-aliverkonmaskin pystyy esittämään kahdella tapaa, desimaaliarvona ja CIDR-muodossa. IPv6-osoitteen pituuden takia ainoastaan CIDR on ainoa mahdollinen tapa esittää aliverkko. Aliverkkomaskin arvo esitetään desimaaliarvona, vaikka IPv6-osoite on hex-desimaaliarvo. (Desmeules 2007, 60.)

Verkon prefixin arvo määräytyy aliverkonmaskin biteistä, joiden arvo on yksi. Tästä ylijäävä osa jää osoitteistukseen. IPv6-protokollassa ei ole varattuja, eikä broadcast-osoitteita ja sen tarjoamat aliverkot yhdelle verkkoalueelle ovat niin suuret, ettei osoitteistussuunnitelmaa eri verkkomaskeilla tarvita. IPv6-protokollan aliverkotus on täten paljon yksinkertaisempaa kuin IPv4-protokollassa. (Desmeules 2007, 60.)

Esimerkkejä asiasta on taulukossa 2.

Taulukko 2. Aliverkot. (Desmeules 2007, 60.)

IPv6 prefix	Kuvaus
2001:310:0:1:0:0:0:45FF/128	Sisältää aliverkon vain yhdellä IPv6-osoitteella.
2001:410:0:1::/64	Verkon prefix, 2001:410:0:1::/64, pystyy antamaan osoitteen 2^{64} eri laitteelle. Tämä on vakio prefixin pituus aliverkolle.
2001:410:0::/48	Verkon prefix, 2001:410:0::/48, pystyy ymmärtämään 2^{16} 64-bittistä verkon prefixiä. Tämä on vakio prefixin pituus paikalle.

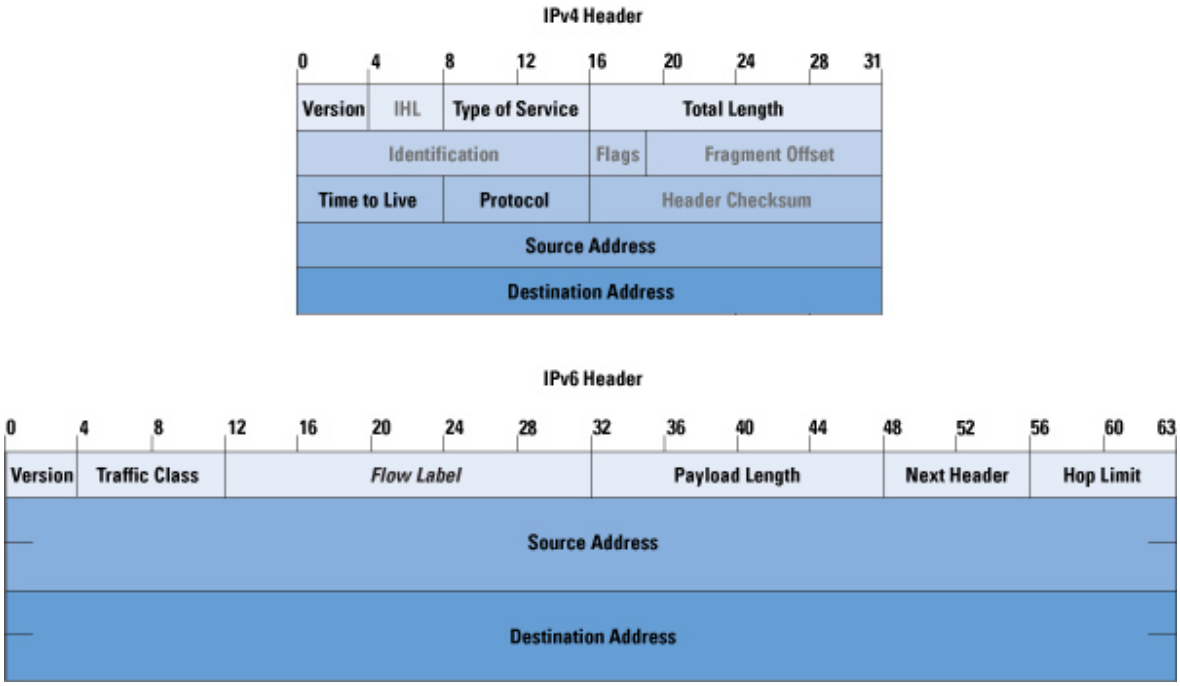
3.5 IPv6-protokollan otsikko

Seuraavassa käydään läpi IPv6-protokollan käyttämä otsikko, sen rakenne ja kentät.

3.5.1 Otsikon rakenne

IP-protokollan keskeisiä osioita ovat lähetettävät datasähkeet, eli otsikot ja siihen liittyvät mekanismit, kuten pakettien osioituminen. Uuden protokollan otsikkoa on yksinkertaistettu IPv4-otsikkoon nähden, paremman suorituskyvyn mahdollistamiseksi. Uuden otsikon kehityksen ideana on ollut pitää otsikko mahdollisimman yksinkertaisena, sekä otsikon koko vakiona. IPv4-protokollan otsikossa on 12 erilaista kenttää, mukaan lukien muutamia valinnaiset kentät, joiden käyttö johtaa vaihtelevaan otsikon kokoon. IPv6-otsikossa on vain 8 kenttää ja niiden yhteiskoko on 40 tavua (320 bittiä), kun taas IPv4-otsikoiden yhteiskoko

on vain 20 tavua (160 bittiä). IPv6-otsikkoon on jätetty vain kaikki tärkeimmät kentät, muut kentät on muutettu valinnaisiksi lisäotsikoiksi. (Dunmore 2005, 7.)



Kuvio 6. IPv6- ja IPv4-otsikot. (Cisco [viitattu 16.09.2011].)

3.5.2 IPv4-otsikkokentät

Ensimmäinen IPv4-otsikon kenttä on versiokenttä (Version, 4 bittiä). Tämä kenttä ilmaisee mikä IP-protokollan versio on käytössä. Tieto on oleellinen kaikille liikennöiville laitteille, sillä tämän avulla laitteet osaavat tulkita saapuvat IP-paketit oikein. Erityisesti Dual Stackia käyttävissä laitteissa tämä on oleellinen tieto. (Anttila 2001, 116.)

Otsikon pituus -kenttä (IHL, 4 bittiä) on toinen kenttä IPv4-otsikossa. Tämä kenttä puuttuu kokonaan IPv6-otsikosta, koska otsikot ovat vakiomittaisia, mutta sisältyy oleellisena osana IPv4-otsikkoon. Kenttä määrittelee kuinka pitkä IP-paketin otsikkokenttä on. Tämän kentän avulla liikennöivä laite tietää, mistä varsinainen dataosuus alkaa. Kentän arvo saadaan laskemalla otsikon pituus ja jakamalla se

luvulla 32. Laskutoimituksen tulos kertoo montako 32 bitin jaksoa otsikossa on. (Anttila 2001, 116.)

Palvelun tyyppi -kenttä (Type of Service, 8 bittiä) kertoo miten pakettia tulisi välittää verkossa. Kenttä jakautuu kolmeen erilaiseen osioon. Ensimmäinen sisältää prioriteetti-kentän, jolla ohjataan perusliikennettä. Seuraava osio sisältää neljä bittiä, jotka määrittelevät minkälaista palvelua halutaan verkolta. Kolmas osa sisältää yhden varatun bitin. (Anttila 2001, 117.)

Paketin koko -kenttä (Total Length, 16 bittiä) kertoo, miten suuri IP-paketin koko on. Maksimissaan kentän arvo voi olla 2^{16}, joka ilmaistaan okteteissa. Normaalisti paketin koko on kuitenkin paljon pienempi ja osalle verkkolaitteista noin suuri koko on hankala käsitellä. Standardeissa on määritelty, että verkkolaitteen tulee pystyä vastaanottamaan IP-paketti, joka on kooltaan 576 oktettia pitkä. (Anttila 2001, 117.)

Yksilöllinen tunniste -kenttä (Identification, 16 bittiä) pitää sisällään yksilöllisen ID-numeron. Paketteja joudutaan joskus osioimaan matkan varrella ja tällöin ID-numero on tärkeässä roolissa. Vastaanottava verkkolaite pystyy määrittelemään sen avulla, mitkä osiot kuuluvat mihinkin pakettiin. (Anttila 2001, 117.)

Seuraava kenttä IPv4-otsikossa on osioimisen määrittely (Flags, 3 bittiä). Kentälle on varattu kolme bittiä, joista ensimmäinen on aina nolla. Seuraava bitti määrää, saako IP-pakettia osioida. Kolmas bitti määrittelee tuleeko tämän osion jälkeen vielä muita osioita. (Anttila 2001, 117.)

Osioiden sijainti -kenttä (Fragment Offset, 13 bittiä) osoittaa, mikä on osion sijainti paketissa. Kentän arvo ilmaistaan 64 bitin jaksoissa. (Anttila 2001, 118.)

Paketin elinaika -kenttä (Time to Live, 8 bittiä) määrittelee miten pitkään paketti voi liikkua Internetissä. Kentän arvosta voidaan lukea, monenko reitittimen kautta paketti saa kulkea matkansa aikana. IANA suosittelee kentän arvoksi 64, mutta sitä voidaan säätää myös ohjelmallisesti. Kenttä toimii siten, että jokainen matkan varrella oleva reititin vähentää lukua yhdellä. Kentän mennessä jonkin reitittimen kohdalla nollaan, on kyseisen reitittimen tehtävänä tuhota paketti ja ilmoittaa siitä ICMP-sanomalla alkuperäisen viestin lähettäjälle. (Anttila 2001, 118.)

Protokollanumero-kenttä (Protocol, 8 bittiä) ilmoittaa seuraavan kerroksen protokollan IP-paketille. Useimmiten käytetyt arvot ovat 1, 2, 6 ja 17 eli ICMP-, IGMP-, TCP- ja UDP-protokollat. (Anttila 2001, 119.)

Tarkistussumma-kenttällä (Header Checksum, 16 bittiä) varmistetaan etteivät IP-otsikkokentän tiedot ole muuttuneet siirron aikana. Tämä kenttä tarkistetaan jokaisen siirtotien varrella olevassa reitittimessä. (Anttila 2001, 120.)

Lähettäjän IP-osoite-kenttään (Source IP Address, 32 bittiä) lähettäjä merkitsee oman IP-osoitteensa. Lähes kaikissa tapauksissa tässä kentässä lukisi lähettäjän verkkokortin primäärinen IP-osoite. Joissain tapauksissa osoite voi olla erikin, esim. verkkolaitteen pyytäessä IP-osoitetta DHCP-palvelimelta osoitekentän arvo on 0.0.0.0. (Anttila 2001, 120.)

Vastaanottajan IP-osoite-kenttään (Destination IP Address, 32 bittiä) merkitään vastaanottavan verkkolaitteen IP-osoite. Päätös siitä, mille reitittimelle matkalla oleva paketti pitäisi lähettää tehdään tämän kentän avulla. (Anttila 2001, 120.)

Optiot-kenttä (Options, korkeintaan 320 bittiä) on valinnainen, eikä siksi esiinny kuviossa 6. Kenttä on varattu erilaisille määrittelyille, jotka voivat liittyä turvallisuuteen ja pakettien reitittämiseen. Optiot ovatkin käytössä vain erityistapauksissa, kuten esim. halutaan ongelmatilanteessa selvittää, ovatko kaikki verkkolaitteet toiminnassa. (Anttila 2001, 126.)

3.5.3 IPv6-otsikkokentät

IPv6-otsikon ensimmäinen kenttä on myös versio (Version, 4 bittiä). Kentässä määritetään käytettävän protokollan numero, joka IPv6-protokollaa käytettäessä on 6. (Hagen 2006, 19.)

Toinen kenttä on liikenneluokka-kenttä (Traffic Class, 8 bittiä). Kenttä on uusi ja se korvaa IPv4-otsikossa olevan palvelun tyyppi -kentän. Kentän tarkoituksena on helpottaa reaaliaikaisen ja muiden erikoiskäsittelyä vaativien datojen käsittelyä. Kentän avulla voidaan määritellä IP-paketeille prioriteettejä. (Hagen 2006, 19.)

Vuon tunnus -kentän (Flow Label, 20 bittiä) ideana on erotella paketit, jotka vaativat samanlaista kohtelua. Paketit erotellaan labeleilla, eli lipuilla. Tämän ansioista reitittimet voivat tunnistaa samoja lippuja käyttävät paketit ja käsitellä niitä niiden vaatimalla tavalla, ilman että reitittimet joutuvat käymään kaikki pakettien otsikot yksitellen läpi. Tämän tarkoituksena on nopeuttaa liikennettä. Kentän arvo on uniikki ja se muodostuu lipun arvosta ja lähettävän laitteen osoitteesta. Verkkolaitteet, jotka eivät tue vuon tunnus -kenttää reitittävät paketit normaalisti, muuttamatta vuon tunnus -kentän arvoa ja jättäen sen vain huomiotta. Kaikilla saman vuon IP-paketeilla täytyy olla sama lähettäjän ja vastaanottajan IP-osoite. (Hagen 2006, 19-20.)

Kuorman pituus -kenttä (Payload Length, 14 bittiä) määrittelee otsikon jälkeen tulevan datan pituuden. Kenttä eroaa IPv4-otsikon paketin koko -kentästä. Paketin koko -kenttä ottaa huomioon myös IPv4-otsikon pituuden, kun taas kuorman pituus -kenttä laskee vain IPv6-otsikkoa seuraavan datan pituuden. Lisäotsikot lasketaan osaksi kuormaa ja ovat siksi osa datan pituutta. Paketin maksimikuorma on enimmillään 64 kB, mutta paketeille, jotka ylittävät tuon rajan voidaan käyttää Jumbogram-lisäotsikkoa. Kyseinen lisäotsikko tukee suurempia pakettien kokoja tarvittaessa. (Hagen 2006, 20.)

Seuraava otsikko -kenttä (Next Header, 8 bittiä) määrittelee, minkä tyyppinen on seuraavaksi tuleva otsikko. IPv4-otsikossa protokollanumero-kenttä vastaa tätä kenttää. Seuraava otsikko -kenttä käyttää UDP- ja TCP-otsikoille samaa protokollanumeroa kuin IPv4-otsikon kentässä. Lisäotsikoille on kuitenkin omat numeronsa ja jos ne ovat käytössä, niin niiden tyyppi ilmaistaan tässä kentässä. Seuraava taulukko esittelee listan mahdollisista arvoista seuraava otsikko -kentässä. (Hagen 2006, 20.)

Taulukko 3. Seuraava otsikko -kentän mahdolliset arvot. (Hagen 2006, 20-21.)

Seuraava otsikko -kentän mahdolliset arvot	
0	Hop-by-Hop Option Header following
1	Internet Control Message Protocol (ICMPv4)

2	Internet Group Management Protocol (IGMPv4)
4	IP in IP (encapsulation)
6	TCP
8	Exterior Gateway Protocol (EGP)
9	IGP
17	UDP
41	IPv6
43	Routing header
44	Fragmentation header
45	Interdomain Routing Protocol (IDRP)
46	Resource Reservation Protocol (RSVP)
50	Encrypted Security Payload header
51	Authentication header
58	ICMPv6
59	No Next Header for IPv6
60	Destination Options header
88	EIGRP
89	OSPF
108	IP Payload Compression Protocol
115	Layer 2 Tunneling Protocol (L2TP)

132	Stream Control Transmission Protocol (SCTP)
134-254	Unassigned
255	Reserved

Hyppyjen määrä -kenttä (Hop Limit, 8 bittiä) määrittelee, kuinka monen reitittimen läpi paketti voi kulkea ennen kuin se tuhotaan. IPv4-otsikossa oleva paketin elinaika -kenttä toimii samalla tavalla. IPv6-otsikossa kenttä uudelleen nimettiin hyppyjen määräksi, jotta se kuvastaa paremmin kentän toimintaa. Paketin elinaika -kentän arvo oli periaatteessa sekunteja ja reitittimet käsittelivät sen hyppyjen määränä. Hyppyjen määrä -kentän arvo vastaa nyt täysin hyppyjen määrää. Reitittimet vähentävät kentän arvoa aina yhdellä käsitellessään paketin ja tuhoavat sen, jos paketti saa arvon nolla. (Hagen 2006, 21.)

Lähettäjän IP-osoite-kenttään (Source Address, 128 bittiä) merkitään lähettäjän IP-osoite (Hagen 2006, 22).

Vastaanottajan IP-osoite-kentässä (Destination Address, 128 bittiä) on vastaanottajan IP-osoite. IPv4-otsikossa kentässä on aina lopullisen paketin saajan osoite, mutta IPv6-otsikossa kentässä ei välttämättä ole. Tämä erityistapaus on käytössä silloin, kun routing-lisäotsikko on käytössä. (Hagen 2006, 22.)

3.5.4 IPv6-otsikkoon siirtyessä poistetut IPv4-otsikkokentät

Aiemmissa väliotsikoissa on tarkasteltu muutoksen läpi käyneitä IPv4-otsikoita. Tässä kappaleessa keskitytään vielä lähemmin tarkastelemaan, mitkä IPv4-otsikkokentät on poistettu kokonaan ja miksi. Poistetut kentät näkyvät kuviossa 3 harmaana.

Otsikon pituus -kenttää ei IPv6-otsikossa tarvita, koska otsikot ovat aina 40 oktettia pitkiä. Otsikon pituus -kenttä ilmaisee paketin kokonaispituuden mukaan luettuna optiot-kentän. IPv6-otsikoissa optiot-kenttä on korvattu kokonaan eri

tavalla toimivilla lisäotsikoilla. Tämä tekee otsikon pituus -kentästä hyödyttömän IPv6-otsikossa. (Desmeules 2007, 43.)

IPv6-otsikosta on poistettu IPv4-otsikon koko toinen rivin, joka on suunniteltu pakettien osioimista varten. Siihen kuuluvat kentät: yksilöllinen tunniste, osioimisen määrittely ja osioiden sijainti. IPv6-otsikoissa mahdollinen osiointi hoidetaan paketin lähettävällä verkkolaitteella, eikä sitä hoideta enää verkon välissä olevilla reitittimillä. Poistamalla osioimis-kentät pystytään vähentämään reitittimien CPU:n kuormitusta. IPv6-protokollassa estetään osioimista PMTUD-mekanismia käyttäen. (Desmeules 2007, 44.)

Tarkistussumma-kenttä on tarpeeton, koska alemman tason siirtoyhteyskerroksella on omat tarkistussummansa ja virheen ehkäisymenetelmänsä. Siirtoyhteyskerroksella on hyvä luotettavuus ja ylemmän tason protokollilla, kuten UDP:llä ja TCP:llä on omat tarkistussummansa. Lisäksi IPv6-protokollaan on tullut UDP:lle oma pakollinen tarkistussumma. Tämän takia tarkistussumma-kenttä on tarpeeton ja sen poistamisella säästetään yksi uudelleenlaskemisprosessi, joka jouduttaisiin aina tekemään kun paketti kulkeutuu uuden reitittimen läpi. (Desmeules 2007, 44.)

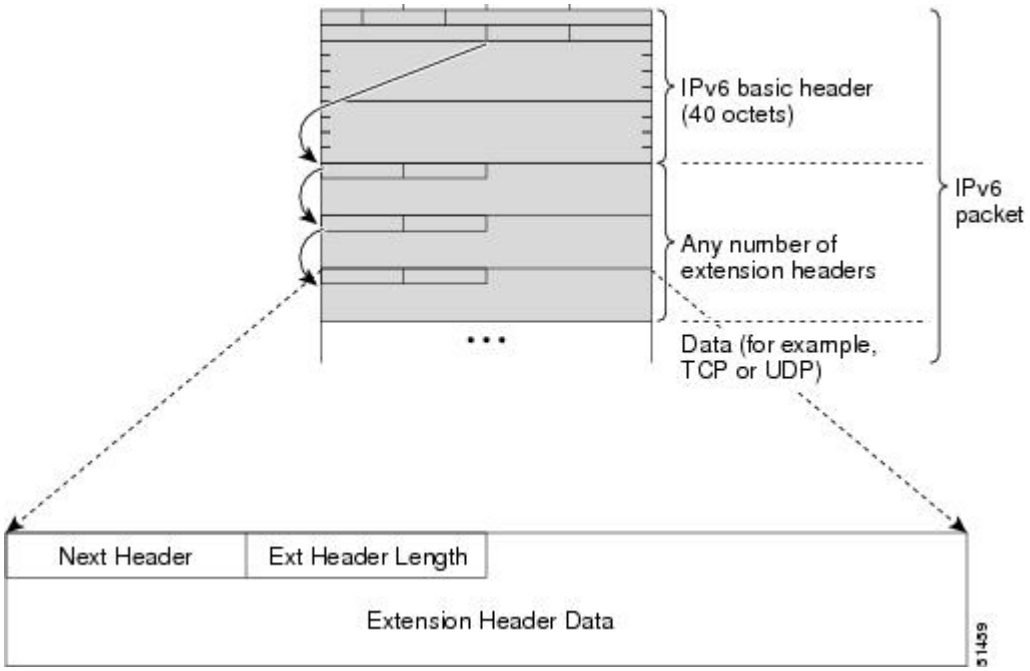
Optiot-kenttää on muutettu radikaalisti IPv6-otsikossa. Käytännössä katsoen optiot-kenttä on poistettu ja tilalle tuotu lisäotsikot hoitamaan samoja tehtäviä kuin optiot-kenttä. Optiot-kentän poistumisen myötä IPv6-otsikko yksinkertaistuu, kun pituus on aina vakio, 40 oktettia. Tämän takia verkon reitittimien prosessointityö pienenee pakettien kulkiessa reitittimen läpi, koska erillistä laskentaa paketin pituudelle ei tarvitse suorittaa. (Desmeules 2007, 44.)

3.5.5 Lisäotsikot

IPv4-otsikkoon voidaan myös määritellä lisäotsikoiden tapaisia optioita, kuten tietoturvaominaisuuksia, lähettäjän määrittelemä reitti ja aikaleimat. Lisäoptioitten huono puoli IPv4-otsikoissa on niiden aiheuttama suorituskyvyn lasku. IPv6-otsikossa nämä optiot on mietitty kokonaan uudestaan ja niistä on tullut erillisiä

lisäotsikoita, eivätkä ne vaikuta pääotsikon kokoon. Tämän erottelun takia yksinkertaisemman otsikon suorituskyky on parempi. (Hagen 2006, 22-23.)

IPv6-protokollassa seuraava otsikko -kenttä määrittelee ovatko lisäotsikot käytössä. Lisäotsikoiden ollessa käytössä ne sijoittuvat pääotsikon jälkeen ja ketjuutuvat peräkkäin, jos useampi kuin yksi lisäotsikko on käytössä. Otsikoiden jälkeen tulee vasta varsinainen data. Peräkkäisten lisäotsikoiden määrää ei ole mitenkään rajattu, ja jokainen lisäotsikko määrittelee myös seuraavaksi tulevan lisäotsikon. Lisäotsikot täytyy käsitellä samassa järjestyksessä, kuin ne ovat IPv6-paketin otsikon jäljessä. Jokainen lisäotsikko on kahdeksan oktettia pitkä ja tämän vakiopituuden ansioista peräkkäiset otsikot pystytään aina kohdistamaan. (Hagen 2006, 23.)



Kuvio 7. Lisäotsikot. (Cisco [viitattu 26.09.2011].)

Reitittimet eivät tarkista erikseen jokaista lisäotsikkoa, vaan ainoastaan vastaanottavan päätelaite tutkii lisäotsikot, eli päätelaite jolla on sama osoite kuin vastaanottajan osoite IPv6-otsikossa. Multicast-osoitteen tapauksessa kaikki multicast-ryhmän jäsenet tutkivat lisäotsikot. Kuitenkin, jos lisäotsikko on hop-by-hop options -otsikko, käyvät kaikki matkan varrella olevat laitteet kyseisen lisäotsikon läpi. (Hagen 2006, 23.)

Seuraava otsikko -kentän arvo voi tuottaa joillekkin verkkolaitteille ongelmia jossain tapauksissa. Jos verkkolaite ei pysty tunnistamaan kyseistä lisäotsikkoa, tämä tuhoaa paketin ja lähettää ICMPv6-ongelmaviestin takaisin paketin lähettäjälle. (Hagen 2006, 24.)

RFC 2460 on määritelty järjestys, jota lisäotsikkoketjujen tulisi käyttää. (Deering & Hinden 1995.)

Taulukko 4. Lisäotsikoiden suositeltu järjestys.

Lisäotsikoiden suositeltu järjestys	
1.	IPv6 -otsikko
2.	Hop-by-Hop Options -otsikko
3.	Destination Options -otsikko
4.	Routing -otsikko
5.	Fragment -otsikko
6.	Authentication -otsikko
7.	Encapsulating Security Payload -otsikko
8.	Destination Options -otsikko
9.	Upper-Layer -otsikko

4 IPV6-PROTOKOLLAN UUDET PALVELUT

4.1 Autokonfiguraatio

Autokonfiguraatio on täysin uusi ja todella hyödyllinen ominaisuus IPv6-protokollassa. Ominaisuus suunniteltiin, ettei jokaiseen verkkolaitteeseen tarvitse manuaalisesti konfiguroida verkko-osoitteita, ennen kuin ne pääsevät verkkoon. Autkonfiguraatio onkin IPv6-protokollan tärkeimpiä ominaisuuksia, varsinkin kun uusia erilaisia verkkoon liitettäviä laitteita ilmestyy tiuhaan tahtiin, TV:stä ja jääkaapeista lähtien. Suuretkaan verkot eivät välttämättä tarvitse erillistä DHCP-palvelinta vaan pärjäävät autokonfiguraatiolla. (Hagen 2006, 87.)

IPv6-protokollassa on kahdentyyppisiä autokonfiguraatiotiloja, tilaton ja tilallinen autokonfiguraatio. Tilallinen autokonfiguraatio vastaa IPv4-protokollan DHCP:tä. Tilaton autkonfiguraatio on uusi ominaisuus, joka luo uniikin osoitteen verkkolaitteelle käyttäen sen omaa MAC-osoitetta ja reitittimeltä saatavaa tietoa. MAC-osoite muunnetaan käyttäen EUI-64-formaattia ja yhdistetään reitittimen tietoihin. Näin isäntälaite saa täysin uniikin IPv6-osoitteen helposti. Tilatonta ja tilallista autokonfiguraatiota voi käyttää myös yhdessä. Tällöin isäntälaite voi käyttää tilatonta autokonfiguraatiota IPv6-osoittteen luontiin ja tilallista toisille parametreille. (Hagen 2006, 87.)

IPv6-osoitteella on kolme erilaista tilaa. Pohjustava osoite (Tentative Address) on osoite, jota ei ole vielä vahvistettu. Osoite on käytössä sen aikaa, kun osoitteen uniikkiutta tarkistetaan. Suositeltu osoite (Preferred Address) on osoite, joka on jo vahvistettu uniikiksi. Osoitetta voidaan käyttää laitteen portissa ilman mitään rajoitteita. Tuomittu osoite (Deprecated Address) on osoite, jonka käyttöä ei suositella, mutta sitä ei ole myöskään kielletty. Tuomittu osoite voi olla osoite, jonka elinikä on pian päättymässä. Kyseistä osoitetta voidaan käyttää vielä palveluissa, jotka katkeaisivat osoitteen vaihdossa, mutta sitä ei enää käytetä uusien yhteyksien lähdeosoitteena. (Hagen 2006, 87-88.)

Kun verkkolaite konfiguroidaan, se käy läpi viisi erilaista toimenpidettä. Ensimmäiseksi luodaan link-local-osoite käyttäen link-localin omaa prefixiä (FE80) ja asetetaan se laitteelle. Luotu osoite on pohjustava osoite. (Hagen 2006, 88.)

Seuraavassa vaiheessa laite liittyy kahteen multicast-ryhmään. Kaikki liittyvät multicast-ryhmään FF02::1 ja pohjustaville osoitteille luotuun ryhmään. Kolmannessa vaiheessa DAD-mekanismi tarkistaa onko osoite jo käytössä vai voiko sen ottaa käyttöön, jonka jälkeen mekanismi muuttaa osoitteen tilan suositelluksi osoitteeksi. (Hagen 2006, 88.)

Neljäs vaihe koskee ainoastaan isäntälaitteita. Isäntälaite lähettää Router Solicitation -viestin multicast-viestinä kaikille reitittimille, jotta se saa selville reitittimen jakaman prefixin. Viimeisessä vaiheessa kaikki reitittimet vastaavat Router Advertisement -viestillä. Jokaista vastaanotettua prefixiä kohden luodaan yksi osoite käyttäen prefixiä ja verkkolaitteen MAC-osoitetta. Sen jälkeen nämä osoitteet lisätään kyseiselle portille. (Hagen 2006, 88.)

Reitittimien uudelleen numeroiminen on helppoa, koska ainoastaan prefix täytyy vaihtaa. Uudelleen numeroidun reitittimen kaikki isäntälaitteet vaihtavat oman prefixinsä uuteen käyttäen autokonfiguraatiota. Reitittimen ulottumattomissa olevat isäntälaitteet luovat itselleen link-local-osoitteen. (Hagen 2006, 88.)

4.2 DHCPv6

DHCPv6 on pääpiirteittään samankaltainen DHCPv4 kanssa, mutta se tuo kuitenkin muutamia parannuksia vanhaan versioon nähden. DHCPv6:n päätehtäviin kuuluu osoitteiden jakaminen, prefixien delegointi ja tilattomat palvelut. (Qin, Tatuya & Keiichi 2007, 291.)

Osoitteiden jakaminen ei ole yhtä tärkeää kuin IPv4-protokollassa autokonfiguraation ominaisuuksien takia, mutta silti suuret verkot tarvitsevat tätä palvelua. Erona DHCPv4 verraten on, ettei DHCPv6 jaa oletusreitittimen tai prefixien pituuden tietoja jakaessaan osoitteita. Muut mekanismit hoitavat näitä palveluita. (Qin, Tatuya & Keiichi 2007, 292-293.)

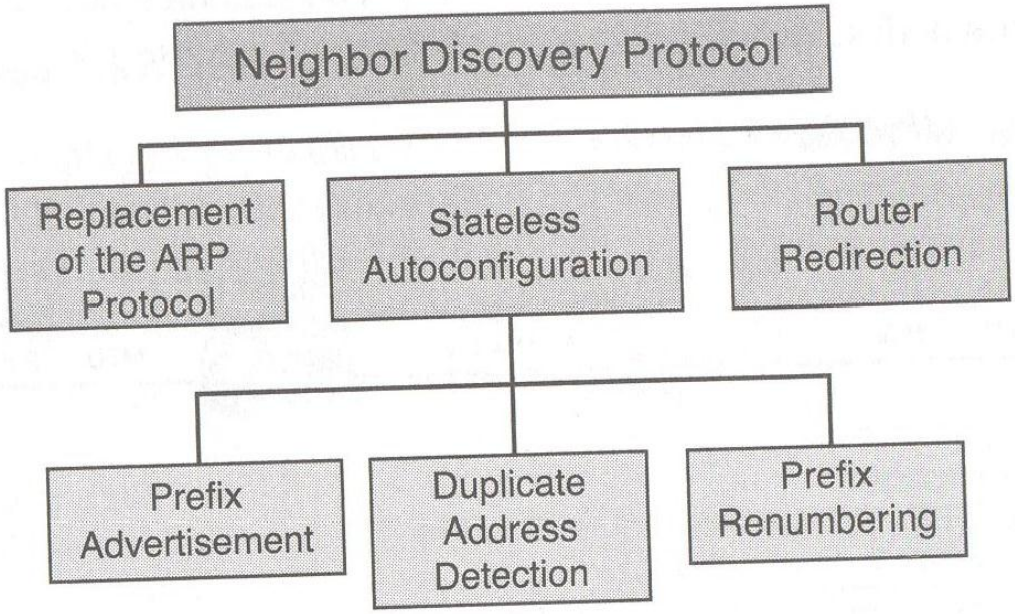
DHCPv6 pystyy hoitamaan prefixien delegointia palveluntarjoajalta asiakkaan alueelle. Tilattomien palveluiden avulla voidaan esim. jakaa nimipalvelimien osoitteita ja muuta konfiguraatiotietoa. Nimipalvelujen jakamiseen voidaan kuitenkin käyttää myös muita mekanismeja. (Qin, Tatuya & Keiichi 2007, 292-293.)

4.3 Path MTU Discovery

Reitittimet eivät osioi paketteja IPv6-protokollassa, vaan lähettäjä hoitaa sen tehtävän. PMTUD varmistaa, että paketti lähetetään käyttäen suurinta mahdollista kokoa, jota valittu reitti tukee. Jos paketin koko on suurempi kuin reitin jokin laite pystyy käsittelemään, lähetetään takaisin ICMPv6-viesti ja pakettia yritetään tämän jälkeen lähettää pienempää MTU-kokoa käyttäen. Tämä prosessi voi tapahtua reitin varrella useammin kuin kerran, mutta paketin MTU-koko ei voi ikinä laskea alle IPv6-protokollan minimirajan, 1280 bittiä. Tämän mekanismin avulla saadaan säästettyä arvokasta prosessointiaikaa osioiduilta paketeilta. (Hagen 2006, 92.)

4.4 Neighbor Discovery Protocol

NDP on yksi tärkeimmistä protokollista IPv6-protokollassa. Sillä on kolme tärkeää päätehtävää ja niistä ensimmäinen on ARP-taulun korvaaminen. IPv6-protokolla tarjoaa uuden tavan paikallisen linkin osoitteiden määrittelemiseen ARP-taulun tilalle. Uudessa mekaniikassa käytetään ICMPv6-viestejä ja multicast-osoitteita ARP-taulun korvaamiseksi. Tilaton autokonfiguraatio on toinen NDP:n ominaisuuksista. Tilattoman autokonfiguraation avulla laitteet pystyvät määrittelemään itsellensä osoitteen käyttäen ICMPv6-viestejä ja multicast-osoitteita. DAD-mekanismi tarkistaa konfiguroidun osoitteen uniikkiuden, eli ettei osoitetta ole jo jollain muulla verkkolaitteella käytössä. Kolmas ominaisuus on Router Redirection. Mekanismin avulla reititin lähettää ICMPv6-viestin, jolla se kertoo IPv6-protokollaa käyttävälle verkkolaitteelle paremmasta reitistä määränpäähän. (Desmeules 2007, 105.)



Kuvio 8. Neighbor Discovery Protocol (Desmeules 2007, 106.)

5 IPV6-PROTOKOLLAN MIGRAATIOTEKNIIKAT

5.1 Yleistä

IPv6-protokolla on alusta asti suunniteltu toimivaan yhteensopivasti IPv4-protokollan kanssa, sillä siirtyminen täysin IPv6-protokollan käyttöön vie vuosia. Tästä johtuen on kehitetty erilaisia tekniikoita, joilla siirtyminen uuden protokollan käyttöön helpottuu. Nämä tekniikat ovat jaettu kolmeen eri kategoriaan: Dual Stack, joka mahdollistaa IPv4- ja IPv6-protokollan yhteiskäytön samassa verkkolaitteessa; tunnelointi, joka mahdollistaa IPv6-protokollan liikenteen kuljettamisen IPv4-verkoissa; Protocol Translation, jonka avulla IPv6-laitteet voivat kommunikoida IPv4-laitteiden kanssa. Näitä eri tekniikoita voi yhdistellä ja verkon muuttaminen IPv6-protokollalle voidaan aloittaa vaikka pelkästään yhdestä aliverkosta. (Hagen 2006, 255.)

5.2 Dual Stack

Seuraavassa käydään läpi Dual Stack -tekniikan toiminta.

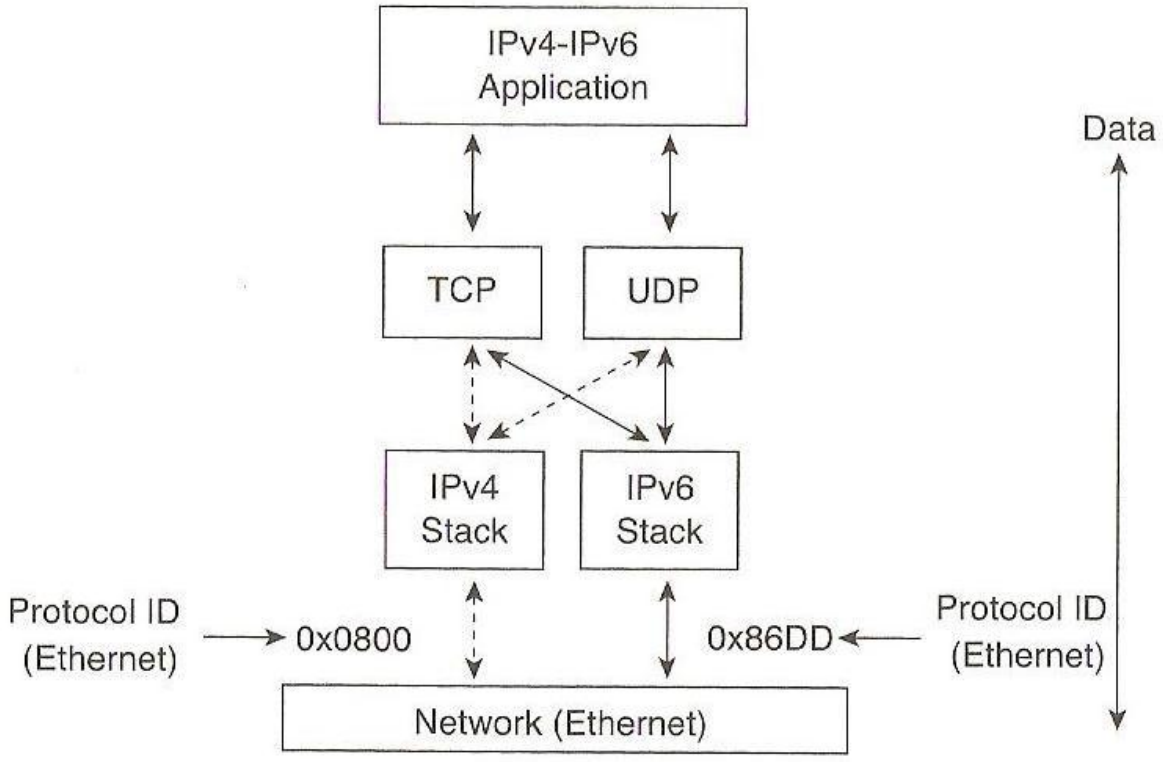
5.2.1 Yleistä

Laite, jossa on Dual Stack -ominaisuudet käytössä, käyttää kahden eri protokollan osoitteita. Tämä tarkoittaa, että käytössä olevalle portille jaetaan vähintään yksi IPv4- ja IPv6-osoite. Näin sama laite pystyy kuljettamaan kahden eri protokollaversion liikennettä. Konfiguroimalla toisen protokollaversion voi kytkeä halutessaan pois käytöstä. (Hagen 2006, 255.)

Reitittimetkin voidaan konfiguroida käyttämään Dual Stack -tekniikkaa, jolloin reititin välittää molempien protokollien liikennettä. Tekniikan haittapuolena on, että reititin joutuu ylläpitämään kaksia eri protokollapinoja. Tämä koskee myös kaikkia taulukoita, esim. reititystauluja. Reitittimeltä Dual Stack -tekniikan käyttöönotto vaatii enemmän muistia ja prosessointitehoa. (Hagen 2006, 256.)

5.2.2 Dual Stackin toiminta

Ennen kuin Dual Stackin käyttöönotosta on hyötyä, ohjelmat täytyy koodata tukemaan IPv6-protokollaa. Useimpien ohjelmien API on koodattu tukemaan vain IPv4-osoitteita, jotka ovat 32 bittisiä. Ohjelmien täytyy pystyä tukemaan 128 bittisiä osoitteita, jotta IPv6-protokollaa voitaisiin käyttää. IPv6-tuen koodaamisen jälkeen ohjelma voi toimia kuten ennenkin, käyttäen IPv4-protokollaa datan kuljetukseen, mutta päivityksen myötä ohjelma voi protokolla-ID:n avulla päättää kumpaa protokollaa halutaan käyttää. Protokolla-ID IPv4-paketilla on 0x0800 ja IPv6-paketilla 0x86DD. Kuvasta näkee ohjelman toimintaperiaatteen kahden protokollan ollessa käytössä. (Desmeules 2007, 228.)



Kuvio 9. IPv6-yhteensopivan ohjelmiston toiminta. (Desmeules 2007, 229.)

Dual Stackia käyttävä verkkolaite ei itse pysty päättämään kumpaa protokollaa se käyttää datan kuljettamiseen. On olemassa kaksi erilaista metodia, jolla verkkolaitteen saa käyttämään IPv6-yhteyttä oletuksena, jos sellainen on saatavilla. (Desmeules 2007, 230.)

Näistä ensimmäinen on käyttäjän manuaalinen syöttö. Tätä menetelmää käyttääkseen tulee käyttäjän tietää kohdeverkkolaitteen IPv6-osoite, jonka avulla pystytään yhteys luomaan. Menetelmä ei ole käytännöllinen päivittäiseen käyttöön, mutta hyvä työkalu vianetsintään. (Desmeules 2007, 230.)

Käytännöllisempi menetelmä on nimipalvelun käyttö. Ohjelmaan pitää konfiguroida FQDN-tiedot, jotka sisältävät IPv4- ja IPv6-osoitetiedot DNS-palveluun. Tämän avulla DNS-serverit pystyvät jakamaan tietoja palvelimista ja palveluista IPv4- ja IPv6-verkon kautta. IPv6-osoitteen tunnus DNS-palvelussa on AAAA, kun vanhan IPv4-protokollan tunnus on yksittäinen A. (Desmeules 2007, 230.)

DNS-palvelimelle voi lähettää kolme erilaista DNS-kyselyä, joista ensimmäinen on kysely IPv4-osoitteesta. IPv4-protokollaa tukeva ohjelmisto pyytää nimipalvelinta kääntämään FQDN-tiedot A-tunnukseksi. Ohjelma alkaa kommunikoida kohteen kanssa IPv4-osoitetta käyttäen, kun saa A-tunnuksen käyttöönsä. (Desmeules 2007, 230.)

Toinen DNS-kysely on kysely IPv6-osoitteesta. Tässä kyselyssä IPv6-protokollaa tukeva ohjelmisto pyytää nimipalvelinta kääntämään FQDN-tiedot AAAA-tunnukseksi. Ohjelma alkaa kommunikoida kohteen kanssa IPv6-osoitetta käyttäen, kun saa AAAA-tunnuksen käyttöönsä. (Desmeules 2007, 230.)

Kolmas DNS-kysely on kaiken tyyppisille osoitteille. Tässä kyselyssä molempia protokollia tukeva ohjelmisto pyytää nimipalvelinta kääntämään FQDN-tiedot kaiken tyyppisille osoitteille. Ohjelmisto käyttää kuitenkin AAAA-tyyppisiä tietoja ensin, jos ne ovat saatavilla. Jos AAAA-tyyppisiä tietoja ei löydy, ohjelmisto alkaa kommunikoida kohteen kanssa käyttäen A-tunnuksen tietoja. (Desmeules 2007, 230.)

5.3 Tunnelointi

Seuraavassa käydään läpi erilaisia tunnelointimekanismeja.

5.3.1 Yleistä

Tunnelointimekanismeja voidaan käyttää IPv6-protokollan pakettien kuljettamiseen IPv4-verkoissa. Tunnelointia kutsutaan myös kapsuloinniksi. Tunneloidessaan IPv6-paketteja tunnelointimekanismi kapsuloi IPv6-paketin IPv4-paketin sisään, jotta paketti pystyy kulkeutumaan IPv4-verkon läpi tunnelin päätepisteelle. Päätepisteellä se enkapsuloidaan ja paketti voi jatkaa matkaansa taas IPv6-verkossa viimeiseen määränpäähänsä. (Hagen 2006, 256.)

5.3.2 Tunneleiden käyttötavat

IPv6-tunneleille IPv4-verkossa on olemassa kolme erilaista käyttötapaa. Ensimmäinen näistä on tunnelointi verkkolaitteelta verkkolaitteelle. IPv4-verkossa eristyksissä olevat verkkolaitteet voivat luoda tunnelin keskenään. Näiden laitteiden täytyy kuitenkin tukea Dual Stack -ominaisuutta. (Desmeules 2007, 237.)

Toinen tunnelointitapa on verkkolaitteelta reitittimelle. Eristyksissä oleva Dual Stack -verkkolaite voi luoda tunnelin Dual Stackia tukevan reitittimen kanssa IPv4-verkon yli. Tämän tekniikan avulla IPv6-verkkolaite voi muodostaa IPv6-yhteyden mihin tahansa IPv6-verkkolaitteeseen reitittimen kautta. (Desmeules 2007, 237.)

Kolmas tekniikka on luoda tunneli reitittimeltä toiselle reitittimelle. Dual Stack -ominaisuudella varustetut reitittimet IPv4-verkoissa voivat luoda tunnelin keskenään. Reitittimiä voidaan käyttää yhdistämään erityksissä olevia IPv6-verkkolaitesaarekkeet. Tämän avulla kaikki IPv6-verkkolaitteet pystyvät luomaan yhteyden kaikkiin IPv6-verkkolaitteisiin. (Desmeules 2007, 237.)

5.3.3 Konfiguroitu tunneli

Konfiguroitu tunneli oli yksi ensimmäisistä tunnelointimenetelmistä IPv6-protokollalle ja melkein kaikki laitteistot tukevat sitä. Konfiguroidut tunnelit aktivoidaan ja konfiguroidaan staattisesti Dual Stack -verkkolaitteissa. IPv4- ja

IPv6-osoitteet konfiguroidaan manuaalisesti jokaiselle tunnelointiportille, ja jokainen portti tarvitsee kolme erilaista osoitetta. (Desmeules 2007, 239.)

Ensimmäinen tarvittavista osoitteista on paikallinen IPv4-osoite, jolla verkkolaite saa yhteyden paikalliseen Dual Stack -verkkolaitteeseen IPv4-verkon yli. Kyseistä osoitetta käytetään lähdeosoitteena ulkoiselle liikenteelle. Toinen osoitteista on päätepisteen IPv4-osoite. Tämän IPv4-osoitteen avulla tavoitetaan Dual Stack -kohdeverkkolaite IPv4-verkossa. Kyseistä osoitetta käytetään kohdeosoitteena ulkoiselle liikenteelle. Kolmas tarvittava osoite on paikallinen IPv6-osoite, joka asetetaan paikallisesti tunnelin portille. (Desmeules 2007, 239.)

5.3.4 Tunnel Broker ja Tunnel Server

IETF on määritellyt Tunnel Broker -nimisen palvelun tunnelointia varten. Tunnel Broker on ulkoinen järjestelmä, joka toimii palvelimen tapaan IPv4-protokollassa. Palvelin vastaanottaa pyyntöjä tunneloinnista Dual Stack -verkkolaitteilta. Dual Stack -verkkolaitteet lähettävät tunnelointipyynnöt IPv4-verkon yli käyttäen HTTP-protokollaa. Tunnel Broker -palvelin vastaa käyttäen samaa protokollaa. Vastauksen mukana Dual Stack -verkkolaite saa itselleen IPv4- ja IPv6-osoitteita, sekä oletusreittejä tunnelin muodostamista varten. Tunnel Broker viimeistelee tunneloinnin konfiguroimalla tunnelin reitittimen ja verkkolaitteen välille. (Desmeules 2007, 243.)

Tunnel Server on yksinkertaistettu versio Tunnel Brokerista. Tunnel Server yhdistää Tunnel Brokerin ja Dual Stack -reitittimen samaan laitteeseen. Tunnel Serverin konfigurointi vastaa Tunnel Brokerin konfigurointia. Pyynnöt lähetetään HTTP-protokollaa käyttäen IPv4-verkon yli, jonka jälkeen saadaan asianmukaiset vastaukset. (Desmeules 2007, 244.)

5.3.5 6to4

Tunnel Brokerin lisäksi IETF on kehittänyt 6to4-tekniikan, jolla voidaan helpottaa IPv6-tunnelointia IPv4-verkkojen yli. RFC3056:ssa on määritelty neljä erilaista pääominaisuutta 6to4-tekniikkaa varten. (Carpenter & Moore 2001.)

Ensimmäinen näistä on dynaaminen ”automaattinen tunnelointi”, joka muodostaa tunneleita IPv6-verkkolaitteiden välille. Tätä mekaniikkaa käyttäessä ei tarvitse tunneleita luodessa staattisesti määritellä IPv4-osoitteita. IPv6-pakettien tunnelointi 6to4-alueiden välillä hoidetaan dynaamisesti, IPv6-kohdeosoitteen perusteella. Tätä menetelmää käytettäessä IPv6-paketti kapsuloidaan IPv4-paketin sisälle ja käytetään IPv4-reititysalueita kuljetuskerroksena. (Desmeules 2007, 245.)

Toinen pääominaisuuksista on ”käytössä verkkokohteiden reunalla”. Pääominaisuuden ideana on suositella 6to4-ominaisuuksien käyttöä eri verkkokohteiden rajareitittimissä, jotta 6to4-reitittimet saavat yhteyden muihin 6to4-kohteisiin ja verkkolaitteisiin käyttäessään IPv4-reititysrakennetta. (Desmeules 2007, 245.)

Kolmas pääominaisuus on ”automaattinen prefixin jakaminen”, minkä tehtävänä on toimittaa yksi aggregatable unicast IPv6-prefix jokaiselle 6to4-verkkokohteelle. Näiden osoitteiden prefixin IANA on varannut erikseen, se on 2002::/16. Jokainen 6to4-verkkokohde käyttää vähintään yhtä IPv4-unicast-osoitetta reitittimellään. IPv4-unicast-osoite muutetaan sen jälkeen hex-desimaalimuotoon ja liitetään aiemmin annettuun prefixiin. Näin lopulliseksi osoitteeksi muodostuu 2002::IPv4-unicast-osoite::/48. Jokainen 6to4-verkkokohde saa myös /48-prefixin perustuen globaaliin IPv4-unicast-osoitteistukseen. Seuraavat 16 bittiä /48-prefixistä ovat käytössä aliverkotusta varten 6to4-reitittimen takana. (Desmeules 2007, 245.)

Viimeinen pääominaisuuksista on IPv6-reitin levittämisen kielto. 6to4-prefixit perustuvat julkisiin ja uniikkeihin IPv4-osoitteisiin, joten niitä ei ole tarvetta levittää kaikkien 6to4-verkkokohteiden kesken. (Desmeules 2007, 245.)

6to4-pääominaisuuksien lisäksi on kehitetty 6to4 relay -mekaniikka. 6to4 relay -mekaniikan avulla 6to4-reititin pystyy luomaan yhteyden muihinkin IPv6-verkon

unicast-osoitteisiin, kuin pelkästään 2002::/16. Yhden 6to4-verkkoalueen reunalla olevan reitittimien voidaan konfiguroida 6to4 relay -reitittimeksi, jotta muihinkin osoitteisiin saadaan yhteys. (Desmeules 2007, 251.)

5.3.6 GRE-tunneli

GRE on standardisoitu tunnelointitekniikka, joka mahdollistaa vakaan ja turvallisen tavan muodostaa point to point -yhteyksiä. GRE-tunneli muistuttaa konfiguroitua tunnelointia. GRE-tunneli joudutaan staattisesti konfiguroimaan reitittimiin, jotta IPv6-pakettien kuljetus IPv4-verkon yli olisi mahdollista. GRE-tunnelointi tarjoaa erityishyötyä organisaatioille, jotka käyttävät verkkoalueessaan IS-IS-reititysprotokollaa. IS-IS-protokollan toimintaperiaatteisiin kuuluu, että se lähettää linkkikerroksen viestejä lähekkäin olevien reitittimien kesken. GRE-tunnelointi on ainoa tunnelointimenetelmä, joka pystyy lähettämään linkkikerroksen viestejä IP-verkkojen yli. GRE-tunnelointia voi siis käyttää samanaikaisesti kuljettamaan IPv6-paketteja ja IS-IS-linkkikerroksen viestejä IS-IS-reitittimien välillä. (Desmeules 2007, 255.)

5.3.7 Teredo

Teredo-tunnelointimenetelmän on kehittänyt IETF. Teredo-tunnelin päätehtävänä on mahdollistaa IPv6-pakettien tunnelointi Dual Stack -verkkolaitteille, jotka ovat NAT-tekniikkaa käyttävän laitteen takana. Normaalit tunnelointimenetelmät eivät toimi NAT-tekniikkaa käyttävän laitteen taakse, mutta Teredo kiertää tätä rajoitusta tunneloimalla IPv6-paketit IPv4-protokollan UDP-datasähkeen avulla. Yhden IPv4-osoitteen ja NAT-laitteen UDP-kartoituksella Teredo mahdollistaa IPv6-yhteyden NAT-laitteen taakse käyttämällä edellä mainittua tekniikkaa. (Desmeules 2007, 261.)

Toimiakseen Teredo-tunnelointi tarvitsee kolme erillistä komponenttiä, joista ensimmäinen on Teredo-palvelin. Teredo-palvelin on yhdistetty IPv4-verkkoon ja siihen voidaan muodostaa yhteys käyttäen IPv4-osoitetta. Teredo relay -laite toimii IPv6-reitittimen tavoin. Teredo relay on yhdistetty IPv6-verkkoon IPv6-yhteyden ja

UDP-pakettien avulla, NAT-laitteen taakse. Teredo-asiakasohjelma sijaitsee IPv4-verkkoalueella NAT-tekniikkaa käyttävän laitteen takana. Teredo-asiakasohjelman tehtävänä on pyytää Teredo-palvelinta hankkimaan IPv6-yhteys Teredo relayn avulla, käyttäen UDP-paketteja. Teredo-asiakasohjelma konfiguroidaan käyttämään Teredo-palvelimen IPv4-osoitetetta. (Desmeules 2007, 261.)

5.4 Network Address and Protocol Translation

Seuraavassa käydään läpi Network Address and Protocol Translation (NAT-PT).

5.4.1 Yleistä

NAT-PT-menetelmän avulla IPv6-verkkolaitteiden on mahdollista kommunikoida IPv4-verkossa olevien verkkolaitteiden kanssa ja toisinpäin. NAT-PT-yhdyskäytävä käyttää julkisia ja uniikkeja IPv4-osoitteita, jotka sidotaan IPv6-osoitteisiin ja näin mahdollistetaan IPv6-verkkolaitteiden kommunikointi IPv4-verkoissa. (Hagen 2006, 278.)

5.4.2 Protocol Transitionin toiminta

NAT-PT-palvelun avulla dataa voidaan kuljettaa kahden erilaista IP-protokollaa käyttävän verkkolaitteen välillä. NAT-PT muuntaa IPv4-paketin mahdollisimman yhtäläiseen IPv6-paketin muotoon ja tarvittaessa toisinpäin. Jotta palvelu toimisi kahden eri protokollan välillä, täytyy NAT-PT:n toimia näiden kahden protokollan yhteyskohtana. (Dunmore 2005, 74.)

NAT-PT:n Network Address -osa toimii aivan samalla tavalla kuin nykyinen NAT-tekniikka IPv4-protokollassa, eli NAT muuntaa globaalit reititettävät IP-osoitteet yksityiseen muotoon. IPv4-protokollasta tutun NAT-tekniikan tapaan NAT-PT käyttää IP-osoitevarastoa, josta se dynaamisesti jakaa osoitteen käännetylle IP-

paketille. NAT-PT:n Protocol Translation -osa hoitaa IP-otsikoiden tulkkaus ja käännöstyön protkollasta toiseen. (Dunmore 2005, 74.)

Dual stack- ja tunnelointimenetelmät eivät muokkaa IP-paketin datan sisältöä, toisin kuin NAT-PT. NAT-PT muuntaa IP-paketin otsikon toisesta protokollasta toiseen, jolloin tulos on uusi otsikko, joka on käytännössä katsoen samanlainen kuin alkuperäinen, muttei kuitenkaan identtinen. Tämän takia on mahdollista, että jotain informaatiota voi kadota muuntamisvaiheessa, kuten informaatio, joka on käytettävissä vain toisessa protokollassa, katoaa muunnosvaiheessa. (Dunmore 2005, 74.)

Ominaisuuksien takia NAT-PT:tä tulisi käyttää vain väliaikaisratkaisuna, kunnes toinen muunnostekniikka saadaan käyttöön. NAT-PT ei tue myöskään IPv6-protokollan edistyneempiä ominaisuuksia ja se toimii verkkotopologian heikkona kohtana, sillä kaikki liikenne kulkee ainoastaan sen läpi. (Hagen 2006, 285.)

6 IPV6-PROTOKOLLA JA TIETOTURVA

6.1 Yleistä

Jotta järjestelmänvalvojat pystyisivät suojelemaan tärkeää dataa, täytyy heidän olla ajan tasalla mahdollisista tietoturvauhista. Hyvässä tietoturvasuunnitelmassa keskitytään moneen muuhunkin, kuin pelkästään haittaohjelmien estoon toisista verkoista. Läheskään kaikki uhat eivät ole ulkoisia, vaan monet ovat sisäisiä. Näihin kuuluvat käyttäjien väärinkäytökset ja virheellinen järjestelmän valvominen. Tämän takia monia riskejä ei voi kontrolloida pelkän tekniikan avulla. (Hagen 2006, 102.)

6.2 IPSec

IPSec on IETF:n luoma avoin standardi, joka on luotu turvallista tiedon kuljettamista varten suojaamattomissa verkoissa, kuten Internetissä. IPSec toimii verkkokerroksella suojaten ja aidontaen IP-paketteja IPSec-laitteiden välillä. IPSecissä on neljä erilaista suojauspalvelua ja jokainen niistä on valinnainen. Näiden suojauspalveluiden käyttö määräytyy paikallisen suojauspolitiikan mukaan. (Dunmore 2005, 232.)

IPSec tarjoaa suojauspalveluissaan datan yksityisyyden suojaa, jolloin kaikki paketit kryptataan ennen lähettämistä. Suojauspalveluihin kuuluu myös datan yhtenäisyyden tarkistus. Vastaanottava IPSec-laite voi aidontaa toiselta IPSec-laitteelta saamansa paketit, varmistaakseen että data on pysynyt muuttumattomana kuljetuksen aikana. (Dunmore 2005, 232.)

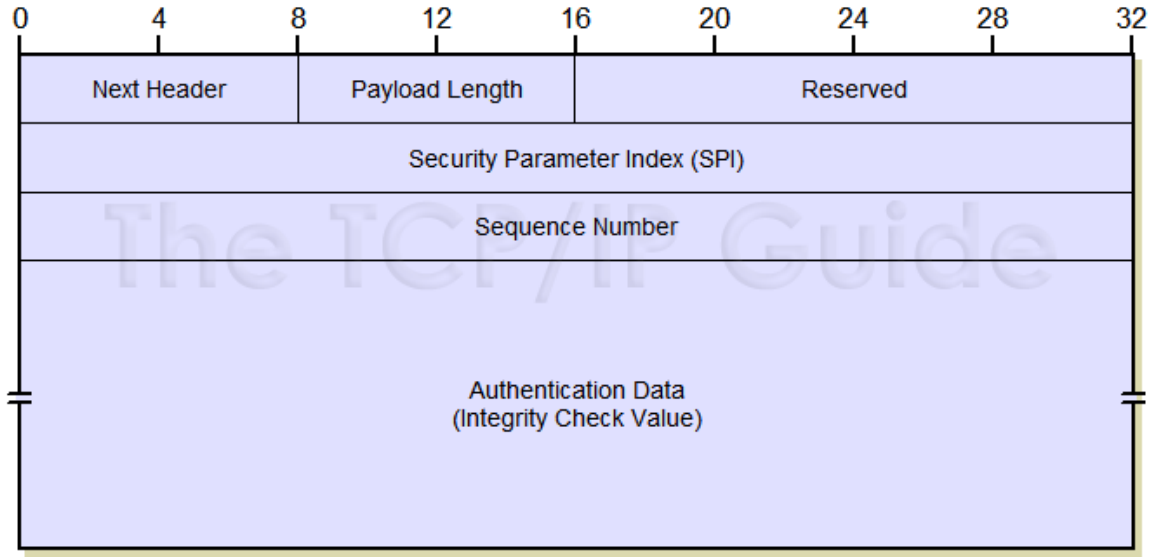
Kolmas IPSecin suojauspalveluista on datan alkuperän aidonnus, jossa vastaanottava IPSec-laite aidontaa lähettäjän IP-pakettien alkuperän. Datan alkuperän aidonnus on riippuvainen datan yhtenäisyyden tarkistuksesta. IPSec-suojauspalvelun viimeinen ominaisuus on toiston esto, jossa vastaanottava IPSec-laite osaa tunnistaa ja hylätä toistetut paketit. IPv6-protokollassa IPSec voidaan

ottaa käyttöön käyttämällä Authentication- ja ESP-lisäotsikoita. (Dunmore 2005, 232.)

6.2.1 Authentication-lisäotsikko

Authentication-lisäotsikko varmistaa paketin eheyden ja mahdollistaa lähettäjän aitouden tarkistuksen. Näiden lisäksi se tarjoaa myös valinnaisen suojauksen uudelleen lähetettyjä pakettien varalle. (Dunmore 2005, 232.)

Authentication-lisäotsikko sijaitsee IPv6-otsikon ja korkeammantason otsikoiden välissä ja sen protokollanumero on 51 (Hagen 2006, 109).



Kuvio 10. Authentication-lisäotsikko. (Kozierok, 2005a.)

Authentication-lisäotsikko koostuu kuudesta eri kentästä, ensimmäinen niistä on Next Header, joka kertoo seuraavaksi tulevan otsikon arvon. Payload Length -kenttä kertoo otsikon pituuden 4 bittisenä lukuna. Kahdeksaa ensimmäistä bittiä ei kuitenkaan oteta laskuissa huomioon. Luku on tärkeä, koska se vaihtelee riippuen mitä algoritmiä käytetään. (Hagen 2006, 110.)

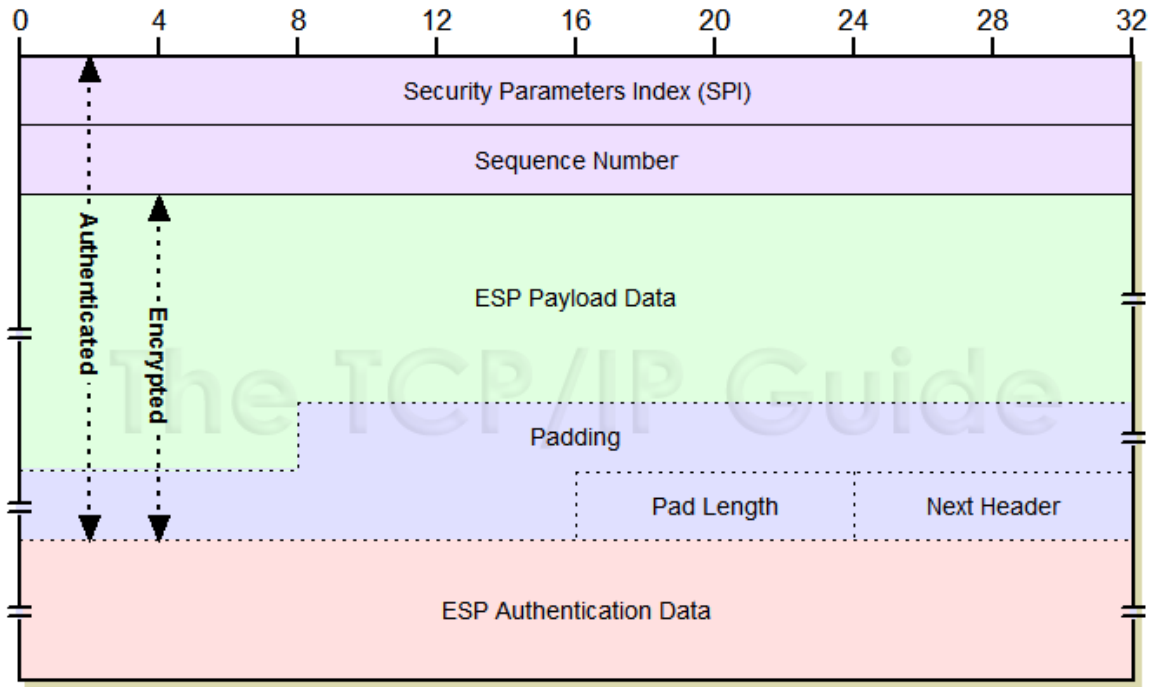
Reserved-kenttä asetetaan aina arvoon nolla. Security Parameter Index -kentän arvo on 32 bittinen luku. Kenttää käytetään ilmoittamaan mitä Security Associationia tuleva paketti käyttää. Kenttä on pakollinen ja kaikkien

Authentication-lisäotsikkoa käyttävien laitteiden tulee tukea sitä. Sequence Number -kenttä on myös 32 bittinen ja kentän tehtävänä on varmistaa, ettei identtisiä paketteja lähetetä peräkkäin. Näin voidaan estää spam-hyökkäykset. Integrity Check Value -kenttä sisältää tarkistussumman paketille. Kentän pituus riippuu käytettävästä algoritmistä. (Hagen 2006, 110.)

6.2.2 Encapsulating Security Payload -lisäotsikko

ESP-lisäotsikko tarjoaa monia ominaisuuksia: salassapidon, lähettäjän aidonnuksen, yhteydettömän pakettien eheyden tarkistuksen, uudelleen lähettämisen eston ja rajoitetun liikenteen salassapidon (Dunmore 2005, 232-233).

ESP-lisäotsikko sijoittuu myös IPv6-otsikon ja korkeammantason otsikoiden väliin, kuten Authentication-lisäotsikkokin. Sen protokollanumero on 50.



Kuvio 11. ESP-lisäotsikko. (Kozierok, 2005b.)

ESP-lisäotsikko muodostuu seitsemästä eri kentästä. Security Paramters Index -kenttä on vastaavanlainen kenttä kuin Authentication-lisäotsikossa. Se on 32 bittinen ja sen avulla tarkastellaan mitä Security Associationia tuleva paketti käyttää. Sequence Number on myös 32 bittinen kenttä, jonka tarkoituksena on

estää identtisien pakettien lähettäminen. Payload Data -kenttä pitää sisällään salatun datan. Padding-kenttää käytetään tasaamaan paketti neljän tavun kerrannaiseksi ja varmistamaan, että paketin koko ylittää vähintään minimipaketin koon. Pad Length -kenttä ilmaisee aiemman kentän pituuden tavuina. Next Header -kenttä ilmaisee otsikon, joka seuraa ESP-lisäotsikkoa. Integrity Check Value -kenttä pitää sisällään tarkistussumman. (Hagen 2006, 112-115.)

6.3 Tietoturva IPv6-protokollassa

Seuraavassa käydään läpi IPv6-protokollan keskeisimmät tietoturvan uhat.

6.3.1 Verkon tietojen kalastelu

Verkkoon kohdistunut hyökkäys aloitetaan yleensä tiedustelulla, joista verkon skannaus on yleisin. Skannauksen tarkoituksena on saada tarvittavaa tietoa kohteesta muita hyökkäystapoja varten. IPv6-protokolla itsessään tarjoaa suojaa skannausta vastaan. IPv6-verkon laaja määrä mahdollisia isäntälaitteita tekee porttien skannauksesta todella vaikeata. /64-aliverkon skannaus kestää todella kauan. Skannerilta, joka pystyisi tutkimaan miljoona osoitetta sekunnissa kestää, 584000 vuotta skannata koko alue läpi. (Dunmore 2005, 233).

Skannausta helpompia menetelmiä on kuitenkin olemassa, joista muutamia ovat arvattava osoitteistus, EUI-64-osoiterakenteen hyväksikäyttö, skannaus verkon sisäpuolelta ja huonosti toteutettu skannausviestien suodatus (Dunmore 2005, 233).

6.3.2 Luvaton käyttö IPv6-verkoissa

Luvaton käyttö on riippuvainen verkon menettelytavoista. Jos tunnistus tehdään TCP/IP-protokollan kolmannella tai neljännellä kerroksella, on se yleensä toteutettu palomuureissa. IPv6-protokollassa tunnistus toimii samalla lailla kyseisillä verkkokerroksilla, mutta mukaan on lisätty muutama suunnittelua

koskeva huomio. Näistä esimerkkinä palomuurien suodatus tulisi olla harkittua IP-paketteja varten, joiden lähdeosoitetta ei kirjata reititystauluihin. IPv4-protokollassa on helpompi estää kaikki kyseisen kaltaiset paketit, kun taas IPv6-protokollassa on helpompaa sallia oikeat paketit ja estää loput. (Dunmore 2005, 234.)

Luvattoman käytön voi myös estää verkkokerroksen alemmallakin tasolla. Portti-tason aidonnusmenetelmät, kuten 802.1x, on turvallinen tapa organisaatiolle suojata verkko. (Dunmore 2005, 234.)

6.3.3 Spoofing IPv6-verkoissa

Denial of Service -hyökkäykset, jotka tulevat tekaistuista tai huijatuista osoitteista ovat ongelmallisia estää. Ingress Filtering -nimeä käyttävä metodi pystyy estämään huijatut lähdeosoitteet. Metodin hyvänä puolena on, että alkuperäisen lähettäjän oikean lähdeosoitteen voi helposti jäljittää, sillä hyökkääjän täytyy käyttää käytössä olevaa ja saavutettavaa lähdeosoitetta. Peruskäyttäjät voivat käyttää samantapaista tekniikkaa, jota kutsutaan Egress Filteringiksi. Tekniikka estää palveluntarjoajaa lähettämästä heille IP-paketteja, jotka eivät kuulu heidän verkkoonsa. (Dunmore 2005, 235.)

Näitä menetelmiä voidaan käyttää myös IPv6-protokollan kanssa. IPv6-protokollan avulla Ingress Filtering on helpompaa, koska tarvitaan vain yksi konfiguroitu prefix. Yleensä yksi /48-aliverkon osoite pitää konfiguroida, ellei pystytä järjestämään automaattisesti antispoofing- tai unicast reverse path forwarding -tarkistusta. Egress Filteringin konfigurointi on lähes samanlainen Ingress Filteringin kanssa, ainoana erona, että se konfiguroidaan käyttäjän laitteisiin. (Dunmore 2005, 235.)

6.3.4 Subverting host initialization IPv6-verkoissa

IPv6-ympäristöön voidataan hyökätä samankaltaisesti, kuten ARP-taulukkoa vastaan IPv4-protokollassa. Mahdollisia hyökkäysmetodeja ovat valheelliset Neighbor Advertisement -viestit, Denial of Service -hyökkäykset, hyökkäykset DAD-mekanismia vastaan tai valheellisten Router Advertisement -viestien

lähettäminen. Neighbor Discovery -protokollaa varten on kehitetty Secure Neighbor Discovery -palvelu, joka helpottaa hyökkäyksiä NDP-protokollaa vastaan. (Dunmore 2005, 236.)

6.3.5 Broadcast amplification IPv6-verkoissa

IPv4-protokollasta tutut broadcast amplification -hyökkäykset eivät ole uhka IPv6-verkoissa kahdesta syystä. IPv6-osoitteilla ei ole broadcast-osoitetta, joten tämän tapainen hyökkäys ei ole mahdollinen. (Dunmore 2005, 236.)

IPv6-protokollan multicast-osoitteet, jotka ovat määrätty erikoisryhmille, voivat kuitenkin olla heikko kohta. Toinen syy on IPv6-protokollan esto, multicast-viestin osoitteille vastaaminen ei ole sallittua. IPv6-protokolla estää ICMPv6-pakettien lähettämisen vastaukseksi kaikissa, paitsi kahdessa erityisessä tapauksessa. Paketti on liian suuri, jolloin PMTUD-viesti lähetetään vastaukseksi. Toinen näistä erityistapauksista on Parameter Problem -viestin lähettäminen. (Dunmore 2005, 236.)

6.3.6 Hyökkäykset reititysinfrastruktuuria vastaan

Reititysinfrastruktuuriin tehtävien hyökkäysten tarkoituksena on häiritä ja korruptoida reitittimen reititysinformaatiota. Tällä tavoin pystytään järjestämään Denial of Service -hyökkäyksiä ja auttamaan toisenlaisien hyökkäyksien tekoa, kuten esim. DNS:n välimuistin myrkyttämistä. (Dunmore 2005, 237.)

IPv6-ympäristössä verkon suunnittelijoiden olisi syytä ottaa huomioon IPv6-protokollan ominaispiirteet. BGP-, IS-IS- ja EIGRP-reititysprotokollia käytettäessä turvallisuusalgoritmit pysyvät samoina. OSPFv3- ja RIP-reititysprotokollat ovat muuttuneet ja ne käyttävät nyt IPSec-protokollaa, joten näitä reititysprotokollia käytettäessä on syytä muistaa IPSecin konfigurointi. Muut reititysinfrastruktuurin hyökkäykset ovat hyvin samanlaisia IPv4-ympäristössä, joten samantapaiset vastatoimenpiteet ovat välttämättömiä. (Dunmore 2005, 237.)

6.3.7 Datan kaappaaminen kesken siirron IPv6-ympäristöissä

Suojaamattoman datan kaappaaminen IPv6-verkoissa toimii samalla tavalla kuin liikenteen urkinta IPv4-ympäristössä. Työkaluja tätä varten on varmasti jo vähintäänkin valmistuksessa, eivätkä ne rajoitu fyysisen kerroksen passiiviseen urkintaan, kuten monet järjestelmän valvojien työkalut. Nämä ongelmat ovat oikea uhka palveluille IPv6-ympäristössä, mutta pakollinen IPSecin käyttö voi helpottaa tilannetta. IPSec suojaa kaikenlaista kommunikaatio, myös esim. SQL database queryjä. (Dunmore 2005, 237.)

6.3.8 Sovelluskerroksen hyökkäykset IPv6-ympäristössä

Useimmat hyökkäykset kohdistetaan sovelluskerrokselle. Tällaiset hyökkäykset mahdollistavat pääsyn järjestelmän resursseihin hyväksikäyttämällä puskurin ylivuotoa tai hankkimalla korkean tason oikeudet suorittamalla koodinpätkän sopimattomalla tarkastuksella. Tämän tyyppiset hyökkäykset eivät ole yhteydessä verkkoprotokollaan, joten muutosta IPv6-ympäristöihin siirryttäessä ei tule olemaan. Järjestelmänvalvojien täytyy kuitenkin olla varuilla näistä ongelmista ja suojata järjestelmänsä näiden uhkien varalle. (Dunmore 2005, 237.)

6.3.9 Man-in-the-middle-hyökkäykset

Ilman IPSecin käyttöä man-in-the-middle-tekniikat toimivat samalla periaatteella myös IPv6-protokollassa kuten IPv4-protokollassa. Pelkästään IPSecin korostuneella käytöllä voidaan välttää ongelmat yhteyksien kaappaamisyritysten kanssa. Tällä hetkellä vallitseva käytäntö IPv6-protokollaan siirtymisessä on kuitenkin olla käyttämättä IPSeciä ollenkaan. Ohjelmistotasolla, esim. nettiselaimissa, sertifikaatit voivat myös tarjota suojaa näitä hyökkäyksiä vastaan. (Dunmore 2005, 237-238.)

6.3.10 Denial of Service -hyökkäykset

Denial of Service -hyökkäykset ovat identtisiä IPv4- ja IPv6-protokollassa. Näiden hyökkäysten estäminen onkin tulvaisuuden haaste, jota varten tarvitaan tehokkaita Denial of Service -hyökkäysten havainnointivälineitä. Näillä välineillä voidaan erotella normaali datavirta erilleen Denial of Service -hyökkäyksen datavirrasta. IPSeciä käytettäessä Denial of Service -hyökkäyksen paketit eivät kulkeudu viimeiseen määränpäähänsä, mutta keskustelukäytävät silti tukkeutuvat, mikä estää oikeita käyttäjiä käyttämästä palvelua. (Dunmore 2005, 238.)

6.4 Tietoturva tunneloinnissa

Tunneloinnin tietoturvaongelmat keskittyvät suurilta osin palomuurien kohdalle. Tunneloitua verkkoliikennettä varten palomuurista joudutaan sallimaan verkkoliikenne protokollalle 41 ja jossain tapauksissa myös protokolla 58 varten. Näiden protokollien salliminen avaa tietoturvariskin tarkasti suojatun verkkokohteen tietoturvaan, koska tämän tyyppinen liikenne päästetään sisään ilman erillistä tutkimista. Tällainen IPv6-liikenne voi olla mitä vain, ja jos IPv6-reititin toimii tunnelin päätepisteenä, reititin kuljettaa tämän IPv6-liikenteen IPv6-verkkoon mahdollistaen väärinkäytöksiä. (Dunmore 2005, 249.)

Paras apu kyseiseen ongelmaan on asentaa IPv6-protokollaa tukeva palomuuri tunnelin päätepisteelle. Palomuuri tutkii ja suodattaa IPv6-liikenteen kunnolla dekapsulointi vaiheen jälkeen ja näin ollen on ainut keino suodattaa vain tietyntyyppinen IPv6-liikenne tunnelin läpi. (Dunmore 2005, 249.)

Tunnelin päätepisteellä sijaitsevan palomuurinkin kanssa täytyy tunnelia rakentaessa olla tarkkana, koska kuka tahansa voi mahdollisesti kalastella toisen päätelaitteen IPv4-osoitteen ja lähettää siihen IP-paketteja. Paikallinen tunnelin päätepiste ei tiedä, että pakettien lähdeosoite paketeissa ei ole todellinen tunnelin päätepiste ja siksi dekapsuloi saapuvaa IPv6-liikennettä suoraa, mikä voi sitten vapaasti kulkea IPv6-verkkoon. Hyökkääjän ei tarvitse edes tietää verkossa käytettäviä IPv6-osoitteita, koska se voi lähettää ICMPv6-paketin kaikille tunneliin yhteydessä oleville isäntälaitteille käyttämällä omaa globaalia IPv6-osoitetta,

saaden vastaukseksi kaikkien verkonlaitteiden IPv6-osoitteet. (Dunmore 2005, 249-250.)

Ongelma ei varsinaisesti ole tunneloinnissa, vaan vika piilee IPv4-osoitteistuksen kalastelussa. Paras tapa suojautua tämän tyyppistä hyökkäystä vastaan on tehdä todella tiukkoja RPF-tarkistuksia verkkokohteen reunalla, mutta siltikään turvallisuus ei ole täysin taattua. Paikallinen IPv6-tunnelin päätepiste voi lisätä turvallisuutta tiputtamalla paketit, jotka osoittautuvat link-local-paketeiksi, dekapsuloinnin jälkeen. (Dunmore 2005, 250.)

7 IPv6-PROTOKOLLAN TESTAUS KÄYTÄNNÖSSÄ

7.1 Yleistä

Käytännön työ suoritettiin Seinäjoen ammattikorkeakoulun tiloissa. Työn tarkoituksena on rakentaa toimiva IPv6-protokollaa käyttävä verkko IPv4-verkon laidalle. Tähän tarkoitukseen valittiin alun perin Dual Stack -tekniikka. Työtä varten ei lopulta kuitenkaan saatu tarvittavia verkkolaitteita, joten päädyttiin käyttämään tunnelointitekniikkaa.

7.2 Ongelmatilanteita

Tunnelointia suunniteltiin tehtäväksi erilaisten Virtual LANien kautta. Tunneli olisi muodostettu normaalisti ensimmäiseltä kytkimeltä, josta se olisi kierrätetty Seinäjoen ammattikorkeakoulun verkon kautta Virtual LANeissa tunnelin toiselle päätepisteelle.

Konfiguroidessa kävi ilmi, että ongelmaksi muodostui verkkolaitteita konfiguroidessa niiden versio, joka ei tukenut kaikkia IPv6-tunneloinnin ominaisuuksia.

gw(config)#Interface tunnel 0

gw(config-if)#Tunnel destination 1.2.3.4

gw(config-if)#Tunnel source vlan2

gw(config-if)#Tunnel mode ipv6ip

% Invalid input detected at '^' marker.

Ongelman ydin on, että ainakaan nykyisellä ohjelmistolla (12.2SE) käytössä olevat Ciscon Catalyst 3560E- ja Catalyst 3750 -kytkimet eivät tue IPv6-tunnelointia, vaikka muuten ovatkin IPv6-kykyisiä.

7.3 IPv6-tunnelointi

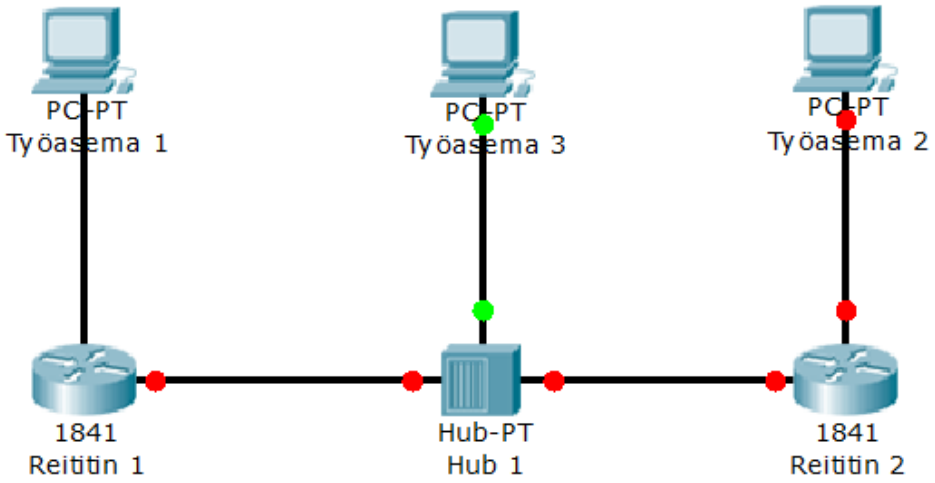
Komplikaatioiden takia päädyttiin tekemään yksinkertainen IPv6-tunnelointi käyttämällä kahta Ciscon 1841 -reititintä. Laitteet eivät tukeneet suoraan IPv6-protokollaa, joten niihin jouduttiin vaihtamaan flash-muistikortit, joihin oli asennettu käyttöjärjestelmän uudempi versio. Tämä uudempi versio tuki IPv6-tunnelointia. Molempiin reitittimiin on yhdistetty Windows 7 -käyttöjärjestelmää käyttävät työasemat. Näiden reitittimien välillä käytettiin HP:n valmistamaa hubia kaiuttamaan liikennettä. Hubiin yhdistetään Windows 7 -käyttöjärjestelmällä varustettu työasema. Työasemaan on asennettuna Wireshark-ohjelmisto, jolla voidaan tutkia hubilta kaiutettua liikennettä.

Tarkoituksena on rakentaa näillä laitteistolla IPv6-protokollaa tukeva tunneli ja testata tämän toimivuutta IPv4-protokollan yli. Testauksen yhteydessä käsitellään Ciscon-konsolin eri komentoja ja tarvittavia IPv4- ja IPv6-protokollan osoitteita.

7.3.1 Kokoonpano

Kokoonpanoa tunnelointia varten rakennettiin kaksi IPv6-protokollalla toimivaa verkkoa ja niiden välille toimiva IPv4-verkko. Työasema 1 ja 2 asetetaan hakemaan itse IPv6-osoite ja molemmista niistä on poistettu IPv4-protokolla käytöstä. Reitittimen 1 FastEthernet 0/0-porttiin asetetaan IPv6-osoite ja FastEthernet 0/1-porttiin asetetaan IPv4-osoite. Reitittimelle 2 tehdään samat toimenpiteet samoille porteille. Reitittimen 1 ja 2 välille muodostuu IPv4-verkko, jonka yli IPv6-protokollaa tukevat työasemat tulevat keskustelemaan asianmukaisten konfiguraatioiden jälkeen.

Seuraavassa on kuva työn kokoonpanosta.



Kuvio 12. Kokoonpano Packet Tracer -ohjelmalla esitettynä.

7.3.2 Konfigurointi

Reitittimiin täytyy tehdä tarvittavat konfiguroinnit tunneloimisen mahdollistamiseksi. Työasemista täytyy väliaikaisesti kytkeä Windowsin oma palomuuri pois käytöstä, jotta pingit kulkeutuvat ongelmitta läpi.

Konfigurointi aloitetaan siirtämällä Reititin 1 enable-tilaan ja siitä eteenpäin configure terminal -tilaan. Konfiguraation esittelyn selkeyttämiseksi salasanojen kyselyt on poistettu.

Router>Enable

Router#Configure terminal

Ciscon reitittimissä IPv6-protokolla ei ole oletusarvoisesti käytössä, joten sen täytyy ottaa käyttöön ensimmäisenä. Tämä tapahtuu seuraavalla komennolla configure terminal -tilassa.

Router(config)#Ipv6 unicast-routing

Seuraavaksi asetetaan oikeille porteille oikeat IP-osoitteet. FastEthernet0/1-porttiin asetetaan IPv4-osoite, jonka jälkeen portti aukaistaan ja lopuksi poistutaan portin konfiguroinnista.

Router(config)#Interface fastEthernet 0/1

Router(config-if)#Ip address 192.168.1.1 255.255.255.0

Router(config-if)#No shutdown

Router(config-if)#Exit

FastEthernet0/0-portti avataan IPv6-protokollan liikenteelle. Tämän jälkeen asetetaan IPv6-protokollaa tukeva osoite portille ja avataan se.

Router(config)#Interface fastEthernet 0/0

Router(config-if)#Ipv6 enabled

Router(config-if)#Ipv6 address 2001:1111::1/64

Router(config-if)#No shutdown

Router(config-if)#Exit

Osoitteistuksen jälkeen aletaan konfiguroimaan tunnelia reitittimen 1 ja 2 välille. Tunnelin konfigurointi tilaan pääsee config terminal -tilasta seuraavalla komennolla:

Router(config)#Interface tunnel tunnel 0

Tunnelin konfigurointitilassa asetetaan tunnelille aluksi IPv6-osoite. Tämän jälkeen määritellään tunnelin lähde- ja kohdeosoitteet.

Router(config-if)#Ipv6 address 2001:1111:1111::1/64

Router(config-if)#Tunnel source 192.168.1.1

Router(config-if)#Tunnel destination 192.168.1.2

Router(config-if)#Tunnel mode ipv6ip

Router(config-if)#Exit

Vielä joudutaan määrittelemään configure terminal -tilassa mille verkolle tunneli osoitetaan. Lopuksi poistutaan config terminal -tilasta ja tallennetaan asetukset reitittimien muistiin.

Router(config)#Ipv6 route 2001::/64 tunnel 0

Router(config)#Exit

Router#Exit

Router>Write

Seuraava vaihe on konfiguroida reititin 2 tukemaan tunnelointia. Alla on lista reitittimelle 2 käytetyistä konsolikomennoista.

Router>Enable

Router#Configure terminal

Router(config)#Ipv6 unicast-routing

Router(config)#Interface fastEthernet 0/1

Router(config-if)#Ip address 192.168.1.2 255.255.255.0

Router(config-if)#No shutdown

Router(config-if)#Exit

Router(config)#Interface fastEthernet 0/0

Router(config-if)#Ipv6 enabled

Router(config-if)#Ipv6 address 2001::1/64

Router(config-if)#No shutdown

Router(config-if)#Exit

Router(config)#Interface tunnel 1

Router(config-if)#Ipv6 address 2001:1111:1111::2/64

Router(config-if)#Tunnel source 192.168.1.2

Router(config-if)#Tunnel destination 192.168.1.1

Router(config-if)#Tunnel mode ipv6ip

Router(config-if)#Exit

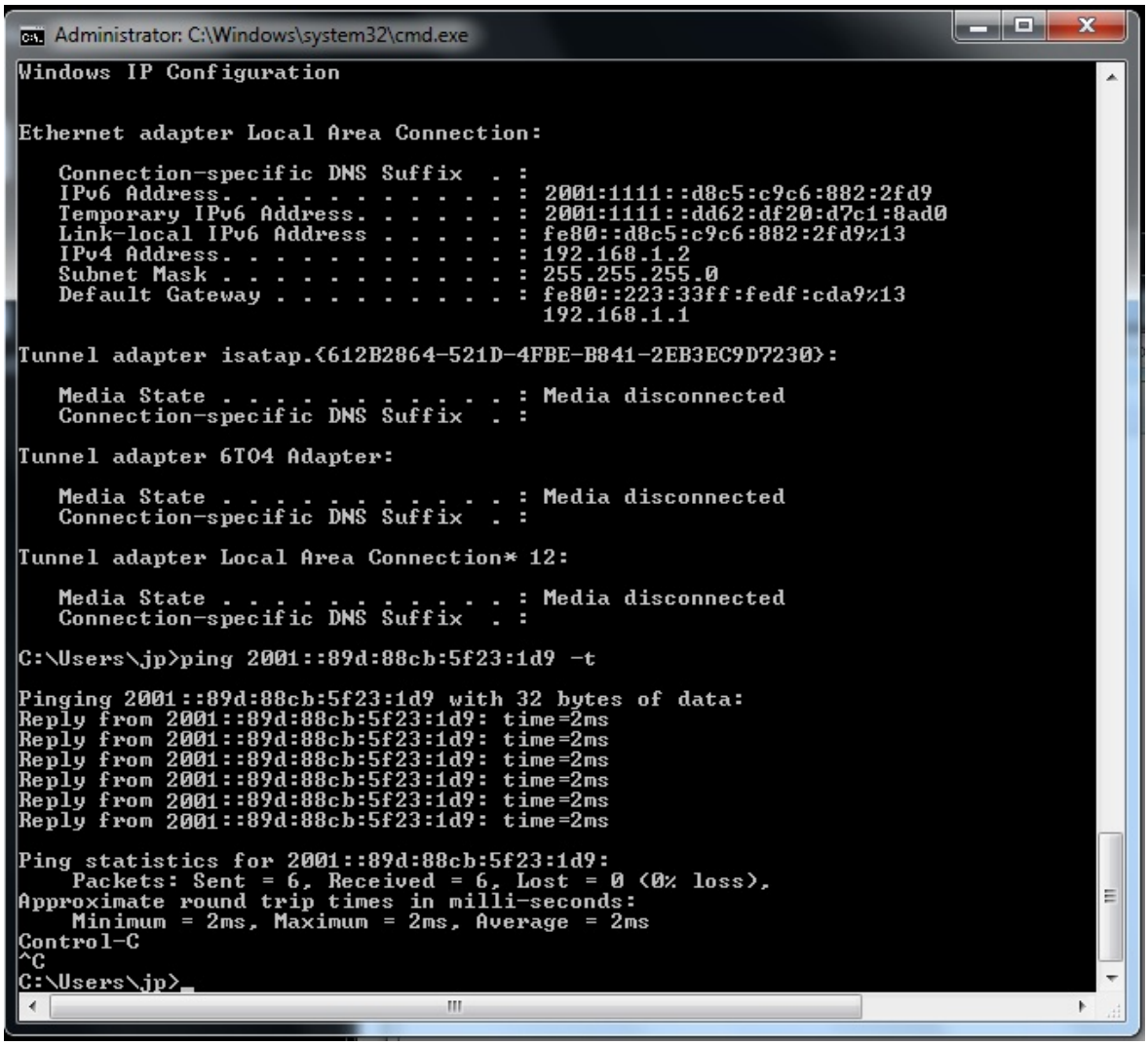
Router(config)#Ipv6 route 2001:1111::/64 tunnel 1

Näiden konfiguraatioiden jälkeen käytössä on toimiva IPv6-tunnelointi. Konfigurointia täytyy kuitenkin vielä testata asianmukaisesti.

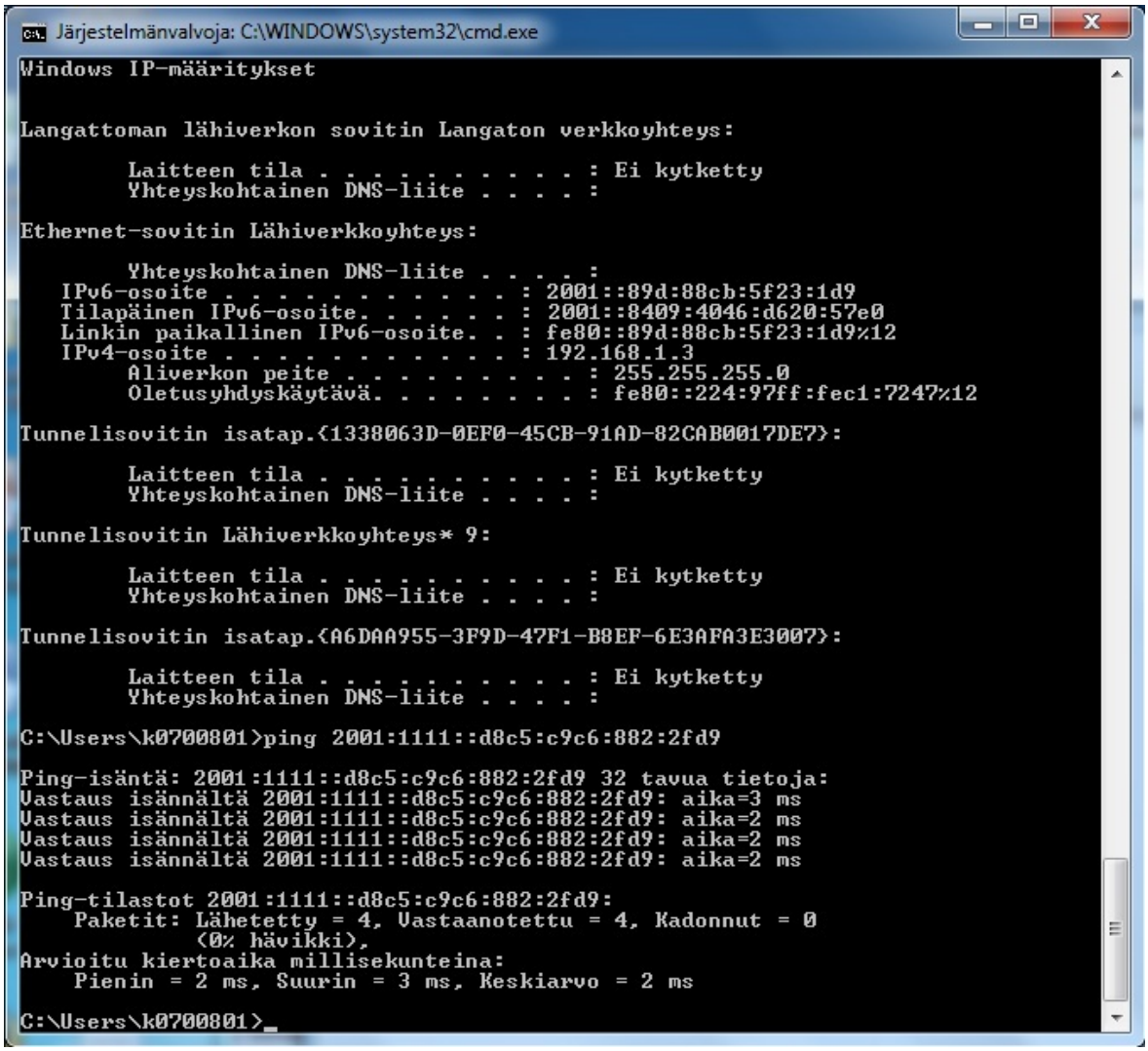
7.4 Konfiguroinnin toiminnan testaus

Ciscon reitittimissä on eri komentoja jo olemassa olevien konfigurointien tarkasteluun. Tunneleiden tarkasteluun on komento, show ipv6 interface tunnel -testi, jolla voidaan tarkastella luodun testi-tunnelin konfiguraatiota. Show running-config -komento kertoo kaikki reitittimessä käytössä olevat asetukset. Yhteyttä voi testata ping-komennolla. Kaikki testit tukivat tunneloinnin onnistunutta konfigurointia.

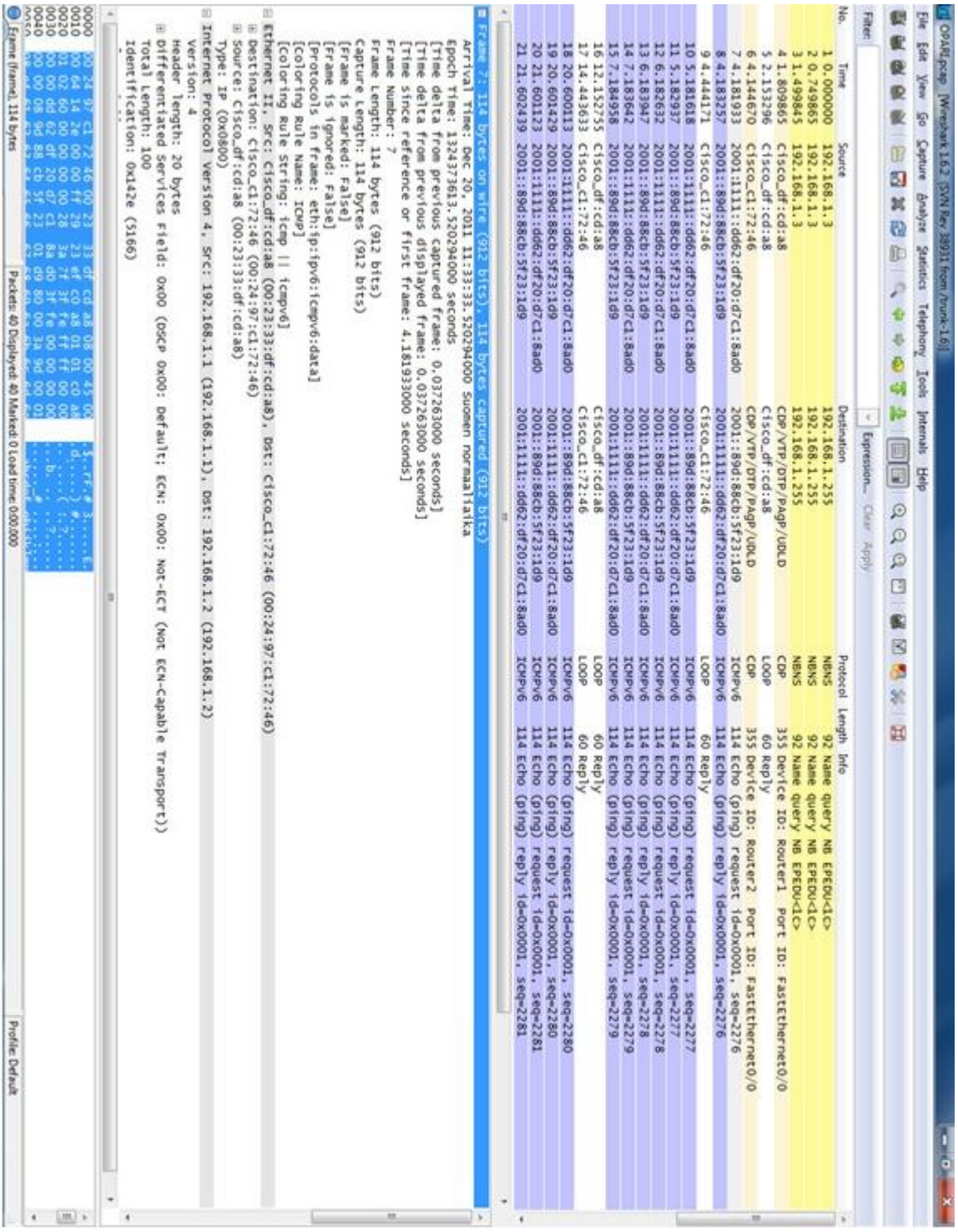
Seuraavassa on kuvat työasemilta suoritetuista ping-testeistä ja Wiresharkin kaappaus.



Kuvio 13. Työasema 1, suoritettu ping-testi.



Kuvio 14. Työasema 2, suoritettu ping-testi.



Kuvio 15. Wireshark-ohjelmiston liikenteen kaappaus.

8 TULOKSET JA YHTEENVETO

8.1 Tulokset

Opinnäytetyössä tutkittiin IPv6-protokollan mukanaan tuomia uusia ominaisuuksia. Tärkeimpinä näistä ominaisuuksista mainittakoon uusi laajennettu osoiteavaruus, otsikkorakenne, autokonfiguraatio ja Neighbor Discovery Protocol. Työssä käytiin läpi myös IPv6-protokollaan liittyvät tietoturvauhat. Lisäksi työssä perehdyttiin IPv6-protokollan yhteensopiviin reititysmenetelmiin.

Opinnäytetyössä onnistuttiin hyvin tutkimaan uudistettua IPv6-protokollaa. Laajennetusta IPv6-osoiteavaruudesta pystyttiin löytämään paljon erilaista tietoa ja vertaamaan sitä IPv4-prokollan kanssa.

IPv4-yhteensopivien IPv6-protokollien testaus suoritettiin käyttämällä tunnelointia. Käytössä oli kaksi Ciscon 1841 -reititintä, HP:n valmistama hubi ja kolme työasemaa. Työn aikana tutustuttiin eri migraatiotekniikoihin: Dual Stack, tunnelointi ja NAT-PT. Näistä eri tekniikoista saatiin todella paljon hyödyllistä tietoa. Työssä testattiin tunnelointitekniikkaa onnistuneesti.

Suurin onnistuminen työssä tuli epäonnistumisista. Epäonnistumisten ansiosta opittiin enemmän IPv6-tekniikoiden vaatimuksista laitteille. Pystyttiin havainnollistamaan IPv6-protokollan täydelliseen tukeen vaadittavat laite-, muisti- ja käyttöjärjestelmävaatimukset. Lisäksi pystyttiin havainnollistamaan mahdolliset laitteiden suorituskykyyn vaikuttavat tekijät. Näiden tietojen avulla Seinäjoen koulutuskuntayhtymä pystyy suunnittelemaan IPv6-protokollaan siirtymisensä paljon tehokkaammin ja ongelmattomammin.

8.2 Yhteenveto

IPv6-protokolla ei ole tähän mennessä kovin laajalle levinnyt protokolla, joten pohjatiedot kyseisestä protokollasta olivat myös vajavaiset. Palkitsevin osa opinnäytetyötä olikin tutustua täysin uuteen protokollaan, tekniikoihin, sen ominaisuuksiin ja miten ne toimivat käytännössä. Tietoa oli paljon saatavilla ja sitä

kerättiin useista erilaisista lähteistä. Työlle asetetut tavoitteet saavutettiin hyvin ja työstä saatiin paljon hyötyä tulevaisuutta varten.

Haastavin osio työssä oli alun pudotus altaan syvään päähän. Protokolla oli työn tekijälle suhteellisen vieras tuttavuus, joten työssä jouduttiin harrastamaan todella ahkeraa tiedon hankintaa. Aihe on hyvin antoisa, mutta myös niin laaja, että opinnäytetyön rajaus oli vaivalloista. Laitteiden käytännön testaus ei tuottanut työntekijälle suuria esteitä erinomaisen dokumentaation ja lähteiden ansiosta.

IPv6-protokollaan siirtyminen on väistämätöntä ja se on erinomainen protokolla tulevaisuutta ajatellen. Erinäisten uusien verkkolaitteiden kehitys ja lisääntyminen takaavat, että uudelle protokollalle on käyttöä jo tänäkin päivänä.

Muutamien vuosien kuluttua IPv6-protokollasta kasvaa vallitseva protokolla IPv4-protokollan hävitessä vähitellen, jääden korkeintaan konehuone käyttöön yhteensopivuustekniikoilla. Uusi ja laajennettu osoiteavaruus on protokollan suurin muutoksentekijä.

LÄHTEET

Anttila, Aki. 2001. TCP/IP tekniikka. 2. korjattu painos. Helsinki: WS Bookwell.

BGPmon. 2009a. IPv6 Deployment. [WWW-dokumentti]. BGPmon.net. [viitattu 16.09.2011] Saatavissa: http://bgpmon.net/blog/wp-content/uploads/2009/04/ipv6-deployment1.png

BGPmon. 2009b. New IPv6 deployment statistics. [WWW-dokumentti]. Bgpmon.net. [viitattu 16.09.2011]. Saatavissa: http://bgpmon.net/blog/?p=166

Carpenter, B. & Moore, K. 2001. Connection of IPv6 Domains via IPv4 Clouds [WWW-dokumentti]. Internet Engineering Task Force. [viitattu 15.09.2011]. Saatavissa: http://www.ietf.org/rfc/rfc3056.txt

Cisco. 2004. IPv6 Extension Headers. [WWW-dokumentti]. Cisco. [viitattu 26.09.2011] Saatavissa: http://www.cisco.com/en/US/i/000001-100000/50001-55000/51001-51500/51459.jpg

Cisco. 2009. IPv6 Header. [WWW-dokumentti]. Cisco. [viitattu 16.09.2011] Saatavissa: http://www.cisco.com/web/about/ac123/ac147/images/ipj/ipj_9-3/93_ipv6_fig1_lg.jpg

Deering, S. & Hinden, R. 1995. Internet Protocol, Version 6 (IPv6) Specification. [WWW-dokumentti]. Internet Engineering Task Force. [viitattu 15.09.2011]. Saatavissa: http://www.ietf.org/rfc/rfc1883.txt

Deering, S. & Hinden, R. 1998. IP Version 6 Addressing Architecture. [WWW-dokumentti]. Internet Engineering Task Force. [viitattu 29.09.2011]. Saatavissa: http://www.ietf.org/rfc/rfc2373.txt

Deering, S. & Hinden, R. 1998. Internet Protocol, Version 6 (IPv6) Specification. [WWW-dokumentti]. Internet Engineering Task Force. [viitattu 15.09.2011]. Saatavissa: http://www.ietf.org/rfc/rfc2460.txt

Desmeules, R. Syyskuu 2007. Cisco Self-Study: Implementing IPv6 Networks (IPv6). 3. painos. United States of America: Cisco Press.

Dornan, A. 2011. What Did IPv6 Day Teach Us? [WWW-dokumentti]. Informationweek.com. [viitattu 16.09.2011]. Saatavissa: http://www.informationweek.com/news/infrastructure/ipv6/230800027

Dunmore, M. 2005. 6net: An IPv6 Deployment Guide [Pdf-julkaisu]. The 6NET Consortium. [viitattu 15.09.2011]. Saatavissa: http://www.6net.org/book/deployment-guide.pdf

Hagen, S. Toukokuu 2006. IPv6 Essentials. 2. painos. O'Reilly Media.

IPv6 Forum. 2008. IPv6 Ready Logo Program. [WWW-dokumentti]. IPv6ready.org. [viitattu 16.09.2011]. Saatavissa: http://www.ipv6ready.org/?page=about

Kaushik, D. 2008a. IPv6 - The History and Timeline. [WWW-dokumentti]. IPv6.com. [viitattu 15.09.2011]. Saatavissa: http://ipv6.com/articles/general/timeline-of-ipv6.htm

Kaushik, D. 2008b. IPv6 Deployment Around The World. [WWW-dokumentti]. IPv6.com. [viitattu 16.09.2011]. Saatavissa: http://ipv6.com/articles/deployment/IPv6-Deployment-Status.htm

Kozierok, C. 2005a. The TCP/IP Guide. [viitattu 26.10.2011] http://www.tcpipguide.com/free/diagrams/ipsecahformat.png

Kozierok, C. 2005b. The TCP/IP Guide. [viitattu 26.10.2011] http://www.tcpipguide.com/free/diagrams/ipsecespformat.png

Lawson, S. 2011. Address allocation kicks off IPv4 endgame. [WWW-dokumentti]. Computerworld. [viitattu 15.09.2011]. Saatavissa: http://www.computerworld.com/s/article/9207438/Address_allocation_kicks_off_IPv4_endgame

Nikulainen, K. 2011. Viimeisetkin vapaat IPv4-osoitealueet jaettiin. [WWW-dokumentti]. www.ITNyt.fi. [viitattu 22.03.2011]. Saatavissa: http://www.itnyt.fi/node/2465-viimeisetkin-vapaat-ipv4-osoitealueet-jaettiin

Palet, J. 2004. IPv6 overall status [Pdf-julkaisu]. IPv6 Task Force [viitattu 16.09.2011]. Saatavissa: http://www.ipv6tf-sc.org/html/public/ipv6tf-sc_pu_d3_4v1_3.pdf

Qin, L., Tatuya, J. & Keiichi, S. 2007. IPv6 Advanced Protocols Implementation. 1. painos. Morgan Kaufmann publisher.

LIITTEET

Liite 1: Reititin 1 running-config.

```
version 12.4
 service timestamps debug datetime msec
 service timestamps log datetime msec
 no service password-encryption
 !
 hostname Router1
 !
 boot-start-marker
 boot-end-marker
 !
 !
 no aaa new-model
 ip cef
 !
 !
 !
 !
 ip auth-proxy max-nodata-conns 3
 ip admission max-nodata-conns 3
 !
 ipv6 unicast-routing
 !
 !
 !
 !
 !
 !
 !
 !
 interface Tunnel0
```

```
 no ip address
 ipv6 address 2001:1111:1111::1/64
 tunnel source 192.168.1.1
 tunnel destination 192.168.1.2
 tunnel mode ipv6ip
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:1111::1/64
 ipv6 enable
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
ip forward-protocol nd
!
!
ip http server
no ip http secure-server
!
ipv6 route 2001::/64::/48 Tunnel0
!
!
!
control-plane
!
!
!
line con 0
line aux 0
```

```
line vty 0 4
 login
!
scheduler allocate 20000 1000
end
```

Liite 2: Reititin 2 running-config.

```
version 12.4
 service timestamps debug datetime msec
 service timestamps log datetime msec
 no service password-encryption
 !
 hostname Router2
 !
 boot-start-marker
 boot-end-marker
 !
 !
 no aaa new-model
 ip cef
 !
 !
 !
 !
 ip auth-proxy max-nodata-conns 3
 ip admission max-nodata-conns 3
 !
 ipv6 unicast-routing
 !
 !
 !
 !
 !
 !
 !
 !
 interface Tunnel1
  no ip address
  ipv6 address 2001:1111:1111::2/64
```

```
 tunnel source 192.168.1.2
 tunnel destination 192.168.1.1
 tunnel mode ipv6ip
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001::1/64
 ipv6 enable
!
interface FastEthernet0/1
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
!
ip forward-protocol nd
!
!
ip http server
no ip http secure-server
!
ipv6 route 2001:1111::/64::/48 Tunnel1
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 login
```

```
!
scheduler allocate 20000 1000
end
```