Eetu Vuori

IPv6-protokollan käyttöönotto palvelinkeskus-verkoissa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

9.5.2016

Metropolia

Tekijä Otsikko Sivumäärä Aika	Eetu Vuori IPv6-protokollan käyttöönotto palvelinkeskusverkoissa 55 sivua 9.5.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaajat	Tietoliikenneasiantuntija Juha Aalto Yliopettaja Matti Puska

Insinöörityön tavoitteena oli toteuttaa selvitystyö palvelinkeskusten käyttämien verkkoympäristöjen IPv4-protokollalla toteutettujen toiminnollisuuksien päivittämisestä hyödyntämään myös uudempaa IPv6-protokollaa. IP-protokolla on yksi nykyaikaisten tietoverkkojen keskeisimmistä kulmakivistä, jonka avulla verkkoihin kytketyt laitteet kykenevät viestimään keskenään. Merkittävin motiivi IPv6-siirtymän toteuttamiselle on IPv4-protokollan mahdollistamien IP-osoitteiden vähäinen määrä, joka on kaikkialla maailmassa johtanut siihen, että IP-osoitteita hallinnoivat organisaatiot eivät kykene enää myöntämään uusia IP-osoiteavaruuksia niitä tarvitseville yrityksille ja organisaatioille.

Varsinaisiin tuotantoverkkoihin ei työssä tehty muutoksia, vaan IPv6-toiminnollisuuksien testaamisessa ja käyttöönoton suunnittelussa hyödynnettiin erillistä, virtualisoitua testipenkkiympäristöä, jolla oli tarkoitus simuloida oikeaa tuotantoympäristöä. Varsinaiselle tuotantoympäristölle ei luonnollisestikaan ollut mahdollista tehdä tämänkaltaisia kokeiluluontoisia toimenpiteitä sen liiketoimintakriittisen luonteen vuoksi.

Selvitystyön tuloksena saatiin luotua kattava yleiskuva käytössä olevan verkkoinfrastruktuurin edellytyksistä toimia IPv6-pohjaisesti. Tärkeimmille käytössä oleville toiminnoille saatiin myös luotua kaksoispinopohjaisen toteuttamisen mahdollistavat esimerkkikonfiguraatiot. Kaksoispino-termillä viitataan verkkolaitteen kykyyn toimia samanaikaisesti IPv4- ja IPv6-pohjaisesti.

Selvitystyön tuloksista ilmeni, että Check Point -merkkisten palomuurien käyttämässä käyttöjärjestelmässä oli muutamia puutteita varsin keskeistenkin toiminnollisuuksien IPv6-tuen suhteen. Muutoin läpikäydyn verkkoinfrastruktuurin tuki IPv6-protokollalle oli riittävällä tasolla halutunlaisen IPv6-siirtymän toteuttamiseksi.

Saatuja tuloksia on mahdollista hyödyntää osana IPv6-siirtymän teknistä suunnittelu- ja toteutusprosessia. Selvitystyöstä saa tätä tarkoitusta varten selkeän kuvan pohjana toimineen verkkoinfrastruktuurin kyvystä toimia IPv6-pohjaisesti ja tärkeimpien käytettyjen toiminnollisuuksien IPv6-pohjaisesta käyttöönotosta.

Avainsanat	IPv6, IPv6-siirtymä, kaksoispino, tietoverkot, palvelinkeskus

Author	Eetu Vuori
Title	Deployment of IPv6 protocol in data center networks
Number of Pages	55 pages
Date	9 May 2016
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Specialisation option	Data Networks
Instructors	Juha Aalto, Network Specialist Matti Puska, Senior Lecturer

The aim of this thesis project was to study the migration of data center environments to support the IPv6 protocol in addition to the older IPv4 protocol. The IP protocol is one of the key technologies in modern computer networks; it is needed in order to enable different network entities to communicate with each other.

Instead of changing the operations of the actual production networks used as the base for this study, this project was carried out as a proof of concept, on a separate, virtualized test bench environment. The test bench environment was built to emulate the actual production environment.

The end-result was a thorough overall assessment of the data center infrastructure's capability to run IPv6 based functions. Example configurations were also made to enable these IPv6 based functions, in addition to the previously existing IPv4 based functions, on the network devices.

The results of the study can be utilized as a part of the planning and execution process of an IPv6 migration. The study gives a clear indication of the network infrastructure's capabilities to run IPv6 based functions. It also gives guidelines on how to enable the functions.

Keywords	IPv6, IPv6 transition, dual-stack, networks, data center

Sisällys

Lyhenteet

BGP *Border Gateway Protocol*. Internetissä käytetty dynaaminen reititysprotokolla, joka suorittaa reitityksen autonomisten järjestelmien, kuten eri internetoperaattoreiden, välillä.

DHCP *Dynamic Host Control Protocol*. Protokolla, jota käyttävän palvelimen avulla voidaan automatisoida verkkoparametrien jakelua verkkoon liitettäville laitteille.

FHRP *First Hop Redundancy Protocol*. Yleisnimitys protokollille, jotka edistävät verkon vikasietoisuutta mahdollistamalla useamman, rinnakkaisen yhdyskäytävän käyttämisen osana yhtä loogista yhdyskäytävää.

FTP *File Transfer Protocol*. Palvelin–asiakasperiaatteella toimiva TCP-pohjainen tiedostonsiirtoprotokolla.

HTTP *Hypertext Transfer Protocol*. Verkkosivustojen palvelinten ja verkkoselainten väliseen viestintään tarkoitettu protokolla.

IGP *Interior Gateway Protocol*. Termi, joka käsittää sellaiset reititysprotokollat, joiden avulla toteutetaan reititystoimintoja yksittäisen autonomisen järjestelmän sisällä.

IP *Internet Protocol*. Protokolla, jonka avulla TCP/IP-pohjaisiin tietoverkkoihin liitetyt laitteet kykenevät viestimään keskenään.

IPsec *Internet Protocol Security.* IPv6:n mukanaan tuoma protokollapino, jonka avulla kyetään todentamaan viestinnän osapuolet, salaamaan lähetettävät viestit ja varmistamaan lähetettyjen viestien eheys.

IS-IS *Intermediate System to Intermediate System*. Operaattoriverkkojen sisällä yleisesti käytetty IGP-reititysprotokolla.

MAC *Media Access Control*. MAC-osoite on jokaisella TCP/IP-verkon verkkolaitteen portilla oleva yksilöllinen arvo, jonka perusteella laite voidaan tunnistaa yksittäisen lähiverkon sisällä.

MPLS *Multiprotocol Label Switching*. Operaattoriverkoissa yleisesti käytetty tekniikka, jonka avulla verkon sisään voidaan luoda VPN-pohjaisia virtuaalisia tunneleita.

MTU *Maximum Transmission Unit*. Useimmiten jonkin verkkolaitteen yhteydessä olevaan linkkiin viittaava suure, joka määrittelee tavuina, miten suuria paketteja linkillä voidaan kuljettaa ja käsitellä.

NAT *Network Address Translation*. Tekniikka, jonka avulla verkkolaite voi muuttaa välittämiensä IP-pakettien otsakkeeseen merkittyjä IP-osoitteita.

NDP *Neigbor Discovery Protocol*. IPv6:n mukanaan tuoma siirtokerroksen protokolla, joka muun muassa muodostaa automaattisesti laitteille globaalit IP-osoitteet, tunnistaa samaan lähiverkkoon liitettyjen solmujen IP-osoitteet ja selvittää niitä vastaavat MAC-osoitteet.

OSI *Open Systems Interconnection*. OSI-malli on standardoitu ja yleisesti käytetty tapa esittää tietoliikennetekniikassa käytettyjen protokollien keskinäisiä suhteita.

RA *Router Advertisement*. IPv6-kykyiset reititinportit lähettävät tietyin väliajoin, ja muiden lähiverkon laitteiden erikseen pyytäessä, RA-paketteja, jotka sisältävät tietoa portista itsestään ja erinäisistä verkkoparametreista.

SIIT *Stateless IP/ICMP Translation*. NAT-mekanismi, jonka avulla voidaan kääntää IPv4-paketti ja sen osoite IPv6-muotoon, ja toisin päin. SIIT kääntää aina tietyn IPv4-osoitteen tiettyyn IPv6-osoitteseen ja toisin päin.

SLAAC *Stateless Address Autoconfiguration*. NDP-protokollaan kuuluva toiminnollisuus, jonka avulla IPv6-pohjaiseen lähiverkkoon kytketyt solmut kykenevät muodostamaan itselleen globaalit IP-osoitteet, samaan lähiverkkoon kytketyn reititinportin osoitteen ja oman MAC-osoitteensa pohjalta.

SSL *Secure Sockets Layer*. Tietoturvaan liittyvä protokolla, jonka avulla varmistetaan verkon välityksellä tapahtuvan viestinnän luottamuksellisuus ja lähetetyn datan eheys.

TCP	*Transmission Control Protocol*. Protokolla, joka on vastuussa yhteyden luonnista ja ylläpidosta kahden verkkoon liitetyn laitteen kesken, lähetettävän datan pilkkomisesta sopivan kokoisiin paketteihin ja pakettien luotettavasta perille menosta.
TMOS	*Traffic Management Operating System*. Verkkolaitevalmistaja F5:n kehittämä käyttöjärjestelmä, jota hyödynnetään sen valmistamissa kuormantasaajissa.
tmsh	*Traffic Management Shell*. F5:n TMOS-käyttöjärjestelmän osa, jonka avulla F5:n laitteita voidaan hallinnoida komentorivipohjaisesti.
URL	*Uniform Resource Locator*. Verkkosivustoa vastaava osoite, joka on ihmiselle helppo muistaa, kuten esimerkiksi www.metropolia.fi. Verkkolaitteet kääntävät URL-muotoiset osoitteet aina niitä vastaaviksi IP-osoitteiksi.
VPN	*Virtual Private Network*. Tunnelointimekanismi, jonka avulla voidaan, tietoturva huomioon ottaen, yhdistää useampia yksityisiä verkkoja, julkista verkkoa, kuten internetiä, rajapintana käyttäen. VPN-tunnelin läpi kulkeva liikenne salataan kaikilta ulkopuolisilta julkisen verkon käyttäjiltä.

1 Johdanto

Insinöörityön tavoitteena on toimia selvitystyönä, jossa käydään läpi työn tilaajayrityksen olemassa olevan palvelinkeskusverkon laiteinfrastruktuuri ja tehdään selvitys sen kyvystä toimia vanhan IPv4-protokollan (Internet Protocol version 4) lisäksi myös uudemmalla IPv6-protokollalla (Internet Protocol version 6). Palvelinkeskuksen laitteiden tärkeimmät IPv4-pohjaisesti toteutetut toiminnot kartoitetaan ja selvitetään tarvittavat toimenpiteet näiden toimintojen toteuttamiseksi myös IPv6-pohjaisesti.

Nykyisissä TCP/IP-pohjaisissa (Transmission Control Protocol / Internet Protocol) tietoverkoissa, kuten esimerkiksi internetissä, IP-protokollan tarkoituksena on toimia välittäjänä, jonka avulla verkkoon liitetyt laitteet kykenevät viestimään keskenään. Tämän viestintätavan toteuttamisessa ovat merkittävässä asemassa erityiset IP-osoitteet. Jokaisella yksittäisellä laitteella, joka kommunikoi tietoverkon läpi, tulee olla uniikki, laitteen yksilöivä IP-osoite.

Pääasiallisena motiivina IPv6-protokollan kehittämiselle ja käyttöönotolle on vanhan IPv4-protokollan sisältämien uniikkien verkko-osoitteiden loppuminen. Esimerkiksi Yhdysvalloissa IP-osoitteita hallinnoiva ja jakeleva organisaatio ARIN (American Registry for Internet Numbers) ilmoitti hallinnoimiensa, vapaasti jaettavien IPv4-osoitteiden loppuneen täysin 24. syyskuuta 2015 [1]. IPv4-standardin mukaiset osoitteet koostuvat 32 bitistä, joilla kyetään esittämään yhteensä 2^{32}, eli noin neljä miljardia, yksilöllistä IP-osoitetta. IPv6-standardissa yksilöllisten osoitteiden määrä on 2^{128}, eli noin 340 sekstiljoonaa (10^{36}). IPv6-protokollan kehityksessä on pyritty toteuttamaan muitakin parannuksia IPv4-protokollaan verrattuna, esimerkiksi lisäämällä tietoturvaominaisuuksia ja tekemällä verkkolaitteiden toteuttamasta IP-pakettien käsittelystä suoraviivaisempaa ja tehokkaampaa.

Tämä insinöörityö toteutetaan Suomessa toimivalle tietoliikenne- ja konesalipalveluita tarjoavalle yritykselle. IPv6-siirtymäprosessiin liittyvän selvityksen toteutusympäristönä toimii yrityksen palvelutuotantoon kuuluva palvelinkeskus, joka on jo valmiiksi liitetty IPv6-kykyiseen runkoverkkoon.

Selvitys rajoittuu palvelinkeskuksen sisäverkkoon ja sen toteuttamisessa hyödynnettäviin laitteisiin. Työhön liittyvät käytännön testit toteutetaan tuotantojärjestelmistä erillisellä, virtualisoidulla testialustalla, jonka on tarkoitus simuloida oikeaa tuotantoympäristöä.

Työn toteuttamisen motiivi on selkeä: IPv4-osoitteiden loppuessa konesali- ja tietoliikennepalveluita tarjoavan yrityksen kaltaiselle toimijalle on liiketoiminnan jatkuvuuden kannalta elintärkeää kyetä jatkamaan palveluidensa tarjontaa myös uutta IPv6-protokollaa hyödyntäen.

2 IP-protokolla ja IPv6

2.1 IP-protokollan ominaisuudet

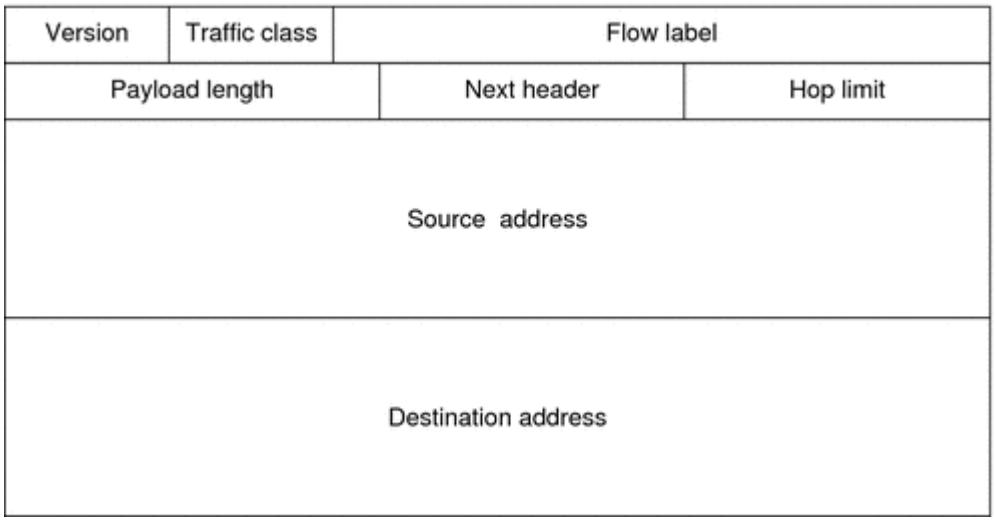
IP-protokollan perimmäisenä tarkoituksena on yksilöidä jokainen solmu (verkkokerroksella toimiva, oman IP-osoitteen omaava laite tai reititinportti), joka haluaa kommunikoida TCP/IP-pohjaisissa tietoverkoissa olevien muiden solmujen kanssa, ja varmistaa näiden laitteiden toisilleen lähettämän datan menevän sille vastaanottajalle, jolle se on tarkoitettu. Jokaista internetiin liitettyä yksilöllistä solmua vastaa IP-osoite, joka toimii samanlaisella periaatteella kuin perinteinen postiosoite: sen avulla, lähetetyt viestit löytävät oikean vastaanottajan luokse.

Jokainen verkkoon kytketty laite, joka haluaa lähettää dataa jollekin toiselle laitteelle, hyödyntää ensin OSI-mallin (Open Systems Interconnection) (kuva 1) kuljetuskerroksen protokollaa, kuten esimerkiksi TCP:tä. Kuljetuskerroksen protokolla pilkkoo ylempien kerrosten luoman lähetettävän datan sopivankokoisiin osiin ja tekee näihin osasiin omia, protokollan toiminnan kannalta keskeisiä merkintöjä. Tämän jälkeen nämä kuljetuskerroksen luomat osaset siirtyvät OSI-mallissa kerrosta alemmas, verkkokerrokselle, jossa IP-protokolla ottaa ne käsiteltäväkseen.

Kuva 1. OSI-malli, joka esittää, miten tietoliikennevirta kulkee verkkolaitteiden protokollapinojen lävitse [2].

2.1.1 IP-paketin rakenne

IP-protokolla kapseloi ylemmän tason protokollalta tulleen paketin sellaisenaan ja lisää päälle omat merkintänsä erilliseen otsakkeeseen. IPv6-protokollan tapauksessa tämä tapahtuu kuvan 2 mukaisesti. Kuten tietotekniikassa yleensäkin, nämä merkinnät toteutetaan binaarilukupohjaisesti, bittien avulla. Paketteja käsittelevät laitteet lukevat nämä merkinnät ja käsittelevät vastaanottamaansa pakettia sen sisältämien arvojen perusteella.



Kuva 2. IPv6-paketin rakenne [3].

IPv6-protokollan käyttämä otsake koostuu seuraavista kentistä:

- Version (4 bittiä). Määrittelee käytetyn protokollan version. IPv6:ssa numero on aina 0110 eli desimaaliluku 6. [4.]

- Traffic class (8 bittiä). Voidaan käyttää paketille annettavan palvelunlaatuprioriteetin määrittelemiseen. Esimerkiksi verkon läpi tapahtuvien IP-puheluiden pakettivirralle voidaan antaa korkeampi käsittelyprioriteetti kuin verkkosivustojen käyttämälle HTTP-liikenteelle (Hypertext Transfer Protocol). Liikennettä eteenpäin ohjaavat verkkolaitteet huomioivat kentän arvon ja reitittävät eri paketteja erilaisilla prioriteeteilla tämän arvon perusteella. [4.]

– Flow label (20 bittiä). Voidaan käyttää ohjeistamaan tiettyä pakettivirtaa käsittelevät laitteet toimimaan tähän virtaan kuuluvien pakettien kohdalla aina samalla tavalla. Toimintoa voidaan käyttää esimerkiksi ohjaamaan tiettyyn pakettivirtaan kuuluvat paketit kulkemaan aina yhtä ja samaa reittiä pitkin, mikäli kohteeseen on useampia vaihtoehtoisia reittejä. Näin voidaan toteuttaa esimerkiksi kuormantasaustoiminto eri reittien kesken jakamalla tasaisesti eri pakettivirrat eri reiteille. [5.]

– Payload length (16 bittiä). Ilmaisee kuljetuskerroksen protokollalta saadun paketin koon tavuina [4].

– Next header (8 bittiä). Ilmaisee paketin sisälle kapseloidun paketin otsakkeen tyypin. Useimmiten kyseessä on kuljetuskerroksen protokollan otsake, mutta kyseessä voi olla myös IPv6:n itsensä luoma ylimääräinen otsake, jolla toteutetaan protokollan harvemmin käytettyjä toimintoja, kuten esimerkiksi tiedonsiirron osapuolten autentikointia. [4; 6.]

– Hop limit (8 bittiä). Vastaa IPv4-protokollan käyttämää TTL-arvoa (Time To Live), jonka tarkoituksena on estää pakettia jäämästä ikuisesti verkkoon, mikäli verkossa esiintyisi, esimerkiksi virheellisen laitemäärittelyn vuoksi, reitityssilmukka. Mekanismi toimii siten, että kun paketti kulkee jonkin verkkokerroksella toimivan laitteen lävitse, laite pienentää kentän arvoa yhdellä, ja kun kenttä saa arvon 0, paketti tuhotaan eikä sitä lähetetä enää eteenpäin. [4.]

– Source address (128 bittiä). Paketin lähdeosoite, eli tavallisesti sen laitteen IP-osoite, joka paketin on luonut [4].

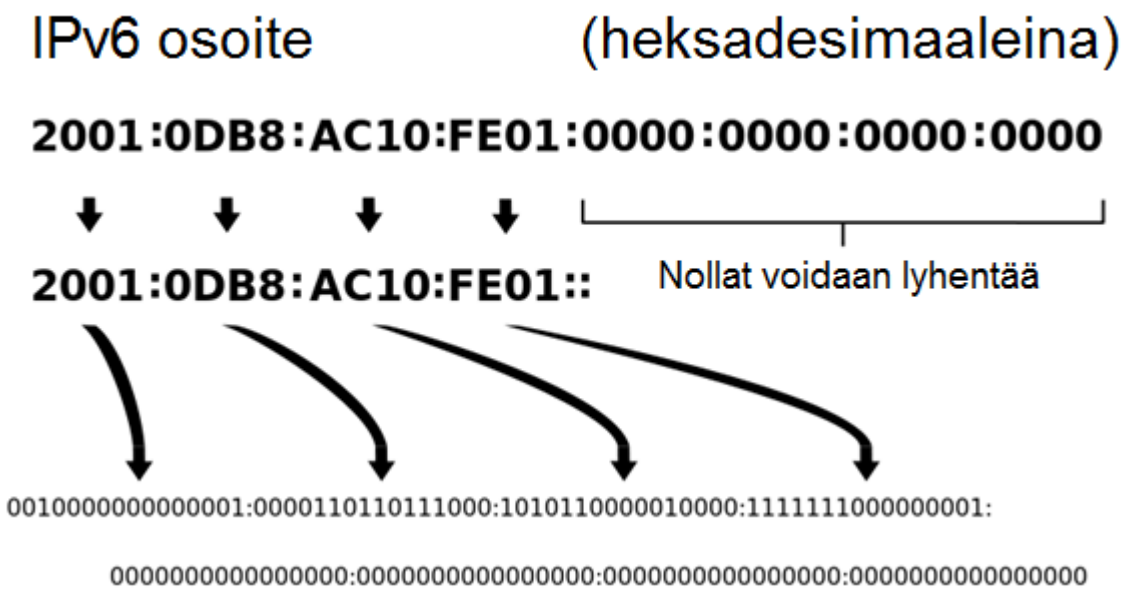
– Destination address (128 bittiä). Paketille määritelty kohdeosoite [4].

Laite, esimerkiksi PC-työasema, joka on lähettämässä dataa verkkoon, siirtää luomansa IP-paketin siirtokerroksen protokollalle kapseloitavaksi ja edelleen eteenpäin lähetettäväksi OSI-mallin esittämän protokollapinon mukaisesti (kuva 1). Vastaanottajan päässä oleva laite taas, saatuaan paketin siirtokerrokselta, käsittelee ja purkaa IP-protokollan luoman otsakkeen ja siirtää paketin protokollapinossa ylöspäin kuljetuskerrokselle.

Myös paketin siirtotiellä olevat laitteet, kuten reitittimet ja palomuurit, hyödyntävät IP-protokollaa ja sen sisältämiä tietokenttiä. Hyödyntäminen tapahtuu esimerkiksi tehtäessä reitityspäätöksiä kohdeosoitteen perusteella tai tarkastettaessa, onko tietyllä tavalla merkittyjä IP-paketteja syytä päästää läpi, esimerkiksi palvelinkeskuksen sisäverkkoon, vai onko ne syytä suodattaa pois.

2.1.2 IP-osoitteiden rakenne

IPv6:n käyttämä osoiteformaatti koostuu 128 bitistä, ja se on tapana esittää heksadesimaalilukuina. Nämä heksadesimaaliluvut on jaoteltu kahdeksaan kuudentoista bitin kenttään, jotka siis voivat saada heksadesimaaliarvon väliltä 0–FFFF. Desimaalilukuina tämä tarkoittaa 65 536 mahdollista yksilöllistä arvoa yhtä kenttää kohden. Mikäli osoitteessa esiintyy useampi peräkkäinen kenttä, joiden kaikkien arvot ovat 0, voidaan nämä kentät lyhentää kahdella kaksoispisteellä kuvan 3 mukaisesti. Luonnollisestikin tämänkaltainen lyhentäminen voidaan tehdä vain yhdelle 0-arvojen riville, jotta esitetyn osoitteen yksiselitteisyys säilyy. [7.]



Kuva 3. IPv6-osoite, peräkkäisten nollien typistäminen ja käännös binaarimuotoon [8].

IPv6-protokolla määrittelee kolme erilaista osoitetyyppiä:

- täsmälähetys (unicast), jolla merkitään paketti, joka halutaan lähettää yhdelle tietylle verkon solmulle [7]

- jokulähetys (anycast), joka vastaa useampaa solmua, joista lähetetty paketti toimitetaan vain yhdelle [7]

- ryhmälähetys (multicast), jolla lähetetään paketteja useammalle solmulle samanaikaisesti [7].

IPv4:n käyttämä yleislähetysosoite (broadcast), eli kaikkia tietyn aliverkon solmuja vastaava osoite, ei ole enää käytössä IPv6-protokollan yhteydessä [7].

Tavanomaisimmin käytetyissä täsmälähetystyyppisissä IP-osoitteissa on IP-protokollan toimintalogiikan kannalta tarkasteltuna kaksi toisistaan erillistä osaa: verkko-osuus ja laiteosuus.

Verkko-osuus on se osa osoitetta, joka yksilöi kyseistä osoitetta vastaavan lähiverkon ja jota verkkokerroksella toimivat laitteet, kuten reitittimet, vertaavat omaan reititystauluunsa ja siten hyödyntävät reitittäessään paketteja kohti oikeaa lähiverkkoa. Reititinten ei kuitenkaan tarvitse ottaa kantaa yksittäisen solmun sijaintiin tämän lähiverkon sisällä, joten IP-osoitteen loppuosaa ei tarkastella. Verkko-osuus eritellään kokonaisesta IP-osoitteesta erityisellä verkon prefiksillä, jolla merkitään se osuus biteistä, joka kuuluu verkko-osuuteen. Esimerkiksi osoite, jonka verkko-osio on 64 bitin pituinen, merkittäisiin prefiksillä /64. Prefiksi esitetään aina varsinaisen osoitteen jälkeen, seuraavan esimerkin mukaisesti: 2001:0db8:ac10:fe01::**/64**. [7.]

Verkko-osuuden jälkeen tulevat bitit kuuluvat laiteosuuteen. Laiteosuus yksilöi yksittäisen solmun lähiverkon sisällä. Laiteosuutta tarkastellaan ainoastaan silloin, kun liikennöidään tämän tietyn lähiverkon sisällä. [7.]

2.2 IPv6-protokollan uudistukset

IPv6-protokollan edeltäjä ja nykyään yhä laajalti käytetty IPv4-protokolla määriteltiin alun perin 1970-luvulla. Tämä tehtiin osana Yhdysvaltojen puolustusministeriön rahoittamaa ARPANET-hanketta (Advanced Research Projects Agency Network), jonka tavoitteena oli luoda tutkimuskäyttöön tarkoitettu, pakettikytkentäinen tietoverkko. Projektin tuloksena luotu ARPANET-verkko alkoi kasvattaa suosiotaan varsin nopeasti ja levitä myös Yhdysvaltojen ulkopuolelle. Vuonna 1990 silloinen ARPANET lopetettiin ja korvattiin nykymuotoisella internetillä. [9.]

Internetin yhä laajentuessa kävi nopeasti selväksi, että alun perin suljetun ARPANET-verkon tarpeisiin kehitetty IPv4-protokolla tulisi kärsimään merkittävistä skaalautuvuusongelmista nopeasti kasvavan internetin kanssa. 1990-luvun alussa aloitettiin työ uuden, IPv4:n puutteita korjaavan protokollan kehittämiseksi, jota tuolloin kutsuttiin nimellä IPng eli IP next generation. Joulukuussa 1995 virallistettiin neljä eri RFC-dokumenttia (Request For Comments), jotka koskivat uutta IPv4-protokollan korvaajaksi tarkoitettua IP-protokollaa, jolle annettiin nimeksi IPv6. RFC-dokumentit ovat internetin käyttämään teknologiaan liittyviä standardeja hallinoivan IETF-järjestön (Internet Engineering Task Force) virallisia dokumentteja, joissa määritellään internetin teknisiä ja hallinnollisia standardeja sekä suositeltavia käytäntöjä. [9; 10.]

Seuraavissa alaluvuissa käsitellään merkittävimpiä IPv6-protokollan mukanaan tuomia uudistuksia vanhaan IPv4-protokollaan verrattuna.

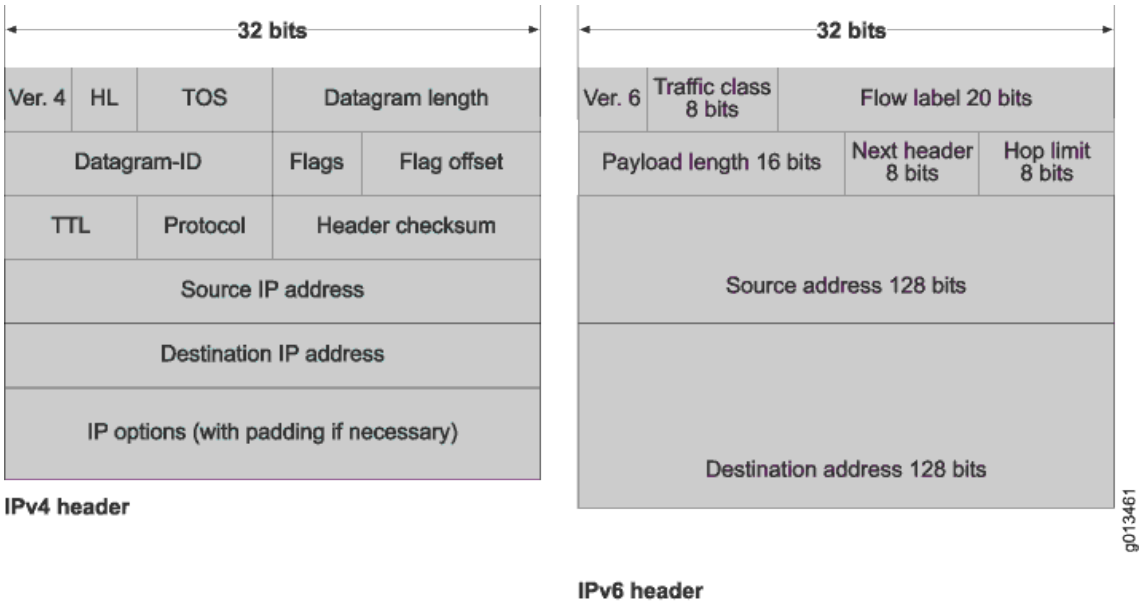
2.2.1 IP-osoitteiden määrän kasvu

Vanhassa IPv4-standardissa osoitteiden esittämiseen käytetään 32 bittiä, mikä tarkoittaa, että uniikkeja osoitteita kyetään teoriassa esittämään yhteensä 2^{32} eli noin 4,3 miljardia. Arvioiden mukaan internetiin kytkettyjä laitteita tulisi vuonna 2020 olemaan noin 26 miljardia, ja niistä merkittävä osa olisi IoT-pohjaisia (Internet of Things) laitteita eli sulautettuja järjestelmiä, kuten kodinkoneita tai erilaisia antureita, joissa on internetyhteys [11]. Täten myös jokainen näistä laitteista vaatii oman, uniikin, sitä laitetta vastaavan IP-osoitteen.

Tärkein IPv6-protokollan mukanaan tuoma uudistus onkin IP-osoiteavaruuden merkittävä kasvu. IPv6-standardissa osoitteiden esittämiseen käytetään 128 bittiä, mikä tarkoittaa, että uniikkeja osoitteita kyetään teoriassa esittämään 2^{128} eli noin 340 sekstiljoonaa (10^{36}) [4]. Esimerkiksi aiemmin mainittu 26 miljardia tästä määrästä olisi vain 7,64 * 10^{-27} %. IPv6 siis epäilemättä ratkaisee uniikkien IP-osoitteiden puutteen aina pitkälle tulevaisuuteen saakka.

2.2.2 Tehostettu paketinkäsittely ja lisätoiminnollisuuksien modulaarisuus

IPv6-protokollan paketin otsakkeen rakennetta on yksinkertaistettu verrattuna IPv4-protokollan vastaavaan (kuva 4). Tämä tarkoittaa, että verkkolaitteiden toteuttama pakettien käsittely saadaan toteutettua aiempaa tehokkaammin ja vähemmän verkkolaitteiden resursseja, kuten prosessoritehoa ja muistia, kuormittavalla tavalla.



Kuva 4. IPv4- ja IPv6-otsakkeet [12].

Paketin rakenteen yksinkertaistaminen on toteutettu siirtämällä tiettyjen IP-protokollan toimintojen käsitteleminen ja suorittaminen dataliikenteen loppupään laitteiden, kuten PC-työasemien, vastuulle. Tällaisia toimintoja ovat esimerkiksi paketin eheyden varmistaminen ja yksittäisen paketin koon määritteleminen siten, että se on korkeintaan pienimmän siirtoväylän linkillä esiintyvän MTU:n (Maximum Transmission Unit), eli sallitun paketin maksimikoon, mukainen. Toisin kuin IPv4-pakettien kohdalla, verkkolaitteet eivät fragmentoi, eli pilko pienempiin osiin, ylisuuria IPv6-paketteja [4.]

Tämänkaltaisten toimintojen käyttäminen ilman erillisiä IP-otsakkeen kenttiä tapahtuu pääosin erillisen extension header -otsakkeen tai otsakkeiden avulla, jotka sijoitetaan IP-protokollan luoman lopullisen paketin sisälle, kuljetuskerroksen ja verkkokerroksen tavanomaisten otsakkeiden väliin. Myös siirtoväylän varrella olevien verkkolaitteiden hyödyntämiä toimintoja on mahdollista toteuttaa tällä tavoin.

Tämänkaltainen toteutustapa tarkoittaa käytännössä myös sitä, että IPv6-protokollaan kyetään modulaarisesti lisäämään aivan uusia toiminnollisuuksia, ilman että standardin määrittelemään tavanomaiseen pääotsakkeeseen olisi tarvetta tehdä minkäänlaisia muutoksia. Tämä varmistaa, että IPv6-protokolla kyetään pitämään tulevaisuudessa ajan vaatimusten mukaisena myös sen sisältämien ominaisuuksien suhteen, ilman että syntyisi tarvetta muuttaa nykyistä, laajalti käytössä olevaa IPv6-otsakkeen standardia tai luoda täysin uutta. [4.]

2.2.3 SLAAC – automatisoitu osoitteiden hallinta

IPv4-pohjaisiin lähiverkkoihin kytketyt loppukäyttäjien laitteet saavat usein verkkoparametrinsa, kuten IP-osoitteen, automatisoidusti erilliseltä verkon ylläpitäjän asentamalta DHCP-palvelimelta (Dynamic Host Control Protocol). Vastaavanlaista palvelinta voidaan hyödyntää myös IPv6-pohjaisissa verkoissa, joissa sitä kutsutaan nimellä DHCPv6 [13]. IP-osoitteiden jakelu voidaan kuitenkin toteuttaa IPv6-pohjaisissa verkoissa myös ilman erillistä DHCP-palvelinta käyttäen apuna määriteltävien laitteiden kanssa samassa lähiverkossa sijaitsevaa reititinporttia, joka hyödyntää IPv6:n mukanaan tuomaa NDP-protokollaa (Neigbor Discovery Protocol). Tätä toiminnollisuutta kutsutaan nimellä SLAAC (Stateless Address Autoconfiguration). [14.]

Jokainen IPv6-pohjainen solmu luo aina käynnistyessään itselleen erillisen link-local-tyyppisen IP-osoitteen, jota voidaan hyödyntää paikallisen lähiverkon sisällä tapahtuvassa viestinnässä, mutta jota käyttäviä paketteja ei kuitenkaan reititetä ulkoisiin verkkoihin. Link-local-osoite muodostuu kahdesta osasta: kiinteästä fe80::/64-verkkoprefiksistä ja laitteen tai portin MAC-osoitteesta (Media Access Control), joka on tavallisesti siirtokerroksen protokollan, kuten Ethernetin, hyödyntämä, laitteen valmistajan jo tehtaalla laitteen lukumuistiin tallentama numerosarja. Tarpeen vaatiessa MAC-osoitetta täydennetään nollilla edestä alkaen, jotta fe80::/64-prefiksin jälkeen tulevat 64 bittiä saadaan kokonaisuudessaan täytetyksi. [14.]

Tämän jälkeen laite voi hyödyntää SLAAC-toimintoa muodostaakseen itselleen yksilöllisen, globaalin IP-osoitteen, jota voidaan hyödyntää esimerkiksi internetin läpi tapahtuvassa viestinnässä. Tämä tapahtuu siten, että verkkoon kytketty laite lähettää link-local-osoitettaan käyttäen erityisen RS-kyselyn (Router Solicitation) ryhmälähetyksenä kaikille lähiverkon solmuille. Kun SLAAC-toimintoa käyttäväksi määritelty reititinportti vastaanottaa tämän kyselyn, se vastaa kyselyn tehneelle laitteelle omalla RA-paketillaan (Router Advertisement). Tämä RA-paketti sisältää muun muassa oletusyhdyskäytävän IP-osoitteen ja reititinportin oman osoitteen, joka puolestaan sisältää /64-prefiksin omaaman verkko-osuuden, jota kyselyn alun perin tehnyt laite käyttää oman globaalin IP-osoitteensa muodostamiseen. Osoite muodostetaan samaan tapaan kuin link-local-osoitekin, eli osoitteen viimeiset 64 bittiä muodostuvat laitteen yksilöllisen MAC-osoitteen perusteella. SLAAC-toiminnon avulla muodostetun osoitteen verkko-osio on luonnollisesti sama kuin kyselyyn vastanneella reitittimen portilla. Huomionarvoista on, että SLAAC-toimintoa hyödyntävän lähiverkon osoitteiden verkko-osion prefiksin tulee aina olla tasan /64. [14.]

Myös DNS-palvelimen (Domain Name System) osoitteen tiedottaminen loppukäyttäjien laitteille onnistuu SLAAC:n kaltaisella toiminnolla, joka toteutetaan samaan tapaan samassa aliverkossa olevan reititinportin ja NDP-protokollan RA-paketin avulla [15]. Vaihtoehtoisesti myös DNS-palvelimen osoitteen automatisoituun tiedottamiseen voidaan soveltaa DHCPv6-palvelinta. DNS-palvelin on verkkopalveluiden käytön kannalta keskeinen osa, joka kääntää ihmisille helposti muistettavat URL-malliset osoitteet (Uniform Resource Locator), kuten www.google.fi, niitä vastaaviksi IP-osoitteiksi, kuten 2607:f8b0:4000:809::1018, joita IP-protokolla ja sitä käyttävät laitteet osaavat hyödyntää [16].

SLAAC-toiminnon lisäksi NDP tuo mukanaan muitakin toiminnollisuuksia, kuten saman lähiverkon solmujen ja niitä vastaavien IP- ja MAC-osoitteiden automaattisen tunnistamisen, päällekkäisten IP-osoitteiden havaitsemisen ja keepalive-funktion eli ajoittaiset tarkistukset, joilla varmistetaan, että aiemmin tunnistetut naapurilaitteet ovat yhä aktiivisina verkossa [17].

2.2.4 Tietoturva- ja yksityisyysominaisuudet

Kun IPv4-protokolla alun perin kehitettiin suljetun ARPANET-verkon tarpeisiin, tietoturva- tai yksityisyyskysymykset eivät olleet lainkaan niin ajankohtaisia kuin nykypäivän

internetissä. Tästä syystä IPv4-standardiin ei alun perin nähty tarpeelliseksi kehittää minkäänlaisia tietoturvaominaisuuksia. Nykypäivän tietoverkoissa ja niiden käyttösovelluksissa tietoturvaominaisuuksien tarve on kuitenkin merkittävästi korostunut, ja tämä onkin huomioitu IPv6:n kehityksessä.

IPv6 pitää sisällään kokonaisen protokollapinon (vrt. OSI-malli) nimeltään IPsec (Internet Protocol Security). IPsec tarjoaa toiminnollisuudet viestinnän osapuolten autentikoimiseen ja lähetettävän tiedon salaamiseen ja sen eheyden varmistamiseen. IPsec hyödyntää toiminnoissaan kolmea erityyppistä protokollaa: AH (Authentication Header), ESP (Encapsulating Security Payload) ja SA (Security Association) [18].

AH- ja ESP-protokollat mahdollistavat lähetetyn datan eheyden varmistamisen ja viestinnän osapuolten autentikoinnin. Näiden ominaisuuksien lisäksi ESP-protokolla mahdollistaa myös lähetettävän datan salaamisen. ESP onkin näistä kahdesta protokollasta ainoa, jonka käyttämisen IPsec-standardi määrittelee pakolliseksi ja joka on useimmiten myöskin ainoa, jota on tarvetta käyttää. [18.]

Iso osa kahden aiemman protokollan toiminnoista perustuu erityisten salausavainten käyttöön, joiden tulee olla kaikkien suojatun viestinnän osapuolten tiedossa. Nämä avaimet voidaan määritellä manuaalisesti, mutta useimmiten senkaltainen ratkaisu on järjestelmän hallinnoinnin kannalta liian työläs ja hankala toteuttaa ja ylläpitää. Tarvittavien salausavainten luontiin ja niiden levittämiseen haluttujen, ja vain haluttujen, osapuolten tietoisuuteen käytetäänkin useimmiten SA-protokollaa [18].

IPsec-salauksen pääte, eli laite jossa liikenteen salaus luodaan tai puretaan, voidaan asettaa varsinaisten loppukäyttäjien laitteiden lisäksi myös erityisiin yhdyskäytäviin, jotka eivät ole lähetettävän tai vastaanotettavan viestinnän päätepisteitä [18]. Esimerkiksi kotoaan työskentelevä, henkilökohtaisen internetliittymänsä päässä oleva työntekijä voisi ottaa julkista internetiä hyödyntäen IPsec-salatun VPN-yhteyden (Virtual Private Network) työpaikkansa sisäverkon reunalla olevaan palomuuriin, saadakseen pääsyn yrityksen sisäverkossa oleviin tietoihin ja resursseihin, niin että yrityksen sisäiseen käyttöön tarkoitettu data kulkee kuitenkin julkisen internetin läpi salatussa muodossa ja vain luotettujen päätepisteiden välillä. Tämänkaltainen VPN-yhteys onkin yksi yleisimmistä IPsec-protokollapinon käyttösovelluksista.

Luvussa 2.2.3 käsitelty SLAAC-tekniikka tuo myös mukanaan tiettyjä tietoturvaan ja yksityisyyteen liittyviä haasteita. Prosessi, jossa laitteelle luodaan globaali IP-osoite sen uniikin MAC-osoitteen perusteella, johtaa aina siihen, että myös muodostettu IP-osoite on tietynlainen ja uniikki. Tämä on tietenkin tekniikalle asetetun tavoitteen mukainen ja toivottu lopputulos, mutta samalla se tarkoittaa myös, että laitteen käyttäjän toimia verkossa kyetään helposti yksilöimään ja täten tarkkailemaan tämän IP-osoitteen perusteella. Myös käytetyn laitteen verkkokortin tarkka malli kyetään määrittelemään MAC-osoitteen perusteella, joka siis näkyy osana käytetyn laitteen julkista IP-osoitetta ja jota voidaan hyödyntää verkkohyökkäysten valmistelussa.

Kuvatun kaltaisten ongelmien ratkaisemiseksi IPv6-protokollan yhteyteen on kehitetty erityinen privacy extensions -lisätoiminnollisuus. Tämän toiminnon avulla SLAAC-toiminnolla luotujen IP-osoitteiden laite-osuuksista voidaan johtaa alkuperäisestä eroavia arvoja käyttämällä esimerkiksi MD5-tiivistefunktiota (Message Digest 5) ja satunnaista salausavainta ja käyttää näin muodostettuja arvoja käytetyn IP-osoitteen laite-osuuden vaihtamiseen aina tasaisin väliajoin [19]. Tätä menetelmää käytettäessä SLAAC-toiminnon luomaa julkista IP-osoitetta käyttävän laitteen verkkotoimintaa on hankalampi yksilöidä, jäljittää ja seurata, eikä näin saadusta IP-osoitteesta ole myöskään mahdollista suoraan päätellä laitteen käyttämän verkkokortin mallia.

2.3 Tekniikat IPv6-siirtymän toteuttamiseen

On selvää, että koko internetin siirtymä IPv4:stä IPv6:een, jotka eivät ole keskenään yhteensopivia, ei tapahdu hetkessä. Vuonna 2014 vasta 0,6 prosenttia internetin läpi kulkeneesta liikenteestä oli IPv6-pohjaista [20]. IPv6-siirtymän toteuttamisesta ei seuraa palveluiden loppukäyttäjille merkittäviä näkyviä hyötyjä, eikä täten myöskään palveluntarjoajilla ole merkittävää liiketoiminnallista motiivia ryhtyä edistämään IPv6-siirtymää, olettaen, että palveluntarjoajalla itsellään on riittävänkokoinen IPv4-osoiteavaruus, kuten vakiintuneilla toimijoilla usein on. Täysin IPv6-pohjaisen internetin sijasta molemmat protokollat – IPv4 ja IPv6 – elävät rinnakkain vielä pitkälle tulevaisuuteen.

IPv6-siirtymää edistämään onkin kehitetty muutamia tekniikoita, joiden avulla laitteet pystyvät tukemaan rinnakkain sekä IPv4- että IPv6-pohjaisia toimintoja tai viestimään keskenään käytetyistä protokollista riippumatta. Näiden tekniikoiden tarkoituksena on

toimia siirtymäkauden ratkaisuina mahdollistaen mahdollisimman sujuvan siirtymän lopulliseen tavoitteeseen eli puhtaasti IPv6-pohjaiseen internetiin.

2.3.1 Kaksoispino

Yksinkertaisin ja yleisesti suositelluin tapa IPv6-siirtymän toteuttamiseksi on hyödyntää kaksoispinomekanismia (dual-stack). Kaksoispino tarkoittaa yksinkertaisesti sitä, että verkon solmu tukee sekä IPv4- että IPv6-protokollia, sillä on molemmantyyppiset IP-osoitteet ja se kykenee luomaan ja käsittelemään molempien standardien mukaisia IP-paketteja. [21.]

Kaksoispinoa voidaan hyödyntää silloin, kun hallinnoitavassa verkossa on välttämätöntä tukea samanaikaisesti sekä IPv4- että IPv6-pohjaisia järjestelmiä. Luonnollisestikin kaksoispinon soveltaminen asettaa lisävaatimuksia verkon ylläpitoprosessien, kuten monitoroinnin, vianselvityksen ja dokumentoinnin, suhteen, kun otetaan huomioon, että kaikki nämä toiminnot on tarpeen suorittaa yhden IP-protokollapinon sijasta kahdella eri protokollapinolla. Myös laitteet, joille on asetettu kaksoispinotoiminto, vaativat tavallista enemmän prosessori- ja muistikapasiteettia, jotta ne kykenevät suorittamaan ja ylläpitämään molempien protokollien vaatimia toimintoja.

Tässä insinöörityössä asetettujen tavoitteiden toteuttamisessa sovelletaan kaksoispinomekanismia. Merkittävin syy kaksoispinopohjaiseen toteutukseen päätymiseen oli ympäristön hallinnan ja palveluiden toimittamisen suoraviivaisuus verrattuna vaihtoehtoisiin ratkaisuihin. Suuressa palvelinkeskusympäristössä, jossa on tarkoitus ylläpitää lukuisia eri IPv4- ja IPv6-pohjaisia palveluita lukuisille eri asiakkaille, palveluiden ylläpitämisen suoraviivaisuus korostuu entisestään ja vaikuttaa myös loppuasiakkaan kokemaan palvelun laatuun.

2.3.2 Tunnelointi

Tunneloinnilla tarkoitetaan tässä yhteydessä sitä, että olemassa olevaa IPv4-pohjaista verkkoinfrastruktuuria hyödynnetään IPv6-liikenteen siirrossa siten, että IPv6-paketit kapseloidaan IPv4-pakettien sisään. Tällöin pakettien siirtotien varrella olevat puhtaasti IPv4-kykyiset laitteet kykenevät välittämään liikennettä pelkkien IPv4-otsakkeiden perusteella, ilman minkäänlaista tarvetta ottaa kantaa IPv4-pakettien sisällä oleviin alkuperäi-

siin IPv6-paketteihin ja niiden käyttämiin otsakkeisiin [21]. Myöhemmässä vaiheessa siirtymää, kun IPv6 on hallitseva protokolla ja IPv4 harvemmin käytetty, voidaan hyödyntää myös sellaisia tunnelointimekanismeja, jotka toimivat vastakkaiseen tapaan eli kapseloivat IPv4-paketteja IPv6-pakettien sisään.

Tämänkaltaisten tunneleiden päätepisteeksi voidaan määritellä joko lopullisena päätepisteenä oleva laite, kuten palvelin, tai lopullista päätepistettä edeltävä verkkolaite, kuten reititin. Asetettaessa päätepiste liikenteen lopullista kohdetta edeltävään verkkolaitteeseen tunnelin käyttämä IPv4-kapselointi puretaan jo siirtoväylällä ja paketti lähetetään eteenpäin kohti lopullista määränpäätä sen alkuperäisessä muodossa. Tällä tavoin voidaan helposti yhdistää kaksi erillistä IPv6-verkkosaareketta, kuten esimerkiksi yrityksen toimipisteiden sisäverkot, yhteen IPv4-pohjaisen verkkoinfrastruktuurin lävitse. Tunneloinnissa lisättävien otsakkeiden käyttämät IP-osoitteet ovat ylläpitäjän määriteltävissä; useimmiten ne ovat tunnelin päätelaitteiden porttien käyttämiä osoitteita. [21.]

2.3.3 Osoitteenmuunnosmekanismit: NAT64 & SIIT

Kolmas vaihtoehto IPv6-siirtymän tukemiseen on NAT-toiminnollisuuden (Network Address Translation) eli osoitteenmuunnoksen soveltaminen. NAT luotiin alun perin pidentämään IPv4-protokollan käyttöikää yhdessä privaattiosoitteiden, kuten 10.0.0.0/8, kanssa. Privaattiosoitteet ovat erikoisryhmä IP-osoitteita, joita kaikki saavat vapaasti käyttää omissa sisäverkoissaan, mutta joita ei reititetä julkisissa verkoissa. IPv4-ympäristössä NAT-osoitteenmuunnosta sovelletaan siten, että sisäisen ja julkisen verkon välille asetetaan erityinen NAT-yhdyskäytävänä toimiva laite, joka toteuttaa osoitteenmuunnoksen. Kun yhdyskäytävän takana oleva sisäverkon laite, jolla on privaattiosoite, haluaa kommunikoida ulkoverkossa sijaitsevan laitteen kanssa, liikenne kulkee NAT-yhdyskäytävän läpi, joka muuttaa paketin otsakkeessa olevan sisäverkon laitteen käyttämän ja merkitsemän privaattiosoitteen erikseen määriteltyyn julkisen verkon osoitteeseen. Paluuliikenteelle sama tehdään toisinpäin: NAT-yhdyskäytävän alun perin antama julkinen kohdeosoite muutetaan takaisin viestinnän aloittaneen laitteen privaattiosoitteeseen ennen paketin perille toimittamista. Tällöin jokaiselle sisäverkon laitteelle ei ole tarvetta määritellä omaa, julkista IP-osoitetta, vaan ne voivat tarpeen vaatiessa, eli viestiessään julkisen verkon suuntaan, väliaikaisesti ”lainata” NAT-yhdyskäytävälle määriteltyjä julkisia IP-osoitteita. Tällä menetelmällä kyetään rajoittamaan harvassa olevien julkisten IPv4-osoitteiden käyttötarvetta. [22.]

IPv6-siirtymässä NAT-osoitteenmuunnosta voidaan hyödyntää kääntämällä IPv6-osoitteita IPv4-osoitteiksi ja toisin päin, jolloin esimerkiksi IPv6-pohjaisesta toimistoverkosta kyetään viestimään IPv4-pohjaisen ulkoverkon suuntaan. Toiminto ei luonnollisestikaan ole yhtä yksinkertainen kuin puhtaissa IPv4-ympäristöissä, kun otetaan huomioon, että IPv4- ja IPv6-otsakkeet ja osoitteet ovat keskenään erityyppisiä. Kääntäminen joudutaan siis tekemään IP-osoitteiden lisäksi myös protokollasta toiseen. Tällä hetkellä tähän tarkoitukseen suunnattuja ja tuettuja NAT-tekniikoita on määriteltynä kaksi: NAT64 ja SIIT (Stateless IP/ICMP Translation).

NAT64 on tarkoitettu kääntämään IPv6-pohjaisen solmun aloittama, IPv4-verkon suuntaan tapahtuva viestintä. Useimmiten tämä tarkoittaa IPv6-pohjaista toimistoverkkoa, jossa loppukäyttäjät sijaitsevat ja joiden on tarkoitus viestiä IPv4-pohjaisten palvelinten kanssa. Halutessaan viestiä IPv4-pohjaisen palvelimen kanssa hyödyntäen NAT64-yhdyskäytävää IPv6-pohjainen laite syöttää halutun kohteen 32-bittisen IPv4-osoitteen osaksi NAT64-standardin määrittelemää IPv6-osoiteformaattia. Tämän formaatin osoitteen verkko-osio on aina 64:ff9b::/96, mikä tarkoittaa sitä, että sen mukaisia IPv6-osoitteita ei ole mahdollista reitittää julkisissa verkoissa, eli osoitteenmuunnoksen tulee tapahtua IPv6-pohjaisen sisäverkon ja IPv4-pohjaisen ulkoverkon välillä. Viestinnän aloittava laite upottaa tämän 64:ff9b::/96-prefiksin jälkeen tuleviin 32 bittiin viestinnän kohteena olevan palvelimen IPv4-osoitteen. Tämän jälkeen paketti toimitetaan NAT64-yhdyskäytävälle, joka toteuttaa tarvittavan NAT-toiminnon ja lähettää paketin eteenpäin IPv4-verkkoon käyttäen kohdeosoitteena alkuperäisen IPv6-paketin kohdeosoitteen viimeiseen 32 bittiin upotettua IPv4-osoitetta ja lähdeosoitteena omaa, ylläpitäjän määrittelemää julkista IPv4-osoitetta, tavallisen NAT-toiminnon tapaan. Paluuliikenteelle NAT64 tekee päinvastaisen eli kääntää paketin otsakkeen IPv6-muotoon ja lähettää sen viestinnän alun perin aloittaneelle laitteelle. [23.]

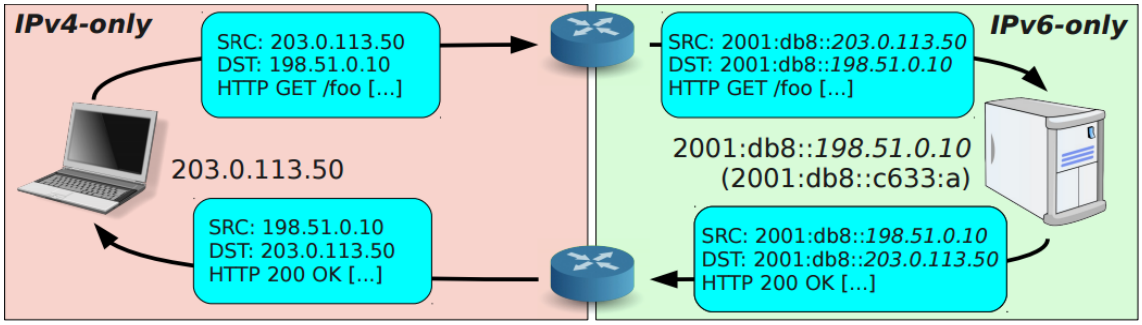
Useimmiten NAT64-toiminnollisuutta hyödyntävä IPv6-pohjainen laite saa tiettyä IPv4-pohjaista palvelinta vastaavan 64:ff9b::/96-prefiksiin pohjautuvan IPv6-osoitteen, johon haluttu IPv4-osoite on upotettu, tähän tarkoitukseen tarkoitetulta DNS-palvelimelta, jota kutsutaan nimellä DNS64. Kun IPv6-pohjainen laite tiedustelee DNS64-palvelimelta jotakin tiettyä URL-osoitetta vastaavaa IP-osoitetta eikä IPv6-osoitetta vastaava AAAA-merkintää kysytylle osoitteelle löydy, mutta IPv4-osoitetta vastaava A-merkintä löytyy, niin DNS64 sulauttaa A-merkinnän sisältävän IPv4-osoitteen NAT64:n käyttämän

64:ff9b::/96-prefiksin jatkoksi ja palauttaa näin saadun osoitteen kyselyn tehneelle laitteelle, joka pystyy osoitteen avulla hyödyntämään NAT64:n toiminnollisuutta ja täten viestimään IPv4-pohjaisen palvelimen kanssa. [24.]

NAT64 on toimintaperiaatteeltaan tilallinen (stateful), mikä tarkoittaa, että se pitää kirjaa jokaisesta yksittäisestä käännöstapahtumasta [23]. Tämä johtaa siihen, että NAT64-yhdyskäytävänä toimiva laite tulee olemaan varsin korkean kuormitusasteen alaisena prosessoritehon ja muistinkäytön suhteen. Kuormantasaamisen ja vikasietoisuuden toteuttaminen usean laitteen avulla ei myöskään ole helposti toteutettavissa NAT64-järjestelmän kanssa, sillä NAT64-yhdyskäytävän läpi mennyttä liikennettä vastaavan paluuliikenteen tulee tilallisen toimintaperiaatteen vuoksi palata aina samaa yhdyskäytävää pitkin.

NAT64-osoitteenmuunnoksen soveltaminen toimistoverkon päässä ei siis ole erityisen skaalautuva ratkaisu, vaikka tilallisen toimintaperiaatteen avulla kyetäänkin tehokkaasti säästelemään ulkoverkkoon suuntautuvaan viestintään tarvittavien IPv4-osoitteiden määrää. NAT64 osaa hyödyntää myös overload-toimintoa eli sisäverkon osoitteiden muuntamista vastaamaan yksittäisiä sokettiosoitteita eli IP-osoitteen ja kuljetuskerroksen hyödyntämän porttinumeron yhdistelmää. Tämänkaltaisten yhdistelmien teoreettinen maksimimäärä on 65 536 yhtä IP-osoitetta kohden. [25.]

IPv4:n ja IPv6:n välinen osoitteenmuunnos voidaan toteuttaa myös tilattomasti SIIT-osoitteenmuunnostekniikan avulla. NAT64:stä SIIT eroaa siten, että se ei tee yhdyskäytävänä toimivan laitteen muistiin minkäänlaisia merkintöjä käännöstapahtumasta, vaan se tekee aina ja poikkeuksetta 1:1-käännöksen tietystä IPv4-osoitteesta aina tiettyyn IPv6-osoitteeseen ja saman toisinpäin (kuva 5). [26.]



Kuva 5. SIIT-osoitteenmuunnoksen toimintaperiaate [27].

SIIT on suunniteltu sovellettavaksi palvelinkeskuksen päässä, joka voidaankin sen avulla toteuttaa puhtaasti IPv6-pohjaisena ratkaisuna, jossa NAT-yhdyskäytävä ei ota kantaa sisään tulevaan IPv6-liikenteeseen, mutta kääntää sisään tulevan IPv4-pohjaisen liikenteen aina IPv6-tyyppiseksi. IPv4-liikenne käännetään siten, että sisään tulevien pakettien otsakkeiden sisältämät 32-bittiset lähde- ja kohdeosoitteet upotetaan IPv6-osoitteiden sisään tietyn /96-prefiksin jälkeen, aivan kuten NAT64-tekniikassakin. Prefiksinä voidaan käyttää standardissa määriteltyä ::ffff:0:0:0/96-prefiksiä, jota ei voida reitittää ulkoverkossa, tai verkon ylläpitäjä voi käyttää omaa, julkista /96-prefiksiä, jolloin ulkoverkossa sijaitsevat IPv6-kykyiset laitteet voivat viestiä palvelinkeskuksen palvelinten kanssa natiivisti IPv6-protokollan välityksellä. [26.]

SIIT-osoitteenmuunnoksen avulla kyetään kiertämään NAT64-osoitteenmuunnoksen heikkouksia, kuten tarvetta symmetriselle reititykselle aina saman yhdyskäytävän lävitse meno- ja paluuliikenteelle, ja yhdyskäytävänä toimivan laitteen korkeita prosessori- ja muistikapasiteettivaatimuksia. Lisäksi SIIT-osoitteenmuunnos säilyttää viestinnän aloittaneen tahon alkuperäisen IPv4-osoitteen osana IPv6-osoitetta, mikä mahdollistaa kohdepalvelimelle toimintoja, kuten esimerkiksi palveluiden tarjoamisen loppukäyttäjän laitteen maantieteellisen sijainnin perusteella tai yhteen tiettyyn laitteeseen yhdistettävien lokitietojen keräämisen.

Kaksoispinoon verrattuna SIIT-osoitteenmuunnoksen avulla kyetään yksinkertaistamaan palvelinkeskuksen ylläpitoa ja hallintaa toteuttamalla palvelinkeskusverkko puhtaasti IPv6-pohjaisena. Tällöin ylläpitoon liittyvät prosessit, kuten monitorointi, vianselvitys ja dokumentointi, ovat helpompia toteuttaa, kun ne tarvitsee toteuttaa vain yhdelle protokollapinolle. Huomionarvoista on kuitenkin, että tämäntyyppinen SIIT-osoitteenmuunnoksen soveltaminen vaati kaikkien palvelinkeskuksen palvelinohjelmistojen toimivan natiivisti IPv6:n avulla.

3 Tutkimuksen tavoitteet ja menetelmät

Insinöörityön tavoitteena on tehdä selvitystyö tilaajayrityksen käyttämän IPv4-pohjaisen palvelinkeskusverkon siirtymästä käyttämään sekä IPv4- että IPv6-protokollaa hyödyntäen kaksoispino-ominaisuutta. Palvelinkeskuksen laitteiden käytössä olevat toiminnollisuudet, jotka on toteutettu IPv4-pohjaisesti, kartoitetaan ja selvitetään käytössä olevien laitteiden ja niiden käyttämien ohjelmistojen kyky toteuttaa samat toiminnollisuudet myös IPv6-pohjaisesti. Tärkeimpien toiminnollisuuksien kohdalla selvitetään tarvittavat toimenpiteet toimintojen IPv6-pohjaiseen toteuttamiseen. Myös siirtymäprosessiin liittyvät mahdolliset haasteet kartoitetaan ja selvitetään näiden haasteiden ratkaisemiseen tai kiertämiseen vaadittavat toimenpiteet.

Tilaajayrityksellä on käytössään useita eri palvelinkeskuksia, mutta tämän työn toteuttamisessa hyödynnetään vain yhtä näistä palvelinkeskuksista. Näin saatua selvitystä voidaan kuitenkin helposti hyödyntää muissakin tilaajayrityksen palvelinkeskuksissa, sillä näiden eri laitetilojen sisältämä laitekanta ja rakenne ovat monilta osin yhteneväisiä.

Työn toteuttamisen tekninen osuus tehdään tuotantoverkosta erillisellä, virtualisoidulla testipenkkialustalla. Tällä tavoin pyritään simuloimaan selvitystyön kohteena olevaa oikeaa tuotantoympäristöä, jolla ei sen liiketoimintakriittisen luonteen vuoksi voida kuitenkaan ajaa testejä, joiden seurauksista ja lopputuloksista ei ole täyttä varmuutta. Tuotantoympäristön laitteita hyödynnetään kuitenkin kartoitettaessa yksityiskohtia, kuten laitteiden käyttöjärjestelmäversioita ja käytössä olevia IPv4-pohjaisia toiminnollisuuksia, jotka on tarve toteuttaa myös IPv6-pohjaisesti.

Jokaisen mahdollisen IPv6-siirtymään liittyvän yksityiskohdan käsitteleminen tässä yksittäisessä insinöörityössä olisi sille asetettujen tavoitteiden kannalta liian laajamittainen kokonaisuus, joten varsinaisen työn toteutus rajataan palvelinkeskusverkon kuormantasaajiin, palomuureihin ja ydinkerroksen reitittimiin. Esimerkiksi palvelinkeskuksen palvelimilla suoritettuihin ohjelmistoihin tai muutosten hallinnolliseen toteuttamiseen ei oteta kantaa.

4 Palvelinkeskuksen verkkoinfrastruktuuri

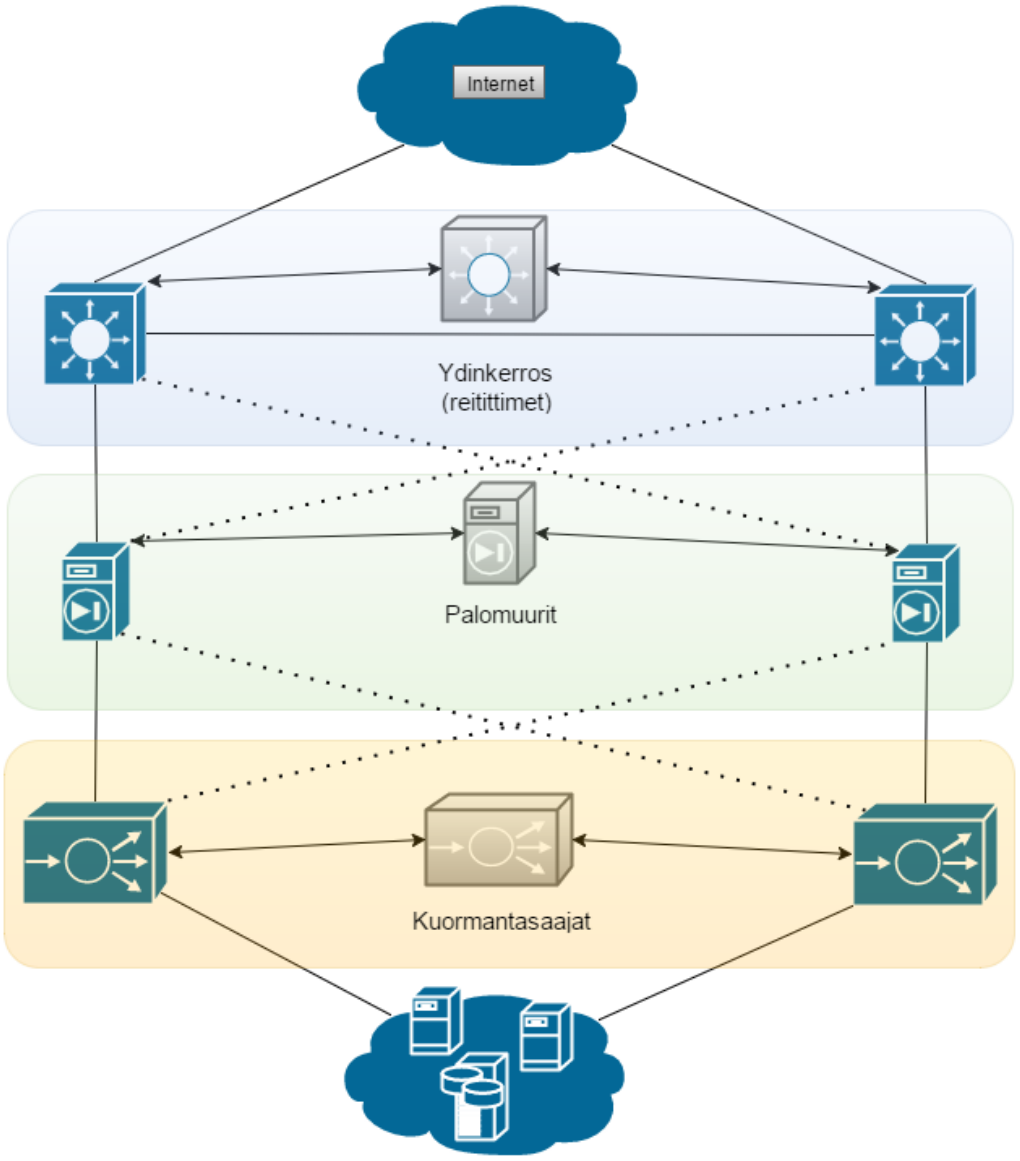
Palvelinkeskus, tai datakeskus, on tila, johon on keskitetty useita palvelinlaitteita, jotka suorittavat verkkopalveluita, kuten verkkosivustoja, tietokantoja tai erilaisia pilvipalveluita. Verkkoon liitetyt loppukäyttäjät pystyvät hyödyntämään näitä palveluita omilla päätelaitteillaan.

Palvelinkeskuksen palvelinjärjestelmien tehokkaan hallinnoinnin ja niiden tarjoamien palveluiden vikasietoisuuden, skaalautuvuuden, tietoturvallisuuden ja korkean käytettävyysasteen varmistamiseksi palvelinkeskuksissa on itse palvelinten lisäksi myös huomattava määrä muutakin laiteinfrastruktuuria, kuten erilaisia verkkolaitteita ja palomuureja. Näitä laitteita, joista palvelinkeskusverkko muodostuu, käydään tarkemmin läpi tässä luvussa, siltä osin kuin insinöörityön tavoitteiden kannalta on tarpeellista. Myös tilaajayrityksen tuotantoympäristöissä käytettyjen laitteiden valmiudet IPv6-pohjaiseen toimintaan käydään läpi.

4.1 Palvelinkeskusympäristön rakenne

Työn kohteena olevaa palvelinkeskusta käytetään alustana lukuisille eri verkkopalveluille, joita tarjotaan niin kuluttaja- kuin yritysasiakkaille ja joita hyödynnetään myös tilaajayrityksen sisäisissä toiminnoissa. Osa näistä palveluista kykenee hyödyntämään ainoastaan IPv4-protokollaa, mikä onkin otettu huomioon työn tavoitteita asetettaessa.

Kuvassa 6 on esitetty yksinkertaistettu rakennekuvaus palvelinkeskuksen verkkotopologiasta yksittäisen palvelun näkökulmasta. Käyttäjien luomat palvelupyynnöt, kuten esimerkiksi HTTP-pyynnöt, tulevat internetin suunnasta, jota kuvassa esittää ylin pilvisymboli. Tämän jälkeen palvelupyynnöt kulkevat tarkasti määritellyllä tavalla kuvassa näkyvän verkkoinfrastruktuurin lävitse kohti alimman pilvisymbolin kuvaamia palvelimia, jotka käsittelevät käyttäjien palvelupyynnöt ja vastaavat niihin.



Kuva 6. Konesaliverkon yksinkertaistettu topologia.

Kuvassa näkyvät harmaat laitesymbolit kuvaavat kahdennettujen laitteiden välisiä, virtuaalisia FHRP-instansseja (First Hop Redundancy Protocol). FHRP on yleisnimitys protokollille, joiden tarkoituksena on edistää verkon vikasietoisuutta mahdollistamalla kahden tai useamman rinnakkaisen yhdyskäytävän hyödyntäminen siltä varalta, että yksi yhdyskäytävistä vikaantuu tai sille johtava reitti katkeaa. Tämänkaltaisen vikatilanteen yhteydessä FHRP-protokollaa hyödyntävän verkon solmu voi alkaa lähettää paketteja pääasiallisen yhdyskäytävänsä rinnalla olevalle vaihtoehtoiselle yhdyskäytävälle. Nämä kahdennetut yhdyskäytävät ovat osana samaa FHRP-instanssia ja yleensä jakavat yhden yhteisen, virtuaalisen IP- ja MAC-osoitteen yhdistelmän. Tätä IP- ja MAC-osoitteen yhdistelmää käyttää kerrallaan vain yksi FHRP-instanssin osana olevista yhdyskäytä-

vistä. Kun tämä yhdyskäytävä vikaantuu, samaan FHRP-instanssiin kuuluva vaihtoehtoinen yhdyskäytävä ottaa instanssin IP- ja MAC-osoiteyhdistelmän omaan käyttöönsä, jolloin liikennettä voidaan yhä välittää saman osoitteen suuntaan samanlaiselle laitteelle yksittäisen laitteen vikaantumisesta huolimatta. [28.]

Kuvassa 6 näkyvien eri laitekerrosten laitteet ovat yhdistettyinä viereisten kerrosten laitteisiin yhden lähiverkon sisällä. Kuvassa katkoviivoin yhdistetyistä laitteista tulee huomioida, että ne saattavat olla fyysisesti hyvinkin kaukana toisistaan, esimerkiksi kokonaan eri laitetiloissa, jolloin niiden kytkeminen samaan, siirtokerroksella toimivaan fyysiseen lähiverkkoon olisi varsin hankalaa. Tämän takia kuvassa katkoviivoin esitetyt yhteydet onkin toteutettu VPLS-tekniikalla (Virtual Private LAN Service). VPLS on VPN-tekniikka, jonka avulla voidaan luoda virtuaalisia, Ethernet-pohjaisia yhteyksiä IP- tai MPLS-tekniikalla (Multiprotocol Label Switching) toteutettujen verkkokokonaisuuksien, kuten operaattoriverkkojen, läpi. Tällä tavoin kyetään yhdistämään useampia fyysisesti erillään olevia lähiverkkoja yhdeksi loogiseksi lähiverkkokokonaisuudeksi, kunhan niiden välillä vain on IP- tai MPLS-pohjainen yhteys. [29.]

4.2 Ydinkerroksen reitittimet

Ydinkerros on tässä tapauksessa kahden reitittimen muodostama kokonaisuus, joka toimii rajapintana operaattoriverkon ja palvelinkeskusverkon välillä ja täten mahdollistaa yhteydet internetistä palvelinkeskukseen. Ydinkerroksen laitteiden läpi virtaa koko palvelinkeskuksen tuottama ja siihen kohdistuva liikenne, joka niiden tulee kyetä käsittelemään ilman palvelunlaadun heikkenemistä pahimpinakaan ruuhka-aikoina. Ydinkerroksen laitteilla on siis verrattain korkeat suorituskykyvaatimukset.

Tässä insinöörityössä tarkastellaan tilaajayrityksen tuotantoympäristöissä käytettyjä Juniper-merkkisiä reitittimiä ja niiden käyttämää Junos-käyttöjärjestelmää.

Juniper lupaa Junos-käyttöjärjestelmälleen varsin kattavan tuen IPv6-protokollalle ja sille määritellyille standardeille ja toiminnollisuuksille. Järjestelmä tukee IPv6-pohjaisesti useita keskeisiä toiminnollisuuksia, kuten esimerkiksi IPv6-kykyisiä BGP- (Border Gateway Protocol) ja IS-IS-reititysprotokollia (Intermediate System to Intermediate System). BGP ja IS-IS ovat internetoperaattoriympäristöissä yleisesti käytettyjä dynaamisia reititysprotokollia. [30.]

4.3 Palomuurit

Palvelinkeskuksen liikenteensuodatus toteutetaan erillisillä, fyysisillä palomuurilaitteilla, jotka on, hieman käyttötarkoituksesta riippuen, sijoitettu jonnekin ulkoverkon ja suojattavan verkkoinfrastruktuurin väliin. Palomuurin tehtävänä on tarkastella ja tarpeen vaatiessa suodattaa ulkoa tulevaa liikennettä siten, että kaikki haitallinen liikenne, kuten esimerkiksi palvelunestohyökkäykseen liittyvä liikenne, pysäytetään palomuuriin, ilman että siitä koituisi haitallista vaikutusta suojattavan verkkoinfrastruktuurin toimintaan tai että mahdollinen haittavaikutus saataisiin minimoitua. Tämän toiminnollisuuden toteuttamiseksi palomuuri tarkastelee pakettien ja pakettivirtojen ominaisuuksia, kuten esimerkiksi verkkokerroksella toimivan IP-protokollan käyttämiä otsakkeita.

Perinteisen palomuurauksen lisäksi palomuurilaitteet toimivat usein myös VPN-yhdyskäytävinä. VPN-yhdyskäytävä tarkoittaa tässä yhteydessä laitetta, joka toimii suojattujen VPN-yhteyksien päätepisteenä palvelinkeskuksen päässä ja joihin VPN-yhteyttä käyttävät käyttäjät luovat suojatun yhteyden omalta päätelaitteeltaan tai omaa toimistoverkkoaan vastaavalta VPN-yhdyskäytävältä.

Tässä insinöörityössä tarkastellaan tilaajayrityksen tuotantoympäristöissä käytettyjä Check Point -merkkisiä palomuurilaitteita ja niiden käyttämää Gaia-käyttöjärjestelmää.

Gaia-käyttöjärjestelmä on käytössä kaikissa nykyisissä Check Pointin valmistamissa palomuurilaitteissa. Käyttöjärjestelmän IPv6-tuessa on tällä hetkellä tiettyjä puutteita. Esimerkiksi palomuurin lokitietojen tarkasteluun tarkoitettu SmartView Tracker -työkalu, ClusterXL Load Sharing -kuormantasaustoiminto ja QoS-toiminto (Quality of Service) eivät ole tuettuina IPv6-pohjaisesti. Kaikki tunnetut puutteet ovat listattuna lähteessä 31. [31.]

4.4 Kuormantasaajat

Kuormantasaajat asennetaan palveluiden käyttäjien ja useamman, samaa palvelua suorittavan palvelinkoneen väliin. Kuormantasaajalla toteutettavan palvelun käyttäjä ottaa aina yhteyden kuormantasaajassa toimivaan virtuaalipalvelimeen tai erilliseen front-end-palvelimeen, jolla on tietty, palvelua vastaava IP-osoite, mutta joka ei kuitenkaan itses-

sään suorita käyttäjän käyttämää palvelua. Tämän jälkeen kuormantasaaja nimensä mukaisesti tasaa käyttäjien luoman kuormituksen varsinaisten, palveluita suorittavien taustapalvelinten kesken, näin hyödyntäen optimaalisesti kaikkea käytössä olevaa palvelinkapasiteettia. Tämänkaltainen kuormantasausmekanismi on mahdollista toteuttaa useilla eri tavoilla; esimerkiksi tilaajayrityksen palvelinkeskusverkossa kuorman tasaus toteutetaan Round Robin -pohjaisesti. Round Robin tarkoittaa yksinkertaisesti sitä, että sisään tulevat palvelupyynnöt ja niitä vastaavat TCP-sessiot jaetaan tasaisesti vuoron perään kuormantasaajan takana oleville taustapalvelimille [32].

Mikäli yksittäinen, kuormantasaajan takana oleva palvelinlaite vikaantuu tai se sammutetaan esimerkiksi huoltotöitä varten, palvelu pysyy silti saatavilla niin kauan, kuin sitä suorittaa yksikin kuormantasaajan takana oleva palvelin. Tämä takaa palvelulle korkean vikasietoisuuden ja saatavuusasteen. Lisäksi kuormantasaaja edistää myös palvelun skaalautuvuutta, sillä sen taakse voidaan palvelun kuormituksen kasvaessa liittää uusia palvelinkoneita ja täten lisätä palvelun käytössä olevaa palvelinkapasiteettia ilman loppukäyttäjille näkyviä huoltokatkoja.

Kuormantasaajien avulla voidaan yleisesti myös siirtää SSL-protokollan (Secure Sockets Layer) käyttämien sertifikaattien varmentamiseen vaadittavat toimenpiteet taustapalvelimilta kuormantasaajalle. Näin voidaan vapauttaa palvelinten käytössä olevia resursseja yksinomaan palvelupyyntöjen käsittelyyn. SSL-protokollaa käytetään muun muassa HTTP-liikenteen salaamiseen ja viestinnän osapuolten varmistamiseen. Tällöin käytetään usein termiä HTTPS (HTTP Secure).

Tässä insinöörityössä tarkastellaan tilaajayrityksen tuotantoympäristöissä käytettyjä F5-merkkisiä kuormantasaajia ja niiden käyttämää TMOS-käyttöjärjestelmää (Traffic Management Operating System).

F5 lupaa TMOS-käyttöjärjestelmälleen varsin kattavan IPv6-tuen, muun muassa kuormantasaajan perusominaisuuksien ja erilaisten hallintaominaisuuksien yhteydessä. TMOS-käyttöjärjestelmää käyttävä kuormantasaaja voidaan myös asettaa välityspalvelimeksi IPv4- ja IPv6-kykyisten verkkosegmenttien välille. Tämänkaltainen välityspalvelin mahdollistaa näiden kahden verkko-osion välisen viestinnän käytettyjen IP-protokollien eroavaisuuksista huolimatta. IPv6-tuki on ollut TMOS-käyttöjärjestelmässä olemassa jo vuodesta 2009. [33.]

5 Laitteiden toiminnot ja niiden IPv6-pohjainen toteuttaminen

Tässä luvussa käydään läpi käsiteltävien laitteiden keskeisimpiä toimintoja ja esitetään tarvittavat toimenpiteet niiden IPv6-pohjaisen toteutuksen mahdollistamiseksi. Käytännössä tämä tarkoittaa testiympäristössä luotuja yksinkertaisia esimerkkikonfiguraatioita.

Esimerkkikonfiguraatioista kannattaa huomioida, että ne ovat nimensä mukaisesti esimerkkiluontoisia ja täten toiminnollisuuksiltaan varsin rajallisia. Niiden ei ole tarkoitus soveltua sellaisenaan kaikkiin tuotantoympäristön vaatimuksiin, vaan niiden on tarkoitus ottaa kantaa vain tiettyihin toimintoihin, jotka käydään läpi siltä osin, kuin niiden IPv6- tai kaksoispinopohjainen toteutus sitä vaatii.

Kaikki esimerkkikonfiguraatioissa käytetyt IP-osoitteet, AS-numerot ja vastaavat ovat privaattityyppisiä. Niitä ei ole mahdollista käyttää julkisissa verkoissa.

5.1 Juniper-reitittimet

Seuraavien alalukujen esimerkkikonfiguraatioissa Juniper-reitittimelle asetetaan sen tavanomaiset reititystoiminnot IPv6-pohjaisesti BGP- ja IS-IS-reititysprotokollilla.

Esimerkeissä esiintyvät Juniperin Junos-käyttöjärjestelmän konfiguraatiot esitetään hierarkkisesti. Jokainen laitteelle annettu yksittäinen komento voidaan lukea siten, että aloitetaan hierarkian yläpäästä ja lopetetaan alapäähän, mitä merkitään puolipisteellä. Esimerkkikonfiguraatio 1 rakentuu siis käytännössä seuraavista set-komennoista:

```
set interfaces xe-0/0/0 unit 0 family inet address 192.168.0.1/24
set interfaces xe-0/0/0 unit 0 family inet6 address 2001:db8::/120
```

Junos-käyttöjärjestelmää käytettäessä tehdyt muutokset tulee aina lopuksi myös muistaa tallentaa laitteelle ***commit*** -komennolla.

5.1.1 Laiteportit

Reitittimen toiminnan yhtenä keskeisimmistä kulmakivistä ovat niiden käyttämät portit, joiden avulla laite kytketään kiinni muihin laitteisiin ja täten kiinnitetään osaksi ulkoisia tietoverkkoja. Verkkokerroksella toimiville porteille tulee aina määritellä oma, sen portin yksilöivä IP-osoite. Esimerkkikonfiguraatio 1 esittää, miten Junos-käyttöjärjestelmässä asetetaan tietty portti käyttämään sekä IPv4- että IPv6-osoitteita.

```
interfaces {
     xe-0/0/0 {
          unit 0 {
               family inet {
                    address 192.168.0.1/24;
               }
               family inet6 {
                    address 2001:db8::/120;
               }
          }
     }
}
```

Esimerkkikonfiguraatio 1. IPv4- ja IPv6-osoitteiden asettaminen porteille Junos-käyttöjärjestelmässä.

Osoitteiden asettamisen jälkeen portti, esimerkin tapauksessa xe-0/0/0, on käytännössä asetettu kaksoispinotilaan, eli se kykenee lähettämään ja vastaanottamaan IPv4- ja IPv6-muotoisia IP-paketteja, jotka voivat liittyä täsmä- tai ryhmälähetyksiin. Huomionarvoista on, että molemmat osoitteet asetetaan saman loogisen yksikön alle. Esimerkkikonfiguraation 1 tapauksessa käytetään yksikköä 0 (unit 0).

5.1.2 BGP-reititys

BGP on internetissä käytetty dynaaminen reititysprotokolla, jonka pääasiallinen tehtävä on suorittaa reititystoimintoja eri autonomisisten järjestelmien, kuten internetoperaattoreiden, välillä. BGP-protokollaa käytetään yleisesti myös autonomisten järjestelmien sisällä. Näin myös tilaajayrityksen palvelinkeskuksen ydinkerroksen ja runkoverkon laitteiden välillä, jotka on asetettu BGP-naapureiksi keskenään.

Alkuperäinen BGP-standardi vuodelta 1991 ei tukenut kuin IPv4-täsmälähetystyyppisen reititysinformaation vaihtamista, mutta sittemmin siihen on julkaistu erillinen MP-BGP-

lisäominaisuus (Multiprotocol BGP), joka mahdollistaa muun muassa IPv6-pohjaisen reititysinformaation jakamisen BGP-toiminnollisuuden omaavien reititinten kesken [34]. Nykyiset Junos-käyttöjärjestelmät tukevat tätä ominaisuutta, ja se voidaan ottaa käyttöön *bgp*-hierarkiatason alla olevan *family*-komennon avulla, jonka käyttö esitetään esimerkkikonfiguraatiossa 2.

```
interfaces {
     lo0 {
          unit 0 {
               family inet6 {
                    address 2001:db8::/128;
               }
          }
     }
}

routing-options {
     autonomous-system 65000;
     router-id 192.168.0.0
}

protocols {
     bgp {
          group kaksoispino {
               type internal;
               local-address 2001:db8::/128;
               family inet {
                    any;
               }
               family inet-vpn {
                    any;
               }
               family inet6 {
                    any;
               }
               family inet6-vpn {
                    any;
               }
               peer-as 65000;
               neighbor 2001:db8::1/128;
          }
     }
}
```

Esimerkkikonfiguraatio 2. BGP-reititysprotokollan asettaminen.

Esimerkkikonfiguraatiossa 2 annetaan aluksi laitteen virtuaaliselle loopback-portille IP-osoite. Toisin kuin monet muut reititysprotokollat, BGP-protokolla käyttää muiden BGP-

reititinten kanssa luotavien naapuruussuhteiden muodostamiseen täsmälähetyspohjaista viestintää ryhmälähetyksen sijasta. Tämä tarkoittaa, että verkon ylläpitäjän tulee määritellä laitteille yksittäiset IP-osoitteet, joita laitteet käyttävät näiden naapuruuksien muodostamiseen. Tämä IP-osoite voi vastata jotakin laitteen fyysisistä porteista, mutta tässä tapauksessa käytetään virtuaalista loopback-osoitetta, joka on käytännössä aina päällä, niin kauan kuin itse laitekin on päällä. Fyysisen portin tapauksessa portin mennessä alas, esimerkiksi fyysisen vian takia, myös sitä vastaavaan IP-osoitteeseen luodut BGP-sessiot menisivät samalla alas.

autonomous-system-komennolla määritellään paikallisen laitteen AS-numero, joka toimii BGP-reititysverkossa sen autonomisen järjestelmän tunnisteena, jonka osana laite on.

router-id-komennolla määritellään laitteen käyttämä router ID -arvo, jonka avulla yksittäinen laite voidaan yksilöidä tietyn reititystopologian sisällä. Tätä arvoa ei ole mahdollista asettaa IPv6-osoitteeksi. Vaikka BGP-protokollaa haluttaisiin soveltaa vain IPv6-ympäristöissä, on laitteen router ID -arvoksi silti asetettava IPv4-osoitteen muotoinen arvo. Tilaajayrityksen ympäristöissä käytössä oleviin AS-numeroihin tai router ID -tunnisteisiin ei ole tarvetta tehdä muutoksia IPv6-siirtymän yhteydessä. [35.]

Esimerkkikonfiguraation varsinaisen BGP-osion alla olevien *family*-komentojen avulla kyetään määrittelemään ne osoitetyypit, joita BGP-protokollan halutaan ottavan huomioon reititysprosessissaan. Esimerkin tapauksessa tällaisiksi osoitetyypeiksi on määritelty IPv4, IPv6 ja molempiin protokolliin pohjautuvien, verkkokerroksen toimintoja hyödyntävien VPN-yhteyksien reititystiedot, joiden avulla kyetään ylläpitämään MPLS-palvelua. MPLS on internetoperaattoreiden suosima tekniikka, jonka avulla voidaan luoda virtuaalisia, VPN-pohjaisia yhteyksiä eri kohteiden, kuten jonkin yrityksen toimipisteiden ja sen käyttämien palvelinkeskusten, välille. Näiden kohteiden välillä liikkuvan datan reititys toteutetaan tehostetusti, lyhyiden 20-bittisten path label -merkintöjen perusteella IP-osoitteiden sijasta.

Esimerkkikonfiguraatiossa BGP-reititinten välinen naapuruuden luonti toteutetaan IPv6-protokollaa ja IPv6-tyyppisiä osoitteita hyödyntäen. Naapuruuden luontiin käytetään tässä tapauksessa paikallisen loopback-portin ja halutun naapurin käyttämää IPv6-pohjaista osoitetta. Huomionarvoista on, että naapuruuden luonnin jälkeen laitteet pystyvät vaihtamaan keskenään myös IPv4-pohjaisia reititystietoja, vaikka niiden välisen naapuruuden luontiin onkin käytetty IPv6-protokollaa.

Luonnollisesti vastaavanlainen konfiguraatio on asetettava myös halutun naapurilaitteen päähän.

5.1.3 IS-IS-reititys

Tilaajayrityksen verkon, eli autonomisen järjestelmän, sisällä sovelletaan myös BGP-protokollasta erillistä IGP-tyyppistä (Interior Gateway Protocol) reititysprotokollaa, jona toimii operaattoriympäristöissä yleisesti käytetty IS-IS. IS-IS-protokollan pääasiallisena käyttötarkoituksena tilaajayrityksen ympäristöissä on BGP-protokollan käyttämien loopback-porttien osoitteiden levittäminen niitä tarvitseville laitteille. IGP-termillä viitataan sellaisiin reititysprotokolliin, joiden on tarkoitus toteuttaa reititystoimintoja yksittäisen tahon hallinnoiman autonomisen järjestelmän sisällä.

IS-IS-protokollan toimintaperiaate on hyvin samantyyppinen yleisesti käytetyn OSPF-protokollan (Open Shortest Path First) kanssa; se on Link State -tyyppinen protokolla, joka käyttää reitinvalintatoiminnoissaan Shortest Path First -algoritmia, hyödyntää eri alueita (area), joiden välillä voidaan suorittaa reittien tiivistystä, ja kykenee luomaan naapuruudet muiden samaa protokollaa suorittavien reititinten kanssa soveltamalla ryhmälähetyksenä lähetettäviä, erityisiä Hello-paketteja [36].

IS-IS-protokollan merkittävimpiin etuihin kuuluu sen toimintojen aiheuttama suhteellisen pieni kuormitus sitä käyttäville laitteille. Tämä tarkoittaa käytännössä sitä, että protokollaa voidaan sujuvammin soveltaa myös suuremmissa verkkokokonaisuuksissa, kuten operaattoriverkoissa, joiden asettamiin vaatimuksiin se skaalautuu huomattavasti paremmin kuin esimerkiksi OSPF, joka lähettää reititystiedotuksiaan useina, pienempinä palasina ja täten aiheuttaa sitä käyttävän verkon laitteille ylimääräistä kuormitusta. [37.]

Insinöörityön tavoitteiden kannalta IS-IS-protokollalla on myös se etu, että se, toisin kuin monet muut reititysprotokollat, toimii verkkokerroksen sijasta siirtokerroksella [36]. Sen reititystoiminnot eivät siis ole erityisen riippuvaisia käytetystä verkkokerroksen protokollasta. Tämä tarkoittaa, että IS-IS-protokollan asettaminen jakamaan IPv4-protokollan reititystietojen lisäksi myös IPv6-reititystietoja on varsin suoraviivaista, kuten esimerkkikonfiguraatiosta 3 voi todeta.

```
interfaces
     xe-0/0/0 {
          unit 0 {
               family inet {
                    address 192.168.0.1/30;
               }
               family iso;
               family inet6 {
                    address 2001:db8::/127;
               }
          }
     }
     lo0 {
          unit 0 {
               family inet {
                    address 192.168.0.4/32;
               }
               family iso {
                    address 49.0002.0001.0002.0003.00;
               }
          }
     }
}
protocols {
     isis {
          interface xe-0/0/0.0;
          interface lo0.0;
     }
}
```

Esimerkkikonfiguraatio 3. IS-IS-reititysprotokollan asettaminen.

Kuten mainittua, IS-IS-protokollan asettaminen tukemaan molempia IP-protokollia ei vaadi pelkkään IPv4-kykyiseen konfiguraatioon verrattuna mitään erityisiä lisätoimia. Ainoa lisävaatimus on IPv6-tyyppisten osoitteiden asettaminen niille porteille, joissa halutaan käyttää IS-IS-protokollaa kaksoispinotilassa.

Huomionarvoista on IS-IS-protokollaa käyttämään asetetun Juniper-reitittimen tapa käyttää router-ID-tunnisteenaan aina lo0-portin IPv4-osoitetta. Kuten myös BGP-protokollan tapauksessa, tätä arvoa ei ole mahdollista asettaa IPv6-osoitteeksi. Vaikka IS-IS-protokollaa haluttaisiin soveltaa vain IPv6-ympäristöissä, on lo0-portille silti asetettava IPv4-osoite, tai pikemminkin IPv4-osoitteen muotoinen arvo, laitteen router ID -arvoksi. Router-ID on IS-IS-protokollan tapa yksilöidä sen kattaman verkkotopologian sisällä olevat yksittäiset reitittimet. [35.]

Esimerkkikonfiguraation ISO-tyyppinen protokollaperhe ei liity mitenkään IP-protokollaan, eikä se täten ota minkäänlaista kantaa myöskään käytettävän IP-protokollan versioon. IS-IS-protokolla on kehitetty alun perin TCP/IP-protokollapinon kanssa kilpailleen CLNP-protokollapinon (Connectionless-mode Network Service) kanssa yhteensopivaksi. Junos-käyttöjärjestelmään ISO-nimellä implementoitu tekniikka on jäänne näiltä ajoilta, ja sen on yhteensopivuussyistä yhä välttämätöntä olla mukana IS-IS-protokollan yhteydessä. Se tulee aina asettaa käyttöön jokaiselle yksilölliselle portille, joka halutaan asettaa käyttämään IS-IS-protokollaa [36]. Kuten myös router-ID:n tapauksessa, jokainen IS-IS-topologiaan osallistuva reititin tarvitsee itselleen oman, uniikin ISO-tyyppisen tunnisteen, joka Juniperin laitteissa asetetaan myös router-ID:n tavoin lo0-portille, esimerkin mukaisesti. Tunnisteen avulla yksilöidään alue, jonka osana reititin on (vrt. OSPF area), ja kyseinen, yksilöllinen reititin.

Tilaajayrityksen verkossa käytössä oleviin ISO- tai router ID -tunnisteisiin ei ole tarvetta tehdä muutoksia IPv6-siirtymän yhteydessä.

5.2 Check Point -palomuurit

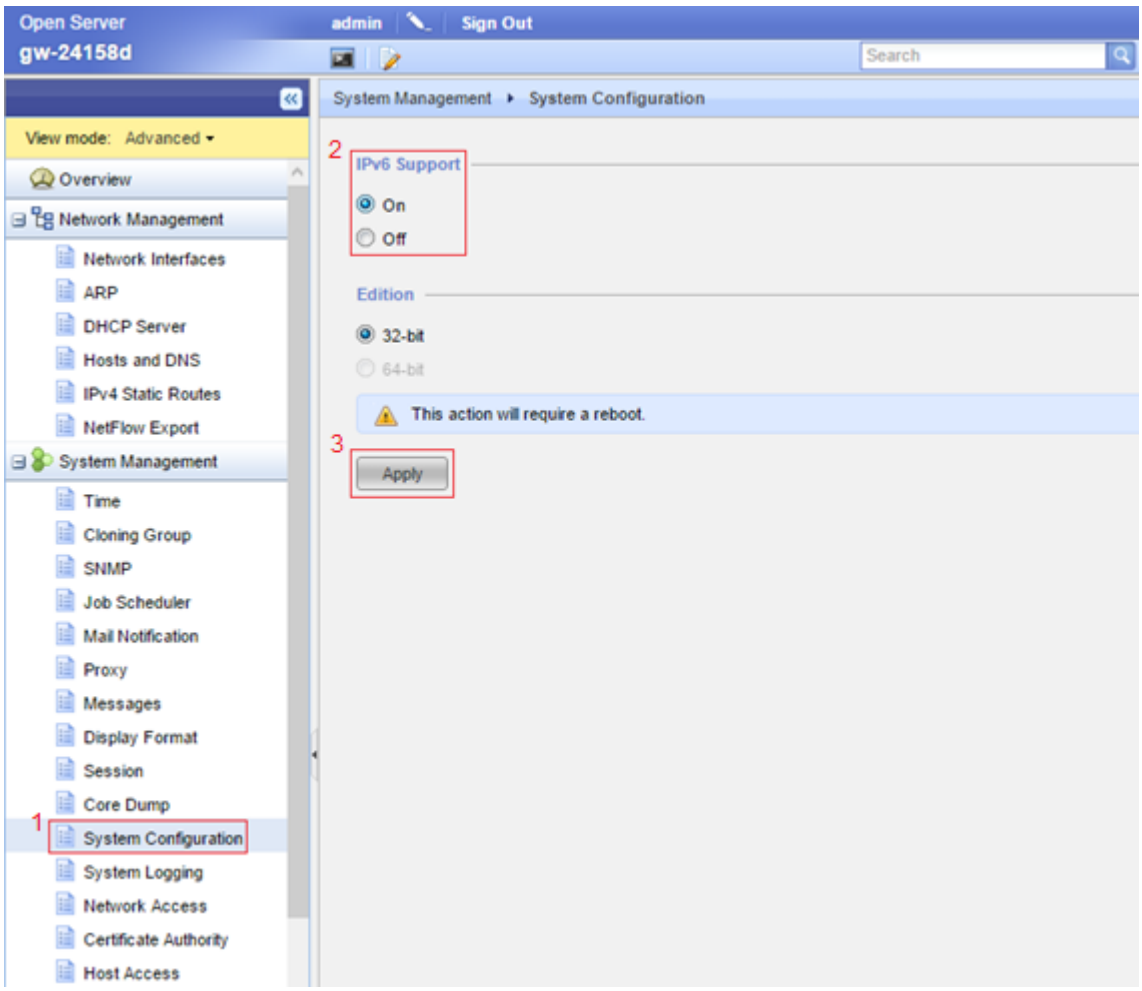
Palomuurien tehtävänä on verrata niiden läpi kulkevaa verkkoliikennettä niille asetettuihin sääntöihin, jonka perusteella ne tekevät päätöksen yksittäisen paketin eteenpäin päästämisen ja suodattamisen välillä. Työssä läpikäytävän palvelinkeskuksen kaltaisessa ympäristössä nämä säännöt ovat varsin monimutkaisia ja niitä tulee pitää jatkuvasti ajan tasalla vastaamaan jatkuvasti muuttuviin tietoturva- ja verkkohyökkäysuhkakuviin. Tämän insinöörityön puitteissa ei oteta kantaa näiden palomuurisääntöjen sisältöön eikä siihen, minkälaisiin uhkiin niillä on tarkoitus varautua. Seuraavien alalukujen esimerkkikonfiguraatioissa esitetään, miten palomuurilaitteen perustoiminnollisuudet otetaan käyttöön IPv6-pohjaisesti.

Alalukujen esimerkkikonfiguraatiot ovat kuvankaappauksia Check Point -palomuurien hallinnassa yleisesti käytetyistä graafisista Gaia portal- ja SmartDashboard-käyttöliittymistä. Gaia portal -käyttöliittymää käytetään laitteen perusasetusten, kuten IP-osoitteiden, asettamiseen ja tässä tapauksessa myös IPv6-toiminnollisuuden aktivointiin. SmartDashboard-käyttöliittymä taas mahdollistaa varsinaisten tietoturvaominaisuuksien, kuten liikenteensuodatuksen, käyttöönoton ja hallinnoinnin.

5.2.1 Palomuurin perusasetukset

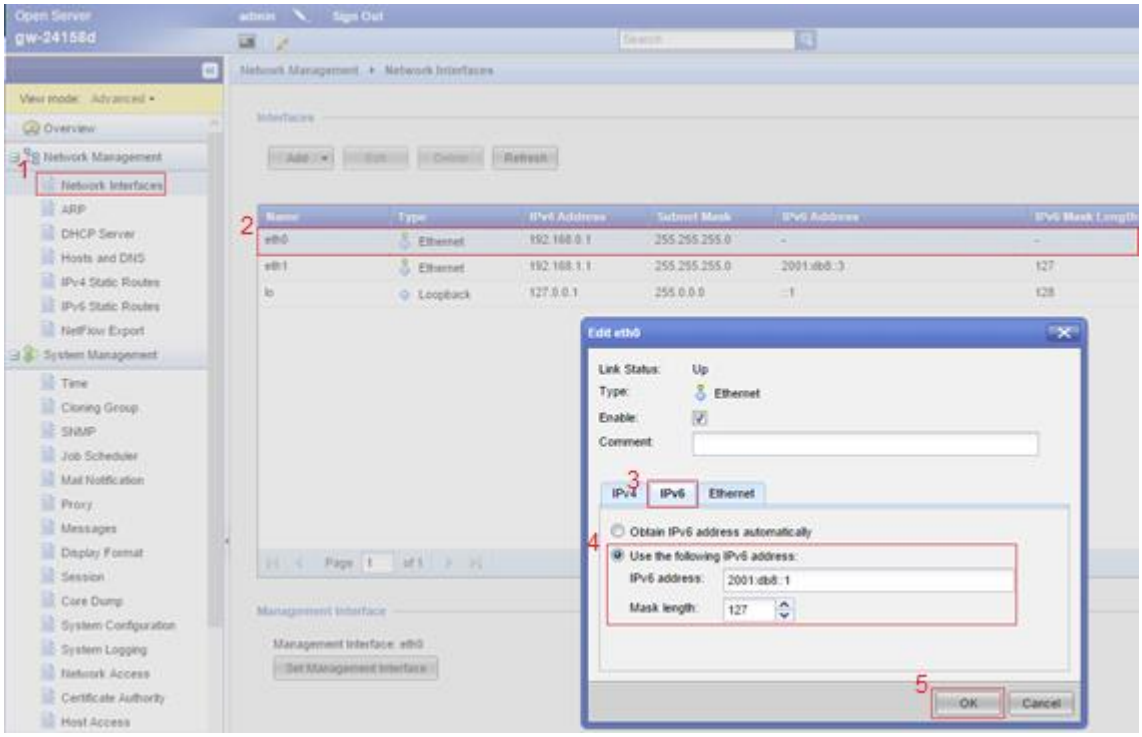
Check Pointin laitteissa IPv6-toiminnollisuus ei ole oletusarvoisesti päällä. Mikäli IPv6-protokollaa halutaan käyttää, se tulee erikseen aktivoida. [31.]

Kuvassa 7 tämä aktivointi toteutetaan Gaia portal -käyttöliittymän avulla. Gaia portalin aloitussivun vasemmassa reunassa olevan **System Configuration** -sivun alta löytyy **IPv6 support** -valikko, joka tulee asettaa **On**-tilaan. Tämän jälkeen valinta vahvistetaan **Apply**-painikkeella. Järjestelmä tulee lopuksi käynnistää uudelleen IPv6-tuen käyttöönottamiseksi.



Kuva 7. IPv6-protokollan käyttöönotto.

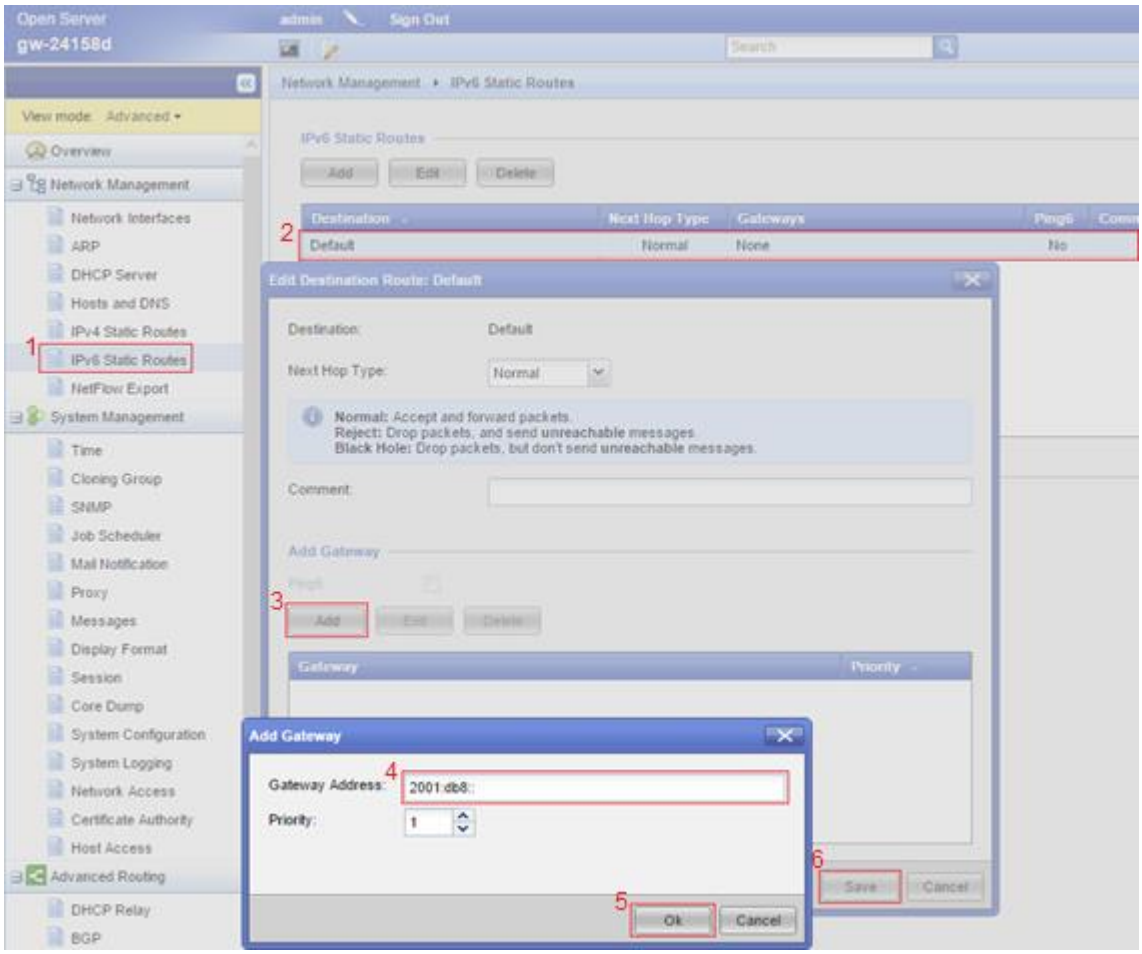
Kuvasssa 8 asetetaan eth0-portille sitä vastaava IPv6-osoite. Tämä tehdään Gaia portalin vasemmassa reunassa olevan **Network Interfaces** -sivun alta, jossa on listaus laitteen porteista. Haluttua porttia kaksoisklikkaamalla saadaan aukaistua sitä porttia vastaava **Edit**-ikkuna, jossa olevan **IPv6**-välilehden kautta on mahdollista asettaa portille haluttu IPv6-osoite ja verkon prefiksi.



Kuva 8. IPv6-osoitteen asettaminen portille.

Huom. Ohjelmistovian vuoksi Gaia-käyttöjärjestelmän R77.30-versiota edeltävät versiot antavat virheilmoituksen, mikäli niitä käyttävän laitteen portille yritetään asettaa /127-prefiksin omaavan lähiverkon ensimmäistä vapaata IP-osoitetta [38]. Suositeltava ratkaisu ongelman korjaamiseksi olisi luonnollisestikin päivittää käyttöjärjestelmä uusimpaan, R77.30-versioon. Vaihtoehtoisesti, ongelma voidaan kiertää asettamalla 127-prefiksin omaavan lähiverkon ensimmäinen osoite Check Pointin laitetta vastapäätä olevan laitteen portille ja toinen, eli viimeinen, osoite Check Pointin laitteen päähän.

IPv6-pohjainen oletusreitti, kuten muutkin staattiset IPv6-reitit, asetetaan Gaia portalissa **IPv6 Static Routes** -sivun kautta kuvan 9 mukaisesti. Sivulla on jo valmiina yksi staattinen reitti, joka on juuri oletusreitti, mutta sille ei kuitenkaan ole oletusarvoisesti asetettuna mitään IP-osoitetta. Tämä IP-osoite voidaan asettaa laitteelle kaksoisklikkaamalla reittiä, valitsemalla **Add Gateway** -osion alta **Add** ja määrittelemällä yhdyskäytävää vastaavaa IP-osoite. IP-osoitteen määrittelemisen jälkeen myös **Edit Destination** -ikkunassa tulee muistaa painaa **Save**. Oletusreitillä viitataan laitteen reititystaulun reittiin, jota käytetään pakettien välittämiseen silloin, kun sille ei löydy tarkempaa, eli käytännössä pidemmän prefiksin omaavaa, reittiä reititystaulusta.



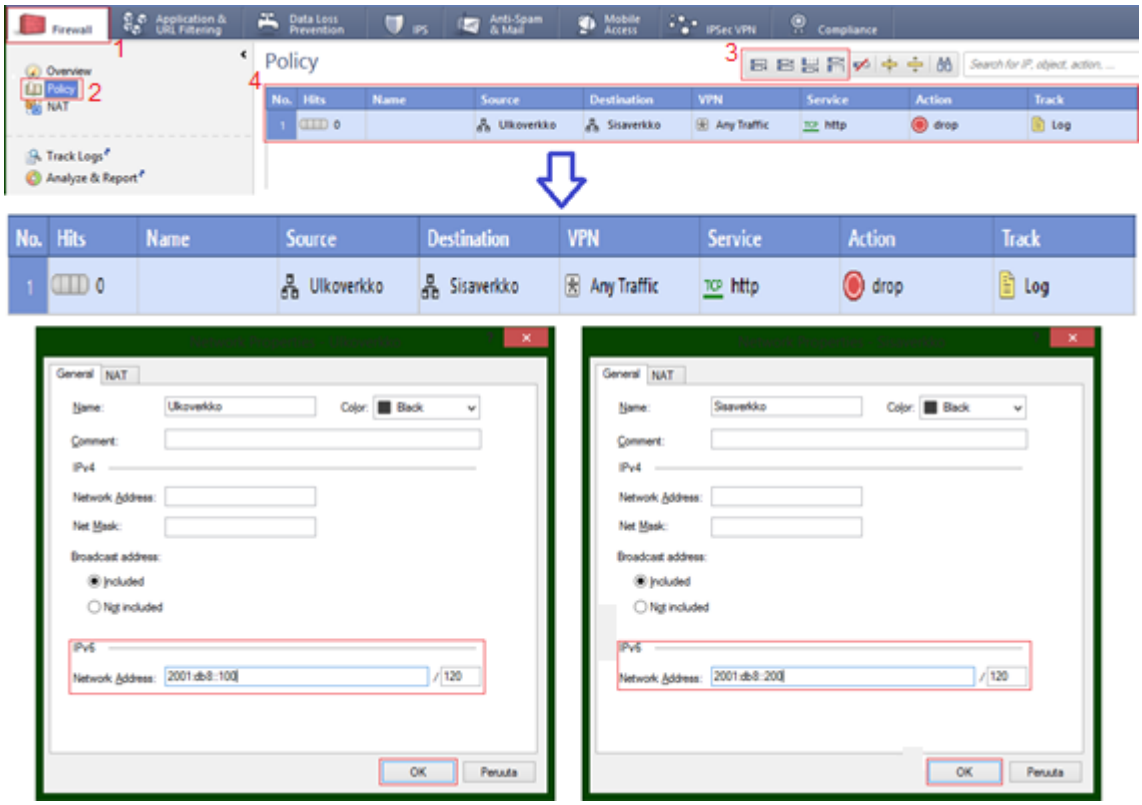
Kuva 9. Oletusreitin asettaminen.

Staattisen reitityksen lisäksi Gaia-käyttöjärjestelmä tukee IPv6-pohjaisesti myös OSPF- ja BGP-reititysprotokollia. Tämänhetkisessä käyttöjärjestelmäversiossa reititysprotokollat eivät kuitenkaan toimi yhdessä ClusterXL-toiminnon kanssa, joka tilaajayrityksellä on IPv4-pohjaisessa verkossaan käytössä. Ongelma on mahdollista kiertää käyttämällä pa-

lomuurien FHRP-protokollana avoimeen standardiin perustuvaa VRRP-protokollaa (Virtual Router Redundancy Protocol). Tällöin tosin menetetään ClusterXL-tekniikan lisäominaisuuksia, kuten yksittäisellä laitteella aktiivisena olevien TCP-sessioihin liittyvien tietojen jakaminen klusterin jäsenten kesken ja VPN-yhdyskäytävien vikasietoisuuden varmistaminen kahden rinnakkaisen yhdyskäytävän avulla. [31.]

5.2.2 Palomuurisäännön asettaminen

IPv6-pohjaiset palomuurisäännöt lisätään aivan samaan tapaan kuin IPv4-pohjaisetkin. SmartDashboard-käyttöliittymän **Firewall**-välilehden alla on **Policy**-sivu, jonka kautta sääntöjä on mahdollista luoda oikean yläreunan luontipainikkeiden avulla. Kuvassa 10 näkyvässä esimerkkisäännössä on estetty ulkoverkosta aloitettu sisäverkkoon suuntautuva HTTP-liikenne. Esimerkissä tämänkaltaisista yhteydenluontiyrityksistä luodaan myös lokimerkintä.



Kuva 10. Palomuurisäännön lisääminen ja verkko-objektien IPv6-osoitteen asettaminen.

Kuvan 10 alaosassa näkyvät palomuurisäännössä käytetyt verkko-objektit eli esimerkin ulkoverkkoa ja sisäverkkoa vastaavat aliverkot. Nämä objektit luodaan täysin samalla

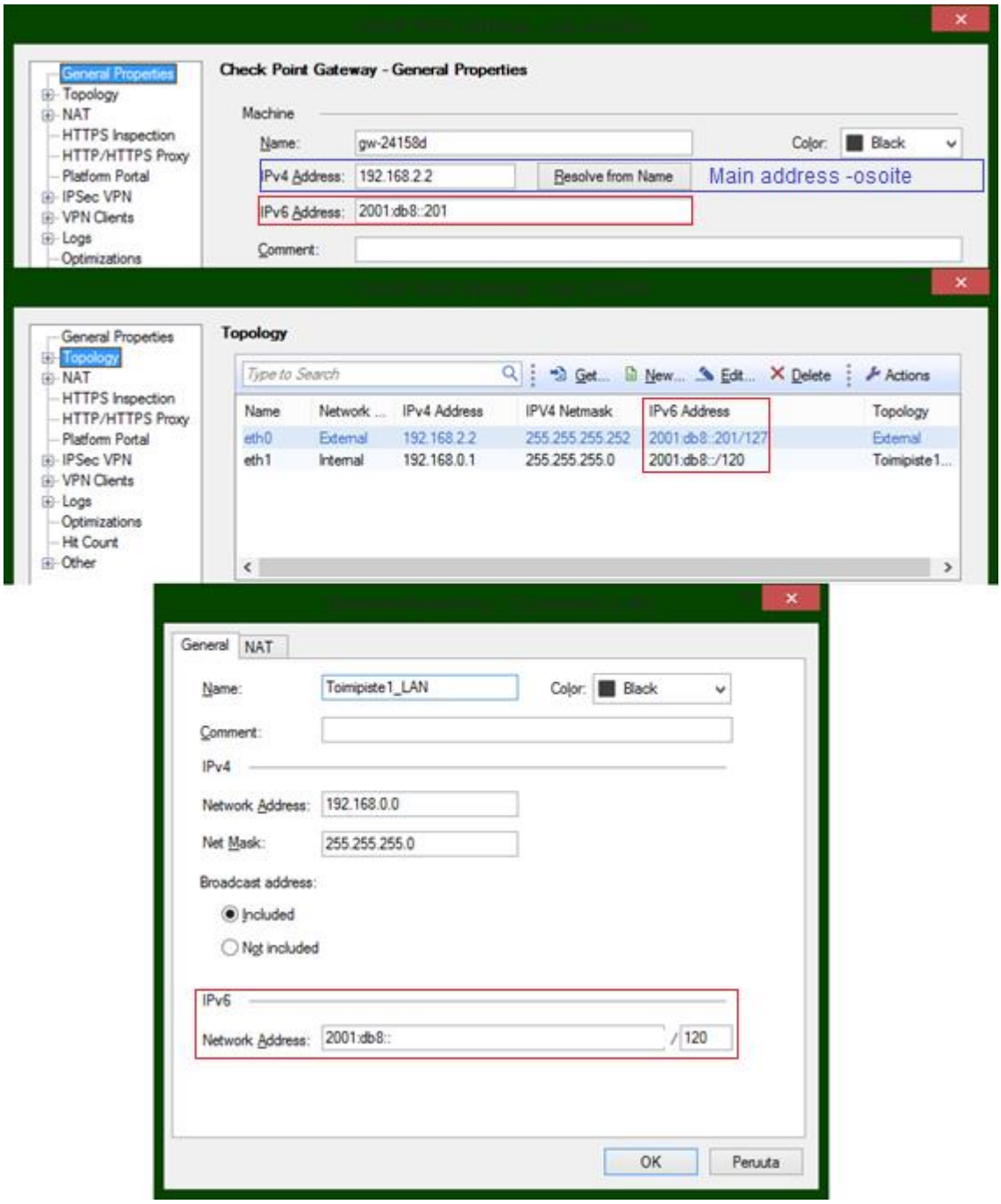
tavalla riippumatta käytetystä IP-protokollasta. Kun objektia vastaamaan halutaan määritellä IPv6-pohjainen verkko, käytetään **Network Properties** -ikkunan alalaidassa olevaa **IPv6**-kenttää.

Kuten kuvasta 10 nähdään, yksittäiselle verkko-objektille voidaan niin haluttaessa antaa sekä IPv4- että IPv6-verkon osoitteet. Näin voidaan luoda esimerkiksi verkko-objekti, joka sisältää tietyn kaksoispinotoimintoa käyttävän sisäverkon molempien IP-protokollien mukaiset IP-osoiteavaruudet. Tämän jälkeen tätä yksittäistä verkko-objektia voidaan käyttää sisäverkkoa koskevien palomuurisääntöjen luomiseen.

Palomuurille ei ole siis välttämätöntä määritellä kaikkia haluttuja sääntöjä kahteen kertaan, molemmille protokollille. Järkevällä palomuurisääntöjen suunnittelulla tämä ominaisuus mahdollistaa huomattavasti yksinkertaisemman ja suoraviivaisemman palomuurin ja sen sääntöjen hallinnan verrattuna tilanteeseen, jossa säännöt tehtäisiin yksitellen molemmille protokollille.

5.2.3 VPN-yhteyden luonti

Eri yhdyskäytävien väliset IPsec-pohjaiset VPN-yhteydet luodaan IPv6-pohjaisesti aivan samaan tapaan kuin IPv4-pohjaisestikin, joten kaikkia tarvittavia konfiguraatioaskelia ei kuvassa 11 nähdä. Kuvassa 11 näytetään vain ne kohdat IPv6-pohjaisen VPN-yhteyden asettamisesta, joissa se eroaa IPv4-pohjaisen VPN-yhteyden luonnista.



Kuva 11. VPN-yhteyden luontiin liittyvät IPv6-parametrit.

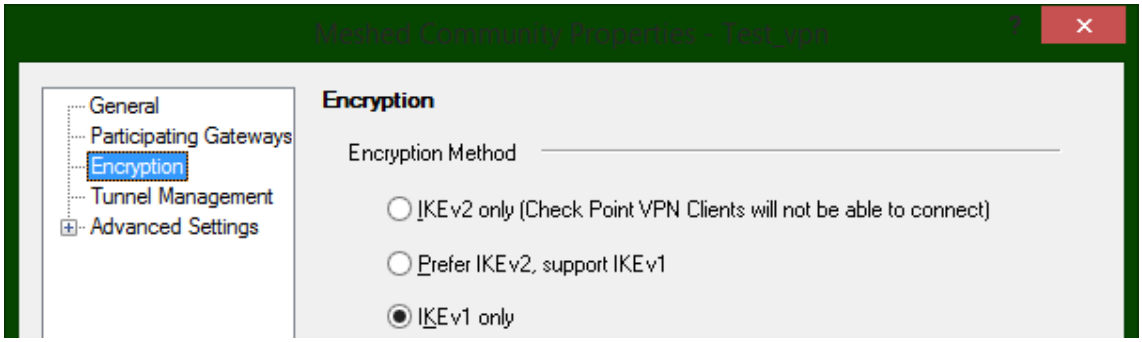
Ylimpänä kuvassa 11 nähdään yhdyskäytävän asetusikkunan **General Properties** -sivu, jossa määritellään yhdyskäytävän käyttämä main address -tyyppinen IP-osoite. Main address -osoitteet ovat VPN-yhteyksien yhteydessä käytännössä ne IP-osoitteet, joiden avulla VPN-yhteyden loppupäinä toimivat yhdyskäytävät keskustelevat keskenään ja täten muodostavat niiden välisen yhteyden. Tämän osoitteen tulee useimmiten olla laitteen ulkoverkon puolella olevan portin osoite, kuten se tämänkin esimerkin tapauksessa on.

Käytettäessä Check Pointin palomuurin VPN-toiminnollisuutta tulee laitteelle aina asettaa main address -tyyppinen IPv4-osoite. Luotaessa IPv6-pohjaista VPN-yhteyttä laite hyödyntää tätä main address -IPv4-osoitetta myös IPv6-tyyppisen main address -osoitten määrittelemisessä. Tämä tapahtuu siten, että laite valitsee VPN-yhteyden luontiin sitä porttia vastaavaan IPv6-osoitteen, johon main address -IPv4-osoite on asetettu. Tämä tapahtuu myös silloin, kun General Properties -sivulle asetettu IPv6-pohjainen osoite eroaa siitä IPv6-pohjaisesta osoitteesta, joka on asetettu samalle portille kuin saman sivun IPv4-pohjainen main address -osoite. Mikäli laitteelle on asetettu myös IPv6-tyyppinen osoite General Properties -ikkunassa, sitä käytetään VPN-yhteyden luontiin silloin, kun IPv4-pohjaisen osoitteen omaavalle portille ei ole erikseen asetettuna IPv6-pohjaista osoitetta. Tämä vaatii kuitenkin sen, että määritelty IPv6-pohjainen osoite on käytössä jollakin laitteen ulkoisista eli external-tyyppisistä porteista.

Kuvan 11 alimmassa osassa näkyy verkko-objekti, jota aiemmin hyödynnettiin myös palomuurisäännön luonnissa. VPN-yhteyden yhteydessä sitä käytetään VPN domain -alueen määrittelyyn eli niiden verkkojen määrittelyyn, joiden välille VPN-tunneli luodaan.

Huomionarvoista on, että Gaia-käyttöjärjestelmä ei nykyisellään tue IPv4-liikenteen tunnelointia IPv6-pohjaisten VPN-yhteyksien lävitse, eikä toisin päin [39]. Tämä tarkoittaa, että molemmille IP-versioille tulee luoda omat VPN-tunnelit. Hallinnallisesti tämä onnistuu kuitenkin yhden verkko-objektin ja yhden määritellyn tunnelin avulla. Verkko-objektille tulee vain asettaa molemmantyyppiset IP-osoiteavaruudet ja käyttää sitä kaksoispinokykyistä verkkoa vastaavana VPN domain -alueena.

Lisähuomiona IPv6-protokollan yli luotavista VPN-yhteyksistä on se, että ne käyttävät yksinomaan IKEv2-protokollaa (Internet Key Exchange) VPN-yhteyksien käyttämien salausavainten hallintaan ja osapuolten autentikointiin. Tämä tapahtuu siis täysin riippumatta siitä, mitä VPN-yhteyden asetuksiin on määritelty (kuva 12). Käytetyn IKE-protokollan valinta koskee tässä tapauksessa vain IPv4-pohjaisia VPN-yhteyksiä. [39.]



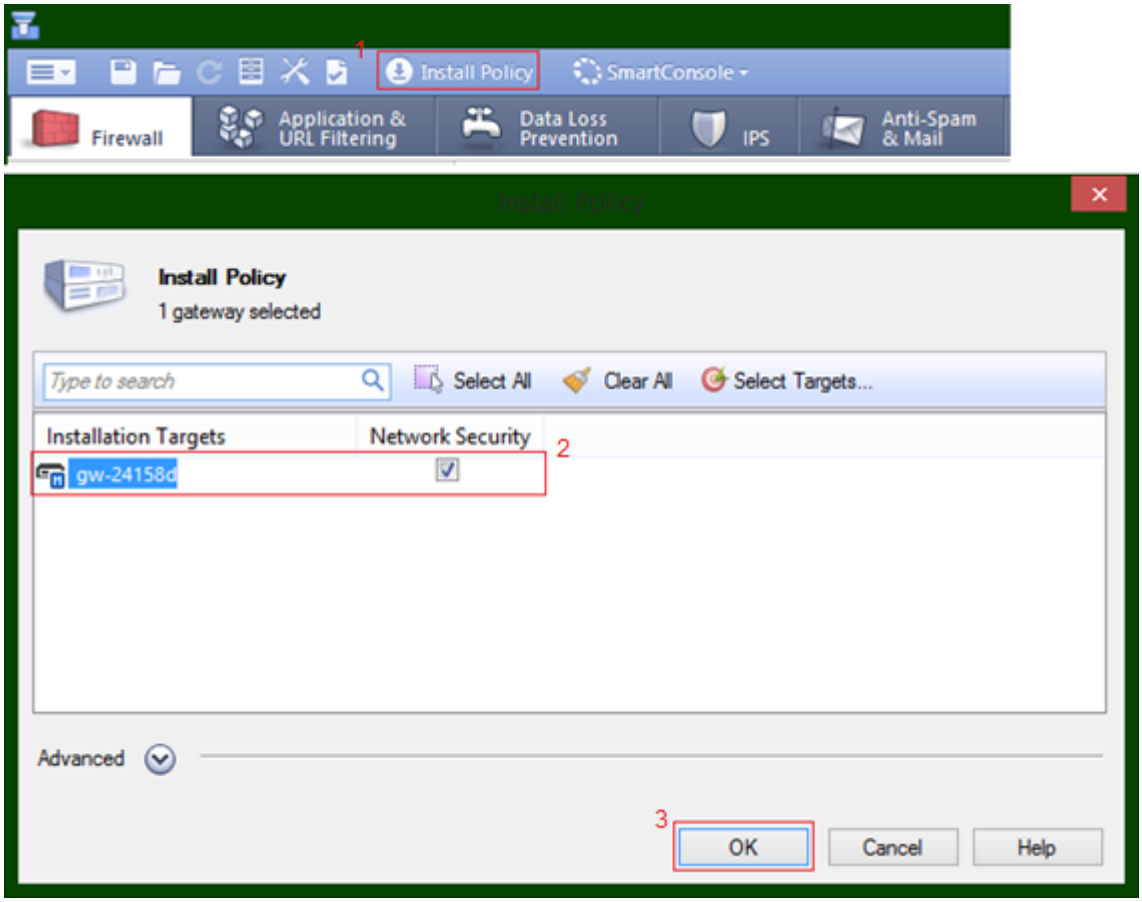
Kuva 12. VPN-yhteyden salausavainten luontiin käytetyn IKE-protokollan valinta.

Huom. Gaia-käyttöjärjestelmä ei tue IPv6-pohjaisia, permanent tunnel -tyyppisiä VPN-yhteyksiä [39]. Permanent tunnel -tyyppisillä VPN-yhteyksillä tarkoitetaan sellaisia yhteyksiä, jotka ovat jatkuvasti päällä ja joiden toimivuutta testataan automaattisesti ja tasaisin väliajoin päätteinä toimivien yhdyskäytävien toimesta. Permanent tunnel -toiminnollisuus mahdollistaa VPN-yhteyksille tehokkaamman ongelmatilanteisiin puuttumisen, sillä jos VPN-tunneli menee poikki, yhdyskäytävä luo siitä automaattisesti loki-ilmoituksen tai hälytyksen, jolloin verkon ylläpitäjä pystyy viipymättä puuttumaan ongelmatilanteeseen. Ilman permanent tunnel -ominaisuutta VPN-yhteyden vikatilanne voidaan havaita vasta siinä vaiheessa, kun sitä yritetään käyttää.

5.2.4 Policy-sääntöjen tallentaminen

SmartDashboard-käyttöliittymää käytettäessä tehtyjä muutoksia ei tallenneta välittömästi hallittaville laitteille, vaan ne tulee aina muistaa tallentaa erikseen Install Policy -toiminnon avulla.

Kuvassa 13 esitetään muutosten vieminen halutuille laitteille. SmartDashboard-käyttöliittymän yläkulmassa on **Install Policy** -painike, josta avautuvasta ikkunasta valitaan ne laitteet, joille halutut muutokset halutaan tallentaa ja valitaan **OK**.



Kuva 13. Policy-sääntöjen vieminen laitteelle.

5.3 F5-kuormantasaajat

Kuten luvussa 4.4 mainittiin, palvelinkeskuksen tarjoamien palveluiden käyttäjät ottavat aina yhteyden suoraan kuormantasaajassa suoritettavaan virtuaalipalvelimeen tai erilliseen, kuormantasaajan yhteydessä olevaan front-end-palvelimeen, jotka taas ohjaavat palvelupyynnöt kuormantasaajan takana oleviin taustapalvelimiin. Käyttäjien luomat palvelupyynnöt kulkevat siis aina kuormantasaajien lävitse. Tämäntyyppinen toiminnollisuus mahdollistaa sen, että tarjotut palvelut on varsin yksinkertaista saada näkymään käyttäjille IPv6-pohjaisina muokkaamalla kuormantasaajien yhteydessä olevaa virtuaalipalvelinta siten, että se toimii IPv6-pohjaisesti ja vastaanottaa palveluiden käyttäjiltä IPv6-pohjaisia palvelupyyntöjä. Nämä palvelupyynnöt kuormantasaaja taas puolestaan ohjaa, tavanomaisen kuormantasauksen toteuttaen, IPv4-pohjaisille taustapalvelimille samalla toteuttaen palvelupyyntöihin liittyvien pakettien otsakkeille IPv6-IPv4-muunnoksen.

Tämä tarkoittaa, että olemassa oleviin IPv4-pohjaisiin taustapalvelimiin ei ole tarvetta tehdä minkäänlaisia muutoksia, mutta näiden palvelinten käyttäjät pystyvät silti käyttämään tarjottuja palveluita omasta näkökulmastaan täysin IPv6-pohjaisesti. IPv4-protokollaa käyttävät käyttäjät voivat edelleen ottaa yhteyden taustapalvelimiin kuten ennenkin, suoraan IPv4-pohjaisen virtuaalipalvelimen kautta, välittämättä IPv6-pohjaisen virtuaalipalvelimen NAT-osoitteenmuunnoksesta. Tämänkaltaisen ratkaisun toteuttaminen esitetään seuraavassa alaluvussa.

Seuraavassa alaluvussa näkyvät esimerkkikonfiguraatiot ovat F5:n BIG-IP TMOS -käyttöjärjestelmän tmsh-muotoisia (Traffic Management Shell) konfiguraatioita, joita tulkitaan hierarkkisesti Juniperin Junos-käyttöjärjestelmää vastaavalla tavalla. tmsh on BIG-IP TMOS -käyttöjärjestelmän osa, jolla F5:n laitteita voidaan hallinnoida komentorivipohjaisesti.

5.3.1 Kuormantasaustoimintojen asettaminen

F5:n laitteissa käytettäviä portteja vastaamaan täytyy asettaa aina vähintään yksi virtuaalilähiverkko eli VLAN (Virtual Local Area Network), kuten esimerkkikonfiguraatiossa 4 on tehty. Ulkoverkon puolella käytetään external-nimistä VLAN:a, jota vastaamaan on asetettu portti 1/1.1 ja jonka kanssa samaan IPv6-pohjaiseen IP-osoitteeseen tullaan myös liittämään käyttäjien palvelupyynnöt vastaanottava IPv6-pohjainen virtuaalipalvelin. Sisäverkon VLAN on nimeltään internal, ja sitä vastaavan 1/1.2-portin takana on erityinen pool-palvelinjoukkio, joka on kuormantasaajan näkemä looginen kokonaisuus, joka sisältää kaikki tiettyä palvelua ajavat taustapalvelimet, joille kuormantasaaja toteuttaa tavanomaisen kuormantasaustoimintonsa.

```
vlan external {
     interfaces 1/1.1
}
vlan internal {
     interfaces 1/1.2
}
self 192.168.0.1 {
     netmask 255.255.255.252
     vlan external
}
self 2001:db8:: {
     netmask ffff:ffff:ffff:ffff:ffff:ffff:ffff:fffe
     vlan external
}
self 192.168.1.1 {
```

```
     netmask 255.255.255.0
     vlan internal
}
```

Esimerkkikonfiguraatio 4. Virtuaalilähiverkkojen, porttien ja kuormantasaajan self IP -osoitteiden asettaminen.

Esimerkkikonfiguraation 4 self-komennoilla asetetaan aiemmin määritellyille VLAN-verkoille niitä vastaavat IP-osoitteet, jotka siis tässä tapauksessa ovat käytännössä laitteen portteja vastaavat IP-osoitteet. Osoitteita vastaamaan asetetaan myös aliverkon peitteet. Ulkoverkon puoleista porttia vastaavalle VLAN:lle, johon käyttäjien palvelupyynnöt saapuvat, on toteutettu kaksoispinotoiminto asettamalla sille IPv4- ja IPv6-muotoiset osoitteet.

IPv4-pohjaiset taustapalvelimet sisältävän sisäverkon puolella olevalle portille asetetaan IPv4-osoite, joka on tässä tapauksessa samassa lähiverkossa taustapalvelinten kanssa. Taustapalvelinten ei ole kuitenkaan välttämätöntä olla samassa lähiverkossa kuormantasaajan sisäverkon puoleisen portin kanssa, vaan niille riittää IP-pohjainen yhteys kuormantasaajan porttiin oletusyhdyskäytäviensä kautta.

Esimerkkikonfiguraatiossa 4 esiintyvä IPv6-osoitteen aliverkon peite saattaa herättää huomiota, mutta se on kuitenkin esitetty F5:n käyttöjärjestelmälle ominaiseen tapaan ja se tulee aina syöttää self IP -osoitteiden yhteydessä esimerkin kuvaamalla tavalla [35]. Esimerkin yhteydessä näkyvän IPv6-pohjaisen aliverkon peitteen periaate on käytännössä sama kuin perinteisissä IPv4-verkoissakin, eli 128-bittisen osoitteen verkko-osion bitit erotetaan laiteosion biteistä 128-bittisellä arvolla, jossa verkko-osuutta kuvaavat bitit saavat arvon 1 ja laiteosuutta arvon 0. Tämä arvo esitetään tavanomaisten osoitteiden tapaan heksadesimaaleina. Tavallisesti IPv6-osoitteiden verkko-osion pituus esitetään prefiksiarvolla, joka olisi esimerkin tapauksessa /127, eli IP-osoitteen ensimmäiset 127 bittiä kuuluvat verkko-osioon.

Esimerkkikonfiguraatiossa 5 määritellään kolme taustapalvelinta, joista käytetään F5:n termistössä nimitystä node. Palvelinten IP-osoitteet määritellään ja niille annetaan niitä vastaavat nimet. Luonnollisesti, käytettävien taustapalvelinten käyttöjärjestelmien päässä tulee olla asetettuina samat IP-osoitteet.

```
node 192.168.1.2 {
     screen Back-end-1
}
```

```
node 192.168.1.3 {
     screen Back-end-2
}
node 192.168.1.4 {
     screen Back-end-3
}
pool IPv4-pool {
     members {
          192.168.1.2:http {}
          192.168.2.3:http {}
          192.168.3.4:http {}
     }
}
```

Esimerkkikonfiguraatio 5. Taustapalvelinten ja pool-ryhmän asettaminen.

Tämän jälkeen esimerkkikonfiguraatiossa 5 määritellään kuormantasaajalle erityinen pool-ryhmä, jolle annetaan tässä tapauksessa nimeksi ”IPv4-pool” ja jonka jäseniksi aiemmin määritellyt node-palvelimet eli taustapalvelimet asetetaan. Pool-ryhmän jäsenten IP-osoitteiden yhteyteen merkitään myös sen palvelun tyyppi, jota ne suorittavat. Esimerkin tapauksessa palvelu on HTTP, joka voitaisiin haluttaessa myös merkitä sitä vastaavalla porttinumerolla 80.

Mikäli haluttaisiin käyttää IPv6-pohjaisia taustapalvelimia, konfiguraatio olisi osoitteita lukuun ottamatta samanlainen.

Esimerkkikonfiguraatiossa 6 toteutetaan viimeinen tarvittava askel kuormantasaajan perustoiminnollisuuden toteuttamiseksi eli virtuaalipalvelinten luonti. Kuormantasaajalla toteutettavan palvelun käyttäjät ottavat yhteyden näihin virtuaalipalvelimiin niiden IP-osoitteiden perusteella.

```
virtual IPv4-VS {
     pool IPv4-pool
     destination 192.168.0.1.http
}
virtual IPv6-VS {
     pool IPv4-pool
     destination 2001:db8::.http
}
```

Esimerkkikonfiguraatio 6. Kuormantasaajan virtuaalipalvelimien asettaminen.

F5:n laitteissa yksittäiselle virtuaalipalvelimelle ei ole mahdollista asettaa sekä IPv4- että IPv6-pohjaista osoitetta, joten yhtä kaksoispinopohjaisesti toimivaa palvelua kohden on välttämätöntä luoda kaksi eri virtuaalipalvelinta kumpaakin IP-protokollaa kohden. Esimerkkikonfiguraatiossa 6 näille virtuaalipalvelimille on annettu nimet IPv4-VS ja IPv6-VS.

Virtuaalipalvelinten käyttämäksi pool-ryhmäksi asetetaan aiemmin määritelty ”IPv4-pool”-niminen ryhmä, joka sisälsi kolme IPv4-pohjaista taustapalvelinta, joille virtuaalipalvelimet ohjaavat saamansa palvelupyynnöt.

Esimerkkikonfiguraatiossa 6 esiintyvällä destination-määreellä virtuaalipalvelimille asetetaan niitä vastaavat IP-osoitteet, jotka ovat esimerkin 6 tapauksessa samat osoitteet, jotka external-VLAN:lle aiemmin määriteltiin. Nämä ovat ne osoitteet, joihin kuormantasaajalla toteutetun palvelun käyttäjät ottavat aina yhteyden. Mikäli palvelulla on jokin sitä vastaava URL-osoite, se tulee asettaa DNS-palvelimelle viittaamaan sitä vastaaviin, nyt määriteltyihin IP-osoitteisiin. Myös protokolla, jota vastaavia palvelupyyntöjä virtuaalipalvelin vastaanottaa, määritellään osoitteen yhteydessä esimerkin 6 osoittamalla tavalla protokollan nimellä tai vaihtoehtoisesti pelkän porttinumeron perusteella.

Kun F5-kuormantasaajan virtuaalipalvelimelle ja käytetylle pool-ryhmälle asetetaan eri versioita olevat IP-osoitteet, laite osaa oletusarvoisesti toteuttaa tarvittavan NAT-toiminnollisuuden niiden välillä [41]. Esimerkin tapauksessa IPv6-pohjaisen paketin saavuttua IPv6-VS-virtuaalikoneelle laite korvaa olemassa olevan IPv6-otsakkeen IPv4-otsakkeella, jonka lähdeosoitteeksi asetetaan aiemmin määriteltyä internal-nimistä VLAN:a vastaava IP-osoite ja kohdeosoitteeksi halutun taustapalvelimen osoite. Palvelupyynnön käsiteltyään taustapalvelin lähettää vastauksensa takaisin internal-VLAN:n osoitteeseen, josta kuormantasaaja lähettää sen eteenpäin palvelupyynnön alkuperäiselle tekijälle, jälleen IPv6-muotoisesti, virtuaalipalvelimen osoitetta lähteenä käyttäen. Sama periaate pätee myös toisin päin, eli IPv4-pohjaisen virtuaalipalvelimen ja IPv6-pohjaisten taustapalvelinten tapauksessa. NAT-toiminnollisuutta ei ole kummassakaan tapauksessa tarvetta asettaa erikseen.

Esimerkkikonfiguraatiossa 7 laitteelle asetetaan yksinkertainen staattinen reititys, joka on tässä yhteydessä myös laitteen oletusreitti. Esimerkkikonfiguraatiossa 7 net route -parametri määrittele reitin kohdeverkon ja gw-parametri taas seuraavan yhdyskäytävän osoitteen, jonka kautta määriteltyyn kohdeverkkoon pääsee.

```
net route ::/0 {
    gw 2001:db8::1
    network ::/0
}
```

Esimerkkikonfiguraatio 7. Staattisen reitin asettaminen.

Huomionarvoista on, että vaikka esimerkkikonfiguraatiossa reitin kohdeosoite näkyy kahdessa eri paikassa, reitti on luotu komennolla **create /net route ::/0 gw 2001:db8::1**, jossa konfiguraatiossa näkyvää network-määrettä ei erikseen anneta.

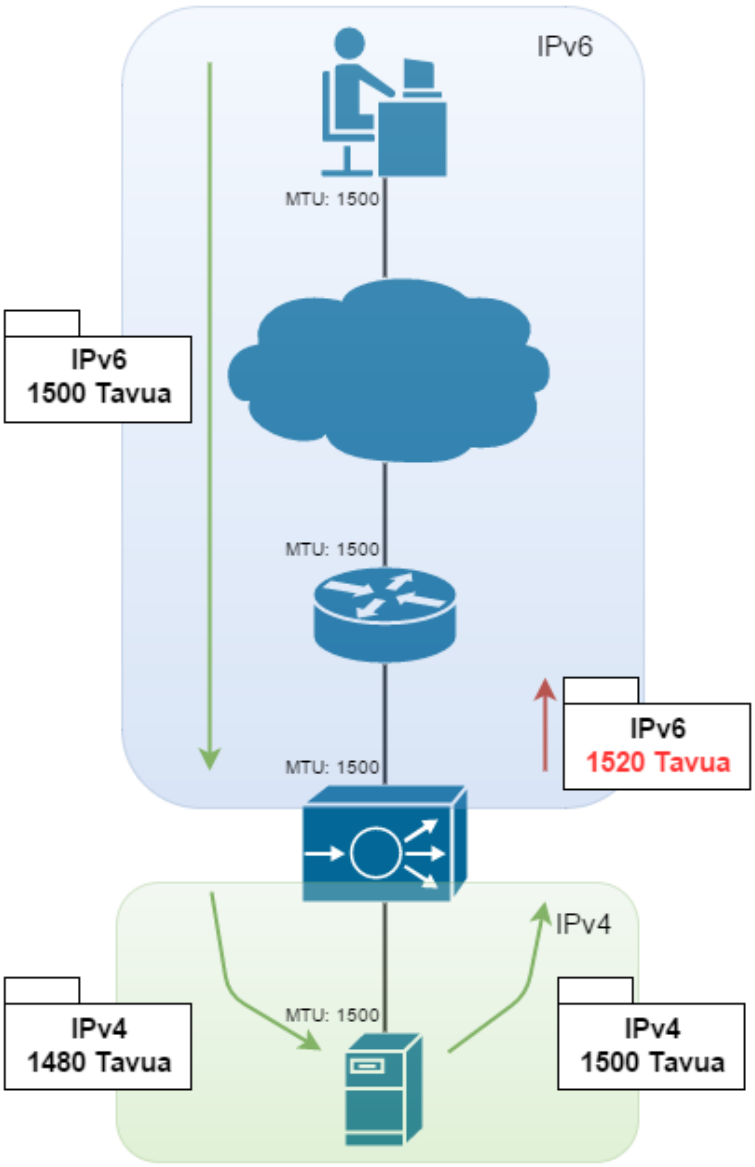
Kuten esimerkissä näkyy, staattisissa reiteissä aliverkon peite annetaan aina tavanomaisessa prefiksi-muodossa, toisin kuin esimerkin 4 self IP -osoitteissa.

Tarvittaessa TMOS-käyttöjärjestelmä tukee myös dynaamisia reititysprotokollia, kuten OSPF ja BGP, IPv6-pohjaisesti [33].

5.3.2 Huomioitavaa IP-protokollien välisestä muunnoksesta

Seikka, joka tulee aina ottaa huomioon IPv4–IPv6-muunnoksen yhteydessä, on IPv4- ja IPv6-pakettien otsakkeiden kokoero. IPv4-paketin otsake ilman ylimääräisiä optioita on kooltaan 20 tavua, kun taas IPv6-paketin otsake on kooltaan 40 tavua [4]. Ethernet-porttien yhteydessä oletusarvoinen MTU eli paketin maksimikoko on 1 500 tavua [42].

IPv4–IPv6-muunnoksen yhteydessä paketin kokonaiskoon suhteen muodostuu ongelmia siinä vaiheessa, kun IPv4-pohjainen solmu luo paketin sen oletusarvoisen MTU:n mukaisesti 1 500 tavun kokoiseksi. Tämän jälkeen NAT-toiminnollisuuden toteuttava laite korvaa 20 tavun IPv4-otsakkeen 40 tavun IPv6-otsakkeella ja yrittää tämän jälkeen lähettää 1 520 tavun kokoisen paketin sellaista reittiä pitkin, jonka varrella on yksikin linkki, jonka MTU on 1 500 tavua. Kuten jo aiemmin luvussa 2.2.2 mainittiin, IPv6-protokollan yhteydessä verkkolaitteet eivät suorita pakettien fragmentointia, vaan ylisuuri IPv6-paketti tuhotaan eikä sitä lähetetä eteenpäin [4]. Ongelmaa on havainnollistettu kuvassa 13.



Kuva 13. Havainnollistus IPv4–IPv6-muunnoksen aiheuttamasta ongelmasta MTU:n kanssa.

Yksinkertaisin tapa kiertää tämänkaltaisen ongelman syntyminen on asettaa kuormantasaajan takana olevien IPv4-kykyisten taustapalvelinten porttien MTU-arvoksi 1480, jolla otetaan huomioon IPv4-protokollasta IPv6-protokollaan tehtävästä otsakkeen muunnoksesta johtuva 20 tavun lisäys paketin kokoon.

Tilaajayrityksen palvelinkeskuksessa käytetään lukuisia eri palvelinkäyttöjärjestelmiä, joissa MTU-arvo asetetaan hieman eri tavoilla. Seuraavassa näkyvät esimerkit Linux CentOS- (esimerkkikonfiguraatio 7) ja Windows Server -käyttöjärjestelmille (esimerkkikonfiguraatio 8).

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth0

…
MTU="1480"
…

# service network restart
```

Esimerkkikonfiguraatio 7. MTU-arvon vaihtaminen Linux CentOS -käyttöjärjestelmässä.

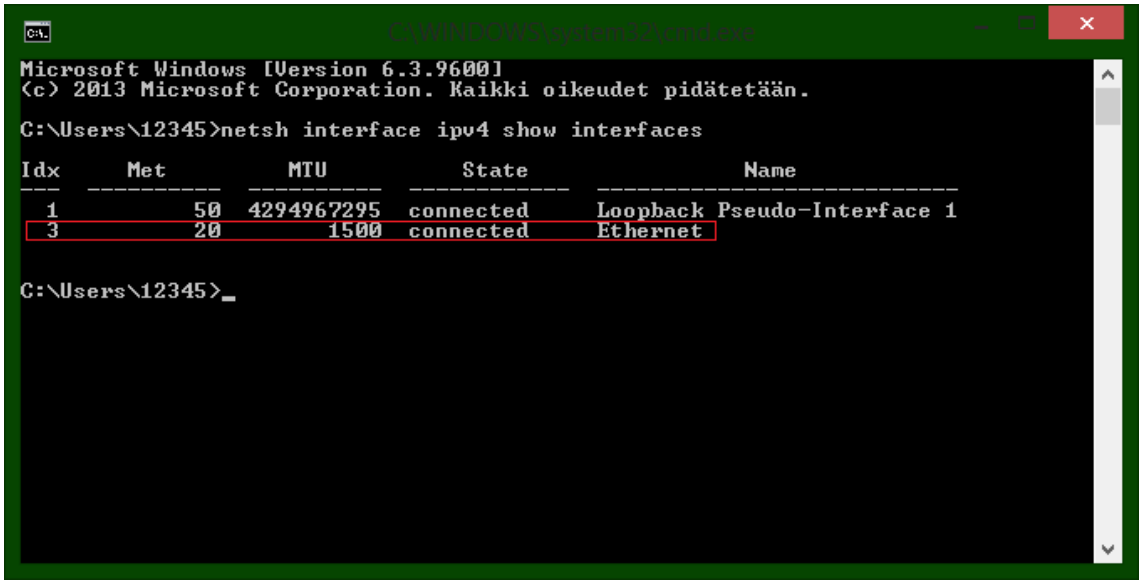
Esimerkkikonfiguraation 7 mukaisesti Linux CentOS-palvelimen käyttämä MTU-arvo vaihdetaan avaamalla palvelimen verkkokortin asetukset määrittelevä ifcfg-eth0-tiedosto, muuttamalla siellä olevan MTU-parametrin arvo halutuksi ja tallentamalla muutos. Muutoksen käyttöönottamiseksi käyttöjärjestelmän TCP/IP-protokollapino tulee käynnistää lopuksi uudelleen esimerkkikonfiguraation 7 viimeisellä komennolla.

```
netsh interface ipv4 show interfaces

netsh interface ipv4 set subinterface "x" mtu=1480 store=persis-
tent
```

Esimerkkikonfiguraatio 8. MTU-arvon vaihtaminen Windows Server -käyttöjärjestelmässä cmd-komentokehotteen avulla.

Esimerkkikonfiguraation 8 mukaisesti Windows Server -pohjaisen palvelimen portin käyttämän MTU-arvon vaihtamista varten tulee ensin selvittää käyttöjärjestelmän verkkokortille asettama, Ethernet-protokollaa vastaava looginen yksikkö. Tämä tehdään esimerkkikonfiguraation ylemmällä komennolla. Komennon antamasta tulosteesta etsitään Ethernet-niminen rivi, josta katsotaan sitä vastaava Idx-arvo. Kuvan 14 tapauksessa oikea arvo on 3.



Kuva 14. Verkkokortin Ethernet-protokollaa vastaavan loogisen yksikön selvittäminen Windows-ympäristössä.

Tämän jälkeen verkkokortin Ethernet-protokollaa vastaava MTU vaihdetaan esimerkkikonfiguraatiossa 8 jälkimmäisenä esiintyvällä komennolla antamalla subinterface-kohdan jälkeiselle parametrille arvoksi aiemmin selvitetty Idx-numero.

Toinen merkittävä haaste IPv4–IPv6-osoitteenmuunnoksessa ovat protokollat, jotka käyttävät viestinnän osapuolten IP-osoitteita osana varsinaista sovelluskerroksen kuormaa, joka on kapseloitu verkkokerroksen IP-paketin sisään. Tavanomainen NAT-osoitteenmuunnos ei kykene ottamaan tällä tavoin käytettyihin osoitteisiin minkäänlaista kantaa. Protokollia, joissa tämänkaltaisia ongelmia esiintyy, ovat muun muassa tiedostojen siirtoon käytetty FTP (File Transfer Protocol), IP-multimediayhteyksien luontiin tarkoitettu SIP (Session Initiation Protocol) ja multimedian suoratoistoon tarkoitettu RTSP (Real Time Streaming Protocol) [43].

Jotkin tämänkaltaiset protokollat, kuten SIP, sisältävät nykyään tuen IPv4- ja IPv6-solmujen väliseen viestintään NAT-osoitteenmuunnoksen lävitse [44]. Tämä ei kuitenkaan välttämättä tarkoita sitä, että tuki sisältyisi automaattisesti kaikkiin tämänhetkisiin tilaajayrityksen palvelinkeskuksen palvelimissa käytettyihin ohjelmistoihin ja niiden protokollaimplementaatioihin. Tämänkaltaisen tuen olemassaolo on asia, joka tulee selvittää aina sovelluskohtaisesti ja tarpeen vaatiessa suorittaa tarvittavat päivitystyöt tai toteuttaa palvelu vaihtoehtoisella, NAT-osoitteenmuunnosta tukevalla ohjelmistolla.

Vaihtoehtoisesti voidaan myös hyödyntää ALG-toimintoa (Application Layer Gateway), joka muuttaa tavanomaista NAT-osoitteenmuunnosta siten, että se osaa tiettyjen protokollien kohdalla ottaa huomioon myös sovelluskerroksella esiintyvät osoitetiedot. F5 TMOS -käyttöjärjestelmä tukee ALG-toimintoa FTP-, SIP-, RTSP- ja PPTP-protokollille [45].

6 Yhteenveto

Insinöörityössä selvitettiin työn pohjana käytetyn palvelinkeskusverkon IPv6-siirtymään liittyvien edellytysten täyttymistä, mahdollisia haasteita ja käytännön toimenpiteitä siirtymän toteuttamiseksi. Työn toteuttamisen keskeisimpänä motiivina oli vapaasti saatavilla olevien IPv4-muotoisten IP-osoitteiden loppuminen.

Työn toteutus onnistui varsin hyvin, ja sille asetetut tavoitteet kyettiin saavuttamaan. Työn tuloksena saatiin kattava yhteenveto selvitystyön kohteena olleen palvelinkeskusverkon kyvystä toimia kaksoispinopohjaisesti, eli IPv4-protokollan lisäksi myös uudemmalla IPv6-protokollalla. Myös laitteiden tärkeimpien toimintojen IPv6-pohjaisen toteuttamisen mahdollistavat esimerkkikonfiguraatiot saatiin toteutettua ja testattua. Huomionarvoista on kuitenkin se, että nyt luodut esimerkkikonfiguraatiot ovat korostetun yksinkertaistettuja, eivätkä ne välttämättä sovellu sellaisenaan kaikkiin tuotantoympäristön tarpeisiin ja vaatimuksiin, joten niitä on todennäköisesti tarpeen jatkosoveltaa varsinaista IPv6-siirtymää toteutettaessa.

Työssä tarkastellun verkkoinfrastruktuurin selkeästi heikoimmaksi lenkiksi IPv6-tuen suhteen osoittautui Check Pointin palomuurien Gaia-käyttöjärjestelmä. Sen uusinkin saatavilla oleva versio oli IPv6-tueltaan varsin puutteellinen, sillä siitä puuttui IPv6-pohjainen tuki hyvinkin keskeisille toiminnoille, kuten esimerkiksi SmartView Tracker -työkalulle, jota käytetään palomuurien loki-ilmoitusten tarkastelemiseen. Juniper Junos- ja F5 TMOS -käyttöjärjestelmien IPv6-tuessa ei ilmennyt huomattavia puutteita eikä täten myöskään mainittavia esteitä kaksoispinotoiminnon käyttöönotolle.

Työn tuloksia on mahdollista hyödyntää osana IPv6-siirtymän teknistä toteutusta, mutta myös hallinnolliset seikat tulee ottaa siirtymää toteutettaessa huomioon. Työn pohjana toiminut palvelinkeskus on ympäristö, jonka tarjoamia palveluita ja toimintoja hyödynnetään lukuisten eri asiakasryhmien ja tilaajayrityksen sisäisten sidosryhmien toimesta. Osana onnistunutta IPv6-siirtymää onkin myös tärkeää ottaa huomioon IPv6-siirtymän mahdolliset vaikutukset näiden sidosryhmien toimintaan ja heidän kokemaansa palvelun laatuun sekä huolehtia näitä vaikutuksia koskevasta tiedottamisesta.

Työssä ei juurikaan otettu kuormantasaajien takana olevien varsinaisten palvelinten toimintaan kantaa, mutta myös niiden käyttämien palvelinohjelmistojen IPv6-siirtymän to-

teuttamista on tulevaisuudessa syytä kartoittaa. Vaikka työssä esitetty kuormantasaajalla toteutettu osoitteenmuunnos IPv6-kykyisen ulkoverkon ja IPv4-pohjaisen palvelinverkon välillä onkin pääosin toimiva siirtymävaiheen tekniikka, on kuitenkin syytä pitää mielessä työssä kuvatun siirtymävaiheen luonne eräänlaisena välietappina, matkalla kohti lopullista tavoitetta eli täysin IPv6-pohjaista internetiä. Tämän tavoitteen saavuttamiseksi kannattaa ottaa käytännöksi aina pyrkiä soveltamaan pelkkää IPv6-protokollaa, siellä missä se vain suinkin on mahdollista.

Lähteet

1 ARIN IPv4 free pool reaches zero. 2015. Verkkodokumentti. ARIN. <www.arin.net/announcements/2015/20150924.html>. Luettu 27.9.2015.

2 OSI-malli. Verkkodokumentti. Wikipedia. <upload.wikimedia.org/wikipedia/fi/4/4c/OSI-malli.jpg>. Luettu 1.10.2015.

3 IPv6-otsake. Verkkodokumentti. Oracle Corporation. <docs.oracle.com/cd/E19120-01/open.solaris/819-3000/images/HeaderFormat.gif>. Luettu 1.10.2015.

4 Deering, S. & Hinden, R. 1998. Internet Protocol, Version 6 (IPv6) Specification. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc2460>. Luettu 1.10.2015.

5 Amante, S., Carpenter, B., Jiang, S. & Rajahalme, J. 2011. IPv6 Flow Label Specification. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc6437>. Luettu 1.10.2015.

6 Kent, S. & Atkinson, R. 1998. IP Authentication Header. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc2402>. Luettu 1.10.2015.

7 Hinden, R. & Deering, S. 1998. IP Version 6 Addressing Architecture. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc2373>. Luettu 5.10.2015

8 IPv6-osoite. Verkkodokumentti. Wikipedia. <en.wikipedia.org/wiki/File:Ipv6_address_leading_zeros.svg>. Luettu 1.10.2015.

9 Kessler, Gary C. 1997. IPv6: The Next Generation Internet Protocol. Verkkodokumentti. <www.garykessler.net/library/ipv6_exp.html>. Luettu 2.10.2015.

10 Request for Comments (RFC). Verkkodokumentti. IETF. <www.ietf.org/rfc.html>. Luettu 2.10.2015.

11 Facts and Forecasts: Billions of Things, Trillions of Dollars. 2014. Verkkodokumentti. Siemens. <www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/internet-of-things-facts-and-forecasts.html>. Luettu 2.10.2015.

12 IPv4- ja IPv6-otsakkeet. Verkkodokumentti. Juniper Networks. <www.juniper.net/techpubs/images/g013461.gif >. Luettu 1.10.2015.

13 Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. & Carney, M. 2003. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Verkkodokumentti. IETF. <tools.ietf.org/html/rfc3315>. Luettu 4.10.2015.

14 Thomson, S., Narten, T. & Jinmei, T. 2007. IPv6 Stateless Address Autoconfiguration. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc4862>. Luettu 3.10.2015.

15 Jeong, J., Park, S., Beloeil, L. & Madanapalli, S. 2010. IPv6 Router Advertisement Options for DNS Configuration. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc6106>. Luettu 4.10.2015.

16 Mockapetris, P. 1987. DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION. Verkkodokumentti. IETF. <www.ietf.org/rfc/rfc1035.txt>. Luettu 4.10.2015.

17 Narten, T., Nordmark, E., Simpson, W. & Soliman H. 2007. Neighbor Discovery for IP version 6 (IPv6). Verkkodokumentti. IETF. <tools.ietf.org/html/rfc4861>. Luettu 11.10.2015.

18 Kent, S. & Seo, K. 2005. Security Architecture for the Internet Protocol. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc4301>. Luettu 6.10.2015.

19 Narten, T., Draves, R. & Krishnan, S. 2007. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc4941>. Luettu 11.10.2015.

20 van Beijnum, Iljitsch. 2014. IPv6 adoption starting to add up to real numbers: 0.6 percent. Verkkodokumentti. <arstechnica.com/business/2014/08/ipv6-adoption-starting-to-add-up-to-real-numbers-0-6-percent/>. Luettu 7.10.2015.

21 Nordmark, E. & Gilligan, R. 2005. Basic Transition Mechanisms for IPv6 Hosts and Routers. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc4213>. Luettu 7.10.2015.

22 Egevang, K. & Francis, P. 1994. The IP Network Address Translator (NAT). Verkkodokumentti. IETF. <www.ietf.org/rfc/rfc1631.txt>. Luettu 10.10.2015.

23 Bagnulo, M., Matthews, P. & van Beijnum, I. 2011. Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc6146>. Luettu 12.10.2015.

24 Bagnulo, M., Sullivan, A., Matthews, P. & van Beijnum, I. 2011. DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc6147>. Luettu 12.10.2015.

25 NAT64 Technology: Connecting IPv6 and IPv4 Networks. 2012. Verkkodokumentti. Cisco. <www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html>. Luettu 13.10.2015.

26 Nordmark, E. 2000. Stateless IP/ICMP Translation Algorithm (SIIT). Verkkodokumentti. IETF. <www.ietf.org/rfc/rfc2765.txt>. Luettu 12.10.2015.

27 Kuva. RIPE. <ripe64.ripe.net/presentations/67-20120417-RIPE64-The_Case_for_IPv6_Only_Data_Centres.pdf>. Luettu 12.10.2015.

28 Nadas, S. 2010. Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc5798>. Luettu 29.11.2015.

29 Kompella, K. & Rekhter, Y. 2007. Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc4761>. Luettu 30.11.2015.

30 Supported IPv6 Standards. 2015. Verkkodokumentti. Juniper Networks. <www.juniper.net/documentation/en_US/junos15.1/topics/reference/standards/ipv6.html>. Luettu 30.11.2015.

31 IPv6 Support FAQ. 2015. Verkkodokumentti. Check Point. <supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk39374>. Luettu 17.12.2015.

32 Configuring Load Balancing Pools. 2015. Verkkodokumentti. F5 Networks. <support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm_configuration_guide_10_0_0/ltm_pools.html>. Luettu 12.2.2016.

33 SOL13013: Overview of IPv6 Gateway Module and Advanced Routing Module. 2015. Verkkodokumentti. F5 Networks. <support.f5.com/kb/en-us/solutions/public/13000/000/sol13013.html>. Luettu 19.12.2015.

34 Bates, T., Chandra, R., Katz, D. & Rekhter, Y. 2007. Multiprotocol Extensions for BGP-4. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc4760>. Luettu 29.12.2015.

35 router-id. 2015. Verkkodokumentti. Juniper Networks. <www.juniper.net/documentation/en_US/junos15.1/topics/reference/configuration-statement/router-id-edit-routing-options.html>. Luettu 12.2.2016.

36 Callon, R. 1990. Use of OSI IS-IS for Routing in TCP/IP and Dual Environments. Verkkodokumentti. IETF. <tools.ietf.org/html/rfc1195>. Luettu 6.12.2015.

37 Bhatia, Manav. 2011. Why providers still prefer IS-IS over OSPF when designing large flat topologies! Verkkodokumentti. <routingfreak.wordpress.com/2011/03/05/why-providers-still-prefer-is-is-over-ospf-when-designing-large-flat-topologies/>. Luettu 12.2.2016.

38 "Invalid combination of IPv6 address and network mask" error when configuring IPv6 address with a subnet mask /127. 2015. Verkkodokumentti. Check Point. <supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoview-solutiondetails=&solutionid=sk105249>. Luettu 12.2.2016.

39 The Check Point VPN Solution. 2015. Verkkodokumentti. Check Point. <sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13868.htm>. Luettu 30.12.2015.

40 Self IP Addresses. 2015. Verkkodokumentti. F5 Networks. <support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-routing-administration-11-6-0/5.html>. Luettu 12.2.2016.

41 SOL9279: The BIG-IP system automatically translates addresses between IPv4 and IPv6 when necessary. 2014. Verkkodokumentti. F5 Networks. <support.f5.com/kb/en-us/solutions/public/9000/200/sol9279.html>. Luettu 12.12.2015.

42 The default MTU sizes for different network topologies. 2016. Verkkodokumentti. Microsoft. <support.microsoft.com/en-us/kb/314496>. Luettu 12.2.2016.

43 Holdrege, M. & Srisuresh, P. 2001. Protocol Complications with the IP Network Address Translator. Verkkodokumentti. IETF. <www.ietf.org/rfc/rfc3027.txt>. Luettu 12.2.2016.

44 Camarillo, G., El Malki, K. & Gurbani, V. 2011. IPv6 Transition in the Session Initiation Protocol (SIP). Verkkodokumentti. IETF. <tools.ietf.org/html/rfc6157>. Luettu 30.10.2015.

45 Using ALG Profiles. 2015. Verkkodokumentti. F5 Networks. <support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/cgn-implementations-11-6-0/6.html>. Luettu 30.12.2015.